KERANGKA KERJA KEPERCAYAAN DIGITAL INDONESIA

Kerangka Kerja Kepercayaan Digital Indonesia

Dr. Bety Hayat Susanti, S.Si., M.E. dkk.

Penerbit
Politeknik Siber dan Sandi Negara Press

Kerangka Kerja Kepercayaan Digital Indonesia

Penulis:
Dr. Bety Hayat Susanti, S.Si., M.E.
Septia Ulfa Sunaringtyas, S.Tr.MP., M.T.
Dimas Febriyan Priambodo, M.Cs.
Fetty Amelia, S.ST., M.T.
Rizka Khairunnisa, S.ST., M.T.
Ir. Budi Rahardjo, M.Sc., Ph.D.
Dr. Magfirawaty, S.Si., M.Si.

Penelaah Ahli:
Nunil Pantjawati, B.Sc., M.E.
Dr. Edit Prima, M.Kom.
Harun Al Rasyid, S.E., CISA, CDPSE, GRCP, GRCA, CEH, CSXF, COBIT5F, COBIT2019F, ISMS27001LA, QMS9001IA.

Penerbit:
Politeknik Siber dan Sandi Negara Press
Jl. H. Usa, Ciseeng, Bogor, Jawa Barat 16120
Telp. (0251) 8541742
Email: `perpustakaan@poltekssn.ac.id`

ISBN cetak: 978-634-04-4954-9
ISBN digital: 978-623-04-4762-0
Cetakan I: 2025
xxiv + 324 halaman; Ukuran: 17 x 24 cm

© 2025
Politeknik Siber dan Sandi Negara Press
Seluruh hak cipta dilindungi Undang-Undang.
Dilarang memperbanyak sebagian atau seluruh isi tanpa izin tertulis.

Ingatlah bahwa kechilafan satu orang sahaja, tjukup sudah menjebabkan keruntuhan negara.

dr. Roebiono Kertopati

Kata Pengantar Kepala BSSN

Di era transformasi digital yang kian cepat, teknologi bukan lagi sekadar alat, melainkan ruang hidup baru yang memengaruhi cara kita berinteraksi, bekerja, dan membangun bangsa. Namun, sebesar apa pun potensi yang ditawarkan, ruang digital hanya akan bermanfaat apabila dibangun di atas fondasi yang aman, inklusif, dan tepercaya. Kepercayaan digital menjadi kunci, tanpanya, interaksi antar pemerintah, pelaku usaha, dan masyarakat tidak akan pernah mencapai daya ungkit optimal bagi pertumbuhan ekonomi maupun kualitas kehidupan berbangsa.

Buku "*Kerangka Kerja Kepercayaan Digital Indonesia*" hadir sebagai respons strategis atas kebutuhan pedoman nasional untuk memperkuat tata kelola ruang siber. Dengan pendekatan lintas sektor dan berbasis prinsip tanggung jawab, karya ini tidak hanya memaparkan prinsip dan strategi, tetapi juga memberikan arah implementasi yang sistematis dan komprehensif.

Keamanan digital di ruang siber adalah *shared responsibility*, sebuah tanggung jawab bersama yang menuntut sinergi seluruh sektor: pemerintah sebagai pengarah kebijakan, industri sebagai penggerak inovasi, akademisi sebagai penjaga nalar kritis, serta masyarakat sebagai pengguna yang cerdas dan berdaya. Hanya dengan kolaborasi lintas sektor inilah kepercayaan digital dapat tumbuh dan ekosistem digital kita benar-benar kokoh. Sejalan dengan semangat tersebut, kita mengusung pesan sederhana namun fundamental: "*Di ruang siber, nyaman karena aman.*"

Badan Siber dan Sandi Negara (BSSN) mendukung penuh penyusunan buku ini sebagai bagian dari upaya memperkuat fondasi keamanan siber di Indonesia. Lebih lanjut, kontribusi yang diberikan sejalan dengan arah kebijakan strategis pemerintah yang menekankan pentingnya integrasi antara regulasi, literasi, teknologi, dan kelembagaan, sekaligus memperhatikan keselarasan dengan agenda global dalam

membangun ekosistem digital yang tangguh.

Saya percaya buku ini akan memberikan manfaat besar bagi para pemangku kepentingan, baik pemerintah, swasta, akademisi, maupun masyarakat luas, dalam memahami dan menerapkan prinsip kepercayaan digital di berbagai sektor. Lebih dari sekadar referensi, saya berharap buku ini menjadi pemicu kolaborasi lintas sektor dalam membangun ruang digital Indonesia yang aman, andal, dan tepercaya.

Akhir kata, saya menyampaikan apresiasi kepada seluruh pihak yang telah berkontribusi dalam penyusunan buku ini. Semoga karya ini menjadi bagian dari langkah kolektif kita menuju masa depan digital Indonesia yang tangguh, berdaya saing, dan berkeadilan.

Nugroho Sulistyo Budi
Kepala Badan Siber dan Sandi Negara (BSSN)
September 2025

Kata Pengantar Direktur Poltek SSN

Perkembangan teknologi digital yang begitu pesat telah mengubah secara fundamental cara individu, organisasi, dan negara berinteraksi dalam ruang siber. Di tengah perubahan ini, kepercayaan digital menjadi elemen penting yang menentukan keberhasilan transformasi digital yang aman, inklusif, dan berkelanjutan. Tantangan terhadap privasi, integritas data, dan keamanan sistem semakin kompleks dan memerlukan pendekatan lintas sektor yang kolaboratif dan berbasis pengetahuan.

Dalam konteks ini, lembaga pendidikan tinggi memegang peran strategis dalam membangun kapasitas sumber daya manusia dan memajukan pemikiran kritis untuk merespons dinamika keamanan dan tata kelola digital. Politeknik Siber dan Sandi Negara (Poltek SSN), sebagai institusi pendidikan vokasi di bawah Badan Siber dan Sandi Negara, berkomitmen untuk turut mendukung upaya penguatan ekosistem digital Indonesia yang berlandaskan nilai kepercayaan dan tanggung jawab.

Buku "*Kerangka Kerja Kepercayaan Digital Indonesia*" ini merupakan hasil kolaborasi antara akademisi, praktisi, komunitas, dan pemerintah dalam merumuskan arah strategis kepercayaan digital nasional. Buku ini mengeksplorasi prinsip-prinsip kepercayaan digital, standar pengelolaan data dan sistem, hingga strategi implementasi lintas sektor. Dengan pendekatan interdisipliner, buku ini memberikan gambaran menyeluruh tentang bagaimana kepercayaan dapat ditumbuhkan dan dijaga di tengah kemajuan teknologi dan pergeseran nilai sosial.

Kami berharap buku ini dapat menjadi referensi penting bagi institusi pendidikan, pembuat kebijakan, pelaku industri, serta masyarakat umum dalam memahami dan mengembangkan ekosistem digital yang tepercaya. Penerapan kerangka kerja ini diharapkan tidak hanya mendorong ketahanan nasional di ruang siber, tetapi juga memperkuat kolaborasi dan inovasi yang berorientasi pada kepentingan publik.

Akhir kata, kami menyampaikan apresiasi setinggi-tingginya kepada semua pihak yang telah berkontribusi dalam penyusunan buku ini. Semoga buku ini dapat menjadi landasan pemikiran dan panduan praktis dalam membangun masa depan digital Indonesia yang lebih aman, inklusif, dan berkelanjutan.

Ir. Arnoldus Triono, M.M., M.Tr. Opsla., CIQNR
Direktur Politeknik Siber dan Sandi Negara
September 2025

Kata Pengantar Rektor ITB

Transformasi digital merupakan salah satu pilar strategis dalam upaya mewujudkan visi Indonesia Emas 2045, yaitu sebuah cita-cita besar untuk menjadikan Indonesia sebagai negara maju yang berdaulat, adil, dan makmur pada usia kemerdekaannya yang ke-100. Transformasi digital tidak hanya mencakup adopsi teknologi informasi dan komunikasi secara luas, tetapi juga mencerminkan perubahan mendasar dalam cara kita bekerja, belajar, berinteraksi, serta mengelola sumber daya dan layanan publik. Namun, transformasi digital tidak akan pernah benar-benar terwujud tanpa adanya elemen dasar yang menopangnya, yaitu **kepercayaan digital** (*digital trust*). Kepercayaan digital mencakup aspek keamanan informasi, privasi data, integritas sistem, dan keandalan teknologi, yang semuanya berperan penting dalam membangun keyakinan masyarakat terhadap ekosistem digital. Tanpa kepercayaan digital, partisipasi publik akan terbatas, inovasi akan terhambat, dan potensi digitalisasi akan sulit dioptimalkan. Dalam konteks inilah, kehadiran buku "*Kerangka Kerja Kepercayaan Digital Indonesia*" menjadi sangat relevan dan strategis. Buku ini merupakan hasil kolaborasi antara Politeknik Siber dan Sandi Negara (Poltek SSN), Institut Teknologi Bandung (ITB), dan Huawei, yang bertujuan untuk menyediakan pemahaman yang komprehensif dan terstruktur mengenai bagaimana kepercayaan digital dapat dibangun, dikembangkan, dan dijaga dalam konteks Indonesia.

Kami meyakini bahwa kolaborasi antara perguruan tinggi dan industri merupakan fondasi penting dalam membangun ekosistem digital yang kuat dan berdaya saing. Kerjasama semacam ini memungkinkan terjadinya sinergi antara keilmuan dan praktik, antara riset dan aplikasi, serta antara kebijakan dan inovasi teknologi. ITB merasa terhormat dapat berkontribusi dalam inisiatif ini, sebagai bagian dari komitmen kami dalam mendukung pengembangan ilmu pengetahuan dan teknologi yang bermanfaat bagi masyarakat luas.

Akhir kata, kami mengapresiasi seluruh pihak yang telah terlibat dalam penyusunan buku ini. Semoga buku "*Kerangka Kerja Kepercayaan Digital Indonesia*" dapat menjadi sumber inspirasi, panduan, dan rujukan bagi seluruh pemangku kepentingan dalam mewujudkan transformasi digital yang aman, inklusif, dan berkelanjutan.

Prof. Dr. Ir. Tatacipta Dirgantara, M.T.
Rektor Institut Teknologi Bandung
September 2025

Kata Pengantar Ketua ICSF

Di era transformasi digital yang mengubah wajah kehidupan masyarakat—mulai dari perdagangan, pendidikan, hingga pemerintahan dan partisipasi publik—pertanyaan tentang kepercayaan menjadi hal yang sangat krusial. Kepercayaan kini tidak hanya dibangun melalui interaksi antarmanusia, tetapi juga melalui sistem, teknologi, dan kebijakan digital yang mengatur dunia terhubung kita.

Pertumbuhan digital Indonesia yang begitu pesat membawa peluang sekaligus tantangan. Di tengah pesatnya adopsi teknologi, belum adanya kerangka kerja kepercayaan digital yang utuh dan terstruktur membuat masyarakat, pelaku usaha, dan institusi menjadi rentan terhadap berbagai risiko mulai dari pelanggaran data, disinformasi, hingga inefisiensi sistemik.

White Paper ini merupakan hasil kolaborasi antara Politeknik Siber dan Sandi Negara (Poltek SSN), Institut Teknologi Bandung (ITB), dan Indonesia Cyber Security Forum (ICSF). Dokumen ini menjadi langkah strategis dalam menjawab kebutuhan tersebut, tidak hanya dengan menawarkan model kepercayaan digital yang komprehensif, tetapi juga dengan menyusun peta jalan bagi Indonesia dalam membangun ekosistem digital yang aman, etis, dan tangguh.

ICSF merasa terhormat dapat menjadi bagian dari upaya ini, menghadirkan ruang diskusi yang mempertemukan pemerintah, akademisi, pelaku industri, dan masyarakat sipil. Kolaborasi lintas sektor ini menjadi bukti komitmen bersama kita dalam membangun masa depan digital yang terpercaya. Semoga dokumen ini menjadi awal dari perubahan, pemicu inovasi kebijakan, kejelasan regulasi, kemajuan teknologi, dan kesadaran publik. Indonesia layak memiliki masa depan digital di mana kepercayaan bukan hanya menjadi harapan, tetapi menjadi fondasi yang dirancang sejak awal.

Ardi Sutedja K.
Pendiri dan Ketua Indonesia Cyber Security Forum (ICSF)
September 2025

Prakata Penulis

Dengan penuh rasa syukur kepada Tuhan Yang Maha Esa, kami mempersembahkan buku ini sebagai hasil kerja kolektif berbagai pihak yang memiliki kepedulian terhadap masa depan ekosistem digital Indonesia. Gagasan awal penyusunan buku ini berangkat dari keprihatinan atas masih rendahnya literasi keamanan digital di masyarakat, serta belum adanya kerangka nasional yang adaptif terhadap tantangan teknologi yang terus berkembang. Buku ini disusun untuk menawarkan landasan konseptual dan praktis dalam memperkuat kepercayaan digital nasional.

Penyusunan buku ini melibatkan kolaborasi lintas disiplin ilmu, mencakup bidang keamanan siber, kriptografi, hukum dan kebijakan publik, arsitektur sistem digital, sosiologi digital, etika teknologi, ekonomi digital, serta pendidikan dan literasi digital. Pendekatan multidisiplin ini dipandang penting untuk membangun kerangka kerja kepercayaan digital yang tidak hanya kuat dari sisi teknis dan legal, tetapi juga responsif terhadap nilai-nilai sosial, budaya, serta kebutuhan nyata pengguna.

Dalam proses penulisan dan penyuntingan, tim penulis memanfaatkan teknologi kecerdasan artifisial generatif (*generative artificial intelligence* / AI) secara terbatas sebagai alat bantu untuk meningkatkan keterbacaan dan koherensi naskah. Teknologi ini digunakan untuk menyempurnakan struktur kalimat, menyelaraskan gaya bahasa, serta membantu merumuskan narasi awal berdasarkan masukan konseptual dari para kontributor. Namun demikian, seluruh substansi, analisis, dan argumentasi dalam buku ini tetap merupakan hasil pemikiran kritis dan kerja ilmiah para penulis. Setiap bagian yang melibatkan dukungan AI telah melalui proses verifikasi, penyuntingan, dan kurasi menyeluruh oleh tim ahli yang berkompeten di bidangnya.

Sebagai kelanjutan dari komitmen tersebut, penggunaan AI dilakukan dengan tetap menjunjung tinggi prinsip integritas akademik, pengawasan manusia (*human oversight*), dan tanggung jawab ilmiah. Teknologi diposisikan sebagai pendukung, bukan pengganti, dalam pengambilan keputusan penulisan. Dengan demikian, kehadiran AI tidak mengurangi peran penulis sebagai aktor utama dalam keseluruhan proses intelektual buku ini. Lebih jauh, buku ini juga telah melalui proses telaah sejawat oleh para pakar di bidang terkait untuk memastikan kualitas isi, akurasi argumentasi, dan relevansi substansi sebelum diterbitkan.

Pendekatan ini mencerminkan komitmen kami untuk menjaga kualitas ilmiah

sekaligus memastikan keterbacaan dan relevansi isi bagi berbagai kalangan pembaca. Dengan memadukan integritas akademik, pemanfaatan teknologi secara etis, dan penyusunan konten yang terkurasi, kami berharap buku ini mampu menjembatani kebutuhan praktis dan konseptual dalam membangun ekosistem digital yang tepercaya.

Melalui diskusi intensif, kajian multisektor, dan penyelarasan dengan prinsip tata kelola yang akuntabel serta inklusif, buku ini dirancang sebagai rujukan strategis bagi para pemangku kepentingan di sektor pemerintahan, industri, akademisi, dan masyarakat sipil. Lebih dari sekadar referensi teknis, kami berharap buku ini menjadi sarana dialog lintas sektor dalam memperkuat ekosistem digital Indonesia yang tangguh, tepercaya, dan berkelanjutan.

Kami menyampaikan apresiasi setinggi-tingginya kepada seluruh kontributor, mitra kerja, dan institusi yang telah mendukung proses penulisan serta penyusunan buku ini. Semoga karya ini menjadi bagian dari upaya kolektif menuju transformasi digital Indonesia yang lebih aman, adil, dan berkepercayaan.

Tim Kepercayaan Digital
September 2025

Daftar Isi

Kata Pengantar Kepala BSSN **v**

Kata Pengantar Direktur Poltek SSN **vii**

Kata Pengantar Rektor ITB **ix**

Kata Pengantar ICSF **xi**

Prakata Penulis **xiii**

Daftar Isi **xix**

Daftar Gambar **xxii**

Daftar Tabel **xxiv**

1 Transformasi dan Ekonomi Digital **1**

1.1 Indonesia dan Ekonomi Global 1

1.2 Peran Transformasi Digital Dalam Pertumbuhan Ekonomi 3

1.3 Indonesia Dalam Ekonomi Digital Global 5

1.4 Meningkatnya Kebutuhan Akan Kepercayaan Digital 14

1.5 Standar Utama untuk Aplikasi Digital 17

1.6 Ikhtisar Kebijakan Indonesia 19

2 Definisi Kepercayaan Digital **21**

2.1 Kepercayaan 22

2.2 Kepercayaan Digital 26

2.2.1 Kepercayaan digital mekanis 28
2.2.2 Kepercayaan digital relasional 30
2.2.3 Ekosistem kepercayaan digital 31
2.3 Teknik Pengembangan Kerangka Kerja 33

3 Praktik Terbaik Kepercayaan Digital 37
3.1 Praktik Terbaik Kepercayaan Digital Negara 40
3.1.1 Singapura 41
3.1.2 Malaysia 49
3.1.3 Uni Eropa 56
3.1.4 Amerika Latin 68
3.1.5 Turki 74
3.2 Analisis Komparatif Praktik Terbaik Kepercayaan Digital Negara . . 83
3.3 Praktik Terbaik Kepercayaan Digital Komunitas 87
3.3.1 World Economic Forum (WEF) 87
3.3.2 PricewaterhouseCoopers (PwC) 93
3.3.3 Information Systems Audit and Control Association (ISACA) 98
3.4 Analisis Komparatif Komunitas 104

4 Regulasi dan Referensi 113
4.1 Undang-Undang (UU) 115
4.1.1 UU Nomor 17 Tahun 2007 tentang Rencana Pembangunan Jangka Panjang Nasional (RPJP Nasional) tahun 2005-2025 . 116
4.1.2 UU Nomor 59 Tahun 2024 tentang Rencana Pembangunan Jangka Panjang Nasional (RPJPN) 2025-2045 117
4.1.3 UU Nomor 11 Tahun 2008 juncto Nomor 19 Tahun 2019 juncto Nomor 1 Tahun 2024 tentang Informasi dan Transaksi Elektronik (ITE) 120
4.1.4 UU Nomor 27 Tahun 2022 tentang Pelindungan Data Pribadi 122
4.1.5 UU Nomor 8 Tahun 1999 tentang Perlindungan Konsumen . 125
4.2 Peraturan Pemerintah (PP) 127
4.2.1 PP Nomor 71 tentang Penyelenggaraan Sistem dan Transaksi Elektronik 127
4.3 Peraturan Presiden (Perpres) 130

4.3.1 Perpres Nomor 95 Tahun 2018 tentang Sistem Pemerintahan Berbasis Elektronik (SPBE) 131
4.3.2 Perpres Nomor 82 Tahun 2022 tentang Pelindungan Infrastruktur Informasi Vital 134
4.3.3 Perpres Nomor 132 Tahun 2022 tentang Arsitektur Sistem Pemerintahan Berbasis Elektronik (SPBE) Nasional 137
4.3.4 Perpres Nomor 82 Tahun 2023 tentang Percepatan Transformasi Digital dan Keterpaduan Layanan Digital Nasional . . . 140
4.3.5 Perpres Nomor 17 Tahun 2023 tentang Percepatan Transformasi Digital di Bidang Pengadaan Barang/Jasa Pemerintah . 142
4.3.6 Perpres Nomor 47 Tahun 2023 tentang Strategi Keamanan Siber Nasional dan Manajemen Krisis Siber 145
4.4 Instruksi Presiden (Inpres) 148
4.4.1 Inpres Nomor 4 Tahun 2025 tentang Data Tunggal Sosial dan Ekonomi Nasional 148
4.5 Peraturan dan Kebijakan Lainnya 150
4.5.1 Peraturan Menteri Komunikasi dan Informatika Nomor 5 Tahun 2020 juncto Nomor 10 Tahun 2021 tentang Penyelenggara Sistem Elektronik Lingkup Privat 150
4.5.2 Peraturan Menteri Komunikasi dan Digital Nomor 6 Tahun 2025 tentang Standar Teknis dan Prosedur Pembangunan dan Pengembangan Aplikasi Sistem Pemerintahan Berbasis Elektronik 154
4.5.3 Visi Indonesia Digital 156
4.5.4 Gerakan Nasional Literasi Digital 162
4.5.5 Peraturan Bank Indonesia Nomor 9/15/PBI/2007 tentang Penerapan Manajemen Risiko dalam Penggunaan Teknologi Informasi oleh Bank Umum 163
4.5.6 Peraturan Bank Indonesia Nomor 2 Tahun 2024 tentang Keamanan Sistem Informasi Dan Ketahanan Siber Bagi Penyelenggara Sistem Pembayaran, Pelaku Pasar Uang Dan Pasar Valuta Asing, Serta Pihak Lain Yang Diatur Dan Diawasi Bank Indonesia 166
4.5.7 Buku Putih Strategi Nasional Pengembangan Ekonomi Digital Indonesia 2030 169
4.5.8 Peraturan Otoritas Jasa Keuangan Nomor 11 Tahun 2022 tentang Penyelenggaraan Teknologi Informasi oleh Bank Umum 172
4.5.9 Peraturan Otoritas Jasa Keuangan Nomor 21 Tahun 2023 tentang Layanan Digital oleh Bank Umum 175

4.5.10 Peraturan Otoritas Jasa Keuangan Nomor 40 Tahun 2024 tentang Layanan Pendanaan Bersama Berbasis Teknologi Informasi 177

4.5.11 Peraturan BSSN Nomor 8 Tahun 2020 tentang Sistem Pengamanan dalam Penyelenggaraan Sistem Elektronik 180

4.5.12 Peraturan BSSN Nomor 4 Tahun 2021 tentang Pedoman Manajemen Keamanan Informasi Sistem Pemerintahan Berbasis Elektronik (SPBE) 183

4.5.13 Peraturan BSSN Nomor 7 Tahun 2023 tentang Identifikasi Infrastruktur Informasi Vital (IIV) 185

4.5.14 Peraturan BSSN Nomor 8 Tahun 2023 tentang Kerangka Kerja Pelindungan Infrastruktur Informasi Vital 189

4.5.15 Peraturan BSSN Nomor 9 Tahun 2023 tentang Peningkatan Kapasitas Sumber Daya Manusia di Bidang Keamanan Siber dan Sandi 192

4.5.16 Peraturan BSSN Nomor 10 Tahun 2023 tentang Pengukuran Tingkat Kematangan Keamanan Siber 194

4.5.17 Peraturan BSSN Nomor 1 Tahun 2024 tentang Pengelolaan Insiden Siber 196

4.5.18 Peraturan BSSN Nomor 2 Tahun 2024 tentang Manajemen Krisis Siber 200

4.5.19 Peraturan BSSN Nomor 5 Tahun 2024 tentang Rencana Aksi Nasional Keamanan Siber 201

4.5.20 Peraturan BSSN Nomor 7 Tahun 2024 tentang Penyelenggaraan Penilaian Kesesuaian Kriteria Umum untuk Evaluasi Keamanan Teknologi Informasi Indonesia 204

4.5.21 Peraturan BSSN Nomor 11 Tahun 2024 tentang Penyelenggaraan Algoritma Kriptografi Indonesia dan Penilaian Kesesuaian Keamanan Modul Kriptografi 207

4.5.22 Strategi Nasional Kecerdasan Artifisial Indonesia 210

5 Potret Kepercayaan Digital Indonesia 215

5.1 Mengapa Kepercayaan Digital Penting (*Why*) 220

5.2 Tujuan Pengenalan Kepercayaan Digital (*What*) 223

5.3 Siapa yang Bertanggung Jawab (*Who*) 230

5.4 Waktu dan Tahapan Implementasi (*When*) 237

5.5 Bagaimana Kepercayaan Digital Diterapkan (*How*) 241

5.6 Inisiatif Kepercayaan Digital Indonesia 248

6 Kerangka Kerja Kepercayaan Digital Indonesia 255

6.1 Prinsip Umum dan Nilai Dasar Kepercayaan Digital Indonesia . . . 256

6.2 Kerangka Kerja Kepercayaan Digital Indonesia 258

6.2.1 Rasional Desain Kerangka Kerja Kepercayaan Digital Indonesia 258

6.2.2 Definisi Kepercayaan Digital 259

6.2.3 Tujuan Kepercayaan Digital 260

6.2.4 Manajemen Kepercayaan Digital 261

6.2.5 Faktor Kunci Kepercayaan Digital 262

6.3 Model Kerangka Kerja Kepercayaan Digital 263

6.3.1 Landasan Penerapan Kepercayaan Digital 264

6.3.2 Pilar Penerapan Kepercayaan Digital 266

6.3.3 Domain Kepercayaan Digital 269

6.3.4 Target, Tujuan, dan Kepemimpinan 271

6.4 Ekosistem Kepercayaan Digital 272

6.4.1 Lini Ekosistem Kepercayaan Digital 273

6.4.2 Interaksi Ekosistem Kepercayaan Digital 277

6.4.3 Kepercayaan Digital dalam Ekosistem G2G, G2B, G2C, B2B, dan B2C 277

6.5 Penerapan Kepercayaan Digital pada STE 280

7 Rekomendasi Strategis Kepercayaan Digital Indonesia 283

7.1 Rekomendasi Strategis 284

7.1.1 Penegasan Prinsip Nasional Kepercayaan Digital 284

7.1.2 Harmonisasi dan Integrasi Regulasi 285

7.1.3 Penguatan Kelembagaan dan Infrastruktur 285

7.1.4 Penerapan Standar Keamanan dan Audit Teknologi 287

7.1.5 Implementasi pada Sektor Prioritas Nasional 287

7.1.6 Prinsip *Trust by Design* dalam Sistem Digital Nasional 289

7.1.7 Pendidikan dan Literasi Kepercayaan Digital 290

7.1.8 Peluang Kecerdasan Artifisial (AI) dalam Keamanan *Online* 290

7.1.9 Kolaborasi *Multi-Stakeholder* dan Diplomasi Digital 291

7.2 Penutup 292

Daftar Referensi 295

Daftar Gambar

1.1 Pertumbuhan GDP Indonesia [6] 3
1.2 Infografis "*Digital Economy in Indonesia*" [24] 7
1.3 DEFA 9 Core [42] 12
1.4 *Digital Trade Standards* 13

3.1 *Smart Nation Singapura* [117] 42
3.2 Tinjauan Umum Strategi Keamanan Siber Singapura 2021 [128] . . . 45
3.3 Model Kepercayaan Digital Malaysia [150] 50
3.4 EU *legislations* pada sektor digital [174] 57
3.5 Garis waktu peraturan terkait *Cybersecurity* EU 59
3.6 Kerangka Kerja Kepercayaan Digital WEF [77] 88
3.7 Peta Jalan Kepercayaan Digital WEF [77] 91
3.8 Kerangka Kepercayaan Digital PwC [78] 96
3.9 Rantai pasok hubungan oleh ISACA [93] 99
3.10 Korelasi aktivitas digital dengan derajat kepercayaan [93] 101

4.1 Korelasi aktivitas digital dengan derajat kepercayaan 119
4.2 Kerangka Kerja Proyek Strategis Nasional 140
4.3 Kerangka Visi Indonesia Digital 2045 [294] 157
4.4 Visi Indonesia Digital 2045 [294] 161

6.1 Kerangka Kerja Kepercayaan Digital Indonesia 259
6.2 Model Kerangka Kerja Kepercayaan Digital Indonesia 264
6.3 Lini Ekosistem Kepercayaan Digital 273
6.4 Pola Interaksi Ekosistem Kepercayaan Digital Indonesia 278

6.5 Penerapan Kepercayaan Digital pada Sistem dan Transaksi Elektronik 281

Daftar Tabel

1.1 Indonesia's Nominal GDP (2010–2023) 2

1.2 Kecepatan seluler dan *broadband* di beberapa negara Asia Tenggara (Mbps) 5

1.3 Strategi Digital, AI dan Green berbagai Negara 10

1.4 Standar dan *Framework* Digital 18

2.1 Beberapa Definisi Kepercayaan Digital Mekanis 29

2.2 Evolusi Definisi Kepercayaan Digital Relasional 30

2.3 Pendekatan *Ekosistem* Terpadu antara Kepercayaan Relasional dan Mekanis 32

3.1 Analisis Komparatif Kepercayaan Digital Negara 84

3.2 Aspek Pertanyaan Tematik Penerapan Kepercayaan Digital oleh Komunitas 105

3.3 Kepercayaan Digital menurut WEF, PwC, dan ISACA 105

3.4 Tujuan Pengenalan Kepercayaan Digital menurut WEF, PwC, dan ISACA 106

3.5 Peran dan Tanggung Jawab Kepercayaan Digital menurut WEF, PwC, dan ISACA 107

3.6 Waktu dan Tahapan Implementasi Kepercayaan Digital menurut WEF, PwC, dan ISACA 108

3.7 Pendekatan Penerapan Kepercayaan Digital menurut WEF, PwC, dan ISACA 109

5.1 Pemetaan Aspek *Why* dengan Regulasi Terkait di Indonesia 222

5.2 Pemetaan Aspek *What* dengan Regulasi Terkait di Indonesia 229

5.3 Pemetaan Aspek *Who* dengan Regulasi Terkait di Indonesia 236

5.4 Pemetaan Aspek *When* dengan Regulasi Terkait di Indonesia 240
5.5 Pemetaan Aspek *How* dengan Regulasi Terkait di Indonesia 248

6.1 Pemetaan Pilar dan Faktor Kunci Kepercayaan Digital 269

1

Transformasi dan Ekonomi Digital

> In a connected world, trust is your most valuable digital currency.
>
> — PwC Global

1.1 Indonesia dan Ekonomi Global

Semua negara di dunia saat ini sedang berjuang untuk meningkatkan kualitas hidup warga negaranya. Berbagai strategi dikembangkan oleh masing-masing negara untuk menjadi negara yang lebih sejahtera.

Indonesia, misalnya, sebagaimana ditunjukkan dalam Tabel 1.1, memiliki Produk Domestik Bruto (PDB) sebesar USD 1,35 triliun dan Pendapatan Nasional Bruto (GNI) per kapita sebesar USD 4.580. Berdasarkan klasifikasi Bank Dunia, Indonesia termasuk dalam kategori negara "berpendapatan menengah atas". Menurut International Monetary Fund (IMF), tingkat pertumbuhan PDB Indonesia pada tahun 2025 mencapai 4,7% (lihat Gambar 1.1).

Sebagai salah satu negara dengan populasi lebih dari 285 juta jiwa, Indonesia menghadapi tantangan besar dalam mencapai pertumbuhan ekonomi yang berkelanjutan. Untuk menjawab tantangan tersebut, pemerintah telah menetapkan visi jangka panjang **Indonesia Emas 2045**, yang bertujuan mewujudkan Indonesia sebagai negara maju, makmur, dan berdaya saing global. Adopsi serta integrasi teknologi digital di berbagai sektor menjadi salah satu pilar utama transformasi ini, menandai kebutuhan mendesak untuk akselerasi transformasi digital secara nasional.

Tabel 1.1: Indonesia's Nominal GDP (2010–2023)

Year	GDP (USD Billion)	Key Notes
2010	755.3	Post-2008 recovery
2011	892.7	Commodity boom
2012	917.9	Slower export growth
2013	912.5	Rupiah depreciation
2014	890.8	End of commodity boom
2015	861.9	Low oil prices
2016	931.9	Fiscal stimulus
2017	1015.4	Infrastructure push
2018	1042.2	Trade war impacts
2019	1119.2	Stable growth
2020	1058.4	COVID-19 contraction
2021	1186.1	Partial recovery
2022	1317.4	Commodity surge
2023	1417.4	Domestic demand-driven

Sumber: diolah kembali dari berbagai referensi [1, 2, 3, 4, 5, 6, 7]

Rencana Pembangunan Jangka Panjang Nasional (RPJPN) [8] 2025–2045 secara tegas menempatkan transformasi digital sebagai kunci peningkatan produktivitas dan efisiensi perekonomian. Dalam "Agenda 2 – Transformasi Ekonomi", peran digitalisasi dinyatakan sangat krusial, tidak hanya dalam meningkatkan daya saing, tetapi juga dalam mendukung ekosistem inovasi dan pelayanan publik yang adaptif. Lebih jauh, 17 Arah Pembangunan Nasional menggarisbawahi pentingnya percepatan transformasi digital melalui "Misi 2 – Transformasi Ekonomi (IE6 – Transformasi Digital)" [9].

Akselerasi adopsi teknologi digital di Indonesia terlihat nyata melalui semakin luasnya penetrasi internet, peningkatan penggunaan *smartphone*, dan pertumbuhan sektor *e-commerce*. Transformasi ini telah memicu perubahan signifikan dalam pola interaksi, pola transaksi, serta model bisnis masyarakat Indonesia. Di satu sisi, peluang pertumbuhan ekonomi baru semakin terbuka, namun di sisi lain, tantangan terkait keamanan digital dan kepercayaan konsumen turut mengemuka, menuntut respons strategis yang menyeluruh.

Pandemi COVID-19 mempercepat pergeseran ke ruang digital. Pembatasan interaksi fisik memaksa banyak aktivitas, baik pendidikan, bisnis, maupun pelayanan publik, beralih ke ranah *online*. Perusahaan menerapkan skema *Work from Home* (WfH) atau *Work from Anywhere* (WfA), jutaan pelajar melanjutkan pembelajaran melalui *online*, dan aplikasi konferensi seperti Zoom menjadi sangat populer. Transformasi digital terjadi secara masif dan cepat, meskipun dalam situasi tersebut aspek kepercayaan digital sempat kurang menjadi perhatian utama karena harus merespons situasi darurat.

Bergesernya masyarakat menuju ekosistem digital membawa perubahan fundamental dari ekonomi tradisional ke ekonomi digital, di mana kebutuhan terhadap kepercaya-

Gambar 1.1: Pertumbuhan GDP Indonesia [6]

an digital semakin mendesak. Kepercayaan digital merupakan hal yang fundamental dalam membangun kepuasan pengguna, memperkuat ekosistem transaksi *online*, dan mendorong pertumbuhan ekonomi secara berkelanjutan. Ruang transaksi kini melampaui batas geografis; interaksi ekonomi digital dapat berlangsung domestik maupun lintas negara. Kondisi ini menuntut pembangunan sistem kepercayaan digital yang kuat, tidak hanya pada lingkup nasional, tetapi juga untuk mendukung integrasi Indonesia dalam ekosistem digital global. Dengan demikian, transformasi digital dan penguatan kepercayaan digital menjadi agenda strategis yang tidak hanya penting untuk pertumbuhan ekonomi nasional, tetapi juga untuk memastikan partisipasi aktif Indonesia dalam perekonomian dunia yang semakin terhubung dan kompetitif.

1.2 Peran Transformasi Digital Dalam Pertumbuhan Ekonomi

Adopsi teknologi digital telah menjadi penggerak utama pembangunan ekonomi di era modern. Menurut laporan dan hasil kajian pustaka Chen dan World Bank [10, 11] menunjukkan bahwa investasi teknologi dan inovasi mampu mendorong peningkatan produktivitas. Bahkan secara statistik mampu meningkatkan produktivitas tenaga kerja hingga 20–30% dan menurunkan biaya operasional sebesar 10–20% bagi organisasi yang mengalokasikan minimal 3% anggaran untuk transformasi digital [12, 13]. Implementasi kecerdasan artifisial (*Artificial Intelligence* - AI), misalnya dalam sektor asuransi dan manufaktur, dapat menghasilkan penghematan biaya 10–15% serta peningkatan efisiensi operasional hingga 30% [12, 13].

Transformasi digital bukan sekadar tren, melainkan instrumen penting untuk mem-

percepat pertumbuhan ekonomi nasional. Penggunaan teknologi digital dan kecerdasan artifisial (AI) terbukti mampu meningkatkan efisiensi operasional, mengurangi biaya, dan mendorong produktivitas yang lebih tinggi. Penerapan AI berbasis sensor, *cloud* dan analisis *big data* dalam pembangunan *smart factory* di Korea mampu secara dramatis meningkatkan produktivitas manufaktur, kualitas produk, efisiensi energi serta biaya kompetitif [14]. Dalam konteks Indonesia berdasarkan kelebihan yang disajikan, transformasi digital berperan strategis apabila Indonesia ingin mendekati target pertumbuhan ekonomi tahunan 6–8% [10, 15, 16].

Temuan global tersebut sejalan dengan kondisi di Indonesia. Penerapan AI dalam manajemen jaringan di Telkom Indonesia, misalnya, mampu menurunkan gangguan layanan dan beban kerja teknisi, sehingga mengurangi biaya intervensi manual [17]. Pada level usaha mikro, kecil, dan menengah (UMKM), integrasi teknologi digital membantu pengelolaan data historis, mengotomatisasi pengambilan keputusan, dan meningkatkan efisiensi proses internal [18]. Fakta ini menegaskan bahwa digitalisasi memiliki dampak nyata dalam menekan biaya sekaligus mempercepat proses bisnis.

Dari perspektif makro, transformasi digital juga berkontribusi terhadap produktivitas total perekonomian. Organisation for Economic Co-operation and Development (OECD) menekankan bahwa digitalisasi di sektor-sektor strategis, termasuk pertanian, dapat mendorong efisiensi dan pertumbuhan jangka menengah hingga panjang [15]. Kajian Economic Research Institute for ASEAN and East Asia (ERIA) menunjukkan bahwa investasi digital memberikan manfaat lebih besar bagi pekerja berpendidikan tinggi, tetapi secara umum tetap meningkatkan produktivitas sektor formal [19]. Sementara itu, McKinsey menegaskan bahwa digitalisasi merupakan salah satu pilar utama jika Indonesia ingin mencapai status pendapatan tinggi menjelang 2045 [16].

Namun, potensi tersebut belum terdistribusi merata dikarenakan beberapa hambatan, antara lain kesenjangan infrastruktur dan rendahnya penetrasi *broadband* (sekitar 20% pada 2022 [20]); keterbatasan sumber daya manusia (SDM) dan literasi digital (45% perusahaan menyebutkan kekurangan talenta AI [21]); penerima manfaat yang lebih terkonsentrasi pada perusahaan besar dan pekerja terampil [19]; serta hambatan dukungan regulasi, perlindungan data, dan tata kelola etika AI yang adaptif.

Dengan kontribusi terhadap efisiensi biaya dan peningkatan produktivitas yang signifikan, transformasi digital berpotensi menjadi motor penggerak utama pertumbuhan ekonomi Indonesia. Jika digitalisasi dapat diperluas secara masif ke sektor padat karya dan wilayah terpencil, maka efek pengganda berupa peningkatan margin usaha, ekspansi kapasitas produksi, serta penciptaan lapangan kerja dapat menjadi motor utama untuk mencapai target pertumbuhan 6–8% per tahun.

Transformasi digital, terutama melalui pemanfaatan AI, bukan lagi pilihan, melainkan kebutuhan strategis. Untuk memastikan dampak positifnya berkelanjutan dan berdampak, Indonesia perlu memperkuat infrastruktur digital, meningkatkan literasi dan kapasitas SDM, serta menyediakan regulasi yang responsif. Dengan langkah-langkah tersebut, digitalisasi dapat menjadi pilar daya saing nasional sekaligus penentu pertumbuhan ekonomi jangka panjang.

1.3 Indonesia Dalam Ekonomi Digital Global

Ekonomi global saat ini tengah mengalami pergeseran signifikan dari model berbasis industri menuju ekonomi berbasis digital. Di kawasan Association of South-East Asian Nations (ASEAN), Indonesia berperan sebagai pemain utama dengan kontribusi hampir 40% terhadap pasar ekonomi digital di Asia Tenggara, menjadikannya pasar digital terbesar di kawasan tersebut. Meski demikian, potensi penuh transformasi digital Indonesia masih dihadapkan pada beragam tantangan struktural yang perlu diatasi.

1. Keterbatasan infrastruktur: Kecepatan internet di Indonesia masih tertinggal dibandingkan negara-negara tetangga di ASEAN. Tantangan ini dipicu oleh cakupan geografis Indonesia yang luas serta jumlah pulau yang sangat banyak, sehingga pengembangan infrastruktur digital menjadi lebih kompleks dan mahal.
2. Kesenjangan literasi digital: Sebagian besar masyarakat belum memiliki keterampilan digital yang memadai [22]. Hal ini berkontribusi pada maraknya penipuan *online* dan tingginya tingkat kepercayaan terhadap berita palsu (hoaks), yang pada akhirnya menghambat pemanfaatan teknologi secara optimal.
3. Masalah keamanan dan kepercayaan: Ancaman terhadap keamanan siber, penipuan digital, dan kekhawatiran mengenai perlindungan data pribadi semakin meningkat. Isu-isu tersebut menjadi faktor utama yang menjadi penghambat utama dalam membangun kepercayaan masyarakat terhadap layanan maupun platform digital.

Analisis perbandingan kecepatan internet di negara-negara ASEAN (Tabel 1.2) menunjukkan bahwa Indonesia, meskipun memiliki tingkat adopsi digital yang tinggi, masih tertinggal dalam hal infrastruktur internet dan hanya unggul dibandingkan dengan Myanmar. Fakta ini menegaskan perlunya percepatan pembangunan infrastruktur serta peningkatan literasi dan keamanan digital guna memaksimalkan kontribusi ekonomi digital Indonesia di tingkat regional.

Tabel 1.2: Kecepatan seluler dan *broadband* di beberapa negara Asia Tenggara (Mbps)

Negara	**Unduh Seluler**	**Unggah Seluler**	**Unduh *Broadband***	**Unggah *Broadband***
Singapura	100+	90+	200+	190+
Malaysia	60–80	30–50	150–180	100–130
Thailand	50–70	25–45	100–150	80–120
Vietnam	40–60	20–40	80–120	50–90
Indonesia	26.6	–	30.2	–
Myanmar	10–20	5–15	20–50	10–30

Indonesia telah menunjukkan pertumbuhan adopsi teknologi digital yang pesat meskipun masih menghadapi sejumlah hambatan. Berdasarkan survei We Are Social per Februari 2025 [23], penetrasi digital di Indonesia mencapai tingkat yang signifikan, dengan:

- Fenomena menarik terjadi dalam ranah konektivitas seluler di Indonesia. Jumlah koneksi seluler aktif telah mencapai lebih dari 356 juta, atau sekitar 125% dari total populasi. Angka ini menunjukkan bahwa banyak individu memiliki lebih dari satu koneksi seluler, baik untuk keperluan pribadi maupun profesional. Ekspansi konektivitas ini didorong oleh kemudahan penggunaan teknologi *eSIM* serta meningkatnya kebutuhan akan konektivitas yang selalu aktif di berbagai aspek kehidupan digital.
- Jumlah pengguna internet di Indonesia telah mencapai lebih dari 212 juta jiwa, atau sekitar 74,6% dari total populasi. Angka ini mencerminkan tingkat adopsi digital yang semakin meluas di berbagai lapisan masyarakat. Meskipun demikian, data tersebut juga menunjukkan bahwa masih terdapat sekitar 25,4% populasi yang belum terjangkau oleh akses internet, yang sekaligus menjadi potensi untuk pertumbuhan dan perluasan infrastruktur digital ke depan.
- Sebanyak 143 juta pengguna media sosial aktif tercatat pada Februari 2025, mencakup 50,2% dari total populasi Indonesia. Angka ini menunjukkan bahwa media sosial telah menjadi bagian yang tak terpisahkan dari kehidupan digital masyarakat, sekaligus menegaskan posisinya sebagai platform utama untuk komunikasi, penyebaran informasi, dan hiburan.

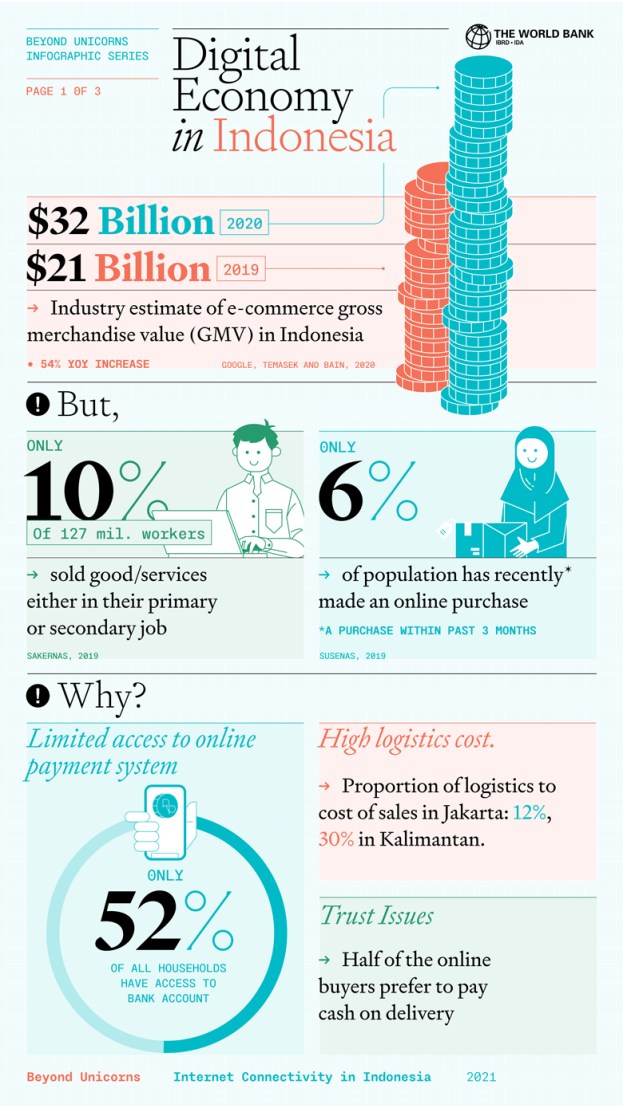
Angka-angka tersebut menunjukkan bahwa Indonesia memiliki potensi besar dalam ekosistem digital, baik dibandingkan dengan negara tetangga maupun dalam skala global. Dengan cakupan internet yang terus diperluas, jumlah pengguna digital diprediksi akan terus meningkat dalam beberapa tahun mendatang.

Transformasi digital di Indonesia tidak hanya berkaitan dengan infrastruktur, tetapi juga mencakup perubahan menyeluruh pada ekosistem layanan publik, bisnis, dan interaksi masyarakat. Beberapa contoh inovasi digital lintas sektor yang telah hadir meliputi:

- *E-Commerce*: Tokopedia, Shopee, Lazada, Bukalapak. Logistik Digital: JNE, J&T, SiCepat, Shopee Express.
- Pembayaran Digital: OVO, GoPay, Shopee Pay, pembayaran melalui QRIS.
- Transportasi Digital: GO-JEK, Grab, Maxim, inDrive, dan beberapa layanan yang sifatnya lokal.
- Kesehatan Digital: Satu Sehat (dahulu Peduli Lindungi), Halodoc, dan beberapa aplikasi yang khusus untuk rumah sakit tertentu.
- *E-Government*: Digitalisasi data kependudukan, sistem pajak *online*

Inovasi digital di Indonesia terus berkembang pesat dan semakin menjadi bagian integral dari kehidupan masyarakat. Saat ini, pemanfaatannya masih lebih banyak bersifat domestik, terutama dalam mendukung layanan publik, pendidikan, keuangan, dan kesehatan. Namun, ke depannya, peluang untuk memperluas inovasi digital

ke pasar global semakin terbuka lebar. Ekspansi ini bukan hanya akan memperkuat posisi Indonesia dalam ekonomi digital dunia, tetapi juga membuka peluang baru dalam bentuk ekspor teknologi, kolaborasi internasional, dan peningkatan daya saing industri kreatif nasional.



Gambar 1.2: Infografis "*Digital Economy in Indonesia*" [24]

Sebagaimana ditunjukkan pada Gambar 1.2, nilai *gross merchandise value* (GMV) *e-commerce* Indonesia meningkat dari USD 21 miliar pada 2019 menjadi USD 32 miliar pada 2020. Namun, hanya sekitar 10% dari 127 juta pekerja yang menjual barang atau jasa secara *online*, dan 6% populasi yang melakukan pembelian *online*

dalam tiga bulan terakhir [24]. Artinya, meski pasar digital berkembang pesat, pemanfaatannya masih terbatas pada segmen tertentu.

Dengan ekosistem digital yang terus berkembang, Indonesia memiliki peluang besar untuk memperluas dampak digitalisasi ke sektor padat karya dan pasar global. Ekspansi ini tidak hanya memperkuat posisi Indonesia dalam ekonomi digital regional, tetapi juga membuka peluang ekspor teknologi, kolaborasi internasional, dan peningkatan daya saing industri kreatif nasional.

Sejalan dengan tren positif transformasi digital tersebut, arah kebijakan pembangunan nasional menunjukkan komitmen yang kuat melalui visi besar yang tertuang dalam Asta Cita [25]. Delapan misi strategis dalam Indonesia Emas 2045 yang digagas oleh Presiden Prabowo Subianto menjadi dasar bagi terwujudnya Indonesia sebagai negara maju yang mandiri, berdaulat, dan berkelanjutan.

1. Memperkokoh ideologi Pancasila, demokrasi, dan hak asasi manusia (HAM).
   Menekankan pentingnya memperkuat pemahaman dan implementasi Pancasila sebagai ideologi negara, memperkokoh sistem demokrasi, serta menjunjung tinggi HAM. Langkah ini bertujuan untuk menciptakan masyarakat yang adil, makmur, dan beradab.

2. Memantapkan sistem pertahanan keamanan negara dan mendorong kemandirian bangsa melalui swasembada pangan, energi, air, ekonomi syariah, ekonomi digital, ekonomi hijau, dan ekonomi biru.
   Fokus pada peningkatan pertahanan dan keamanan nasional melalui modernisasi alat utama sistem persenjataan (alutsista) dan peningkatan kesejahteraan prajurit. Selain itu, pemerintah berupaya mencapai kemandirian dalam bidang pangan, energi, dan air untuk memastikan ketahanan nasional yang komprehensif.

3. Melanjutkan pengembangan infrastruktur dan meningkatkan lapangan kerja yang berkualitas, mendorong kewirausahaan, mengembangkan industri kreatif, serta mengembangkan industri agromaritim di sentra produksi melalui peran aktif koperasi.
   Pemerintah berkomitmen menciptakan lapangan kerja berkualitas dengan mendorong pertumbuhan industri kreatif dan melanjutkan pembangunan infrastruktur. Selain itu, pengembangan kewirausahaan ditingkatkan melalui pelatihan dan akses permodalan bagi UMKM.

4. Memperkuat pembangunan SDM, sains, teknologi, pendidikan, kesehatan, prestasi olahraga, kesetaraan gender, serta penguatan peran perempuan, pemuda (generasi milenial dan generasi Z), dan penyandang disabilitas.
   Menitikberatkan pada pengembangan sumber daya manusia melalui peningkatan kualitas pendidikan, kesehatan, dan akses terhadap teknologi. Pemerintah juga mendorong kesetaraan gender dengan meningkatkan peran perempuan, pemuda, dan penyandang disabilitas dalam berbagai sektor pembangunan.

5. Melanjutkan hilirisasi dan mengembangkan industri berbasis sumber daya alam untuk meningkatkan nilai tambah di dalam negeri.

Pemerintah berfokus pada hilirisasi dan industrialisasi sumber daya alam untuk meningkatkan nilai tambah ekonomi. Langkah ini diharapkan dapat mendorong pertumbuhan ekonomi yang berkelanjutan dan meningkatkan daya saing produk Indonesia di pasar global.

6. Membangun dari desa dan dari bawah untuk pertumbuhan ekonomi, pemerataan ekonomi, dan pemberantasan kemiskinan.
   Pembangunan dimulai dari desa dengan tujuan pemerataan ekonomi dan percepatan pengentasan kemiskinan. Program ini melibatkan peningkatan akses infrastruktur, pendidikan, dan layanan kesehatan di daerah pedesaan.

7. Memperkuat reformasi politik, hukum, dan birokrasi, serta memperkuat pencegahan dan pemberantasan korupsi, narkoba, judi, dan penyelundupan.
   Pemerintah berkomitmen untuk melakukan reformasi di bidang politik, hukum, dan birokrasi guna meningkatkan transparansi dan akuntabilitas. Selain itu, upaya pemberantasan korupsi dan narkoba akan diperkuat melalui penegakan hukum yang tegas dan kolaboratif.

8. Memperkuat penyelarasan kehidupan yang harmonis dengan lingkungan alam dan budaya, serta peningkatan toleransi antarumat beragama untuk mencapai masyarakat yang adil dan makmur.
   Penekanan pentingnya menjaga harmoni antara lingkungan dan budaya, serta mendorong toleransi antarumat beragama. Hal ini bertujuan untuk menciptakan masyarakat yang kolaboratif, toleran, dan berkelanjutan.

Transformasi digital bukanlah sekadar gerakan tanpa arah atau akhir yang jelas. Sebaliknya, konsep ini merupakan proses terstruktur dan strategis yang kini diadopsi secara luas oleh negara-negara di seluruh dunia, termasuk kawasan ASEAN, sebagai respons terhadap dinamika global menuju ekonomi digital yang aman dan berkelanjutan. Komitmen ini tercermin dalam data global yang menunjukkan bahwa lebih dari 170 negara telah menyusun strategi digital nasional masing-masing. Dari jumlah tersebut, sekitar 60 negara telah memperbarui strategi mereka untuk mengakomodasi kemunculan teknologi mutakhir seperti kecerdasan artifisial (AI), *Internet of Things* (IoT), dan *blockchain*. Selain itu, sebanyak 151 negara dan kawasan telah meluncurkan rencana aksi untuk pembangunan hijau (*green development*), yang menunjukkan kesadaran global akan pentingnya transformasi digital yang tidak hanya inovatif, tetapi juga ramah lingkungan dan berkelanjutan.

Di tingkat regional, negara-negara ASEAN juga aktif mengambil peran dalam mendorong agenda transformasi digital melalui kebijakan bersama, penguatan infrastruktur digital, dan kolaborasi lintas batas. Inisiatif ini menunjukkan bahwa transformasi digital tidak hanya bersifat teknologis, tetapi juga menjadi pilar strategis dalam mencapai kemandirian digital, daya saing ekonomi, dan ketahanan sosial kawasan. Beberapa data pendukung terkait adopsi strategi digital global dan kawasan disajikan dalam Tabel 1.3.

Tabel 1.3: Strategi Digital, AI dan Green berbagai Negara

Negara	Strategi Digital	Strategi AI	Strategi Green
Jerman	Digital Strategy 2025: Industry 4.0	National AI Strategy	Climate Action Act 2030
Perancis	International Digital Strategy; Digital Infrastructures and Spatial Planning (2023–2025)	National Strategy for AI Phase II (2021–2025)	National Low Carbon Strategy
Mesir	Egypt Vision 2030	Egypt National Artificial Intelligence Strategy 2025-2030	Integrated Sustainable Energy Strategy (ISES) to 2035
Kenya	ICT Authority Strategic Plan (2024–2027)	National AI Strategy 2025-2030	National Energy Efficiency and Conservation Strategy
Maroko	Morocco Digital 2030	Strategy and National Roadmap for Developing the AI Ecosystem	National Energy Strategy
Afrika Selatan	National Development Plan 2030; Digital and Future Skills Strategy	South Africa AI Policy Framework 2024	Low Emission Development Strategy 2050 (LEDS)
Uni Emirat Arab	The UAE Centennial 2071: Best country in the world (economy, government, society)	Strategy for Artificial Intelligence 2031: World Leader in AI	National Energy Strategy 2050
Arab Saudi	Vision 2030; Smart Government Strategy 2020–2024	National Strategy for Data & AI	Circular Carbon Economy National Program; Saudi Green Initiative (SGI)
China	14th 5-Year Plan and 2035 Long-Range Objectives; China New Infrastructure Plan	AI Strategy	2030 & 2060 Dual Carbon Targets
Thailand	Thailand 4.0; ASEAN Digital Hub	National AI Strategy and Action Plan (2022–2027)	Thailand Integrated Energy Blueprint; Energy 4.0
Malaysia	MyDIGITAL; ASEAN Digital Hub	National Artificial Intelligence Roadmap 2021–2025	National Energy Policy 2022–2040
Singapura	Smart Nation 2025; Digital Economy Framework Action Plan	National AI Strategy 2.0	Singapore Green Plan 2030
Indonesia	Digital Indonesia Roadmap 2021–2024	Indonesia National AI Strategy 2020–2045	Long-Term Strategy for Low Carbon and Climate Resilience 2050

Negara	Strategi Digital	Strategi AI	Strategi Green
Meksiko	National Development Plan for 2019–2024; Universal Internet; Bridging the Digital Divide	National AI Agenda 2030	2020–2024 Energy Sector Program
Brazil	Digital Transformation Strategy (E-Digital) 2022–2026	Artificial Intelligence Strategy 2021	National Energy Plan 2030

Sumber: diolah kembali dari berbagai referensi [26, 27, 28, 29, 30, 31, 32, 33, 34, 35, 36, 37, 38]

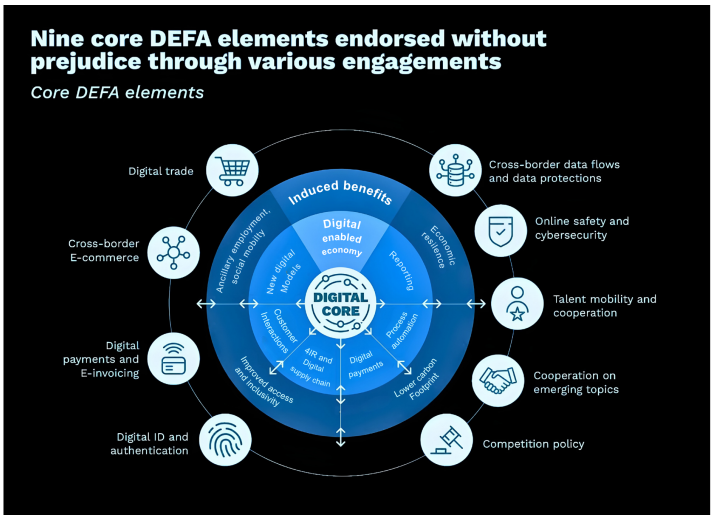
Mengutip data dari berbagai inisiatif *Digital Economy Agreements* (DEA), tercatat lebih dari 60 negara telah berpartisipasi dalam skema kerja sama yang bertujuan memperkuat kerja sama digital lintas negara. Fokus utama dari DEA mencerminkan elemen-elemen krusial dalam ekosistem ekonomi digital masa kini, antara lain pengembangan kecerdasan artifisial yang etis dan bertanggung jawab, produk dan layanan berbasis *data-driven*, sistem identitas digital (*digital ID*), serta interoperabilitas melalui aliran data lintas negara (*cross-border data flow*). Di samping itu, aspek penting seperti perlindungan data pribadi, penguatan sektor keuangan digital berbasis *e-payment* dan *e-invoicing*, keterbukaan informasi pemerintahan (*Open Government Information*), standarisasi sistem perdagangan digital (*Digital Trade Standard System*), serta pemberdayaan UMKM melalui digitalisasi turut menjadi perhatian utama.

Seluruh fokus tersebut tercermin dalam sembilan elemen inti *Digital Economy Framework Agreement* (DEFA) [39, 40, 41] sebagaimana ditampilkan pada Gambar 1.3. Kerangka ini disepakati dalam ASEAN Economic Minister (AEM) Meeting ke-55 dan secara resmi diluncurkan pada ASEAN Economic Community (AEC) Council ke-23 pada 21 Oktober 2023. DEFA berfungsi sebagai acuan strategis bagi negara anggota, termasuk Indonesia, dalam merumuskan kerangka kepercayaan digital yang menuntut keseimbangan antara inovasi teknologi, kedaulatan data, serta perlindungan hak-hak digital warga negara.

Sebagai inisiatif utama dalam kepemimpinan Indonesia di ASEAN, DEFA diharapkan mampu menggandakan nilai ekonomi digital kawasan menjadi 2 triliun USD pada tahun 2030, meningkat dari perkiraan sebelumnya sekitar 1 triliun USD tanpa adanya perjanjian tersebut. DEFA tidak hanya berfokus pada aspek teknis dan regulasi, tetapi juga pada pengembangan talenta digital, standar keamanan siber, *reskilling* dan *retraining* tenaga kerja, infrastruktur, serta interoperabilitas sistem.

Kerangka kerja DEFA memegang relevansi yang sangat tinggi bagi Indonesia, khususnya sebagai landasan dalam merancang arsitektur strategi nasional, termasuk penyusunan kerangka kerja kepercayaan digital yang komprehensif. Sebagai ekonomi digital terbesar di kawasan, Indonesia dapat memanfaatkan DEFA sebagai panduan normatif untuk menyeimbangkan dua kepentingan vital: mendorong inovasi teknologi yang disruptif dan, pada saat yang sama, mempertahankan kedaulatan data serta perlindungan hak digital warganya secara ketat. Melalui kesepakatan ini,

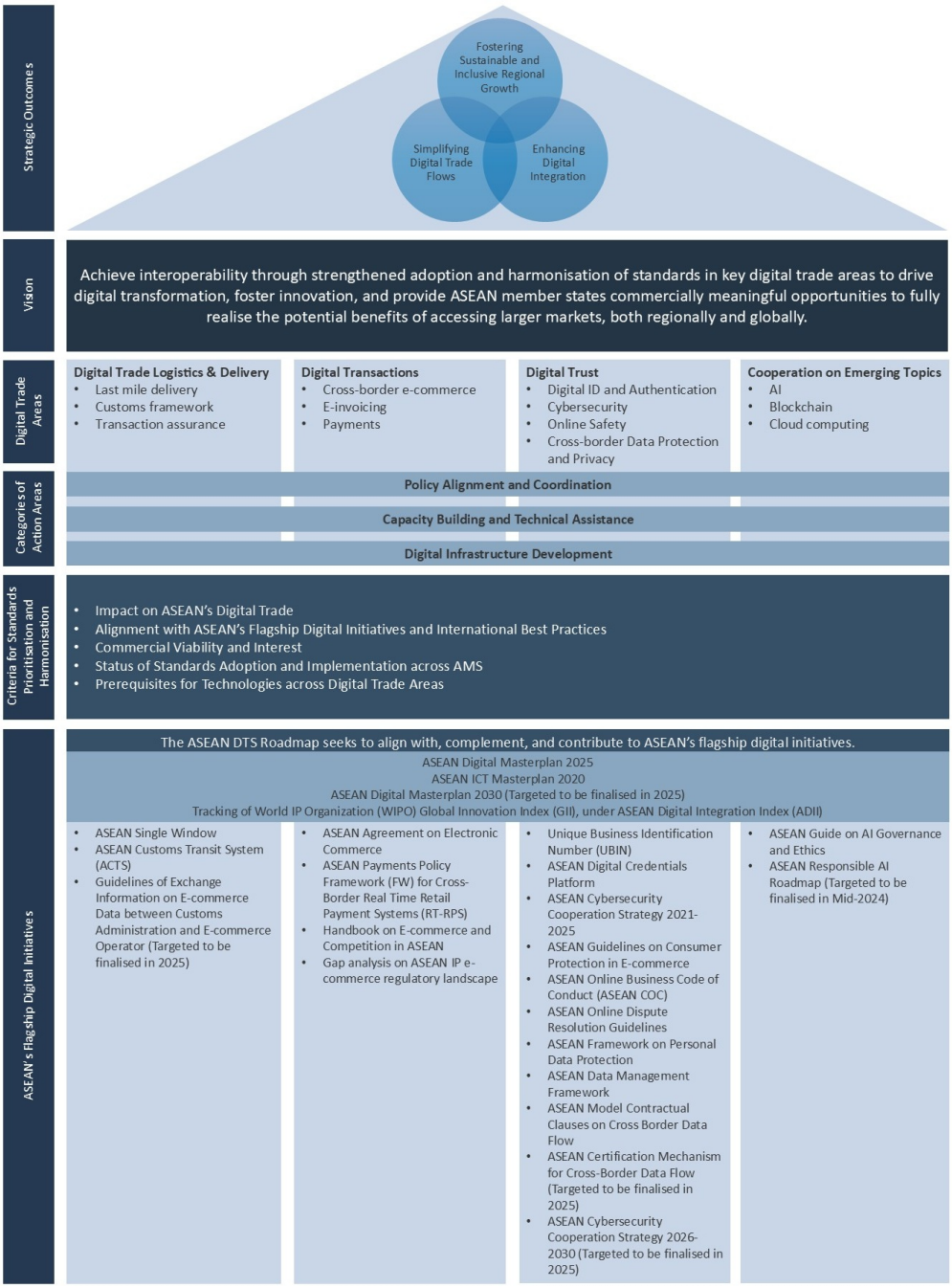
Indonesia tidak hanya menyelaraskan regulasi dan infrastruktur digitalnya dengan standar regional, tetapi juga menghilangkan hambatan non-tarif dalam perdagangan lintas batas. Langkah harmonisasi ini krusial untuk memperkuat posisi Indonesia sebagai pusat pertumbuhan ekonomi digital di Asia Tenggara, sekaligus memberikan kepastian hukum bagi investor dan pelaku industri.



Gambar 1.3: DEFA 9 Core [42]

Dalam konteks regional, menjadikan DEFA sebagai acuan utama memungkinkan Indonesia dan negara-negara ASEAN lainnya untuk mengakselerasi laju transformasi digital secara kolektif. Kerangka ini dirancang untuk memupuk ekosistem digital yang kolaboratif, di mana interoperabilitas sistem dan aliran data lintas batas yang tepercaya (*Data Free Flow with Trust*) menjadi pilar utamanya. Hal ini esensial demi mewujudkan kepercayaan digital yang kokoh, yang merupakan mata uang utama dalam ekonomi masa depan. Lebih jauh lagi, DEFA menawarkan mekanisme fleksibilitas yang mengakomodasi beragam tingkat kesiapan digital di antara negara-negara anggota. Pendekatan yang inklusif ini memungkinkan ASEAN untuk mengatasi kesenjangan digital antarnegara secara efektif, sembari tetap responsif dalam menyikapi perkembangan teknologi yang sangat dinamis dan cepat berubah, seperti kecerdasan buatan dan komputasi awan.

Sebagai tindak lanjut operasional dari sembilan elemen inti yang telah disepakati dalam DEFA, yang mencakup aspek krusial seperti perdagangan digital, pembayaran elektronik, hingga keamanan siber, diperlukan sebuah panduan teknis untuk memastikan implementasi yang terukur. Oleh karena itu, langkah strategis selanjutnya adalah merumuskan kerangka kerja yang lebih terperinci guna menerjemahkan prinsip-prinsip DEFA ke dalam praktik standar perdagangan yang seragam. Kerangka strategis ini diformalkan dalam *ASEAN Digital Trade Standards Roadmap* (lihat Gambar 1.4), yang berfungsi sebagai peta jalan teknis untuk harmonisasi standar, penilaian kesesuaian, dan regulasi teknis di seluruh kawasan.



Gambar 1.4: *Digital Trade Standards*
Sumber: diolah dari berbagai sumber [43, 44, 45]

Dalam dokumen "*ASEAN Digital Trade Standards Roadmap*", kepercayaan digital diidentifikasi sebagai salah satu pilar utama yang harus dibangun untuk mewujudkan visi bersama ekonomi digital ASEAN. Kepercayaan digital dalam konteks ini menjadi landasan yang menjamin keamanan, transparansi, dan integritas dalam transaksi digital lintas batas. Visi tersebut dijabarkan sebagai berikut:

> *Achieve interoperability through strengthened adoption and harmonisation of standards in key digital trade areas to drive digital transformation, foster innovation, and provide ASEAN member states commercially meaningful opportunities to fully realise the potential benefits of accessing larger markets, both regionally and globally.*

Visi bersama ASEAN tersebut mencerminkan bagaimana kawasan dapat mencapai interoperabilitas melalui adopsi serta harmonisasi standar pada sektor-sektor kunci, kesiapan menghadapi ancaman *emerging threat*, pembangunan infrastruktur digital yang andal, serta pengembangan langkah strategis terkait keamanan siber. Dengan demikian, negara-negara anggota ASEAN dapat mengambil peluang sekaligus mengoptimalkan pembangunan ekonomi digital mereka [46]. Lebih jauh lagi, dokumen ini menegaskan bahwa kepercayaan digital tidak hanya menjadi isu ekonomi digital nasional semata, melainkan telah meluas menjadi kepercayaan lintas batas, baik di tingkat kawasan maupun global.

Sebagai anggota ASEAN, Indonesia perlu menerapkan prinsip kepercayaan digital sebagai bagian integral dari standar digital yang diadopsi di kawasan ini. Pilar-pilar lain beserta elemen pendukungnya juga harus terus dikembangkan secara paralel untuk memastikan ekosistem digital yang kokoh dan berkelanjutan. Meskipun *roadmap* ini belum dirinci hingga ke level aktivitas operasional maupun tonggak capaian (*milestones*), kerangka besar yang disajikan dapat dijadikan panduan strategis bagi perencanaan dan pelaksanaan program nasional ke depan.

1.4 Meningkatnya Kebutuhan Akan Kepercayaan Digital

Dalam berbagai aktivitas sehari-hari, masih banyak bentuk interaksi yang belum sepenuhnya terintegrasi dengan teknologi digital. Contohnya dapat ditemukan saat seseorang berbelanja di pasar, di mana pembeli cenderung melihat langsung siapa penjualnya, menilai kondisi barang secara fisik, dan bahkan mencoba produk seperti pakaian atau sepatu sebelum memutuskan untuk membeli. Informasi yang disampaikan, termasuk melalui media video sekalipun, belum sepenuhnya mampu menggantikan pengalaman langsung tersebut. Di sisi lain, penjual pun melakukan penilaian terhadap pembeli, seperti memastikan bahwa uang yang digunakan bukanlah uang palsu atau kartu kredit yang diberikan memang sah. Interaksi semacam ini mencerminkan pentingnya kepercayaan terhadap identitas dalam transaksi. Ketika transaksi melibatkan pelaku usaha dan konsumen, situasi

ini dikategorikan sebagai interaksi *Business-to-Customer* (B2C), sedangkan bila kedua pihak merupakan individu, maka disebut sebagai *Customer-to-Customer* (C2C).

Calon pembeli umumnya memperhatikan reputasi atau citra dari penjual maupun penyedia jasa [47, 48]. Reputasi yang baik mencerminkan tingkat kepercayaan yang tinggi terhadap layanan yang ditawarkan. Penilaian ini sering kali dibentuk dari pengalaman dan ulasan pembeli lainnya, yang dalam praktiknya memiliki pengaruh lebih kuat dibandingkan dengan iklan konvensional. Meski demikian, kredibilitas ulasan sangat bergantung pada kejelasan identitas pihak yang memberikan pendapat. Oleh karena itu, validitas identitas digital menjadi aspek fundamental dalam membangun kepercayaan. Dalam konteks transaksi antarperusahaan, validasi identitas dilakukan melalui pertukaran dokumen resmi seperti *Non-Disclosure Agreement* (NDA), perjanjian kerja sama (PKS), dan dokumen hukum lainnya. Tujuan utama dari proses ini adalah membangun landasan kepercayaan untuk menjalankan kerja sama yang bersifat *Business-to-Business* (B2B). Proses verifikasi identitas juga terjadi dalam layanan publik. Saat seseorang membuka rekening di bank, diperlukan dokumen identitas seperti Kartu Tanda Penduduk (KTP) atau Kartu Keluarga. Layanan identitas kependudukan yang disediakan pemerintah merupakan bentuk interaksi *Government-to-Citizen* (G2C), di mana lembaga perbankan menempatkan kepercayaan pada sistem identitas yang dikelola negara.

Meskipun contoh-contoh di atas terjadi dalam dunia fisik, prinsip serupa juga berlaku di ruang digital. Saat mengakses situs web, pengguna perlu memastikan keabsahan halaman tersebut. Ketika mengakses layanan perbankan digital, pengguna harus yakin bahwa halaman tersebut benar-benar milik institusi perbankan yang sah, bukan situs palsu atau *phishing*. Sebaliknya, penyedia layanan juga harus memastikan bahwa pengguna benar-benar merupakan pemilik akun yang sah. Kepercayaan tetap menjadi unsur utama dalam menjaga integritas interaksi digital.

Namun, tantangan muncul karena di ruang digital, identitas fisik tidak mudah diverifikasi. Seseorang dapat dengan mudah menyamar, bahkan menggunakan identitas palsu atau menampilkan diri dengan gender yang berbeda. Kondisi ini menimbulkan persoalan mendasar: bagaimana memastikan keaslian identitas di lingkungan digital yang serba anonim? Tanpa adanya sistem verifikasi yang kuat serta infrastruktur kepercayaan digital yang dapat diandalkan, interaksi *online* berisiko kehilangan legitimasi. Akibatnya, proses komunikasi, transaksi, maupun kolaborasi digital tidak hanya menjadi rentan terhadap penipuan dan penyalahgunaan, tetapi juga sulit membangun rasa aman dan saling percaya yang menjadi dasar keberlanjutan ekosistem digital itu sendiri.

Digital trust atau kepercayaan digital dapat dipahami sebagai keyakinan pengguna terhadap keandalan sistem digital, platform, serta transaksi yang terjadi di dalamnya (penjelasan lebih lengkap mengenai konsep ini akan disampaikan pada bab berikutnya). Berbagai aspek utama yang termasuk dalam cakupan kepercayaan digital meliputi:

- Keamanan data dan privasi (misalnya, perlindungan terhadap ancaman siber

dan penipuan).

- Keandalan platform digital (misalnya, *e-commerce*, perbankan *online*, dan layanan pemerintah).
- Kerangka regulasi yang memastikan interaksi digital yang etis dan transparan.

Ancaman di ruang siber terus berkembang seiring dengan semakin canggihnya teknik dan taktik serangan. Indonesia turut mengalami peningkatan baik dari sisi volume maupun kompleksitas insiden, termasuk penipuan *online*, serangan *phishing*, dan kebocoran data. Varian ancaman seperti *ransomware* yang merupakan bentuk penyalahgunaan teknologi kriptografi, hingga risiko penggunaan teknologi *deepfake* yang dapat digunakan untuk memanipulasi opini publik atau bahkan menciptakan identitas sintetis (*synthetic identity fraud*), menjadi tantangan nyata dalam ekosistem digital. Di sisi lain, pemanfaatan kecerdasan artifisial (AI) oleh pihak tidak bertanggung jawab telah melahirkan bentuk-bentuk serangan baru seperti *AI-powered phishing* dan *AI-hacktivism*, serangan ini juga dikenal dengan *AI-driven cyber threat. Ransomware* dan *supply chain attacks*-nya pun juga mulai bervariasi.

Teknologi penyadapan pun mengalami evolusi. Jika sebelumnya hanya dilakukan dengan perangkat sederhana seperti alat perekam atau pemancar radio, kini metode yang digunakan mencakup eksposur satelit dan komunikasi berbasis *Low Earth Orbit (LEO)*, *third-party compromise*, hingga teknik *DNS tunneling.* Ancaman dari dalam (*insider threat*) juga semakin relevan, dipicu oleh kerentanan sosial, konflik nilai, atau rasa ketidakpuasan yang dimiliki individu terhadap institusi, dan dieksploitasi oleh aktor tertentu, termasuk intelijen asing.

Di tengah pesatnya kemajuan teknologi digital, ancaman terhadap keamanan informasi tidak hanya muncul dari celah sistem atau perangkat lunak, tetapi juga dari faktor manusia yang sering kali menjadi titik paling rentan. Serangan yang menargetkan sisi psikologis manusia terbukti lebih sulit diantisipasi karena melibatkan aspek perilaku, kebiasaan, dan emosi yang tidak dapat sepenuhnya dikendalikan oleh sistem keamanan teknis.

Di Indonesia, rendahnya tingkat literasi digital yang belum merata memperlebar peluang bagi pelaku kejahatan siber untuk memanfaatkan kelemahan ini melalui teknik rekayasa sosial (*social engineering*). Teknik ini beroperasi dengan cara mengeksploitasi sifat dasar manusia, seperti rasa percaya, keinginan untuk membantu, atau kecenderungan untuk menghindari konflik, sehingga korban tanpa sadar memberikan informasi sensitif atau melakukan tindakan yang berpotensi membahayakan sistem. Dalam banyak kasus, bukan teknologi yang gagal, melainkan manusia yang berhasil diperdaya untuk membuka jalan bagi serangan.

Dari perspektif tata kelola data (*data governance*), kompleksitas pengelolaan data semakin meningkat dari tahun ke tahun. Hal ini diperburuk oleh tumpang tindih regulasi dan kewenangan antarlembaga, serta terus munculnya kebijakan baru yang belum sepenuhnya sinkron. Akibatnya, upaya membangun kepatuhan sebagai landasan kepercayaan digital menjadi bias, karena banyak pelaku tidak memiliki

kejelasan arah terhadap aturan yang berlaku. Di sisi lain, isu etika dalam ruang digital juga masih menjadi perdebatan. Etika tidak semata-mata didasarkan pada regulasi formal, tetapi juga pada nilai moral pribadi dan konsensus moral kolektif. Tanpa batasan yang jelas, kebebasan berpendapat di ruang digital berisiko berkembang menjadi penyebaran ujaran kebencian, yang justru dapat menghambat kematangan ekosistem digital dalam masyarakat yang berkembang.

Pada tataran yang lebih luas, serangan yang didukung oleh negara (*state-sponsored attacks*) telah berkembang menjadi ancaman strategis yang signifikan dalam ekosistem keamanan siber global. Berbagai insiden yang melibatkan negara-negara seperti Iran dan Israel, Rusia dan Ukraina, serta Tiongkok dan Amerika Serikat, memperlihatkan bahwa operasi siber terorganisir bukan lagi sekadar hipotesis, melainkan kenyataan yang terus berlangsung dan semakin kompleks. Serangan-serangan tersebut tidak hanya berorientasi pada aktivitas spionase untuk memperoleh informasi strategis, tetapi juga mencakup upaya sabotase terhadap infrastruktur digital yang kritis serta manipulasi ruang informasi guna membentuk opini publik atau melemahkan legitimasi politik lawan. Dengan demikian, dimensi keamanan siber kini tidak dapat lagi dipisahkan dari dinamika pertahanan nasional dan hubungan internasional, karena telah menjadi instrumen baru dalam kompetisi kekuatan antarnegara di era digital.

Berbagai bentuk ancaman tersebut menegaskan urgensi pembentukan kerangka kerja kepercayaan digital yang kokoh. Dalam ekosistem digital yang terus berkembang, membangun kepercayaan bukan hanya soal perlindungan teknis, tetapi juga menyangkut dimensi sosial, hukum, dan etika. Kepercayaan digital menjadi landasan utama untuk memastikan bahwa pertumbuhan ekonomi digital Indonesia berlangsung secara aman, kolaboratif, merata, dan berkelanjutan.

1.5 Standar Utama untuk Aplikasi Digital

Kebutuhan akan kepercayaan digital telah mendorong lahirnya berbagai standar internasional yang mencakup aspek-aspek seperti *digital life*, *digital finance*, *emerging topics*, *digital infrastructure*, hingga keamanan siber (lihat Tabel 1.4). Indonesia secara aktif merespons perkembangan ini dengan mentransformasi standar-standar global tersebut ke dalam bentuk Standar Nasional Indonesia (SNI) yang lebih kontekstual dan bermuatan lokal. Beberapa standar yang telah diadopsi dan disesuaikan antara lain ISO/IEC 27001 yang diterbitkan sebagai SNI ISO/IEC 27001:2013 dan diperbarui menjadi SNI ISO/IEC 27001:2022. Kontrol terhadap Keamanan Informasi diatur dalam SNI ISO/IEC 27002:2022. Selain itu, ISO/IEC 38500 tentang tata kelola teknologi informasi telah diadopsi dalam SNI ISO/IEC 38500:2016, dan telah diperbaharui menjadi SNI ISO/IEC 38500:2024. Terkait tata kelola pusat data juga diatur melalui SNI 8799 (*family*), sedangkan kerangka kerja perlindungan privasi ISO/IEC 29100 telah diadopsi menjadi SNI ISO/IEC 29100:2024 yang menggantikan SNI 8545:2018.

Tabel 1.4: Standar dan *Framework* Digital

Bidang	**Sub Bidang**	**Standar dan *Framework***
Aplikasi Digital - *Digital Life*	AR/VR	ISO/IEC 18038:2020, ISO/IEC 18039:2019, IEEE P2048, IEEE P3141
	IoT	SNI ISO/IEC 30162:2022, SNI ISO/IEC 30147:2021, SNI ISO/IEC 21823-1:2019, SNI ISO/IEC TR 22417:2017, ETSI SR 003 680, ETSI EN 303 645, OWASP IoT Verification Standard
	Biometrics	SNI 9236:2023, SNI ISO/IEC 19794-2,6,13:2011, ISO/IEC JTC 1 SC 37 (Series)
	Healthcare	SNI ISO/IEC 14971, SNI ISO/IEC 62443, ISO 62304
Aplikasi Digital - *Digital Finance*	*Interchange Messaging*	SNI ISO 8583, ISO 20022
	Information Security	PCI DSS, PCI SSF
	Digital Payments	EMV QR
	Economic Development Support	*Open Digital Architecture* (ODA)
Emerging Topics	AI/ML/RPA	SNI ISO/IEC 23053:2022, SNI ISO/IEC 38507:2022, ISO/IEC TR 24028:2020, ISO/IEC JTC 1/SC 42, ISO/IEC 42001:2023
	Big Data	SNI ISO/IEC 20546:2019, SNI ISO/IEC TR 20547:2020, IEEE BDGMM
	Blockchain	SNI ISO 23257:2022, ITU-T SG16 Q22, ITU-T F.751.1/2/6/7/19/21, ITU-T Y.4560
	Distributed Computing	SNI ISO/IEC 22989:2022, ISO/IEC TR 23188:2020, ISO/IEC JTC 1/SC 38
Digital Infrastructure	*Mobile Network*	3GPP Release 15–19, GSMA Mobile CKB, 3GPP TS 33.813
	Wireless Equipment	ITU-T SG17 X.5G Sec Guide, NESAS, SCAS
	Cloud Service	SNI ISO/IEC 27017/27034/19790, CSA CCM, SOC 1/2/3, PCI DSS
	Fixed Network	SNI ISO/IEC 15408, CCRA
	Data Center	SNI 8799-1-3, ISO/IEC 22237
Strategic Construction	—	SNI ISO/IEC 38505-1:2017, *Gartner Data Security Governance Framework*
Cybersecurity Management	—	SNI ISO/IEC 27001/27002, SNI ISO/IEC 27011/27005/27014/27015, SNI ISO/IEC 38500, ISO/TC 309
Personal Privacy/Information	—	SNI ISO/IEC 27701

1.6 Ikhtisar Kebijakan Indonesia

Sejalan dengan perkembangan ASEAN Digital Trade Standards, yang mencerminkan transformasi besar-besaran dalam lanskap digital kawasan, Indonesia turut mengintegrasikan visi transformasi digital ini ke dalam arah kebijakan pemerintah Presiden Prabowo Subianto. Visi tersebut tercermin dalam Asta Cita ketiga mengenai pembangunan infrastruktur yang dapat diartikan termasuk juga infrastruktur digital, serta Asta Cita keenam yang menekankan pada pemerataan dan peningkatan akses infrastruktur. Komitmen terhadap transformasi digital juga terlihat dari peluncuran Visi Indonesia Digital 2045 pada 13 Desember 2023 sebagai peta jalan menuju Indonesia Emas 2045 oleh Kementerian Komunikasi dan Informatika (Kemenkominfo) yang sekarang bertransformasi menjadi Kementerian Komunikasi dan Digital (Kemkomdigi). Visi ini menekankan pembangunan ekosistem digital yang kolaboratif, didukung oleh inovasi teknologi, pemerintahan berbasis digital, serta masyarakat yang cerdas. Keselarasan ini memperkuat keterkaitan Indonesia dengan kerangka kerja digital ASEAN yang mendorong pertumbuhan ekonomi digital untuk kemaslahatan umum, tidak hanya nasional, namun juga berdampak secara regional hingga global.

Namun, Indonesia juga dihadapkan pada paradoks regulasi: peraturan yang terlalu longgar memang dapat mempercepat pertumbuhan ekonomi digital, tetapi juga meningkatkan kerentanan terhadap serangan siber [49]. Dalam menghadapi tantangan ini, Badan Siber dan Sandi Negara (BSSN) memainkan peran sentral sebagai lembaga yang bertanggung jawab atas keamanan ruang siber nasional. Melalui pendekatan yang terstruktur dan adaptif, BSSN merumuskan dua kebijakan strategis utama: *Strategi Keamanan Siber Nasional* (SKSN) dan *Rencana Aksi Nasional Keamanan Siber* (RAN-KS) [50]. SKSN menekankan pelindungan infrastruktur informasi vital, peningkatan kapasitas nasional, penegakan hukum siber, serta kemitraan internasional, sementara RAN-KS berfungsi sebagai dokumen operasional yang memuat implementasi kebijakan, peningkatan SDM, pembentukan *Computer Security Incident Response Team* (CSIRT) nasional, harmonisasi kebijakan, hingga audit tata kelola sistem elektronik.

Selain itu, kerangka regulasi Indonesia telah diperkuat oleh berbagai instrumen hukum sebagaimana diuraikan dalam Bab 4. Beberapa regulasi utama mencakup Undang-Undang (UU) ITE beserta revisinya, UU PDP (2022) yang mengukuhkan perlindungan hak digital warga negara, serta UU RPJPN 2025–2045 yang menempatkan transformasi digital sebagai pilar pembangunan jangka panjang. Pada tataran kebijakan operasional, hadir Peraturan Presiden (Perpres) SPBE (No. 95/2018) yang mengakselerasi digitalisasi pemerintahan, Perpres No. 82/2022 tentang Pelindungan Infrastruktur Informasi Vital, serta Perpres No. 82/2023 mengenai Percepatan Transformasi Digital dan Keterpaduan Layanan Digital Nasional. Kebijakan tersebut dilengkapi dengan inisiatif strategis lain seperti pembangunan *Digital Public Infrastructure* (identitas digital, pertukaran data, dan sistem pembayaran digital), Gerakan Literasi Digital Nasional, serta digitalisasi pengadaan barang/jasa pemerintah melalui Perpres No. 17/2023.

Dengan kerangka regulasi yang semakin komprehensif, arah kebijakan Indonesia tidak hanya fokus pada aspek pertumbuhan ekonomi digital, tetapi juga menekankan keamanan, kepercayaan publik, serta tata kelola digital yang transparan dan akuntabel. Sinergi antara visi politik, regulasi strategis, serta implementasi teknis tersebut memperlihatkan keseriusan Indonesia dalam membangun ekosistem digital yang aman, kolaboratif, menyeluruh, dan berdaya saing global.

2

Definisi Kepercayaan Digital

> Digital trust is built at the intersection of privacy, security, ethics, and resilience.
>
> — Deloitte Insights

Kepercayaan digital (*digital trust*) dalam menghadapi dinamika transformasi digital yang kian pesat semakin menjadi bahasan dan fokus kunci. Kepercayaan digital menjadi elemen penting dalam menciptakan ekosistem digital yang aman, kolaboratif, dan berkelanjutan, seiring dengan meningkatnya interaksi *online*, pertukaran data, serta penggunaan layanan digital di berbagai sektor kehidupan.

Uraian pada bagian ini dimulai dari pemahaman dasar secara umum hingga ke ranah penerapannya dalam konteks digital. Tujuannya adalah membangun dasar konseptual untuk perumusan kerangka kerja kepercayaan digital pada tingkat nasional. Untuk mencapai tujuan tersebut, pembahasan dimulai dengan penelusuran konsep kepercayaan secara umum sebelum beranjak pada dimensi digitalnya. Dengan kata lain, bahasan diawali dengan eksplorasi kepercayaan sebagai konstruksi sosial, bagaimana kepercayaan terbentuk, dipertahankan, dan berperan dalam interaksi antarindividu maupun institusi dalam masyarakat. Dalam kerangka sosiologis, kepercayaan tidak hanya berfungsi sebagai dasar dari hubungan sosial, tetapi juga sebagai mekanisme yang memungkinkan kolaborasi, pengambilan keputusan kolektif, serta legitimasi terhadap otoritas. Pemahaman mengenai kepercayaan sebagai konstruksi sosial memberikan landasan penting untuk melihat bagaimana nilai dan mekanisme kepercayaan mengalami transformasi ketika dimediasi oleh teknologi digital.

Setelah memahami kepercayaan dalam konteks sosial dan relasi antarindividu, pembahasan kemudian beralih ke bagaimana kemajuan teknologi mengubah bentuk dan mekanisme kepercayaan itu sendiri. Seiring dengan berkembangnya teknologi informasi dan komunikasi, dinamika kepercayaan juga mengalami perubahan mendasar, khususnya bagaimana perkembangan teknologi informasi dan komunikasi mengubah bentuk dan mekanisme kepercayaan itu sendiri.

Di era digital, relasi kepercayaan tidak lagi dibangun hanya melalui tatap muka, melainkan melalui sistem, platform, dan protokol yang bekerja secara otomatis dan tersimpan di balik antarmuka pengguna. Perubahan ini menandai pergeseran penting dari kepercayaan yang bersifat personal menuju kepercayaan terhadap sistem dan infrastruktur digital, yang kemudian melahirkan bentuk baru yang dikenal sebagai kepercayaan digital.

Untuk memahami fenomena ini secara utuh, diperlukan integrasi antara perspektif sosial dan teknologis. Gabungan dari dua pendekatan ini, baik sosiologis maupun teknologis, membuka jalan bagi pemahaman tentang kepercayaan digital, yakni bentuk kepercayaan yang muncul dalam ekosistem digital, di mana entitas yang saling berinteraksi dapat berupa manusia, perangkat, algoritma, atau institusi. Pemahaman konseptual ini menjadi dasar penting sebelum melangkah pada aspek metodologis dalam membangun kerangka kerja kepercayaan digital nasional.

Setelah memahami dasar konseptual kepercayaan dan kepercayaan digital dari berbagai perspektif, bab ini menguraikan metodologi pengembangan kerangka kerja kepercayaan digital nasional, yang mencakup tinjauan literatur, kajian regulasi nasional, analisis konseptual berbasis pendekatan 5W1H (*Where, Why, What, Who, When, How*), serta validasi melalui penilaian pakar dan praktisi. Metodologi ini memberikan landasan sistematis bagi perumusan kerangka kerja yang sesuai dengan kebutuhan Indonesia sekaligus selaras dengan praktik terbaik internasional. Dengan demikian, bab ini membentuk jembatan antara landasan teoritis dan pendekatan praktis dalam pengembangan kepercayaan digital di Indonesia.

2.1 Kepercayaan

Saat ini, kita tengah berada pada masa krusial dalam pengembangan ekonomi digital, di mana perlu dilakukan refleksi mendalam mengenai bagaimana dan di mana data pribadi digunakan, serta siapa yang berhak memperoleh keuntungan komersial dari wawasan yang dihasilkan oleh data digital pengguna. Situasi ini menuntut organisasi untuk mengevaluasi kembali komitmennya terhadap *kepercayaan digital* (*digital trust*), sebuah konsep menyeluruh yang mencakup prinsip perilaku dan nilai budaya terkait privasi data, keamanan, perlindungan, dan tata kelola yang etis [51, 52].

Di era ketika pola pikir dan perilaku digital terus berkembang, batas-batas tanggung jawab terhadap privasi menjadi semakin kabur. Hal ini turut membentuk ulang ekspektasi masyarakat terhadap bagaimana data mereka seharusnya dilindungi [53, 54]. Akibatnya, organisasi dihadapkan pada tantangan besar dalam menyesuaikan

budaya internal agar sejalan dengan upaya membangun dan menjaga kepercayaan digital secara berkelanjutan.

Sebelum membahas lebih jauh mengenai kepercayaan digital, penting untuk memahami terlebih dahulu konsep dasar dari *kepercayaan* (*trust*) itu sendiri. Hingga kini, belum terdapat satu definisi baku atau otoritatif yang secara universal digunakan untuk mendefinisikan kepercayaan. Berbagai studi menunjukkan bahwa kepercayaan merupakan konsep multidimensi yang mencakup aspek kognitif, afektif, dan kontekstual [55]. Secara umum, kepercayaan dapat dipahami sebagai landasan utama dalam berbagai bentuk interaksi, baik antarindividu maupun antarorganisasi, dalam konteks pribadi maupun profesional. Dalam lingkungan bisnis, kepercayaan sering kali didasarkan pada keyakinan bahwa pihak lain akan bertindak secara konsisten, dapat diprediksi, dan sesuai dengan norma yang disepakati bersama [54, 56].

Pada tahun 1950-an, Deutsch [57] memulai penelitian mengenai kepercayaan dalam ranah psikologi sosial. Sejak saat itu, topik kepercayaan menarik perhatian para ilmuwan dari berbagai disiplin ilmu. Meskipun banyak bidang studi yang meneliti "kepercayaan", belum ada definisi tunggal yang disepakati secara universal. Para peneliti mendefinisikan kepercayaan secara berbeda tergantung pada bidang kajian dan perspektif penelitian masing-masing, baik dari sisi kognitif, emosional, maupun perilaku. Mereka menekankan bahwa dasar pengembangan kepercayaan adalah proses kognitif yang membedakan individu dan institusi sebagai pihak yang layak dipercaya.

McKnight mendefinisikan kepercayaan sebagai "keyakinan terhadap pihak lain" (*trusting beliefs*) pada tahun 1998 [58], yaitu kondisi di mana seseorang meyakini bahwa pihak lain bersifat baik, cakap, jujur, atau dapat diprediksi dalam konteks tertentu. Definisi tersebut didasarkan pada nilai-nilai kepercayaan yang telah diteliti sebelumnya, yaitu karakteristik dan atribut dari pihak yang dipercaya (*trustee*), seperti kemampuan, niat baik (*goodwill*), dan integritas. Unsur integritas mencakup dua aspek: keadilan dan konsistensi. McKnight mengkonseptualisasikan integritas sebagai dua struktur yang dapat dibedakan: pikiran yang jujur dan pikiran yang dapat diprediksi. Dalam model yang dikembangkan oleh Kim dan Tadisina [59], konsep prediktabilitas ini dimasukkan dalam kategori sikap kognitif karena mengandung proses psikologis yang terfokus, yang lebih dekat dengan struktur sikap kognitif. Kejujuran dan niat baik dianggap serupa dengan *goodwill* dalam model tersebut dan menjadi salah satu komponen dari keyakinan terhadap pihak lain. Sementara itu, kompetensi disamakan dengan daya saing (*competitiveness*) dalam model tersebut dan membentuk komponen lainnya dalam keyakinan terhadap pihak lain.

Salah satu dimensi dari sikap kepercayaan adalah keyakinan atau kepercayaan diri (*confidence*). Konsep lain, seperti ketergantungan (*dependence*) juga sering kali diasosiasikan dengan kepercayaan diri dalam pengukuran. Kepercayaan diri mencerminkan kondisi psikologis seseorang dalam membuat keputusan untuk mempercayai pihak lain. Tingkat kepercayaan ini umumnya memerlukan waktu dan interaksi untuk memastikan kemampuan serta niat dari pihak yang dipercayai. Dimensi lain

dari kepercayaan adalah kecenderungan suka (*liking tendency*), dan banyak peneliti telah mengonfirmasi bahwa bentuk kepercayaan berbasis emosi ini merupakan salah satu dimensi dari sikap kepercayaan. Isi emosional dari kepercayaan didasarkan pada keterikatan emosional, dan emosi yang kuat, seperti rasa suka, merupakan bagian dari kepercayaan yang berlandaskan emosi. Oleh karena itu, sikap kepercayaan mencakup dua bentuk utama: kepercayaan berbasis keyakinan (*confidence trust*) dan kepercayaan emosional (*emotional trust*). Kepercayaan emosional ini juga mencakup aspek emosi dan keyakinan [60].

Dalam konteks intensi untuk mempercayai, Zand [61] menegaskan bahwa perilaku kepercayaan membuat pihak yang mempercayai (*trustor*) berada dalam posisi rentan karena harus menghadapi risiko dalam hubungan dengan orang lain. Pandangan ini sejalan dengan Moorman dkk. [62] yang memandang kepercayaan sebagai kemauan untuk bergantung pada mitra pertukaran yang dianggap layak dipercaya. Dengan demikian, kepercayaan memperoleh makna khusus dalam situasi yang penuh ketidakpastian dan potensi kerugian, sehingga aspek intensi menjadi elemen penting dalam definisi kepercayaan [60].

Selanjutnya, Deutsch [57] menambahkan bahwa kepercayaan mencakup keyakinan individu terhadap niat dan kemampuan mitra afiliasi, serta ekspektasi bahwa mitra tersebut akan bertindak sesuai dengan harapan. Dengan kata lain, kepercayaan tidak hanya terkait dengan kerentanan dan kesediaan untuk mengambil risiko, tetapi juga dengan keyakinan positif bahwa pihak lain akan memenuhi komitmennya.

Fishbein dan Ajzen [63] mengusulkan kerangka teoritis mengenai kepercayaan melalui pendekatan tiga perspektif berdasarkan teori aksi beralasan (*reasoned action*) dan perilaku terencana (*planned behavior*). Kerangka ini terdiri atas tiga komponen: keyakinan (*belief*), sikap (*attitude*), dan niat (*intention*). Keyakinan mencerminkan proses psikologis sederhana dalam menilai karakteristik dan atribut pihak lain, seperti perasaan atau pendapat seseorang terhadap sesuatu. Sikap mencerminkan kesiapan untuk memberikan perhatian atau bertindak, sementara niat adalah kemungkinan aktif bahwa seseorang akan melakukan atau menjalankan tindakan tertentu.

Mengacu pada logika Fishbein dan Ajzen, McKnight dkk. [58] berpendapat bahwa *trusting beliefs* dan *trusting intentions* dapat mewakili dua aspek utama dari kepercayaan. Berdasarkan hal ini, Yang [60] menambahkan dimensi *trusting attitudes* dan mendefinisikan kepercayaan sebagai terdiri atas tiga aspek: keyakinan, sikap, dan niat. Selain itu, Lewis dan Weigert [64] menyarankan bahwa kepercayaan dapat dijelaskan melalui tiga proses yang dapat dibedakan secara konseptual.

Kepercayaan juga diyakini merupakan konstruksi sosial yang dipengaruhi secara signifikan oleh latar belakang budaya dan kondisi sosial masyarakatnya. Ferrin dan Gillespie [65] menegaskan bahwa tingkat dan bentuk kepercayaan dapat berbeda secara signifikan antarbudaya, tergantung pada nilai, norma, dan praktik sosial yang dianut. Misalnya, dalam budaya yang lebih individualistik, kepercayaan sering dibangun berdasarkan kalkulasi risiko dan kemampuan, sementara dalam budaya kolektivistik, kepercayaan lebih banyak didasarkan pada hubungan interpersonal jangka panjang dan norma sosial yang mengatur loyalitas kelompok. Perbedaan ini

juga dipengaruhi oleh dimensi budaya, seperti jarak kekuasaan, tingkat ketidakpastian yang dapat diterima, dan pola komunikasi. Dalam konteks sosial yang lebih luas, dinamika seperti struktur kekuasaan, sejarah sosial, dan interaksi sosial juga dapat mengubah cara kepercayaan terbentuk dan berkembang. Hal ini sangat penting ketika diterapkan pada konteks digital, di mana interaksi lintas budaya dan sosial semakin meluas, dan kepercayaan digital harus mempertimbangkan variabilitas budaya serta norma sosial yang beragam.

Dalam konteks penelitian ini, fokus utama adalah pada kepercayaan publik, yakni bentuk kepercayaan yang diberikan oleh warga negara terhadap institusi pemerintahan dan aparatur negara. Menurut Bank Dunia (2010) [66], kepercayaan publik mencerminkan sejauh mana masyarakat menilai legitimasi pemerintah dalam menjalankan wewenangnya, membuat dan menegakkan kebijakan, serta memenuhi komitmen kepada warga negara. Dengan kata lain, kepercayaan publik merupakan sikap atau keyakinan masyarakat terhadap integritas, kapabilitas, dan akuntabilitas pemerintah dalam menjalankan fungsinya. Agar kepercayaan dapat terbentuk, terdapat sejumlah elemen penting yang harus tersedia:

- Kehadiran dua aktor, yaitu pemberi kepercayaan (*trustor*) dan pihak yang dipercaya (*trustee*);
- Adanya unsur kerentanan, di mana kepercayaan muncul dalam situasi yang penuh ketidakpastian;
- Kepercayaan diwujudkan melalui tindakan nyata yang mengandung risiko;
- Kepercayaan bersifat sangat subjektif, bergantung pada individu, konteks, dan lingkungan.

Perlu dicermati bahwa prinsip-prinsip dan tantangan yang telah dibahas sebelumnya tetap relevan dalam konteks lingkungan digital. Transformasi menuju dunia digital tidak menghapus kompleksitas yang ada, melainkan menghadirkannya dalam bentuk baru yang menuntut pendekatan yang berbeda. Oleh karena itu, pemahaman terhadap dinamika dan karakteristik lingkungan digital menjadi penting untuk memastikan keberlangsungan dan keamanan berbagai aktivitas di dalamnya. Pembahasan yang lebih rinci mengenai aspek-aspek spesifik dari ekosistem digital akan diuraikan pada bagian selanjutnya.

Dalam hal kerentanan, internet sering dipandang sebagai ruang yang sarat dengan ketidakpastian dan potensi risiko. Keterbukaan, interkonektivitas, dan anonimitas yang menjadi ciri utama dunia digital, di satu sisi, memperluas peluang interaksi, namun, di sisi lain, meningkatkan eksposur terhadap ancaman keamanan dan penyalahgunaan data. Dalam situasi ini, kepercayaan digital menjadi faktor penentu dalam keberlangsungan interaksi *online*.

Sebagai ilustrasi, seorang konsumen yang melakukan transaksi melalui platform perdagangan elektronik harus menyerahkan berbagai informasi sensitif, seperti data pribadi dan rincian kartu kredit. Tindakan tersebut secara inheren mengandung risiko, sehingga keputusan untuk melanjutkan transaksi bergantung pada tingkat

kepercayaan terhadap penyedia layanan maupun sistem keamanan yang diterapkan. Apabila muncul keraguan terhadap kredibilitas platform atau jaminan perlindungan data, konsumen cenderung membatalkan transaksi sebagai bentuk perlindungan diri.

Oleh karena itu, penyedia layanan digital dituntut untuk membangun dan memelihara kepercayaan pengguna melalui penerapan prinsip transparansi, keamanan, dan akuntabilitas. Upaya menjaga kepercayaan ini tidak hanya bersifat teknis, melainkan juga mencakup aspek etis dan institusional. Keberhasilan dalam menciptakan rasa aman dan keyakinan pada pengguna merupakan prasyarat utama dalam membangun ekosistem digital yang andal, berkelanjutan, dan berorientasi pada kepentingan publik.

2.2 Kepercayaan Digital

Sebagaimana telah dibahas sebelumnya, konsep kepercayaan telah berkembang melampaui ranah interpersonal dan kelembagaan untuk mencakup ruang digital, yang kemudian dikenal dengan istilah "*digital trust*". Dalam perspektif akademik, bidang ini masih tergolong relatif baru dan belum sepenuhnya matang. Studi literatur yang dilakukan oleh Pietrzak dan Takala [67] mengungkapkan bahwa referensi ilmiah mengenai kepercayaan digital masih terbatas. Meskipun penelitian awal di bidang ini telah dimulai sejak tahun 1996, pertumbuhan publikasi yang signifikan baru terlihat setelah tahun 2016, menandakan meningkatnya perhatian terhadap isu kepercayaan dalam ekosistem digital.

Meskipun demikian, belum terdapat kesepakatan konseptual yang utuh mengenai definisi kepercayaan digital di kalangan akademisi. Mubarak dan Petraite [68] berpendapat bahwa kepercayaan digital dapat dimaknai sebagai kepercayaan para pemangku kepentingan terhadap kemampuan aktor, teknologi, dan proses dalam membangun jaringan bisnis yang andal dan aman. Mereka menemukan bahwa kepercayaan digital secara signifikan meningkatkan inovasi terbuka (*open innovation*). Selain itu, kapasitas absorptif yang terealisasi, kapasitas absorptif potensial, dan orientasi teknologi menjadi mediator dalam hubungan antara kepercayaan digital dan inovasi terbuka suatu perusahaan.

Kozhevnikov dan Korolev [69] menyatakan bahwa kepercayaan digital merujuk pada hubungan antara seseorang dan agen kecerdasan independen yang ada di lingkungan digital. Dalam lingkungan digital, seseorang menaruh kepercayaan pada agen tersebut, yang menunjukkan bahwa agen tersebut mampu memenuhi kebutuhan harian pihak yang memberi kuasa dengan melakukan transaksi atas nama pihak tersebut. Oleh karena tidak ada batasan frekuensi transaksi di lingkungan digital, optimalisasi interaksi antara pembeli dan penjual pada akhirnya dapat menimbulkan ambiguitas dalam konsep transaksi. Dalam konteks ini, transaksi tidak lagi dilihat sebagai peristiwa individual, melainkan sebagai tindakan seseorang dalam memilih agen kepercayaannya.

Model kepercayaan digital juga dikembangkan oleh Buechner dan Tavani [70], yang

mengklasifikasikan kepercayaan dalam tiga jenis: antara agen manusia, antara agen buatan dan manusia, serta antaragen buatan. Model ini dinilai relevan dalam menjelaskan mekanisme kepercayaan digital. Namun, revisi lanjutan [71] menunjukkan bahwa aspek kepercayaan terhadap diri sendiri (*self-confidence*) belum tercakup, padahal aspek ini seharusnya menjadi bagian penting dalam membentuk kepercayaan di lingkungan digital.

Wu [72] berpendapat bahwa kepercayaan digital ditandai oleh sifat teknis, relasional, mediatif, dan komprehensif. Kepercayaan digital merupakan rekonstruksi dari kepercayaan antarpribadi dan kepercayaan terhadap sistem melalui teknologi digital, serta merupakan hasil dari "transfer kepercayaan" antarsaluran dan intra-saluran kepercayaan. Mekanisme pembentukan kepercayaan digital mencakup mekanisme *hard trust* dan *soft trust*. Keamanan dan desain sistem merupakan bagian dari *hard trust*, sedangkan modal sosial digital, sistem reputasi *online*, transparansi dan responsivitas, serta kepuasan hasil merupakan elemen dari *soft trust*. Kedua mekanisme ini bekerja secara terpadu untuk merekonstruksi kepercayaan dalam masyarakat digital. Dengan merangkum definisi dari berbagai akademisi dan mempertimbangkan situasi sosial digital, studi ini mendefinisikan kepercayaan digital sebagai gabungan antara kepercayaan kognitif dan kepercayaan emosional. Kepercayaan kognitif mencakup aspek-aspek seperti fungsionalitas, komitmen terhadap eksekusi, kejujuran, dan niat baik. Sementara kepercayaan emosional mencakup aspek-aspek seperti rasa suka dan keyakinan.

Transformasi digital di lingkungan kerja juga memunculkan kebutuhan baru terhadap pengukuran kepercayaan. Marcial dan Launer [73] menyusun kerangka teoretis berdasarkan prinsip sistem informasi dan model input-output untuk mengukur kepercayaan digital di dunia kerja. Pendekatan ini mencerminkan perubahan cara pandang masyarakat terhadap reliabilitas dalam era teknologi.

Dalam ranah *e-commerce*, Hermawan [74] meneliti bagaimana kepercayaan digital memengaruhi persepsi konsumen terhadap citra merek dan loyalitas pelanggan. Komunikasi antara pengguna dan penyedia layanan digital menjadi salah satu faktor penentu dalam membangun hubungan yang berbasis kepercayaan.

Mukherjee dkk. [75] berpendapat bahwa isu privasi dan keamanan memengaruhi sikap publik dan niat mereka dalam proses adopsi teknologi. Mereka meneliti pengaruh kepercayaan terhadap teknologi *blockchain* dengan menganalisis persepsi masyarakat terhadap isu privasi dan keamanan melalui lima variabel utama: sikap, privasi, kepercayaan, keamanan, dan niat.

Keragaman definisi dan perspektif mengenai kepercayaan digital dalam berbagai literatur mencerminkan kompleksitas konsep ini dalam praktiknya. Beberapa definisi institusional berikut dapat memberikan pemahaman komparatif tentang bagaimana kepercayaan digital dimaknai dalam konteks global:

- ISACA [76]: "*the confidence in the integrity of the relationships, interactions, and transactions among providers and consumers within an associated digital ecosystem.*"

- Pietrzak & Takala [67]: "*digital trust is the measure of confidence which workers, consumers/buyers, partners and other stakeholders have in an organisation's ability to protect data and the privacy of individuals.*"
- WEF [77]: "*the expectation by individuals that digital technologies and services – and the organizations providing them – will protect all stakeholders' interests and uphold societal expectations and values.*"
- PwC [78]: "*the level of confidence individuals and organizations place in digital technologies, systems, and the organizations that provide them, ensuring the protection of stakeholders' interests and upholding societal expectations.*"

Dari berbagai pandangan di atas, dapat disimpulkan bahwa kepercayaan adalah konstruksi multidimensi yang mencakup unsur kognitif (keyakinan akan kemampuan dan integritas pihak lain), afektif (rasa suka dan keterikatan), serta intensional (kemauan untuk mengambil risiko dalam hubungan sosial). Ketiga dimensi inilah yang menjadi dasar dalam memahami dan mengembangkan kepercayaan dalam konteks digital.

2.2.1 Kepercayaan digital mekanis

Berbagai literatur mendefinisikan kepercayaan digital dari sudut pandang yang beragam. Tinjauan yang dilakukan terhadap beberapa definisi utama menunjukkan bahwa kepercayaan digital dapat dikategorikan dalam tiga pendekatan: sebagai *mechanical trust*, *relational trust*, dan sebagai konsep terpadu yang mencakup keduanya, yang sering disebut sebagai *trust ecosystem*. Pendekatan terpadu ini tidak hanya menekankan pada keandalan sistem digital secara teknis, tetapi juga memperhatikan norma sosial dan struktur kelembagaan yang menopang keberlangsungan ekosistem digital.

Penting untuk dicatat bahwa dalam literatur kontemporer, beberapa lembaga otoritas seperti WEF dan ISACA sering kali menyajikan definisi yang bersifat inklusif. Meskipun definisi tersebut mencakup elemen mekanis (teknis) dan relasional (sosial) secara bersamaan, dalam tinjauan ini, dilakukan dekonstruksi terhadap definisi tersebut untuk menonjolkan aspek spesifik yang relevan dengan masing-masing kategori guna memberikan pemahaman yang lebih granular.

Kepercayaan digital mekanis berfokus pada objektivitas teknis, yaitu keandalan dan prediktabilitas sistem serta teknologi digital dalam memberikan hasil yang diharapkan. Kepercayaan ini berfokus pada aspek dan mekanisme teknis yang memastikan sistem berfungsi sebagaimana mestinya, sehingga memungkinkan kinerja yang konsisten dan dapat diandalkan. Jenis kepercayaan ini sering kali dievaluasi berdasarkan faktor-faktor seperti keamanan siber, keselamatan, transparansi, dan auditabilitas [79]. Berikut merupakan beberapa definisi kepercayaan digital mekanis yang berasal dari berbagai referensi (lihat Tabel 2.1).

Tabel 2.1: Beberapa Definisi Kepercayaan Digital Mekanis

Definisi	**Aktor**	**Sumber**
Individuals' expectation that digital technologies and services — and the organisations providing them — will protect all stakeholders' interests and uphold societal expectations and values.	Konsumen dan bisnis	WEF (2022) [80]
The confidence in the integrity of relationships, interactions and transactions among providers and consumers within an associated digital ecosystem.	Penyedia layanan, konsumen, dan auditor	ISACA (2022) [76, 79]
Consumer faith in cybersecurity, data privacy, and responsible AI.	Konsumen dan bisnis	McKinsey & Company (2022) [81]
The foundation of security that enables confidence that digital interactions, identity, and connections are authentic and secure.	Pengguna, perangkat, dan sistem	DigiCert (2022) [82]
The level of confidence that consumers enjoy while interacting digitally for consuming their various services.	Konsumen dan bisnis	Singh & Malhotra (2022) [83]
People's confidence that a platform will protect their information and provide a safe environment for them to create and engage with content.	Pengguna dan platform	Business Insider Intelligence (2020) [84]; Williamson (2022) [85]
An attitude of confident expectation in an online situation of risk that one's vulnerabilities will not be exploited.	Konsumen dan bisnis	Corritore dkk. (2003) [86]
Digital trust is an evolution of traditional trust models to cover the additional requirements of digital business, deriving levels of measurable confidence to make risk-based decisions.	Konsumen dan bisnis	Gaehtgens and Allan (2017) [87]

Berbagai literatur dan lembaga internasional telah mengemukakan definisi kepercayaan digital dari beragam perspektif, mulai dari perlindungan informasi, privasi, dan keamanan, hingga pemenuhan nilai-nilai sosial dalam interaksi *online*. Meskipun terdapat variasi terminologi dan penekanan, seluruh definisi tersebut memiliki benang merah yang sama, yaitu adanya keyakinan terhadap keandalan teknologi dan aktor digital dalam menciptakan lingkungan digital yang aman dan bertanggung jawab. Berdasarkan sintesis dari beberapa sumber tersebut, berikut adalah definisi kepercayaan digital yang dirumuskan secara komprehensif.

> *Kepercayaan digital mekanis* adalah keyakinan yang dimiliki individu atau organisasi bahwa teknologi, layanan, dan penyedia digital akan melindungi informasi, menjamin keamanan dan privasi, memenuhi nilai-nilai sosial dan etika, serta tidak mengeksploitasi kerentanan pengguna bahkan dalam situasi berisiko, sehingga memungkinkan interaksi dan pengambilan keputusan berbasis risiko secara aman dan nyaman.

2.2.2 Kepercayaan digital relasional

Kepercayaan digital relasional merujuk pada keyakinan yang dimiliki individu ketika berinteraksi dengan teknologi dan layanan digital, yang terbentuk melalui akumulasi pengalaman pribadi, persepsi terhadap kredibilitas penyedia layanan, serta norma sosial yang membentuk konteks interaksi tersebut. Konsep ini menekankan aspek manusiawi dari kepercayaan, berbeda dengan kepercayaan terhadap sistem teknis atau algoritma, dengan mempertimbangkan elemen-elemen seperti persepsi terhadap integritas, transparansi komunikasi, dan rekam jejak reputasi penyedia layanan.

Dalam era transformasi digital yang terus berkembang, kepercayaan relasional memiliki peran strategis dalam membangun hubungan jangka panjang antara pengguna dan penyedia layanan. Tidak hanya berperan dalam tahap awal adopsi teknologi, kepercayaan ini juga menjadi faktor penting dalam menciptakan loyalitas dan kepuasan yang berkelanjutan. Dukungan terhadap praktik digital yang etis, aman, dan berorientasi pada pengguna sangat bergantung pada keberadaan kepercayaan relasional yang kuat, terutama dalam konteks pengelolaan data pribadi dan interaksi lintas platform.

Pemahaman yang mendalam mengenai dinamika sosial dan psikologis pengguna menjadi prasyarat utama dalam memperkuat kepercayaan digital relasional. Harapan terhadap jaminan keamanan, transparansi, dan akuntabilitas dari penyedia layanan digital tidak dapat diabaikan. Dalam hal ini, literasi digital yang memadai, komunikasi yang terbuka dan konsisten, serta ketersediaan mekanisme umpan balik yang responsif menjadi faktor kunci dalam memperkuat kepercayaan yang bersifat relasional.

Tabel 2.2: Evolusi Definisi Kepercayaan Digital Relasional

Definisi	**Aktor**	**Sumber**
A reliance on a firm by its stakeholders with regard to its business activities in the electronic medium, and in particular, its website.	Konsumen dan Bisnis	Shankar dkk. (2002) [88]
Confidence is placed in an organisation to collect, store, and use the digital information of others in a manner that benefits and protects those to whom the information pertains.	Konsumen dan Bisnis	Accenture (2014) [89]
Belief that a brand is reliable, capable, safe, transparent, and truthful in its digital practices.	Konsumen dan Bisnis	Lynch dkk. (2016) [90]
Individuals' expectation that digital technologies and services – and the organizations providing them – will protect all stakeholders' interests and uphold societal expectations and values.	Individu, Organisasi, dan Masyarakat	World Economic Forum (2022) [77]

Definisi	Aktor	Sumber
The confidence in the integrity of the relationships, interactions and transactions among providers and consumers within an associated digital ecosystem.	Penyedia Layanan dan Konsumen	ISACA (2022) [76, 79]
Confidence in an organization to protect consumer data, enact effective cybersecurity, offer trustworthy AI-powered products and services, and provide transparency around AI and data usage.	Konsumen dan Organisasi	McKinsey (2022) [52]

Tabel 2.2 menyajikan beragam definisi kepercayaan digital relasional yang dirumuskan oleh berbagai literatur dan lembaga, yang secara umum menekankan pentingnya persepsi pengguna terhadap keandalan, keamanan, dan keterbukaan praktik digital organisasi. Berdasarkan sintesis dari definisi-definisi tersebut, rumusan berikut dapat dijadikan acuan komprehensif dalam memahami konsep ini:

> *Kepercayaan digital relasional* adalah keyakinan konsumen atau pemangku kepentingan bahwa suatu organisasi dapat diandalkan, bertanggung jawab, dan transparan dalam mengelola aktivitas digital, termasuk pengumpulan, penyimpanan, dan penggunaan informasi, serta menjalankan praktik *online* secara aman, jujur, dan sesuai kepentingan pihak yang dilayani.

2.2.3 Ekosistem kepercayaan digital

Pemisahan antara dimensi mekanis dan relasional dalam bagian sebelumnya dilakukan untuk mempermudah pembedahan komponen dasar kepercayaan digital secara granular. Namun, kehadiran definisi dari lembaga otoritas seperti ISACA dan WEF dalam kedua kategori tersebut sebenarnya membuktikan bahwa kepercayaan digital pada dasarnya merupakan sebuah kesatuan yang multidimensi. Sebagai contoh, pada Tabel 2.1, kutipan dari lembaga tersebut ditinjau dari aspek prediktabilitas sistem, sementara pada Tabel 2.2, fokus dialihkan pada ekspektasi kepentingan pemangku kepentingan.

Oleh karena itu, pendekatan ekosistem yang dibahas dalam sub-bab ini berfungsi sebagai sintesis yang menyatukan kembali elemen teknis dan sosial yang sebelumnya dipisahkan untuk tujuan analisis. Ekosistem kepercayaan digital dipandang sebagai jaringan kompleks yang terdiri atas individu, organisasi, dan teknologi yang saling terhubung. Di sini, kepercayaan berfungsi sebagai prasyarat utama untuk memungkinkan terjadinya interaksi digital yang aman, andal, dan berkelanjutan.

Ekosistem kepercayaan digital merupakan suatu jaringan kompleks yang terdiri atas individu, organisasi, dan teknologi yang saling terhubung dan berinteraksi dalam ruang digital secara kolektif. Ekosistem ini dibangun atas dasar kepercayaan, yang berfungsi sebagai prasyarat utama untuk memungkinkan terjadinya interaksi digital yang aman, andal, dan berkelanjutan. Keberadaan standar bersama, protokol

interoperabilitas, serta infrastruktur teknologi yang dapat dipercaya menjadi pilar penting dalam memastikan keamanan, privasi, dan keandalan dalam setiap transaksi maupun pertukaran informasi digital di dalamnya [91].

Pemahaman terhadap ekosistem kepercayaan digital tidak dapat dilepaskan dari pendekatan holistik yang menggabungkan dimensi relasional dan dimensi mekanis secara seimbang. Dimensi relasional menekankan pentingnya interaksi antarmanusia dan antarlembaga yang dilandasi oleh integritas, akuntabilitas, dan reputasi. Sementara itu, dimensi mekanis berfokus pada keandalan sistem, prosedur operasional, serta teknologi yang mendasari berlangsungnya proses digital. Keterpaduan antara kedua dimensi tersebut menjadi kunci dalam menciptakan lingkungan digital yang tidak hanya fungsional secara teknis, tetapi juga dapat dipercaya secara sosial.

Tabel 2.3: Pendekatan *Ekosistem* Terpadu antara Kepercayaan Relasional dan Mekanis

Definisi	**Aktor**	**Sumber**
Digital trust is trusting not only in people we know and abstract systems, but also in technical and technological systems.	Pengguna, platform, dan bisnis	Kożuch (2021) [87]
Confidence that participants have in the digital ecosystem to interact securely, in a transparent, accountable, and frictionless manner.	Pengguna, platform, dan bisnis	SGTech (2022) [92]
Confidence in the integrity of the relationships, interactions, and transactions among suppliers or providers and customers or consumers within an associated digital ecosystem.	Konsumen, bisnis, dan auditor	ISACA (2023) [93]
A shared expectation that digital technologies and services – and the organizations providing them – will protect all stakeholders' interests and uphold societal values.	Masyarakat, Pemerintah, dan Swasta	WEF (2024) [94]
A condition that enables decisions to be made between two or more entities that reflects a level of confidence in the security, privacy, and ethical handling of the interaction.	Ekosistem Bisnis dan Teknologi	IDC (2023) [95]
The level of confidence in people, processes, and technology to build a secure digital world.	Pengguna, platform, dan bisnis	Paliszkiewicz & Chen (2023) [96]

Tabel 2.3 menyajikan beragam definisi mengenai ekosistem kepercayaan digital dari sejumlah referensi tepercaya. Masing-masing definisi menyoroti bagaimana kepercayaan dibangun melalui hubungan yang kuat dan terjaga antaraktor dalam ruang digital, termasuk pengguna akhir, penyedia layanan, institusi regulator, serta sistem dan teknologi pendukung. Sintesis dari berbagai perspektif tersebut menunjukkan bahwa kepercayaan digital bukan sekadar hasil dari perangkat teknis, melainkan

merupakan hasil interaksi dinamis antara aktor dan sistem dalam lingkungan yang saling bergantung.

Berdasarkan integrasi konsep dari sumber-sumber tersebut, berikut dirumuskan definisi operasional kepercayaan digital berbasis ekosistem:

> *Kepercayaan digital berbasis ekosistem* adalah tingkat keyakinan kolektif antara pengguna, penyedia layanan, dan pelaku bisnis terhadap integritas hubungan, transparansi interaksi, serta keandalan proses dan teknologi dalam mendukung transaksi digital yang aman, akuntabel, dan tanpa hambatan di dalam suatu lingkungan digital yang saling terhubung dan terkelola secara kolaboratif.

Ketiga bentuk kepercayaan digital—mekanis, relasional, dan ekosistemik—akan menjadi pilar utama dalam penyusunan kerangka kerja kepercayaan digital nasional yang dijelaskan pada bagian selanjutnya. Pendekatan ini memastikan bahwa aspek teknis, sosial, dan kelembagaan terintegrasi secara seimbang.

2.3 Teknik Pengembangan Kerangka Kerja

Setelah memahami dasar konseptual kepercayaan dan bentuk-bentuknya dalam ranah digital, bagian ini menguraikan metodologi yang digunakan untuk merancang kerangka kerja kepercayaan digital nasional. Metodologi ini berfungsi sebagai panduan sistematis dalam menghubungkan konsep teoretis dengan praktik kebijakan.

Teknik dalam penyusunan kerangka kerja (*framework*) dapat bervariasi, bergantung pada konteks dan tujuan yang ingin dicapai. Buku ini menggunakan pendekatan *summarization*, yaitu merangkum temuan penelitian terdahulu serta praktik yang ada dan mengadaptasikannya ke dalam konteks nasional. Dalam kajian metodologis, *summarization* telah lama diakui sebagai teknik penting untuk menyaring informasi dari berbagai sumber. Nenkova dan McKeown [97] meninjau secara komprehensif metode *extractive* maupun *abstractive*, sedangkan Mani [98] menekankan perannya dalam mengolah informasi kompleks menjadi ringkasan terstruktur yang lebih mudah disesuaikan dengan kebutuhan tertentu. Dengan merujuk pada landasan tersebut, kajian ini menerapkan *summarization* untuk mengintegrasikan temuan dan praktik yang relevan, kemudian menyesuaikannya dengan kebutuhan nasional.

Beberapa studi sebelumnya menjadi rujukan, antara lain penelitian Nakamura [99] dalam pengembangan kerangka kerja di bidang robotika, serta penelitian Bajaj [100] dalam penyusunan kerangka kerja semantik *Internet of Things* (IoT). Kedua kajian tersebut menggunakan metode 4W1H (*Who, What, When, Where, How*) sebagai alat analisis sistematis. Secara rinci, metode 4W1H menjelaskan:

- *Who*: Identifikasi penanggung jawab atau aktor utama.
- *What*: Definisi isu atau objek yang dikaji.

- *When*: Urutan waktu atau fase peristiwa.
- *Where*: Lokasi atau ruang lingkup implementasi.
- *How*: Metode, proses, atau mekanisme pelaksanaan.

Seiring perkembangannya, metode 4W1H banyak diterapkan dalam berbagai bidang, mulai dari manajemen, kebijakan publik, hingga teknologi, karena metode ini mampu menyederhanakan persoalan kompleks ke dalam struktur analisis yang sistematis [100, 101]. Dalam perkembangannya, pendekatan ini sering diperluas menjadi 5W1H dengan menambahkan unsur *Why*, yang berfungsi untuk menggali motif, alasan, dan latar belakang mendasar suatu fenomena atau keputusan strategis [102].

Pendekatan 5W1H dapat memastikan bahwa kebijakan maupun kerangka kerja yang disusun didasarkan pada pemahaman yang jelas tentang tujuan, nilai-nilai, dan potensi *trade-off* yang terlibat dalam berbagai pendekatan regulasi. Analisis ini juga membantu menjelaskan kekuatan inisiatif-inisiatif dan area-area yang mungkin memerlukan pengembangan lebih lanjut [102].

Tujuan utama kajian ini adalah menyusun sebuah kerangka kerja konseptual (*conceptual framework*) pada tingkat nasional. Oleh karena itu, metodologi harus disajikan secara sistematis untuk menunjukkan bagaimana kerangka kerja dirancang, disusun, dan divalidasi. Adapun tahapan metodologi meliputi:

1. Tinjauan Literatur
   Tahap pertama adalah kajian pustaka terhadap literatur akademis maupun praktis. Kajian mencakup teori dasar kepercayaan digital, standar internasional seperti NIST dan ISO/IEC, serta kerangka kerja yang dikembangkan di negara lain maupun komunitas. Tujuan dari kajian ini adalah mengidentifikasi konsep, prinsip, dan praktik terbaik yang relevan, sehingga dapat diadopsi atau disesuaikan dengan konteks Indonesia.

2. Kajian Regulasi Nasional
   Analisis terhadap regulasi dan kebijakan nasional yang terkait dengan kepercayaan digital, mulai dari Undang-Undang (UU), Peraturan Pemerintah (PP), Peraturan Presiden (Perpres), hingga kebijakan teknis Kementerian/Lembaga. Analisis ini memastikan keselarasan dengan kerangka hukum dan kebutuhan strategis Indonesia. Regulasi turunan, seperti peraturan menteri, pedoman teknis, strategi nasional, hingga surat edaran, juga diperhatikan karena berperan langsung dalam isu spesifik seperti keamanan siber, tata kelola data, perlindungan konsumen digital, dan ekonomi berbasis teknologi.

3. Pengembangan Kerangka Kerja dengan Analisis 5W1H
   Kerangka kerja kemudian dikembangkan menggunakan metode 5W1H (*Where, Why, What, Who, When, How*). Metode ini dipilih karena mampu memetakan elemen fundamental dalam penyusunan kerangka kerja kepercayaan digital secara sistematis.

- *Where*: menganalisis negara atau wilayah yang telah menerapkan standar maupun kerangka kerja kepercayaan digital.
- *Why*: menganalisis alasan strategis dan urgensi kerangka kerja kepercayaan digital.
- *What*: mendefinisikan isu utama dan ruang lingkup kepercayaan digital.
- *Who*: mengidentifikasi aktor yang terlibat dalam perencanaan, penerapan, dan pengendalian kepercayaan digital.
- *When*: menjelaskan tahapan atau lini masa implementasi kepercayaan digital.
- *How*: merinci strategi penerapan kerangka kepercayaan digital.

Hasil analisis ini dirumuskan dalam bentuk skema konseptual yang memadukan aktor, tujuan, tahapan, metode, serta alasan strategis berdasarkan lokasi wilayah tertentu.

4. Penilaian Pakar dan Praktisi
   Tahap akhir adalah validasi melalui penilaian pakar dan praktisi. Validasi dilakukan dengan berbagai metode, seperti *focused group discussion* (FGD), wawancara mendalam, serta tinjauan draf kerangka kerja dan naskah buku. Para pakar yang dilibatkan berasal dari kalangan akademisi, regulator, swasta/industri, serta komunitas keamanan siber.
   Penilaian ini menitikberatkan pada tiga aspek utama: (i) kelayakan konsep, (ii) relevansi dengan kebutuhan Indonesia, dan (iii) tingkat implementabilitas. Hasil validasi digunakan sebagai dasar untuk menyempurnakan kerangka kerja, sehingga dapat diimplementasikan secara efektif, sekaligus mendukung terwujudnya kepercayaan digital nasional yang berkelanjutan.

Pendekatan metodologis ini memberikan dasar yang kokoh bagi penyusunan kerangka kerja kepercayaan digital yang tidak hanya kontekstual dengan kebutuhan Indonesia, tetapi juga sejalan dengan praktik terbaik internasional. Secara keseluruhan, rangkaian pembahasan dalam bab ini menguraikan bagaimana kepercayaan berkembang dari tataran sosial hingga digital, serta bagaimana konsep tersebut diterjemahkan menjadi pendekatan metodologis yang sistematis. Dengan demikian, bab ini membangun landasan konseptual dan metodologis bagi analisis serta pengembangan kerangka kerja kepercayaan digital yang akan dijelaskan lebih lanjut pada bab-bab berikutnya.

3

Praktik Terbaik Kepercayaan Digital

> Trust takes years to build, seconds to break, and forever to repair.
>
> — Anonymous

Transformasi digital telah mengubah paradigma manajemen organisasi, menekankan pentingnya memanfaatkan peluang sekaligus mengelola tantangan yang muncul. Keberhasilan organisasi dalam era digital sangat bergantung pada kepercayaan para pemangku kepentingan terhadap organisasi dan teknologi yang digunakan. Kepercayaan digital, yang didefinisikan sebagai keyakinan terhadap keamanan, keandalan, dan transparansi sistem serta layanan digital, terbentuk dari kebutuhan kontekstual, kondisi pendukung seperti infrastruktur teknologi, serta peran aktor seperti pemerintah, sektor swasta/industri, dan masyarakat dalam interaksi ekonomi dan sosial. Berbagai penelitian menunjukkan bahwa kepercayaan merupakan faktor kunci keberhasilan bisnis *online* [103, 104, 105, 106, 107]. Berbeda dengan kepercayaan tradisional yang mengandalkan interaksi fisik serta isyarat verbal/nonverbal, kepercayaan digital berfokus pada keamanan data, privasi, dan integritas sistem, misalnya melalui mekanisme konsensus terdesentralisasi pada *blockchain* yang menggantikan kebutuhan akan kepercayaan interpersonal. Oleh karena itu, kepercayaan digital menjadi elemen penting dalam membangun hubungan yang kuat dengan pemangku kepentingan, baik di dalam organisasi (misalnya, karyawan dan manajemen) maupun di luar (pelanggan, mitra bisnis, dan masya-

rakat). Untuk mewujudkan kepercayaan digital yang berkelanjutan, diperlukan upaya sistematis yang tidak hanya menekankan aspek teknologi, tetapi juga tata kelola, kebijakan, dan kolaborasi lintas sektor.

Pembangunan kepercayaan digital membutuhkan pendekatan yang terstruktur dan menyeluruh, dengan melibatkan seluruh pemangku kepentingan, termasuk pemerintah, sektor swasta/industri, dan masyarakat luas, yang memiliki komitmen terhadap penerapan standar keamanan siber terintegrasi, seperti NIST, ISO/IEC, dan standar lain yang relevan. Komitmen ini juga mencerminkan kesiapan kolektif untuk mengadopsi ekosistem keamanan siber yang adaptif dan dinamis dalam menghadapi tantangan yang terus berkembang.

Dalam konteks penerapan yang lebih operasional, keberhasilan kerangka kerja kepercayaan digital ditentukan oleh sejauh mana kebijakan, praktik, dan prosedur yang dirancang mampu mengidentifikasi, menilai, dan mengelola berbagai risiko siber, termasuk serangan peretasan dan pelanggaran data. Kompleksitas risiko ini dipengaruhi oleh percepatan inovasi teknologi, dinamika kebijakan nasional dan global, serta faktor ekonomi dan sosial yang saling berkaitan.

Penerapan langkah-langkah teknis seperti enkripsi data, autentikasi dua faktor, serta sistem deteksi dan respons terhadap intrusi berkontribusi signifikan dalam memperkuat persepsi kepercayaan terhadap layanan digital, khususnya dalam ekosistem yang semakin mengandalkan konektivitas dan pertukaran data secara *real-time*. Selain berfungsi sebagai mekanisme pengelolaan risiko, kepercayaan digital juga memiliki peran strategis dalam mendorong pertumbuhan ekonomi digital dan peningkatan daya saing nasional.

Kerangka kerja kepercayaan digital juga berperan penting dalam meningkatkan daya saing wilayah dan negara dalam ekonomi digital. Tujuannya adalah menciptakan ekosistem digital yang aman, transparan, dan kolaboratif, yang mendukung inovasi seperti layanan *e-government* yang efisien atau platform perdagangan *online* yang andal. Dengan kepercayaan digital, masyarakat dan pelaku usaha dapat berpartisipasi secara lebih luas dalam aktivitas ekonomi berbasis teknologi, misalnya melalui sistem pembayaran digital, layanan keuangan bersama, atau perdagangan lintas batas yang berbasis data. Hal ini mendorong efisiensi, memperluas pasar, dan memperkuat posisi kompetitif suatu negara dalam ekonomi global. Dalam jangka panjang, penerapan kepercayaan digital berkontribusi terhadap pembangunan ekonomi yang berkelanjutan, penciptaan lapangan kerja baru, serta peningkatan inovasi di berbagai sektor.

Namun, di balik peluang ekonomi tersebut, pembangunan kepercayaan digital juga menghadapi sejumlah tantangan sosial dan struktural. Rendahnya literasi digital, ketimpangan akses terhadap teknologi, serta kekhawatiran terhadap perlindungan privasi menjadi faktor yang dapat menghambat adopsi ekosistem digital secara merata. Untuk mengatasi hal tersebut, kerangka kerja kepercayaan digital perlu mengintegrasikan kebijakan edukasi digital yang komprehensif, mekanisme perlindungan data yang kuat—seperti yang diatur dalam UU Nomor 27 Tahun 2022 tentang Pelindungan Data Pribadi (UU PDP) di Indonesia—serta desain sistem yang aman dan menyeluruh agar setiap lapisan masyarakat dapat memperoleh

manfaat yang setara dari transformasi digital. Pendekatan ini memastikan bahwa penguatan kepercayaan digital tidak hanya memperkuat daya saing nasional, tetapi juga mendorong pemerataan manfaat ekonomi dan sosial di seluruh wilayah.

Setelah memahami urgensi dan tantangan dalam membangun kepercayaan digital, langkah berikutnya adalah mengidentifikasi praktik terbaik yang dapat menjadi acuan. Untuk mempermudah identifikasi praktik terbaik kepercayaan digital, hasil analisis disajikan dengan pendekatan 5W1H (*Where, Why, What, Who, When, How*). Proses identifikasi dilakukan dengan menjawab enam pertanyaan tematik yang terdiri dari:

1. *Where*: Di mana negara atau wilayah yang telah menerapkan standar maupun kerangka kerja kepercayaan digital?
2. *Why*: Mengapa kerangka kepercayaan digital menjadi hal penting bagi negara atau wilayah tersebut?
3. *What*: Apa saja yang menjadi tujuan dan ruang lingkup kerangka kerja kepercayaan digital?
4. *Who*: Siapa saja aktor yang terlibat dalam perencanaan, penerapan, dan pengendalian kepercayaan digital?
5. *When*: Kapan target implementasi kepercayaan digital tercapai berdasarkan lini masanya?
6. *How*: Bagaimana strategi penerapan kerangka kepercayaan digital untuk mencapai tujuan?

Enam pertanyaan tersebut menjadi panduan utama dalam menelaah berbagai praktik terbaik yang telah dikembangkan di tingkat nasional maupun komunitas.

Berdasarkan pendekatan tersebut, pembahasan berikut menyoroti implementasi kepercayaan digital di berbagai negara dan komunitas. Pembahasan dalam bab ini berfokus pada praktik terbaik kepercayaan digital yang diterapkan di beberapa negara dan komunitas, dengan menyoroti keragaman pendekatan serta tantangan yang dihadapi masing-masing. Kepercayaan digital tidak hanya dipengaruhi oleh infrastruktur teknologi dan regulasi yang ada, tetapi juga oleh konteks sosial, budaya, dan tingkat kesiapan masyarakat dalam mengadopsi solusi digital. Setiap negara memiliki kebijakan dan prioritas yang berbeda dalam membangun ekosistem digital yang aman, kolaboratif, dan berkelanjutan, sementara komunitas sering kali mengembangkan praktik unik yang disesuaikan dengan kebutuhan dan nilai-nilai mereka. Dengan melihat pembahasan dari dua perspektif ini, yaitu negara dan komunitas, diharapkan dapat dipahami bagaimana kepercayaan digital dibentuk secara holistik, mulai dari level kebijakan makro hingga implementasi mikro di masyarakat. Pendekatan ini penting untuk mengidentifikasi peluang kolaborasi, memperkuat literasi digital, serta menciptakan model kepercayaan digital yang adaptif dan berkelanjutan di berbagai lapisan masyarakat. Secara khusus, pembahasan mengenai negara akan mencakup inisiatif kepercayaan digital yang telah

diterapkan. Inisiatif ini mencakup kebijakan, regulasi, program, dan teknologi yang dirancang untuk memastikan keamanan, transparansi, serta keandalan ekosistem digital. Tujuan utamanya adalah membangun kepercayaan publik dan sektor bisnis dalam penggunaan teknologi digital, termasuk transaksi *online*, pertukaran data, dan layanan digital pemerintah. Dengan demikian, kajian terhadap kedua perspektif ini diharapkan dapat memberikan gambaran menyeluruh tentang bagaimana kepercayaan digital dapat dibangun, dikelola, dan dipelihara secara berkelanjutan di berbagai konteks sosial dan institusional.

3.1 Praktik Terbaik Kepercayaan Digital Negara

Di era transformasi digital, kepercayaan digital, yaitu keyakinan pengguna terhadap keamanan, privasi, dan keandalan sistem elektronik, menjadi fondasi utama untuk mendukung adopsi teknologi di berbagai sektor, seperti pemerintahan, kesehatan, dan perdagangan [108]. Tantangan seperti pelanggaran data, serangan siber, dan kurangnya regulasi yang memadai mendorong negara-negara untuk mengembangkan strategi unik guna membangun ekosistem digital yang tepercaya [109]. Dengan pendekatan yang mencakup regulasi, teknologi, dan kolaborasi lintas sektor, negara-negara berupaya memastikan keamanan data pribadi, ketahanan terhadap ancaman siber, dan transparansi dalam penggunaan teknologi.

Berbagai negara telah menunjukkan praktik terbaik dalam membangun kepercayaan digital melalui pendekatan yang disesuaikan dengan konteks lokal mereka. Analisis praktik terbaik kepercayaan digital dimulai dengan menjawab pertanyaan tematik *Where* (di mana negara atau wilayah yang telah menerapkan standar maupun kerangka kerja kepercayaan digital?). Hasil analisis menunjukkan bahwa beberapa negara berikut telah menerapkan kerangka kerja kepercayaan digital:

1. Singapura menerapkan Personal Data Protection Act (PDPA) 2012, yang mewajibkan organisasi melindungi data pribadi dengan standar keamanan tinggi dan memberikan hak kepada individu untuk mengelola data mereka [110].

2. Malaysia mengikuti dengan Personal Data Protection Act (PDPA) 2010, yang mengatur penggunaan data di sektor komersial dan menetapkan denda hingga RM 1.000.000 untuk pelanggaran [111].

3. Uni Eropa memimpin dengan General Data Protection Regulation (GDPR) sejak 2018, yang menetapkan standar global untuk perlindungan privasi dengan persyaratan kepatuhan ketat, termasuk denda hingga 4% dari pendapatan tahunan perusahaan untuk pelanggaran [112].

4. Di Amerika Latin, Brasil memperkuat kepercayaan digital melalui Lei Geral de Proteção yang mewajibkan pelaporan pelanggaran data dalam 72 jam, menyerupai GDPR [113].

5. Turki berinvestasi dalam infrastruktur keamanan siber melalui Ulusal Siber Güvenlik Operasyon Merkezi (Pusat Operasi Keamanan Siber Nasional) untuk mengatasi ancaman siber geopolitik dan melindungi data sensitif [114].

Berdasarkan data negara-negara yang telah menerapkan praktik terbaik kepercayaan digital, analisis selanjutnya dilakukan dengan menjawab 5 (lima) pertanyaan tematik lainnya, yaitu *Why, What, Who, When, How* untuk setiap negara yang telah teridentifikasi. Lima pertanyaan tematik tersebut bertujuan untuk menganalisis bagaimana kebijakan, regulasi, dan teknologi di negara-negara tersebut membentuk ekosistem digital yang tepercaya. Dengan mempertimbangkan tantangan lokal seperti keterbatasan infrastruktur teknologi di Indonesia, analisis ini akan mengidentifikasi strategi yang dapat diadaptasi untuk memperkuat kepercayaan digital, seperti penguatan UU PDP atau penerapan teknologi autentikasi berbasis biometrik untuk layanan publik, sebagaimana diadopsi oleh Singapura [115]. Dengan melibatkan pemangku kepentingan dari sektor pemerintah, swasta/industri, dan masyarakat sipil, Indonesia dapat membangun ekosistem digital yang aman dan mendukung transformasi digital yang menyeluruh di tingkat nasional maupun global.

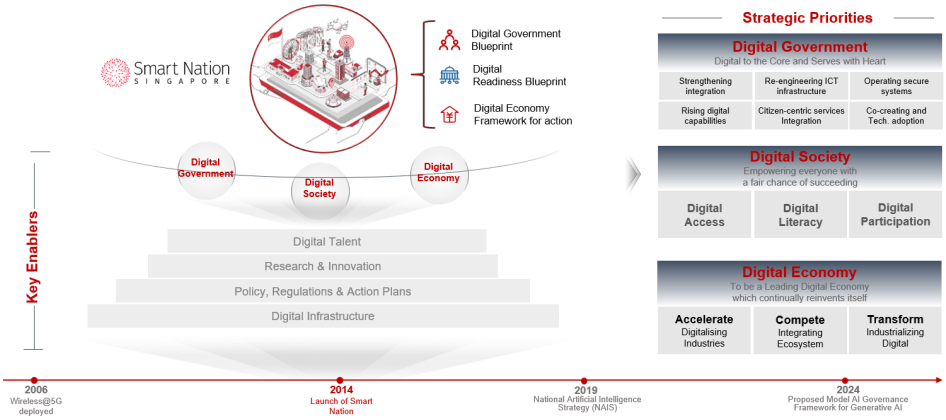
3.1.1 Singapura

Strategi Keamanan Siber Singapura 2021 menjadi panduan utama untuk melindungi Smart Nation dari ancaman siber yang berkembang seiring dengan kemajuan teknologi digital [116]. Smart Nation Singapore mempunyai beberapa *key enablers* antara lain Digital Government, Digital Society, dan Digital Economy [117]. Pada bidang *digital government*, pemerintah Singapura mencanangkan *digital to the core and serve with heart* melalui penguatan integrasi, menumbuhkan kemampuan digital, rekayasa ulang infrastruktur ICT, integrasi layanan berbasis *citizen centric*, menjalankan sistem yang aman, serta menciptakan atau mengadopsi teknologi. *Digital society* dengan semboyan *empowering everyone with a fair chance of succeeding* melalui akses digital, literasi digital, dan partisipasi digital. Untuk menjadi terkemuka dalam ekonomi digital, Singapura melakukan percepatan digitalisasi industri, meningkatkan integrasi ekosistem, dan mengubah lini bisnis untuk industrialisasi digital (lihat Gambar 3.1).

Berikut adalah pemetaan kerangka kerja kepercayaan digital Singapura berdasarkan lima pertanyaan tematik, yang mengintegrasikan regulasi, teknologi, dan kolaborasi lintas sektor untuk membangun ekosistem digital yang aman, kolaboratif, dan berkelanjutan.

Mengapa Kepercayaan Digital Penting (*Why*)

Kepercayaan digital, yaitu keyakinan masyarakat terhadap keamanan, privasi, dan keandalan sistem digital, merupakan landasan ekonomi digital Singapura [118]. Dalam dunia yang semakin terhubung, kepercayaan digital memungkinkan masyarakat, bisnis, dan pemerintah berinteraksi dengan aman, mendorong inovasi,



Gambar 3.1: *Smart Nation Singapura* [117]

dan meningkatkan produktivitas. Data dari Cyber Security Agency (CSA) menunjukkan bahwa 92% warga Singapura merasa lebih percaya pada layanan digital yang terlindungi, meningkatkan adopsi teknologi [119]. Kepercayaan digital juga melindungi data pribadi dan kepentingan publik, mengurangi risiko pelanggaran data, yang merugikan SGD 1 miliar pada 2022 [120]. Dengan ekosistem digital yang terlindungi, Singapura memperkuat daya saing global sebagai pusat teknologi, menarik investasi asing sebesar SGD 22 miliar di sektor digital pada 2023 [121].

Tujuan Pengenalan Kepercayaan Digital (*What*)

Pemerintah Singapura memperkenalkan konsep kepercayaan digital dengan tujuan utama menciptakan lingkungan digital yang aman dan andal, di mana data pribadi, informasi sensitif, dan transaksi digital terlindungi dari berbagai ancaman siber [52]. Dalam era transformasi digital yang semakin pesat, kepercayaan digital menjadi dasar penting untuk memastikan bahwa masyarakat, bisnis, dan pemerintah dapat berinteraksi, bertransaksi, dan berbagi data dengan keyakinan penuh akan keamanannya. Tujuan ini tidak hanya terbatas pada perlindungan teknis terhadap serangan siber, tetapi juga mencakup pembangunan kerangka kerja kepercayaan sosial yang memungkinkan semua pemangku kepentingan merasa aman dan nyaman dalam memanfaatkan ekosistem digital.

Dengan menciptakan lingkungan digital yang aman, Singapura bertujuan untuk mendorong inovasi, meningkatkan produktivitas, dan memperkuat pertumbuhan ekonomi berbasis digital. Kepercayaan digital juga menjadi kunci dalam melindungi kepentingan publik, termasuk privasi individu dan keamanan data, yang merupakan aspek krusial dalam membangun hubungan yang harmonis antara teknologi dan masyarakat. Selain itu, pemerintah menyadari bahwa kepercayaan digital adalah prasyarat untuk menarik investasi asing dan mempertahankan daya saing global Singapura sebagai pusat ekonomi digital terkemuka.

Melalui pendekatan ini, Singapura tidak hanya berfokus pada aspek keamanan,

tetapi juga pada pembangunan ekosistem digital yang kolaboratif dan berkelanjutan. Dengan memastikan bahwa semua pihak, mulai dari individu, perusahaan, hingga lembaga pemerintah, dapat beroperasi di ruang digital dengan rasa aman, Singapura berupaya menciptakan landasan yang kokoh untuk masa depan digital yang lebih cerah dan tangguh.

Siapa yang Bertanggung Jawab (*Who*)

Pemerintah Singapura memegang peran utama dalam membangun kepercayaan digital melalui lembaga-lembaga seperti Cyber Security Agency (CSA) dan Smart Nation and Digital Government Office (SNDGO)/Smart Nation and Digital Government Group (SNDGG). CSA bertugas mengembangkan standar dan regulasi keamanan siber, antara lain melalui *Cybersecurity Act* serta inisiatif sertifikasi seperti *Cyber Essentials* dan *Cyber Trust Marks*, sekaligus menjalin kolaborasi dengan industri dan mitra global untuk memperkuat pertahanan siber nasional [122, 123, 124]. Di sisi lain, SNDGG bersama GovTech berperan dalam transformasi digital pemerintahan dan pembangunan infrastruktur digital yang aman dan tepercaya, dengan menekankan prinsip *Trust* sebagai salah satu pilar *Smart Nation 2.0* yang memastikan keamanan, privasi, dan keandalan sistem digital Singapura [125, 126]. Melalui pendekatan kolaboratif ini, seluruh pemangku kepentingan, pemerintah, sektor swasta, dan masyarakat, dilibatkan dalam menciptakan ekosistem digital yang aman dan tepercaya.

Waktu dan Tahapan Implementasi (*When*)

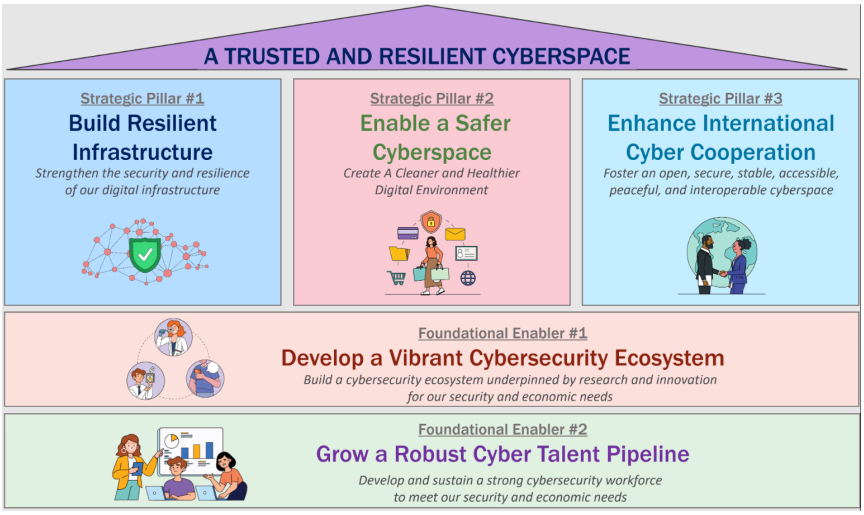
Kepercayaan digital di Singapura dikembangkan melalui rencana jangka panjang yang disesuaikan dengan perubahan teknologi, regulasi, dan kebutuhan keamanan. Implementasi program dilakukan secara bertahap, dengan setiap tahap menyesuaikan diri terhadap perkembangan ancaman siber baru, perubahan kebijakan global, dan kemajuan teknologi keamanan. Dengan perencanaan yang terstruktur, Singapura terus memperbarui pendekatannya agar dapat merespons tantangan dan kebutuhan terkini dalam keamanan siber. Hal ini ditunjukkan dengan adanya perubahan dokumen strategi keamanan siber Singapura tahun 2016 [127] yang diperbarui dengan dokumen tahun 2021 [116] dengan pendekatan terbaru, yaitu *zero trust* dan memperluas ketahanan digital dari infrastruktur nasional menjadi ketahanan digital yang menyeluruh, sehingga tidak hanya berfokus pada sektor kritis saja. Personal Data Protection Act (PDPA) yang pertama kali disahkan pada 2012 dan berlaku penuh pada 2014 juga mengalami amandemen pada tahun 2020 dengan adanya penambahan kewajiban pelaporan insiden pelanggaran data kepada Komisi Perlindungan Data Pribadi (Personal Data Protection Commission/PDPC) dan memperkenalkan konsep baru yang memungkinkan organisasi untuk mengumpulkan dan menggunakan data pribadi tanpa persetujuan eksplisit dalam kondisi tertentu.

Bagaimana Kepercayaan Digital Diterapkan (*How*)

Pendekatan Singapura dalam membangun kepercayaan digital tercermin dalam Strategi Keamanan Siber Singapura yang dikembangkan oleh pemerintah pada tahun 2021. Strategi ini menguraikan tujuan dan prioritas Singapura untuk menjaga keamanan dunia maya negara tersebut, memastikan bahwa pengguna digital di Singapura merasakan keamanan siber yang kuat, dan mengadvokasi pembentukan norma serta standar dunia maya global [128]. Strategi ini terdiri atas tiga pilar strategis dan dua pendorong dasar (lihat Gambar 3.2).

Pemerintah Singapura menerapkan kepercayaan digital melalui berbagai inisiatif kebijakan, kerangka peraturan, dan program pendidikan yang menargetkan publik serta sektor bisnis. Beberapa langkah penting yang diambil meliputi:

- Kampanye Kesadaran dan Edukasi: Pemerintah melaksanakan kampanye untuk meningkatkan kesadaran masyarakat tentang pentingnya keamanan digital dan langkah-langkah untuk melindungi data pribadi. Kampanye ini melibatkan pelatihan dan materi edukasi yang ditujukan kepada individu maupun perusahaan untuk mengidentifikasi dan menghadapi ancaman siber.
- Kerangka Regulasi dan Kebijakan: Singapura mengembangkan dan menerapkan peraturan ketat yang mengatur privasi dan keamanan data, seperti Personal Data Protection Act (PDPA) [129] dan kebijakan perlindungan data lain yang mengatur tanggung jawab organisasi dalam melindungi data pribadi. Kerangka ini memberikan panduan tentang praktik keamanan siber yang harus diterapkan oleh semua entitas yang terlibat dalam ekonomi digital.
- Teknologi Keamanan Canggih: Singapura menginvestasikan sumber daya dalam teknologi keamanan mutakhir, seperti enkripsi, sistem deteksi intrusi, dan platform analitik keamanan yang digunakan untuk melindungi infrastruktur penting dan data sensitif. Hal ini bertujuan untuk memperkuat perlindungan terhadap aset-aset strategis dari potensi ancaman siber yang semakin kompleks.
- Kemitraan dan Kolaborasi Internasional: Singapura membangun kerja sama internasional untuk menghadapi ancaman siber yang melampaui batas negara. Melalui kolaborasi dengan organisasi internasional dan negara lain, Singapura berpartisipasi dalam berbagi informasi, teknologi, dan praktik terbaik untuk memperkuat keamanan digital di tingkat global.



Gambar 3.2: Tinjauan Umum Strategi Keamanan Siber Singapura 2021 [128]

Inisiatif Kepercayaan Digital Singapura

Singapura telah meluncurkan berbagai inisiatif untuk membangun kepercayaan digital sebagai bagian dari strategi transformasi digitalnya. Inisiatif-inisiatif ini mencakup regulasi, teknologi, kolaborasi, dan edukasi untuk memastikan bahwa ekosistem digital negara tersebut aman, andal, kolaboratif, dan berkelanjutan. Berikut adalah penjelasan rinci mengenai inisiatif-inisiatif utama yang dilakukan oleh Singapura.

1. *Cybersecurity Strategy*
   Pada tahun 2016, Singapura meluncurkan *Singapore's Cybersecurity Strategy* [127] untuk melindungi infrastruktur digital nasional dari ancaman siber. Strategi ini bertujuan untuk memperkuat keamanan jaringan kritis seperti sistem perbankan, energi, transportasi, dan kesehatan.
   Inisiatif utama yang dilakukan adalah sebagai berikut:

   - Pembentukan *Cyber Security Agency of Singapore* (CSA) untuk mengoordinasikan upaya keamanan siber di tingkat nasional.
   - Pengembangan *Critical Information Infrastructure* (CII) untuk melindungi sektor-sektor vital.
   - Peluncuran program pelatihan seperti *Cybersecurity Associates and Technologists* (CSAT) untuk meningkatkan kapasitas tenaga ahli keamanan siber.

   Dokumen ini diperbaharui pada tahun 2021 [128] dengan beberapa perubahan sebagai berikut:

- Fokus Strategis
  Peralihan dari ketahanan infrastruktur nasional menjadi pendekatan *zero trust* dan lebih menekankan pada ketahanan digital menyeluruh.
- Lingkup perlindungan
  Target perlindungan *Critical Information Infrastructure* (CII) diperluas melingkupi bisnis skala kecil dan menengah (SMEs), individu, dan komunitas digital.
- Penguatan Kapabilitas Siber
  Pembangunan kapabilitas nasional dalam mendeteksi, merespons, dan memitigasi ancaman siber diintegrasikan dengan otomasi dan AI.
- Kolaborasi dan Regulasi
  Perluasan kemitraan antara pemerintah dan sektor industri dengan kerja sama internasional, termasuk berbagi intelijen ancaman dan penguatan regulasi untuk layanan digital lintas batas.
- Penguatan Sumber Daya Manusia dan Kesadaran Siber
  Pelatihan tenaga kerja siber melalui program pendidikan dan peningkatan keterampilan menjadi lebih masif dalam membangun budaya keamanan siber di masyarakat, termasuk edukasi bagi individu dan bisnis kecil.

2. *Personal Data Protection Act* (PDPA)
   PDPA [129] adalah undang-undang yang mengatur perlindungan data pribadi individu di Singapura. Undang-undang ini memastikan bahwa organisasi hanya mengumpulkan, menggunakan, dan mengungkapkan data pribadi dengan persetujuan pengguna. Inisiatif utama yang dilakukan termasuk pada amandemen tahun 2020 adalah sebagai berikut:

   - Memperkenalkan aturan baru seperti *mandatory breach notification* (pemberitahuan wajib atas pelanggaran data).
   - Penegakan hukum terhadap organisasi yang gagal melindungi data pengguna, termasuk denda besar sekitar 10% dari omzet tahunan bagi pelanggar.
   - Perluasan konsep persetujuan dengan memperkenalkan "*deemed consent*" sehingga organisasi dapat menggunakan data pribadi tanpa persetujuan namun dibatasi pada kondisi tertentu.
   - Pengenalan pelanggaran pidana bagi individu yang dengan sengaja memperoleh atau mengungkapkan data pribadi secara ilegal.

3. *Trusted Data Sharing Framework*
   Kerangka kerja ini dirancang untuk memfasilitasi pertukaran data antarorganisasi secara aman dan transparan, dengan tujuan mendorong inovasi tanpa mengorbankan privasi atau keamanan data. Inisiatif utama yang dilakukan adalah sebagai berikut:

   - Pengembangan pedoman untuk pertukaran data yang sesuai dengan prinsip *privacy-by-design* [130].

- Kolaborasi dengan industri untuk mengimplementasikan standar *data sharing* yang dapat dipercaya, seperti *Trusted Data Sharing Framework* oleh IMDA/PDPC di Singapura [131] dan skema *International Data Spaces* [132].

4. MyInfo dan SingPass
   MyInfo adalah platform di Singapura yang memungkinkan pengguna SingPass untuk berbagi data pribadi mereka secara aman dan terverifikasi dengan organisasi pemerintah maupun sektor swasta, setelah memberikan persetujuan. SingPass sendiri merupakan identitas digital nasional yang berfungsi sebagai sistem autentikasi tunggal bagi warga untuk mengakses layanan pemerintah dan komersial [133]. Inisiatif utama yang telah dilaksanakan antara lain:

   - Integrasi MyInfo dengan lebih dari 1.000 layanan digital pemerintah dan swasta/industri untuk mempermudah akses serta mengurangi pengisian data berulang [134].
   - Implementasi fitur keamanan seperti autentikasi dua langkah (2FA) atau *multi-factor authentication* (MFA), termasuk SMS-OTP, token, dan autentikasi biometrik melalui aplikasi SingPass, guna melindungi akun pengguna [135].

5. *AI Governance Framework*
   Singapura telah mengembangkan kerangka tata kelola AI agar penggunaan kecerdasan artisial berlangsung secara etis, transparan, dan bertanggung jawab. Dua inisiatif utama adalah sebagai berikut:

   - Publikasi *Model AI Governance Framework* (2019, diperbarui 2020) yang memberikan pedoman praktis bagi organisasi untuk mengelola risiko-risiko AI [136].
   - Peluncuran *AI Verify* oleh IMDA dan PDPC, yaitu *framework* pengujian dan *toolkit self-assessment* yang membantu organisasi melakukan pemeriksaan teknis dan proses agar sesuai dengan prinsip tata kelola AI [137].

6. *National Digital Identity* (NDI)
   Program ini bertujuan menyediakan identitas digital yang aman dan seragam bagi semua warga Singapura. NDI mendukung layanan digital yang efisien dan tepercaya di seluruh sektor publik maupun swasta. Inisiatif utamanya meliputi:

   - Pengembangan aplikasi mobile *SingPass Mobile* yang memudahkan autentikasi dengan biometrik, *passcode*, maupun *two-factor authentication* [138].
   - Ekspansi penggunaan NDI ke sektor perbankan dan asuransi, dengan lembaga swasta seperti OCBC Bank, Prudential, dan Income Insurance yang telah mengintegrasikan SingPass untuk autentikasi dan verifikasi digital [138, 139].

7. *GoSafeOnline Campaign*
   Kampanye *GoSafeOnline* yang diluncurkan oleh CSA Singapura bertujuan untuk meningkatkan kesadaran publik mengenai keamanan siber. Fokus utama kampanye ini adalah mendorong praktik aman di dunia digital, seperti penggunaan kata sandi yang kuat, kewaspadaan terhadap *phishing*, serta pembaruan perangkat lunak secara rutin. Selain penyuluhan melalui materi *online*, kampanye ini juga melibatkan kerja sama dengan organisasi publik dan swasta untuk memperluas jangkauan edukasi keamanan siber [140].

8. *Smart Nation Sensor Platform* (SNSP)
   SNSP merupakan inisiatif pemerintah Singapura yang dikembangkan oleh GovTech untuk mengintegrasikan, mengumpulkan, dan menganalisis data dari berbagai sensor di ruang publik guna mendukung program Smart Nation [141, 142]. Platform ini dirancang agar bersifat *secure* dan *scalable*, dengan fokus pada interoperabilitas perangkat sensor, penerapan mekanisme keamanan data, serta kepatuhan terhadap standar dan regulasi privasi. Inisiatif utamanya meliputi:

   - Penerapan mekanisme enkripsi dan kontrol akses untuk melindungi data sensor.
   - Pemantauan kepatuhan terhadap standar interoperabilitas IoT (misalnya SS 695) dan regulasi privasi nasional.

9. *Blockchain Innovation Programme*
   Singapura aktif mengembangkan teknologi *blockchain* untuk meningkatkan transparansi dan keamanan dalam berbagai sektor, termasuk keuangan, logistik, dan pemerintahan. Inisiatif utama meliputi:

   - Peluncuran platform seperti *TradeTrust*, yang berfungsi sebagai jaringan interoperabilitas untuk pertukaran dokumen perdagangan digital lintas batas [143].
   - Dukungan terhadap perusahaan lokal melalui program R&D dan pengembangan *Proof of Concept* (PoC) di bawah *Singapore Blockchain Innovation Programme* (SBIP), serta kegiatan seperti *hackathon* dan kolaborasi industri-akademik [144, 145].

10. *International Collaboration*
    Singapura bekerja sama dengan organisasi internasional untuk mempromosikan standar global dalam keamanan siber dan privasi data. Inisiatif utama yang dilakukan adalah sebagai berikut:

    - Kerja sama antara Monetary Authority of Singapore (MAS), International Finance Corporation (IFC), dan World Economic Forum (WEF) untuk memajukan kolaborasi digital di pasar negara berkembang [146].
    - Partisipasi aktif dalam *ASEAN Ministerial Conference on Cybersecurity (AMCC)*, termasuk peluncuran fasilitas fisik ASEAN Regional CERT di bawah ASEAN-Singapore Cybersecurity Centre of Excellence (ASCCE) [147].

Analisis Penerapan Kepercayaan Digital Singapura

Pemerintah Singapura telah menerapkan Singapore Cybersecurity Strategy yang komprehensif dan ketat. Namun, tidak semua organisasi memiliki kapasitas untuk mengimplementasikan langkah-langkah keamanan yang diatur dalam strategi nasional tersebut. Hal ini membuat strategi tersebut kurang efektif dalam menghadapi ancaman siber yang dinamis dan kompleks. Untuk mengatasi masalah ini, CSA memperkenalkan solusi alternatif, yaitu SG *Cyber Safe Trustmark* dan *Cyber Hygiene Mark*, sebagai upaya meningkatkan kesiapan keamanan siber di tingkat organisasi [128].
Di sisi perlindungan data pribadi, Singapura mengadopsi PDPA. Meskipun demikian, PDPA tidak secara eksplisit mendefinisikan apa yang dimaksud dengan data pribadi sensitif [148]. Selain itu, PDPA juga tidak mencantumkan hak-hak seperti hak untuk diberi informasi, hak membatasi pemrosesan, hak menolak pemrosesan, dan hak menolak pemrosesan otomatis. Terkait kedaulatan data, PDPA membatasi transfer data pribadi ke luar Singapura, meskipun organisasi telah memberikan jaminan tingkat keamanan yang memadai [149]. PDPA juga mengatur bahwa data hanya boleh disimpan selama diperlukan, dan setelahnya harus dihapus atau di-anonimkan. Namun, seiring perkembangan teknologi, data yang telah di-anonimkan dapat diidentifikasi kembali melalui teknik seperti *cross-referencing* dengan *dataset* lain, sehingga risiko rekonstruksi ulang data tetap ada.
Perlu dicatat bahwa PDPA tidak mengikat lembaga negara, karena awalnya dirancang untuk sektor privat. Untuk mengatasi hal ini, pada tahun 2018, Singapura menetapkan Public Sector (Governance) Act, yang mengatur perlindungan data pribadi di sektor publik, termasuk lembaga negara dan agensi pemerintah. Di sisi lain, upaya Trusted Data Sharing masih menghadapi kendala dalam mencapai kesepakatan dan membangun kepercayaan antarorganisasi. Selain itu, sistem seperti MyInfo dan Singpass juga mengalami tantangan dalam integrasi dengan aplikasi yang sudah ada, yang memerlukan waktu dan berpotensi mengurangi kenyamanan pengguna.

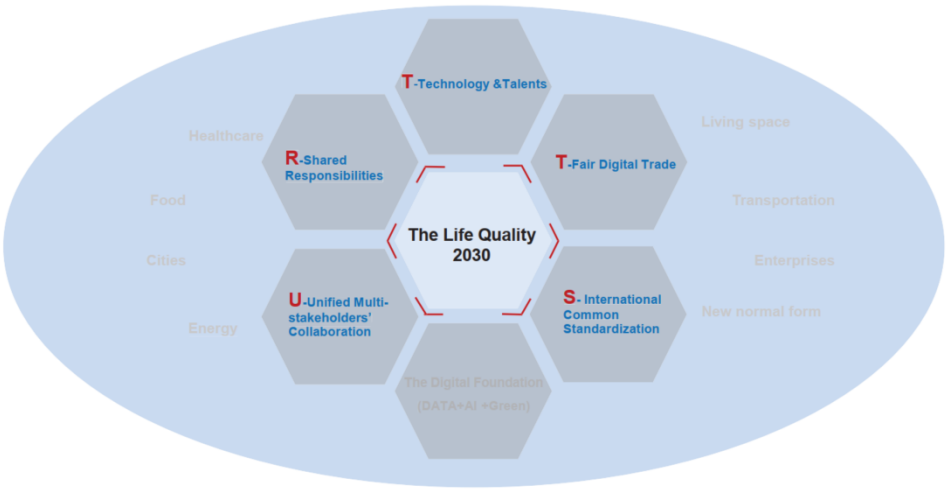
3.1.2 Malaysia

Menuju Dunia Cerdas 2030, visi Malaysia dalam model kepercayaan digital bertujuan meningkatkan kualitas hidup melalui pola makan yang sehat, ramah lingkungan, dan ruang hidup yang lebih nyaman. Masa depan ini diharapkan bebas dari kemacetan dan polusi, memanfaatkan energi ramah lingkungan secara penuh, serta menawarkan layanan digital yang inovatif. Pekerjaan berulang dan berbahaya akan dikelola oleh robot, memberikan lebih banyak waktu bagi individu untuk berkegiatan kreatif dan mengejar minat pribadi. Dalam konteks ini, kepercayaan digital menjadi komponen penting yang mendorong perkembangan di berbagai industri [150]. Berikut merupakan pemetaan kerangka kerja kepercayaan digital Malaysia berdasarkan 5 (lima) pertanyaan tematik.

Mengapa Kepercayaan Digital Penting (*Why*)

Kepercayaan digital memainkan peran penting sebagai dasar ekosistem keamanan siber yang tangguh, mampu menghadapi ancaman, perubahan kebijakan, kemajuan teknologi, serta perubahan ekonomi dan sosial. Selain itu, kepercayaan digital memperkuat daya saing ekonomi digital dan mendukung inovasi layanan, yang pada gilirannya meningkatkan kualitas hidup di era dunia cerdas. Dengan demikian, kepercayaan digital menciptakan dunia yang lebih aman, terhubung, dan berkelanjutan melalui kolaborasi lintas sektor [150].

Tujuan Pengenalan Kepercayaan Digital (*What*)



Gambar 3.3: Model Kepercayaan Digital Malaysia [150]

Kerangka kerja atau model kepercayaan digital di Malaysia mencakup aspek keamanan data, privasi, dan integritas dalam platform serta layanan digital [150]. Perlindungan data, keamanan siber, dan penggunaan teknologi secara etis menjadi fokus utama. Model kepercayaan digital melibatkan berbagai pemangku kepentingan dengan komponen sebagai berikut (lihat Gambar 3.3):

- T - *Technology and Talent*: Pemanfaatan teknologi dan pengembangan talenta yang sesuai untuk mendukung keamanan digital.
- R - *Shared Responsibilities*: Pembagian tanggung jawab antarpemangku kepentingan dalam membangun ekosistem keamanan siber.
- U - *Unified Multi-stakeholders Collaboration*: Kolaborasi dari berbagai pemangku kepentingan, termasuk sektor publik, sektor swasta/industri, masyarakat sipil, dan akademisi.

- S - *International Common Standardization*: Standarisasi internasional untuk memastikan keseragaman dan kepatuhan dalam praktik keamanan siber.
- T - *Fair Digital Trade*: Dukungan terhadap perdagangan digital yang adil untuk meningkatkan daya saing ekonomi secara global.

Komponen-komponen tersebut tidak berdiri sendiri, tetapi saling terkait dalam membangun ekosistem digital yang tepercaya. Sebagaimana yang ditunjukkan pada Gambar 3.3, kelima unsur TRUST mendukung pencapaian visi *Life Quality 2030*. Kepercayaan digital bukan sekadar aspek teknis keamanan siber, melainkan fondasi untuk meningkatkan kualitas hidup masyarakat melalui sektor kesehatan, pangan, energi, kota pintar, transportasi, dan ruang hidup yang lebih berkelanjutan.

Selain itu, model ini menekankan bahwa TRUST bertumpu pada *Digital Foundation* yang terdiri atas data, kecerdasan artifisial (AI), dan prinsip keberlanjutan (*green*). Dengan demikian, pengembangan kepercayaan digital di Malaysia diarahkan tidak hanya untuk melindungi ekosistem digital, tetapi juga untuk mendukung transformasi sosial-ekonomi yang aman, adil, dan berdaya saing global.

Siapa yang Bertanggung Jawab (*Who*)

Model kepercayaan digital Malaysia melibatkan berbagai pemangku kepentingan dalam penyelenggaraannya. Menurut PIKOM [150], model *Digital TRUST* menekankan pentingnya peran lintas-sektor, meliputi pemerintah, swasta/industri, masyarakat, dan akademisi.

- Sektor pemerintahan
  Bertanggung jawab untuk membuat dan menegakkan regulasi, serta menyediakan infrastruktur dan pengawasan dalam penerapan kepercayaan digital [151, 152].
- Sektor swasta/industri
  Berperan dalam mengembangkan dan menerapkan teknologi yang sesuai dengan prinsip-prinsip kepercayaan digital, menjaga keamanan sistem, serta mematuhi standar yang ditetapkan [153].
- Masyarakat
  Berperan untuk mengadvokasi hak-hak individu, meningkatkan kesadaran publik, serta mempromosikan praktik etis dalam ruang digital [150, 152].
- Akademisi
  Berkontribusi melalui penelitian dan pengembangan praktik terbaik (*best practice*) kepercayaan digital, memberikan wawasan terkait teknologi yang berkembang, serta mendukung edukasi publik [152].

Waktu dan Tahapan Implementasi (*When*)

Timeline model penerapan kepercayaan digital di Malaysia diinisiasi melalui beberapa fase strategis di bawah kerangka MyDIGITAL [154] dan Malaysia Cyber Security Strategy (MCSS) 2020–2024 [155]. Tujuan utama dari inisiasi ini adalah membangun keamanan siber yang terintegrasi dengan digitalisasi ekonomi nasional. Berikut tahapan kunci penerapannya:

- Tahun 2021–2022: fokus pada peningkatan literasi digital, dengan pelatihan dan kesadaran tentang keamanan siber untuk meningkatkan adopsi teknologi di berbagai sektor, terutama di pemerintahan dan sektor UMKM. Strategi *Cloud-First* mulai diterapkan di pemerintahan untuk mengadopsi penyimpanan data berbasis *cloud*.
- Tahun 2023–2025: implementasi kerangka kerja standar nasional di bidang keamanan digital yang memprioritaskan kolaborasi publik-swasta/industri. Fase ini mencakup penyempurnaan kebijakan, pengembangan standar internasional, dan penguatan kolaborasi dengan lembaga internasional. *Digital Compass* diperkenalkan untuk membantu perusahaan memahami dan memanfaatkan solusi digital sesuai dengan tingkat kesiapan mereka.
- Tahun 2025 ke atas: fokus pada keberlanjutan dan pertumbuhan ekonomi digital yang terintegrasi di berbagai sektor, termasuk industri strategis, pendidikan, dan layanan publik. Malaysia bertujuan untuk menjadikan keamanan digital dan kepercayaan digital sebagai daya saing nasional yang mendorong inovasi layanan publik dan peningkatan kualitas hidup.

Bagaimana Kepercayaan Digital Diterapkan (*How*)

Kepercayaan digital di Malaysia melibatkan pendekatan terstruktur berbagai pemangku kepentingan dan menekankan kolaborasi lintas sektor. Aspek-aspek utama penerapan model ini antara lain:

- Membuat kerangka regulasi, misalnya *Personal Data Protection Act 2010 (Act 709)* yang baru-baru ini diamandemen untuk memperkuat perlindungan data pribadi [156].
- Mempromosikan kolaborasi antar *stakeholder*, seperti melalui kerja sama PDP Malaysia dengan Futurise dalam pengembangan standar perlindungan data [157].
- Berfokus pada keamanan siber, dengan inisiatif nasional seperti pendirian Malaysia Cyber Security Academy [158].
- Meningkatkan literasi digital melalui program *Rakyat Digital*, yang bertujuan menumbuhkan budaya tanggung jawab dan kesadaran mengenai data pribadi [159].

- Berkolaborasi dengan mitra internasional dalam kerangka kerja lintas batas, termasuk melalui APEC *Cross-Border Privacy Rules* (CBPR) dan perjanjian regional lainnya [160].
- Peningkatan berkelanjutan, di mana pemangku kepentingan didorong untuk beradaptasi dan menyempurnakan strategi mereka berdasarkan perkembangan teknologi dan ancaman yang muncul, agar tetap relevan dalam membangun kepercayaan digital [161].

Inisiatif Kepercayaan Digital Malaysia

Malaysia telah mengambil langkah-langkah signifikan dalam membangun kepercayaan digital sebagai bagian dari upayanya untuk menjadi negara yang lebih maju secara digital. Inisiatif-inisiatif ini mencakup regulasi, infrastruktur teknologi, edukasi publik, dan kolaborasi antara pemerintah, sektor swasta/industri, dan masyarakat. Berikut adalah penjelasan rinci tentang inisiatif kepercayaan digital yang dilakukan oleh Malaysia.

1. Regulasi dan Kebijakan
   - *Personal Data Protection Act* (PDPA) 2010 [162]: PDPA adalah undang-undang utama yang mengatur perlindungan data pribadi di Malaysia. Undang-undang ini menetapkan prinsip-prinsip pengumpulan, penggunaan, dan pengungkapan data pribadi. Tujuannya adalah untuk memastikan bahwa organisasi menggunakan data secara etis dan bertanggung jawab, sehingga meningkatkan kepercayaan masyarakat terhadap layanan digital.
   - *National Cyber Security Policy* (NCSP): NCSP adalah kajian kebijakan nasional yang dirancang untuk melindungi infrastruktur kritis dan sistem informasi dari ancaman siber. Kebijakan ini mencakup strategi untuk meningkatkan kesadaran akan keamanan siber, memperkuat kerangka hukum, dan membangun kapasitas keamanan siber nasional [163].
   - *Cyber Security Act* 2024 [164]: Undang-Undang Keamanan Siber Malaysia yang bertujuan untuk memperkuat pertahanan siber nasional dan meningkatkan ketahanan terhadap ancaman siber yang adaptif. Regulasi ini juga memberikan landasan hukum untuk pembentukan Komite Keamanan Siber Nasional (*National Cyber Security Committee*) serta adanya perhatian terhadap pengelolaan Infrastruktur Informasi Kritis Nasional (NCII).
   - *Digital Malaysia Blueprint* (2021–2030): *Blueprint* ini adalah rencana strategis untuk mempercepat transformasi digital di Malaysia. Salah satu pilar utamanya adalah membangun kepercayaan digital melalui regulasi yang kuat, privasi data, dan keamanan siber.
2. Infrastruktur Teknologi

- *National Fiberisation and Connectivity Plan* (NFCP): Inisiatif pemerintah Malaysia untuk meningkatkan infrastruktur digital dengan memastikan akses internet yang cepat, berkualitas, dan terjangkau di seluruh negeri. Diperkenalkan oleh Kementerian Komunikasi dan Multimedia Malaysia (KKMM), program ini bertujuan untuk mengatasi kesenjangan digital antara kawasan perkotaan dan pedesaan.
- *Government Online Services* 2.0 (GOS 2.0): Inisiatif yang dikelola oleh Unit Pemodenan Tadbiran dan Perancangan Pengurusan Malaysia (MAMPU) untuk meningkatkan kualitas layanan digital pemerintah di Malaysia. Program ini bertujuan untuk menciptakan ekosistem *e-government* yang lebih efisien, aman, dan ramah pengguna.
- *National E-Commerce Strategic Direction*: Inisiatif dari Ministry of Investment pemerintah Malaysia untuk mempercepat pertumbuhan dan adopsi *e-commerce* guna meningkatkan daya saing ekonomi digital negara. Program ini diluncurkan sebagai bagian dari strategi nasional untuk mendukung Transformasi Digital dan memperkuat peran Malaysia dalam perdagangan digital global.
- *Trade and Industry and Sharing Economy Roadmap*: Inisiatif dari Kementerian Perdagangan dan Industri Antarabangsa Malaysia (MITI) yang bertujuan untuk mengoptimalkan sumber daya digital dan mempromosikan model bisnis berbasis platform.
- *MyDIGITAL Initiative* [154]: MyDIGITAL adalah inisiatif pemerintah untuk mendorong adopsi teknologi digital di semua sektor, termasuk pemerintahan, bisnis, dan masyarakat. Salah satu fokusnya adalah membangun infrastruktur digital yang aman, seperti *cloud computing* yang sesuai dengan standar keamanan global.
- *National Digital Identity* (NDI): NDI adalah sistem identitas digital yang memungkinkan warga Malaysia untuk mengakses layanan pemerintah dan swasta/industri secara aman. Sistem ini menggunakan teknologi enkripsi dan autentikasi dua faktor untuk memastikan keamanan dan privasi pengguna.
- *Blockchain Technology*: Pemerintah Malaysia sedang menjajaki penggunaan *blockchain* untuk meningkatkan transparansi dan keamanan dalam berbagai sektor, seperti logistik, keuangan, dan rantai pasokan.

3. Edukasi dan Kesadaran Publik

- *CyberSAFE Program*: Program ini bertujuan untuk meningkatkan kesadaran masyarakat tentang keamanan siber melalui kampanye edukasi dan pelatihan. Targetnya adalah membekali individu, perusahaan, dan institusi dengan pengetahuan tentang cara melindungi diri dari ancaman siber.
- *Digital Literacy Programs*: Pemerintah Malaysia bekerja sama dengan lembaga pendidikan untuk meningkatkan literasi digital masyarakat, termasuk pemahaman tentang privasi data, *phishing*, dan praktik keamanan *online*.

- Kolaborasi dengan Sektor Swasta/Industri: Perusahaan teknologi besar seperti MDEC (Malaysia Digital Economy Corporation) dan Telekom Malaysia (TM) aktif mengadakan lokakarya dan seminar untuk mendidik masyarakat tentang pentingnya kepercayaan digital.

4. Keamanan Siber

   - National Cyber Coordination and Command Centre (NC4): NC4 adalah pusat koordinasi keamanan siber nasional yang bertugas untuk memantau, mendeteksi, dan merespons ancaman siber secara *real-time*. Hal ini untuk memastikan bahwa insiden keamanan siber dapat ditangani dengan cepat untuk meminimalkan dampaknya.
   - CyberSecurity Malaysia: Badan ini bertanggung jawab untuk mengembangkan strategi keamanan siber nasional, menyediakan layanan forensik digital, dan memberikan sertifikasi keamanan kepada organisasi.
   - *Public-Private Partnerships*: Pemerintah Malaysia bekerja sama dengan perusahaan swasta/industri untuk membangun ekosistem keamanan siber yang tangguh. Contohnya, program *CyberSecurity Professional Development* untuk melatih tenaga ahli keamanan siber.

5. Kolaborasi Internasional

   - *ASEAN Collaboration*: Malaysia aktif berpartisipasi dalam inisiatif regional ASEAN untuk membangun kepercayaan digital, seperti *ASEAN Cybersecurity Cooperation Strategy*. Kerjasama ini bertujuan untuk memperkuat keamanan siber lintas batas dan mempromosikan standar kepercayaan digital yang seragam di wilayah ASEAN.
   - *Global Partnerships*: Malaysia bekerja sama dengan organisasi internasional seperti International Telecommunication Union (ITU) dan World Economic Forum (WEF) untuk mengadopsi praktik terbaik dalam keamanan siber dan privasi data.

6. Fokus pada AI dan Teknologi Baru

   - *AI Governance Framework*: Pemerintah Malaysia sedang mengembangkan kerangka tata kelola AI untuk memastikan bahwa teknologi AI digunakan secara etis dan bertanggung jawab. Hal ini mencakup transparansi algoritma, perlindungan privasi, dan mitigasi bias dalam pengambilan keputusan berbasis AI.
   - *Smart City Initiatives*: Kota-kota pintar seperti Cyberjaya dan Putrajaya sedang dikembangkan dengan fokus pada keamanan digital dan privasi warga. Teknologi IoT digunakan dengan hati-hati untuk memastikan bahwa data yang dikumpulkan aman dan digunakan sesuai dengan persetujuan pengguna.

Analisis Penerapan Kepercayaan Digital Malaysia

Meskipun pemerintah Malaysia telah memperkenalkan *National Cyber Security Policy* (NCSP), implementasinya masih menghadapi tantangan, terutama dalam hal koordinasi antarberbagai agen yang terlibat. Tantangan ini mencakup koordinasi respons terhadap ancaman dan keterbatasan sumber daya yang menyebabkan kebijakan tidak berjalan secara optimal [165, 166]. Selain itu, faktor politik juga sering memengaruhi keputusan yang diambil, sehingga menghambat efektivitas kebijakan tersebut [167, 166].

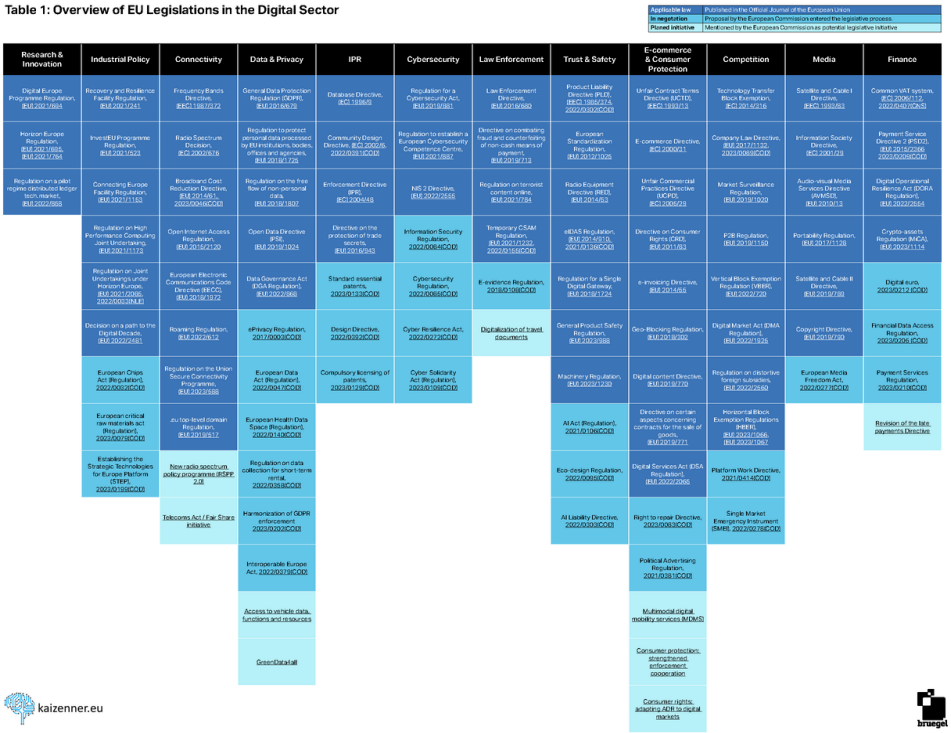
Sementara itu, penerapan *Malaysia Digital Economy Blueprint* atau *MyDIGITAL* juga terkendala oleh perbedaan tingkat kesiapan dan kapasitas antara sektor publik dan swasta dalam memenuhi langkah-langkah strategis yang diusulkan. Beberapa target dinilai terlalu ambisius sehingga memerlukan kolaborasi lintas sektor yang lebih kuat untuk memastikan keberhasilan implementasinya [167, 168].

Di sisi lain, meskipun *Personal Data Protection Act* (PDPA) telah diberlakukan sejak 2010, ruang lingkupnya masih terbatas karena tidak mencakup pemerintah federal maupun pemerintah negara bagian [169, 170]. Hal ini menimbulkan celah dalam perlindungan data yang justru penting di era digital. Selain itu, kesadaran dan literasi masyarakat tentang pentingnya privasi data masih perlu ditingkatkan agar kebijakan ini dapat diimplementasikan secara lebih efektif [171, 172].

3.1.3 Uni Eropa

Dalam era transformasi digital yang terus berkembang, Uni Eropa (*European Union* - EU) telah mengambil langkah strategis untuk membangun dan memperkuat kepercayaan digital sebagai faktor penting dalam ekonomi dan masyarakat digital. Kepercayaan digital tidak hanya menjadi prasyarat untuk mendorong inovasi dan pertumbuhan ekonomi, tetapi juga berperan sebagai kunci dalam melindungi hak-hak digital warga negara, memastikan keamanan siber, serta menjaga integritas ekosistem digital.

Melalui berbagai kebijakan dan kerangka kerja yang komprehensif, Uni Eropa berupaya menciptakan lingkungan digital yang aman, transparan, dan dapat diandalkan bagi semua pemangku kepentingan. Kerangka kerja kepercayaan digital tersebut dirancang untuk menghadapi tantangan kompleks yang timbul akibat dinamika teknologi, risiko siber, serta perubahan sosial dan ekonomi. Pada saat yang sama, EU memastikan bahwa nilai-nilai fundamental, seperti privasi, keamanan, dan keberlanjutan, tetap terjaga [173, 174, 175, 176, 177]. Beberapa aspek dari kerangka kerja ini dapat dilihat pada Gambar 3.4.



Gambar 3.4: EU *legislations* pada sektor digital [174]

Mengapa Kepercayaan Digital Penting (*Why*)

Kepercayaan digital merupakan elemen krusial bagi pengembangan layanan dan teknologi digital yang andal dan berkelanjutan. Tingkat kepercayaan ini tidak hanya mendorong inovasi, tetapi juga memastikan penerimaan pengguna dan menjaga integritas interaksi digital [178]. Di Uni Eropa, perlindungan privasi menjadi prioritas utama untuk melindungi data dan identitas pengguna dari risiko penipuan dan pencurian.

Salah satu bukti nyata dari komitmen ini adalah penerapan *General Data Protection Regulation* (GDPR) yang berlaku secara langsung di semua negara anggota Uni Eropa dan wilayah ekonomi Eropa (679/2016/EC) [179]. GDPR membentuk kepercayaan digital masyarakat dengan memberikan hak atas perlindungan data, baik saat diproses oleh pengguna data maupun saat dipindahkan ke pihak lain. Selain GDPR, Uni Eropa juga mengembangkan *European Self-Sovereign Identity Framework* (eSSIF), yang bertujuan memberikan kontrol penuh kepada individu atas informasi mereka ketika digunakan oleh situs web, layanan, dan aplikasi digital. Dengan pendekatan SSI, pengguna tidak lagi bergantung pada penyedia identitas terpusat seperti *Facebook Connect* atau *Google Sign-In*, yang selama ini

mendominasi pengelolaan identitas [180]. Konsep ini diperkuat oleh teknologi seperti *Decentralized Identifiers* (DIDs), yang menghadirkan mekanisme autentikasi terdistribusi untuk mendukung kedaulatan data dan meningkatkan kepercayaan digital dalam ekosistem yang semakin terdesentralisasi.

Kepercayaan digital juga memiliki dampak signifikan terhadap kelangsungan dan daya saing bisnis. Menurut penelitian McKinsey [52], perusahaan yang dianggap sebagai pemimpin dalam kepercayaan digital (*digital trust leaders*) 1,6 kali lebih disukai oleh konsumen dan secara global mengalami peningkatan pendapatan *Earnings Before Interest and Taxes* (EBIT) setidaknya 10%. Hal ini menunjukkan bahwa investasi dalam keamanan, privasi, dan transparansi bukan hanya kewajiban regulatif, melainkan juga strategi bisnis yang memberikan nilai kompetitif.

Tujuan Pengenalan Kepercayaan Digital (*What*)

Kepercayaan digital mencakup tiga aspek utama: keamanan, privasi, dan kredibilitas sistem digital. Aspek-aspek ini diatur dalam regulasi *electronic IDentification, Authentication and trust Services* (eIDAS), yang mencakup berbagai layanan kepercayaan seperti *Electronic Signature* (eSignature), *Electronic Seal* (eSeal), *Electronic Timestam*p (eTimestamp), *Website Authentication Certificates* (WACs), dan *Electronic Registered Delivery Service* (eDelivery) [176]. Uni Eropa, melalui Komisi Eropa, memperluas cakupan kepercayaan digital dengan memasukkan privasi sebagai aspek penting melalui GDPR [179] dan EU Digital Identity (EUDI), yang ditetapkan dalam revisi regulasi eIDAS 2.0 [181]. Selain itu, kredibilitas sistem atau produk digital dijaga melalui *EU Cybersecurity Act* [182] dan *Cyber Resilience Act* [183], dengan implementasi dan pengawasan yang banyak melibatkan European Union Agency for Cybersecurity (ENISA).

Siapa yang Bertanggung Jawab (*Who*)

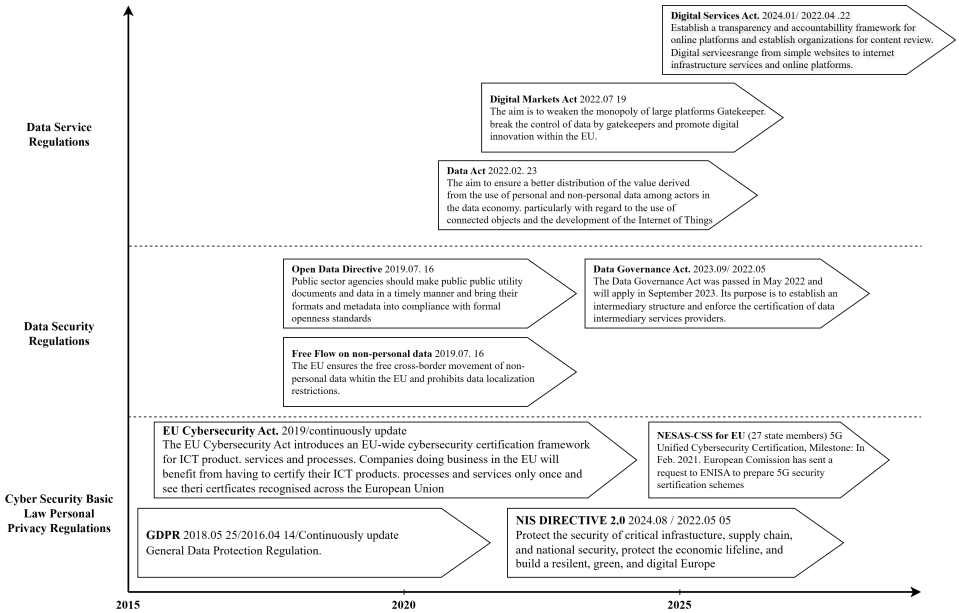
Tanggung jawab utama dalam membangun kepercayaan digital di Uni Eropa berada di tangan Komisi Eropa, Parlemen Eropa, dan Dewan Uni Eropa. Komisi ini terdiri atas perwakilan dari 27 negara anggota Uni Eropa yang memiliki wewenang untuk membuat regulasi yang berlaku di seluruh wilayah Uni Eropa (Regulation - EU - 2024/1183 - EN - EUR-Lex). European Union Agency for Cybersecurity (ENISA) adalah badan yang dibentuk untuk meningkatkan kepercayaan terhadap produk digital, layanan, dan proses melalui skema sertifikasi yang sesuai dengan kebutuhan negara-negara anggota Uni Eropa. ENISA juga bertugas menyesuaikan strategi keamanan siber untuk menghadapi tantangan masa depan [184].

Pemangku kepentingan dalam kerangka kerja kepercayaan digital mencakup warga Eropa, warga negara asing yang tinggal di Eropa, serta bisnis yang beroperasi di Uni Eropa. Selain itu, pemerintah, swasta/industri, dan organisasi yang menyediakan layanan identitas digital serta layanan kepercayaan juga terlibat aktif dalam memastikan kepatuhan terhadap regulasi seperti eIDAS, GDPR, *EU Cyber Security Act*, dan *EU Cyber Resilience Act*. Penyedia layanan yang memenuhi persyaratan

eIDAS dapat dimasukkan dalam *The European Union Trusted Lists* (EUTL), yang menjadi indikator kepercayaan dan keandalan produk serta layanan digital.

Waktu dan Tahapan Implementasi (*When*)

Uni Eropa membangun kepercayaan digital tidak dalam waktu singkat. Jika dihitung dari inisiasi, maka kepercayaan digital dibangun melalui proses yang berlangsung selama beberapa dekade. Serangkaian regulasi diperkenalkan secara bertahap dengan tujuan membangun kepercayaan publik terhadap tata kelola digital, keamanan data, serta integritas pasar digital. Gambar 3.5 menunjukkan tahapan regulasi utama dalam rentang waktu 2015–2025, yang dikelompokkan mulai dari regulasi dasar terkait keamanan siber dan privasi, kemudian berlanjut pada tata kelola dan keamanan data, hingga akhirnya pada regulasi yang mengatur layanan digital.



Gambar 3.5: Garis waktu peraturan terkait *Cybersecurity* EU diolah kembali dari [175, 176, 177]

Pada lapisan dasar, Uni Eropa memperkenalkan regulasi yang berfokus pada identitas elektronik, perlindungan privasi, dan keamanan siber. Tonggak penting dimulai dengan *eIDAS Regulation* tahun 2014 [176], yang menetapkan kerangka identitas elektronik dan layanan kepercayaan. Regulasi berikutnya adalah *General Data Protection Regulation (GDPR)* tahun 2016, berlaku penuh pada 2018, yang menjadi kerangka hukum perlindungan data pribadi paling komprehensif di dunia [179]. Regulasi *Network and Information Security Directive (NIS)* 2016, kemudian diperbarui menjadi *NIS 2* pada 2022, memperluas cakupan keamanan siber [185,

186]. Selain itu, *EU Cybersecurity Act* tahun 2019 memperkenalkan kerangka sertifikasi keamanan siber di tingkat Uni Eropa [187].

Tahap selanjutnya menekankan keterbukaan dan tata kelola data. Regulasi *Free Flow of Non-Personal Data* (2018) memastikan bahwa data nonpribadi dapat bergerak bebas di seluruh EU [188]. *Open Data Directive* (2019) mendorong keterbukaan data publik untuk inovasi dan transparansi [189]. Lebih jauh, *Data Governance Act* (2022) memperkenalkan mekanisme perantara data dan konsep *data altruism* untuk meningkatkan kepercayaan dalam berbagi data [190].

Pada tahap lanjutan, regulasi berkembang ke arah ekonomi digital. *Data Act* (2022) dirancang untuk memastikan distribusi nilai yang lebih adil dari pemanfaatan data, khususnya data IoT [191]. Sementara itu, *Digital Markets Act (DMA)* (2022) mengatur dominasi perusahaan besar penyedia platform atau *gatekeepers* agar persaingan tetap sehat [192]. Regulasi puncaknya adalah *Digital Services Act (DSA)* (2022, berlaku penuh 2024), yang menetapkan transparansi dan akuntabilitas bagi penyedia layanan daring [193].

Lebih baru, Uni Eropa memperluas regulasi ke ranah kecerdasan buatan dan ketahanan produk digital. *Artificial Intelligence Act (AI Act)* (2024) mengatur penggunaan sistem AI agar etis, transparan, dan aman [194]. *EU Cyber Resilience Act* (2023) melengkapi regulasi keamanan dengan memastikan perangkat digital, termasuk IoT, memenuhi standar keamanan minimum [195]. Selain itu, inisiatif *EU Digital Identity (EUDI)* dan *EU Digital Identity Wallet* memperkuat implementasi identitas digital lintas negara anggota, melanjutkan kerangka eIDAS [196, 197].

Proses pengembangan kerangka regulasi ini berlangsung secara bertahap dan berlapis. Masing-masing regulasi memiliki tujuan yang saling melengkapi: ada yang menekankan perlindungan privasi individu, ada yang berfokus pada penguatan infrastruktur keamanan siber, dan ada pula yang mengatur tata kelola serta pemanfaatan data untuk inovasi ekonomi digital. Untuk memberikan gambaran lebih rinci, berikut adalah regulasi-regulasi kunci yang membentuk dasar kepercayaan digital Uni Eropa dari 2014 hingga 2024:

- eIDAS (*electronic IDentification, Authentication and trust Services*)
  Regulasi Uni Eropa No. 910/2014/EC, yang diadopsi pada 23 Juli 2014 dan berlaku efektif mulai 1 Juli 2016, menetapkan kerangka kerja untuk identitas elektronik dan layanan kepercayaan (*trust services*) [176]. Tujuannya adalah menjamin keamanan transaksi elektronik antara warga negara, bisnis, dan otoritas publik. Regulasi ini juga mengamanatkan pembentukan identitas elektronik dan tanda tangan elektronik (*e-signature*) yang sah di seluruh Uni Eropa. Kejelasan proses bisnis dalam penerapan identitas elektronik dan layanan kepercayaan menjadi fokus utama, guna memastikan integritas dan keamanan penggunaannya di berbagai sektor.

- *General Data Protection Regulation* (GDPR)
  Regulasi Uni Eropa 679/2016/EC, yang mengatur privasi informasi di Uni Eropa dan Wilayah Ekonomi Eropa (EEA), disahkan pada 14 April 2016 dan mulai berlaku pada 25 Mei 2018 [179]. Sebagai regulasi, GDPR dapat

langsung diterapkan tanpa perlu transposisi ke hukum nasional. Namun, regulasi ini memberikan fleksibilitas bagi negara anggota untuk memodifikasi beberapa ketentuannya. GDPR juga telah menginspirasi regulasi serupa di luar Uni Eropa, seperti UK GDPR di Inggris setelah Brexit dan *California Consumer Privacy Act* (CCPA) di Amerika Serikat, yang diadopsi pada 28 Juni 2018. Pelaksanaan GDPR diawasi oleh Data Protection Authority (DPA) di masing-masing negara anggota, yang memperhatikan baik hukum GDPR maupun hukum lokal.

- *Open Data Directive*
  Regulasi Uni Eropa 1024/2019/EC dirancang untuk memperkuat penggunaan data publik baik untuk tujuan komersial maupun nonkomersial [189]. Penggunaan format terhadap data publik yang dapat diakses oleh khalayak umum maupun mesin diwajibkan sehingga meningkatkan kompetensi di pasar informasi. Data untuk penelitian khususnya yang dibiayai oleh publik harus mengikuti prinsip terbuka secara *default*.

- *Free Flow of Non-Personal Data*
  Regulasi Uni Eropa 1807/2018/EC yang dirancang untuk memastikan bahwa data yang tidak berhubungan dengan orang tertentu dapat bergerak bebas di seluruh Uni Eropa sehingga memudahkan pengolahan dan penyimpanan data di beberapa negara anggota [188].

- *Data Governance Act*
  Regulasi Uni Eropa 868/2022/EC ditetapkan untuk meningkatkan kepercayaan dalam berbagi data baik organisasi maupun lembaga negara [190]. Meskipun adanya penggunaan data kembali oleh lembaga lain diatur juga adanya layanan intermediasi data sehingga layanan berbagi data ini menjadi dapat diandalkan. Konsep data altruisme juga diatur dalam peraturan ini untuk memperluas dampak sosial kemasyarakatan.

- *Artificial Intelligence Act* (AI Act)
  Regulasi Uni Eropa 1689/2024/EC dirancang untuk menciptakan kerangka hukum yang seragam bagi pengembangan, penawaran, dan penggunaan sistem kecerdasan artifisial (AI) di Uni Eropa [194]. Regulasi ini juga bertujuan untuk memastikan perlindungan kesehatan, keselamatan, hak dasar, dan hak lingkungan.

- *EU Digital Identity* (EUDI)
  EU Digital Identity diperkenalkan oleh Presiden Komisi Eropa, Ursula Von Der Leyen, pada 16 September 2020, sebagai respons terhadap meningkatnya kekhawatiran terkait penggunaan data pribadi dalam aplikasi digital. Pada 3 Juni 2021, Komisi Eropa menerbitkan *Commission Recommendation* yang melibatkan negara-negara anggota dalam pengembangan *Toolbox*, sebuah perangkat yang mencakup *Architecture and Reference Framework* (ARF) untuk eIDAS. *Toolbox* ini dirancang untuk melengkapi regulasi EUDI dan membangun kerangka kerja yang kuat untuk identifikasi dan autentikasi

digital berbasis standar umum di seluruh Uni Eropa, guna memastikan tingkat kepercayaan yang tinggi dalam transaksi digital.

- *EU Digital Identity Wallet*
  Pada 1 April 2023, Uni Eropa meluncurkan empat proyek besar untuk pengembangan identitas digital. Proyek pertama, *EU Digital Identity Wallet Consortium* (EWC), bertujuan meningkatkan manfaat identitas digital melalui *Digital Travel Credentials* yang dapat digunakan secara universal [197]. Proyek kedua, *POTENTIAL*, fokus pada inovasi dan kolaborasi di enam sektor utama: layanan pemerintah, perbankan, telekomunikasi, surat izin mengemudi, tanda tangan elektronik, dan kesehatan. Proyek ketiga, NOBID, merupakan kolaborasi negara-negara Nordik, Baltik, Italia, dan Jerman, yang menguji coba penggunaan *EU Digital Identity Wallet* untuk pembayaran produk dan layanan. Proyek keempat, DC4EU, mendukung sektor publik dan swasta/industri dalam pendidikan dan jaminan sosial melalui infrastruktur layanan digital lintas negara.

- *The European Union Trusted Lists* (EUTL)
  EUTL adalah daftar yang terdiri atas lebih dari 200 Trust Service Providers (TSPs) yang terakreditasi dan memenuhi regulasi eIDAS. Pasal 22 eIDAS mewajibkan setiap negara anggota untuk membuat, memelihara, dan mempublikasikan EUTL dalam format yang aman dan dapat diproses secara otomatis.

- *Network and Information Security Directive* (*NIS Directive*)
  Regulasi Uni Eropa No. 1148/2016/EU ini bertujuan meningkatkan keamanan siber di seluruh negara anggota. *NIS Directive* mencakup langkah-langkah mitigasi risiko, tata cara pelaporan insiden, rencana tanggap darurat, dan kerjasama antarotoritas yang berwenang untuk meningkatkan ketahanan bisnis dan perlindungan data [185].

- *Network and Information Security* 2 (NIS2)
  NIS2, yang ditetapkan pada 16 Januari 2023, merupakan perluasan dari *NIS Directive*. Regulasi ini menetapkan tingkat keamanan siber yang lebih tinggi dan memperluas cakupan sektor yang diatur, termasuk sektor esensial dan vital. NIS2 mewajibkan negara anggota untuk memastikan manajemen risiko keamanan siber, pelatihan khusus, dan penilaian keamanan rantai pasokan. Regulasi ini juga menekankan pentingnya penanganan insiden siber secara proaktif. Negara anggota diwajibkan mengadopsi dan mensosialisasikan langkah-langkah kepatuhan paling lambat 17 Oktober 2024.

- *EU Cyber Security Act*
  Regulasi Uni Eropa No. 881/2019/EC ini memberikan mandat kepada European Union Agency for Cybersecurity (ENISA) untuk mengembangkan kerangka kerja sertifikasi produk, layanan, dan proses *Information and Communication Technology* (ICT) [187]. Regulasi ini mulai berlaku penuh pada 28 Juni 2021. Pada 18 April 2023, Komisi Eropa mengusulkan amandemen untuk memenuhi

kebutuhan masa depan, termasuk *managed security services* seperti *incident response*, *penetration testing*, *security audits*, dan *consultancy*.

- *EU Cyber Resilience Act*
  Diperkenalkan pertama kali pada September 2021, *EU Cyber Resilience Act* bertujuan mengisi celah regulasi antara produk digital dan produk ICT. Regulasi ini mencakup perangkat seperti *Internet of Things* (IoT), kamera terkoneksi, dan perangkat cerdas lainnya. Pada 30 November 2023, regulasi ini disepakati oleh negara anggota Uni Eropa sebagai pelengkap kerangka kerja keamanan siber yang ada, guna memastikan keamanan dan kepercayaan digital yang lebih luas [195].

Proses bertahap ini menunjukkan bahwa Uni Eropa membangun kepercayaan digital melalui strategi regulasi yang berlapis. Dimulai dengan perlindungan individu melalui GDPR dan penguatan infrastruktur keamanan lewat *EU Cybersecurity Act* serta *NIS Directive*, regulasi kemudian berkembang pada aspek tata kelola dan keterbukaan data melalui *Open Data Directive* dan *Data Governance Act*. Selanjutnya, pengaturan meluas ke sektor ekonomi data dengan *Data Act* dan *Digital Markets Act*, dan pada akhirnya menyentuh ekosistem layanan digital secara menyeluruh melalui *Digital Services Act*. Dengan pendekatan yang sistematis dan berlapis, Uni Eropa berhasil menata landasan kepercayaan digital yang tidak hanya melindungi privasi, tetapi juga mendorong persaingan sehat, keterbukaan, dan akuntabilitas di era digital.

Bagaimana Kepercayaan Digital Diterapkan (*How*)

Uni Eropa membangun kepercayaan digital melalui serangkaian kebijakan strategis di bidang keamanan siber, perlindungan data, dan tata kelola teknologi digital. Strategi Keamanan Siber Uni Eropa [198] menjadi pilar utama dalam mewujudkan ekosistem digital yang aman dan andal. Hal ini tercermin dalam implementasi *Network and Information Security Directive* (*NIS Directive*) dan pembaruannya melalui NIS2, yang berfungsi sebagai kerangka kerja komprehensif untuk keamanan siber lintas sektor. Di samping itu, *EU Cybersecurity Act* dan *EU Resilience Act* memperluas cakupan perlindungan dengan memperkuat sertifikasi dan ketahanan digital.

Sebagai bagian dari strategi tersebut, Uni Eropa juga membentuk *Joint Cyber Unit* (JCU) sebagai platform koordinasi antarinstitusi dan lembaga keamanan digital. JCU bekerja berdampingan dengan ENISA dan *Computer Emergency Response Team* (CERT-EU) guna meningkatkan respons dan kolaborasi terhadap insiden siber lintas negara.

Di ranah perlindungan data, Uni Eropa menerapkan *General Data Protection Regulation* (GDPR) yang memberikan kendali penuh kepada individu atas pemrosesan dan peredaran data pribadi mereka. Untuk data nonpribadi, *Open Data Directive* dan *Free Flow of non-Personal Data Regulation* mengatur pemanfaatannya agar tetap mendukung keterbukaan sekaligus menjaga kepercayaan pengguna.

Identitas digital juga menjadi aspek krusial dalam kepercayaan digital. Uni Eropa mengembangkan *European Digital Identity* (EUDI), termasuk *EUDI Wallet*, yang memungkinkan transaksi elektronik yang aman dan tepercaya. Kepercayaan terhadap layanan dan identitas digital diperkuat melalui *EU Trusted List* (EUTL), yang memuat entitas penyedia layanan tepercaya. Semua ini berada dalam kerangka eIDAS, yang merupakan standar untuk layanan identifikasi dan tanda tangan elektronik di wilayah Uni Eropa. Untuk memperkuat ekosistem digital, Uni Eropa juga memberlakukan *Digital Services Act* dan *Digital Markets Act*, yang tidak hanya menjamin perlindungan hak pengguna dan penyedia layanan digital, tetapi juga menyediakan kerangka *co-regulatory*. Hal ini mencakup *EU Code of Practice on Disinformation*, yang ditujukan untuk mengatasi penyebaran informasi palsu serta memastikan akuntabilitas platform dalam menangani akun palsu dan konten yang merugikan.

Inisiatif kepercayaan digital turut diperluas ke teknologi baru, seperti *blockchain* dan kecerdasan artifisial. Melalui *European Blockchain Partnership* dan *Blockchain Strategy*, Uni Eropa membangun infrastruktur layanan *blockchain* yang tepercaya, aman, dan efisien untuk mendukung layanan publik lintas batas. Sementara itu, *Artificial Intelligence Act* (AI Act) disusun untuk memastikan bahwa pengembangan dan penggunaan AI tetap berada dalam kerangka etis dan legal, sejalan dengan Piagam Hak Dasar Uni Eropa, sehingga dapat mendorong adopsi AI yang bertanggung jawab dan dapat dipercaya.

Inisiatif Kepercayaan Digital Uni Eropa

Uni Eropa telah mengambil langkah strategis dalam membangun kepercayaan digital guna menciptakan ekosistem yang aman, transparan, dan kolaboratif. Berbagai inisiatif dirancang untuk melindungi hak individu, memperkuat keamanan siber, serta memastikan pemanfaatan teknologi secara etis dan bertanggung jawab. Berikut ini disajikan uraian mengenai inisiatif utama yang menjadi dasar kebijakan kepercayaan digital di kawasan Uni Eropa.

1. Regulasi perlindungan Data: *General Data Protection Regulation* (GDPR)
   GDPR adalah regulasi EU yang diberlakukan pada tahun 2018 untuk melindungi privasi data warga negara EU [179]. Regulasi ini menetapkan standar global untuk perlindungan data pribadi dan memberikan kontrol yang lebih besar kepada individu atas data mereka.
   Tujuan Utama:
   - Memberikan transparansi mengenai bagaimana data dikumpulkan, diproses, dan disimpan.
   - Memastikan organisasi bertanggung jawab atas pelanggaran data atau penggunaan data yang tidak sah.
   - Mengharuskan persetujuan eksplisit dari pengguna sebelum mengumpulkan data pribadi.

Dampak Global:

- GDPR menjadi model bagi banyak negara lain dalam merancang undang-undang perlindungan data.
- Perusahaan di seluruh dunia harus mematuhi GDPR jika mereka menangani data warga EU.

2. *Digital Services Act* (DSA) dan *Digital Markets Act* (DMA)
   DSA bertujuan untuk menciptakan aturan yang lebih adil dan aman untuk platform digital, seperti media sosial, *marketplace*, dan mesin pencari [199].
   Fokus utamanya adalah:

   - Melawan konten ilegal (misalnya, ujaran kebencian, informasi palsu).
   - Meningkatkan transparansi algoritma rekomendasi.
   - Melindungi hak pengguna dan memastikan platform bertanggung jawab atas konten yang mereka *host*.

   Digital Markets Act (DMA) menargetkan "*gatekeeper*" besar (perusahaan teknologi raksasa seperti Google, Amazon, dan Apple) untuk mencegah praktik anti-persaingan. Aturan ini memastikan bahwa perusahaan besar tidak menyalahgunakan posisi dominan mereka untuk membatasi inovasi atau merugikan konsumen [200].
   Tujuan Bersama:

   - Membangun pasar digital yang lebih adil, terbuka, dan kompetitif.
   - Meningkatkan kepercayaan pengguna terhadap platform digital.

3. *European Cybersecurity Strategy*
   Strategi ini dirancang untuk melindungi infrastruktur digital EU dari ancaman siber dan memastikan keamanan sistem kritis [182, 201].
   Komponen Utama:

   - *EU Cybersecurity Act* (2019):
     - Membentuk European Union Agency for Cybersecurity (ENISA) sebagai badan utama untuk koordinasi keamanan siber.
     - Menetapkan skema sertifikasi keamanan siber untuk produk, layanan, dan proses.
   - *Joint Cyber Unit*: Sebuah unit kolaboratif untuk merespons insiden siber lintas negara anggota EU.
   - *NIS2 Directive*: Revisi dari *Network and Information Systems Directive* untuk memperkuat kerangka keamanan siber di sektor-sektor penting seperti energi, transportasi, dan kesehatan.

   Tujuan:

   - Meningkatkan resiliensi siber di seluruh EU.

- Memastikan bahwa organisasi memiliki kapasitas untuk mendeteksi, mencegah, dan merespons serangan siber.

4. *Artificial Intelligence Act* (AI Act)
   AI Act adalah proposal EU untuk mengatur pengembangan dan penggunaan kecerdasan artifisial (AI) berdasarkan tingkat risiko [202].
   Pendekatan Berbasis Risiko:

   - Risiko Tidak Dapat Diterima: Larangan total terhadap AI yang dianggap membahayakan hak asasi manusia (misalnya, pengawasan massal menggunakan pengenalan wajah).
   - Risiko Tinggi: AI yang digunakan dalam sektor-sektor penting (kesehatan, pendidikan, dan kepolisian) harus mematuhi persyaratan ketat, termasuk audit dan transparansi.
   - Risiko Rendah: AI dengan dampak minimal hanya memerlukan pedoman sukarela.

   Tujuan:

   - Memastikan bahwa AI digunakan secara etis dan bertanggung jawab.
   - Meningkatkan kepercayaan publik terhadap teknologi AI.

5. *European Blockchain Partnership* (EBP) dan *Blockchain Strategy*
   EU telah membentuk *European Blockchain Partnership* untuk mendorong pengembangan *blockchain* sebagai teknologi yang transparan dan aman [203].
   Inisiatif Utama:

   - Pengembangan *European Blockchain Services Infrastructure* (EBSI) untuk menyediakan layanan *blockchain* lintas negara anggota.
   - Penerapan *blockchain* dalam bidang seperti rantai pasokan, identitas digital, dan kontrak pintar.

   Tujuan:

   - Meningkatkan transparansi dan kepercayaan dalam transaksi digital.
   - Mengurangi ketergantungan pada entitas pusat (desentralisasi).

6. *EU Code of Practice on Disinformation*
   Kode Etik ini dirancang untuk memerangi disinformasi *online* di platform digital [204].
   Langkah-Langkah Utama:

   - Platform besar seperti Facebook, Google, dan Twitter diminta untuk mengambil tindakan aktif melawan konten palsu.
   - Meningkatkan transparansi iklan politik dan kampanye disinformasi.

   Tujuan:

- Meningkatkan literasi digital masyarakat.
- Memastikan bahwa informasi *online* dapat dipercaya.

7. *Horizon Europe* dan Investasi dalam Teknologi Digital
   Horizon Europe adalah program penelitian dan inovasi EU senilai €95,5 miliar untuk mendukung proyek-proyek teknologi digital [205]. Fokus Utama:

   - Pengembangan teknologi yang aman dan berkelanjutan.
   - Mendukung *startup* dan perusahaan kecil untuk berinovasi dalam bidang keamanan siber, AI, dan *blockchain*.

   Tujuan:

   - Mendorong inovasi yang selaras dengan nilai-nilai EU seperti privasi, keamanan, dan transparansi.

Analisis Penerapan Kepercayaan Digital Uni Eropa

Meskipun Uni Eropa telah menetapkan berbagai regulasi yang bersifat mengikat tidak hanya bagi negara anggotanya, tetapi juga bagi subjek di Kawasan Ekonomi Eropa, penerapannya tetap menghadapi sejumlah tantangan. Salah satu tantangan utama terletak pada perbedaan persepsi mengenai dasar pemrosesan data pribadi. Berdasarkan GDPR, data dapat diproses secara sah apabila memenuhi salah satu dari lima dasar hukum, yaitu persetujuan, kepentingan vital, kewajiban hukum, kepentingan publik, atau pelaksanaan kontrak. Namun, dalam praktiknya, interpretasi terhadap dasar-dasar ini tidak selalu seragam antarnegara maupun antarentitas pengendali data. Misalnya, *Data Protection Act* 2018 di Inggris, meskipun secara umum mengadopsi ketentuan GDPR dan memiliki definisi yang serupa untuk pengendali data (*data controller*) dan prosesor data (*data processor*), menunjukkan perbedaan dalam konsep subjek data (*data subject*). GDPR mendefinisikan *data subject* secara lebih komprehensif, sehingga membuka ruang bagi *data controller* dan *data processor* untuk saling berbagi data pribadi selama dilakukan dengan aman, adil, dan proporsional [206].

Selain itu, GDPR juga menetapkan sejumlah pengecualian terhadap perlindungan data pribadi. Penggunaan data dalam konteks domestik, seperti pertukaran informasi antaranggota keluarga atau teman, tidak termasuk dalam cakupan regulasi ini. Demikian pula, pemrosesan data untuk kepentingan penegakan hukum, termasuk investigasi kepolisian atau operasi intelijen, memperoleh pengecualian tertentu. Namun, celah tetap muncul dalam situasi darurat. GDPR tidak secara eksplisit melarang pertukaran data pribadi dalam kondisi gawat darurat, yang berpotensi dimanfaatkan oleh pihak tidak bertanggung jawab untuk mengakses atau menyebarkan data tanpa dasar hukum yang kuat [207].

Di lapangan, prinsip kepercayaan digital yang menjadi landasan GDPR belum sepenuhnya terwujud. Misalnya, hak untuk "dilupakan" (*right to be forgotten*), yang seharusnya menjamin penghapusan data pribadi atas permintaan individu, tidak

selalu diterapkan secara konsisten. Beberapa *data controller* masih melanjutkan pemrosesan data pribadi dengan dalih bahwa data tersebut diperoleh secara sah, meskipun tidak lagi memiliki dasar hukum yang berlaku. Kondisi ini menegaskan perlunya pedoman yang lebih tegas mengenai penghapusan jejak digital guna memperkuat kepercayaan masyarakat terhadap ekosistem data.

Selain aspek hukum, pendekatan teknis juga menjadi bagian penting dalam menjaga kepatuhan. Konsep *pseudonymization* atau penghilangan identitas, misalnya, dapat mengurangi risiko penyalahgunaan data, tetapi tidak sepenuhnya menghapus kemungkinan identifikasi ulang apabila pengelolaannya tidak dilakukan secara benar. Oleh karena itu, mekanisme teknis dan tata kelola harus berjalan beriringan agar perlindungan data tetap efektif. Dalam konteks intermediasi data sebagaimana diatur dalam *Data Governance Act*, baik lembaga publik maupun sektor swasta perlu berhati-hati dalam mengelola dan menyalurkan data, mengingat pelanggaran terhadap ketentuan ini dapat berimplikasi pada sanksi hukum yang serius serta menimbulkan dampak pada kepercayaan publik.

3.1.4 Amerika Latin

Amerika Latin, sebagai wilayah yang semakin terhubung secara digital, menghadapi tantangan dan peluang yang unik dalam membangun kepercayaan digital. Dengan pertumbuhan ekonomi digital yang pesat dan meningkatnya penggunaan teknologi di berbagai sektor, kepercayaan digital menjadi dasar penting untuk memastikan keberlanjutan dan keamanan transformasi digital di kawasan ini [208]. Kerangka kerja kepercayaan digital di Amerika Latin dirancang untuk menciptakan lingkungan digital yang aman, adil, dan efisien, di mana masyarakat, bisnis, dan pemerintah dapat berinteraksi dengan keyakinan penuh. Melalui kolaborasi antara negara-negara di kawasan, sektor swasta/industri, dan organisasi internasional, kerangka kerja ini bertujuan untuk melindungi data pribadi, meningkatkan keamanan siber, dan mempromosikan inovasi yang bertanggung jawab [209]. Dengan pendekatan yang holistik, Amerika Latin berupaya membangun ekosistem digital yang tidak hanya mendukung pertumbuhan ekonomi, tetapi juga melindungi hak-hak dan kepentingan pengguna digital di seluruh wilayah [210].

Mengapa Kepercayaan Digital Penting (*Why*)

Kepercayaan digital sangat penting bagi suatu negara karena menciptakan lingkungan digital yang aman dan transparan. Hal ini mendukung kelangsungan berbagai sektor, termasuk pemerintah, bisnis, dan organisasi sosial. Dengan kepercayaan digital, pengguna dapat berinteraksi dengan solusi digital secara percaya diri, sehingga meningkatkan partisipasi dalam *e-commerce*, pembelajaran *online*, dan layanan digital lainnya yang berkontribusi pada pertumbuhan ekonomi serta kesejahteraan masyarakat [211, 212].

Selain itu, kepercayaan digital berperan dalam melindungi informasi pribadi dan keuangan, yang krusial untuk menjaga kepercayaan pengguna serta mencegah

serangan siber [213]. Pembentukannya memerlukan kolaborasi antara pemerintah, bisnis, dan masyarakat guna memastikan kepatuhan terhadap standar keamanan siber, yang pada akhirnya memperkuat ekosistem digital secara keseluruhan [208, 209].

Tujuan Pengenalan Kepercayaan Digital (*What*)

Tujuan utama negara dalam memperkenalkan kepercayaan digital adalah menciptakan ruang digital yang aman, transparan, dan bertanggung jawab bagi seluruh pemangku kepentingan, mulai dari pemerintah, sektor swasta, organisasi sosial, hingga pengguna individu. Kepercayaan digital menjadi prasyarat penting bagi berkembangnya ekonomi dan masyarakat digital, karena tanpa adanya keyakinan terhadap keamanan dan transparansi, adopsi teknologi akan terhambat [214].

Selain itu, negara berperan dalam memastikan bahwa teknologi dan layanan digital menghormati hak dasar warga, melindungi data pribadi, serta menjunjung tinggi nilai-nilai sosial. Langkah ini juga bertujuan mencegah serta menanggulangi serangan siber dan kebocoran data, yang berpotensi merusak kepercayaan publik terhadap sistem digital [215]. Dengan demikian, keterlibatan pemerintah dalam menetapkan regulasi, standar, dan tata kelola digital merupakan pilar utama untuk memperkuat kepercayaan masyarakat dalam ruang digital.

Siapa yang Bertanggung Jawab (*Who*)

Kepercayaan digital tidak dapat dibangun hanya oleh pemerintah, melainkan memerlukan keterlibatan ekosistem yang lebih luas. Operator telekomunikasi menyediakan infrastruktur jaringan yang andal dan menjadi jembatan antara teknologi serta pengguna akhir. Sementara itu, perusahaan pengembang teknologi, baik penyedia perangkat lunak, perangkat keras, maupun platform digital, berperan sebagai motor inovasi yang menentukan evolusi teknologi digital. Regulator hadir untuk memastikan keseimbangan antara kepentingan publik, komersial, dan teknis melalui kebijakan yang kolaboratif dan adaptif [216].

Sebagaimana ditegaskan oleh Chew, Tan, dan Soon [217], kepercayaan digital mencakup dimensi mekanis (keamanan, privasi, transparansi) dan dimensi relasional (literasi digital, pengalaman pengguna, dan kolaborasi). Oleh karena itu, sinergi antarpemangku kepentingan, regulator, operator, dan pengembang teknologi, menjadi kunci untuk menciptakan tata kelola digital yang solid. Pendekatan ekosistem yang kolaboratif ini diperlukan untuk menyelaraskan kepentingan bisnis, teknis, dan regulasi, sehingga penerapan kepercayaan digital dapat berjalan efektif dan berkelanjutan.

Waktu dan Tahapan Implementasi (*When*)

Di Amerika Latin dan Karibia (LAC), penyerapan teknologi digital telah tumbuh pesat dan penyebaran pita lebar seluler yang cepat, khususnya, memungkinkan

semakin banyak orang untuk terhubung ke jaringan digital. Pada akhir tahun 2017, 391 juta dari 628 juta orang di wilayah LAC telah *online*, atau sekitar 62% dari populasi [208].

Semua pemangku kepentingan, pemerintah, bisnis, masyarakat sipil, serikat pekerja, dan komunitas teknis dan akademis, perlu bekerja sama untuk membentuk masa depan yang mewujudkan potensi transformasi digital untuk semua, sebagai pendorong penting pertumbuhan yang merata. Transformasi digital akan membutuhkan pengembangan ekosistem digital yang sehat, dan pembagian tanggung jawab antara masyarakat, bisnis, serikat pekerja, masyarakat sipil, dan pemerintah.

Pendekatan kebijakan yang seimbang yang mencakup kombinasi antara pengaturan mandiri, standar sukarela dan yang digerakkan oleh pasar, serta berbagi praktik terbaik, penerapan peraturan yang ada, dan kerangka kebijakan dan peraturan yang diperbarui dan fleksibel, perlu dipertimbangkan. Hal ini memerlukan upaya mengatasi hambatan organisasi terhadap kolaborasi antarbadan pemerintah, berbagi dan pengambilan keputusan horizontal, penekanan yang lebih kuat pada antisipasi potensi perubahan dan dampak, serta penggunaan data dan teknologi digital yang lebih besar dalam pembuatan kebijakan.

Untuk mendukung para pembuat kebijakan, OECD berkontribusi pada diskusi internasional mengenai transformasi digital melalui proyek lintas sektoral *Going Digita*l [208], melalui kerja untuk G20 dan G7, dan melalui kerja di tingkat nasional dan regional, termasuk*OECD-IDB Broadband Toolkit* 2016 untuk Amerika Latin dan Karibia [218], tinjauan terkini kebijakan telekomunikasi di Meksiko dan Kolombia (dan tinjauan berkelanjutan di Brasil), serta tinjauan *Going Digital* yang sedang berlangsung di Kolombia dan Brasil. Pekerjaan OECD dalam berbagi pengalaman dan praktik inovatif dapat membantu memperkuat kapasitas lembaga yang terlibat dalam pembuatan kebijakan. Selain itu, menyediakan data dan indikator komparatif memungkinkan pemahaman yang lebih baik tentang berbagai masalah kebijakan yang dipengaruhi oleh transformasi digital dan dapat membantu menunjukkan prioritas nasional dan internasional untuk tindakan kebijakan.

Setelah kemajuan luar biasa yang dialami pada pergantian abad ke-21, pertumbuhan ekonomi dan kemajuan sosial-ekonomi di LAC telah melemah sejak 2011 [219]. Potensi pertumbuhan PDB yang lebih rendah dari yang diharapkan, sekitar 3% per tahun, mencerminkan pertumbuhan produktivitas tenaga kerja yang rendah. Memang, dalam beberapa dekade terakhir, produktivitas tenaga kerja telah turun hingga sekitar 40% dari tingkat Uni Eropa. Pada gilirannya, pertumbuhan dan produktivitas yang tidak memadai menghambat pengurangan lebih lanjut dalam kemiskinan dan ketimpangan pendapatan. Bersamaan dengan tren ini, kelas menengah telah berkembang hingga mewakili sepertiga dari populasi, tetapi juga "kelas menengah yang rentan" (berisiko jatuh kembali ke dalam kemiskinan) mewakili hampir 40% dari populasi. Kelas menengah yang sedang tumbuh memiliki aspirasi dan tuntutan yang lebih besar untuk layanan dan lembaga publik yang lebih berkualitas; seringkali tidak terpenuhi. Misalnya, persentase penduduk yang puas dengan sistem pendidikan turun dari 63% menjadi 56% dari 2006 hingga 2017, di bawah level OECD sebesar 65% [220, 219]. Kawasan LAC telah membuat kemajuan

penting dalam pembangunan ekonomi dan sosial selama beberapa dekade terakhir, yang memungkinkan puluhan juta rumah tangga miskin untuk bergabung dengan kelas menengah global. Meskipun demikian, kawasan LAC masih tertinggal dalam hal standar hidup, tingkat ketimpangan pendapatan dan ketimpangan dalam kesempatan, pangsa ekonomi informal, pendidikan, investasi, akuntabilitas pemerintah dan kepercayaan warga, infrastruktur, produktivitas, dan konektivitas.

Bagaimana Kepercayaan Digital Diterapkan (*How*)

Kepercayaan digital terbangun melalui hubungan transparan antara berbagai aktor dalam ekonomi digital, termasuk penyedia teknologi, operator, dan regulator. Operator memegang peran kunci karena mereka menjembatani teknologi dan pengguna, sehingga berkontribusi langsung dalam membangun kepercayaan digital melalui pengelolaan jaringan [221].

Keamanan siber menjadi faktor krusial dalam mencegah serangan dan kebocoran data yang dapat merusak kepercayaan. Banyak negara di Amerika Latin telah merumuskan strategi keamanan siber nasional serta mengadopsi praktik terbaik, seperti prinsip *zero-trust*, untuk memperkuat perlindungan infrastruktur digital [222, 223]. Kepatuhan terhadap standar keamanan serta adopsi praktik terbaik oleh perusahaan juga memperkuat ekosistem digital yang lebih aman. Selain itu, kebijakan privasi yang jelas dan mudah diakses, seperti yang diatur dalam berbagai undang-undang perlindungan data di Brasil, Argentina, Kolombia, dan Uruguay, membantu pengguna memahami pengelolaan data mereka, yang menjadi dasar penting dalam membangun kepercayaan [224, 225]. Secara keseluruhan, kepercayaan digital bertumpu pada transparansi [226], keamanan siber yang efektif, dan manajemen data yang bertanggung jawab.

Inisiatif Kepercayaan Digital Amerika Latin

Amerika Latin telah mengambil langkah signifikan dalam membangun kepercayaan digital melalui regulasi, infrastruktur, dan kolaborasi regional. Berikut adalah inisiatif utama yang telah teridentifikasi:

1. Kebijakan dan Regulasi
   Beberapa negara di kawasan Amerika Latin telah memperkuat landasan hukum digital melalui kebijakan perlindungan data, keamanan siber, dan kerangka hukum elektronik yang sejalan dengan praktik global seperti GDPR Uni Eropa.
   - Perlindungan Data Pribadi
     Sejumlah negara telah mengadopsi regulasi yang mengatur pengelolaan dan perlindungan data pribadi:
     - Brasil: *Lei Geral de Proteção de Dados* (LGPD), berlaku sejak 2020 [227].

  - Argentina: *Personal Data Protection Law* No. 25.326 [228].
  - Meksiko: *Ley Federal de Protección de Datos Personales en Posesión de los Particulares* (2010) [229].
- Keamanan Siber
  Pemerintah di berbagai negara mengembangkan strategi nasional untuk memperkuat ketahanan digital dan menanggapi ancaman siber:
  - Kolombia: *Estrategia Nacional de Seguridad Digital* 2023–2027 [230].
  - Chile: *Estrategia Nacional de Ciberseguridad* serta pembentukan CSIRT nasional [231].
- Kerangka Hukum Digital
  Uruguay mengesahkan *Ley N° 18.600* yang mengatur tanda tangan digital dan dokumen elektronik [232].

2. Infrastruktur Teknologi
   Kemajuan infrastruktur digital menjadi dasar utama bagi transformasi ekonomi dan pelayanan publik di kawasan.
   - Identitas Digital
     Kolombia mengimplementasikan *Registro Único Empresarial y Social* (RUES) sebagai sistem terintegrasi untuk verifikasi identitas bisnis [233].
   - *Blockchain* dan Teknologi Terdesentralisasi
     Bank Sentral Brasil mengembangkan mata uang digital nasional, DREX, sebagai *Central Bank Digital Currency* (CBDC) untuk meningkatkan efisiensi sistem keuangan [234].
3. Kolaborasi Regional
   Kerja sama antarnegara menjadi pendorong penting dalam membangun ekosistem digital yang aman, andal dan interoperabel.
   - Forum dan Aliansi Regional
     - Organisasi Negara-Negara Amerika (OAS) melalui CICTE menjalankan berbagai program keamanan siber regional [235].
     - Mercosur mengadopsi *Decision 15/21* yang mendorong harmonisasi kebijakan *e-commerce* dan interoperabilitas digital antarnegara anggota [236].
4. Inklusi Digital
   Upaya memperluas akses terhadap teknologi digital menjadi prioritas utama untuk mengurangi kesenjangan konektivitas di kawasan.
   - Akses Internet
     Brasil menjalankan program *Internet para Todos* untuk memperluas konektivitas hingga wilayah terpencil [237].
     Meksiko mengembangkan proyek *Red Compartida* guna menyediakan jaringan telekomunikasi nasional yang lebih merata [238].

5. Fokus pada AI dan Teknologi Baru
   Panama telah membukukan langkah revolusioner dalam penggunaan teknologi baru melalui PanamaFuture [239]. *Blockchain* yang selama ini sebagai mata uang digital dapat dikonversikan menjadi aset yang lebih riil dengan konversi kepemilikan *real estate* berbasis token [240]. Kesadaran terhadap potensi sekaligus risiko kecerdasan buatan (AI) mulai meningkat di kawasan. Brasil dan Argentina telah memulai diskusi publik mengenai etika, regulasi, dan pemanfaatan AI secara bertanggung jawab [241, 242].

Analisis Penerapan Kepercayaan Amerika Latin

Amerika Latin mengalami pertumbuhan pesat dalam adopsi teknologi digital, terutama selama dan setelah pandemi COVID-19, yang mendorong percepatan penggunaan layanan digital di sektor pendidikan, keuangan, dan administrasi pemerintahan. Perubahan ini menciptakan momentum penting bagi transformasi digital di kawasan, sekaligus menegaskan urgensi pembangunan kepercayaan digital untuk mendukung keberlanjutan ekosistem digital yang aman, adil dan berkelanjutan.

Namun, di balik pertumbuhan tersebut, kawasan ini juga menghadapi sejumlah tantangan struktural yang kompleks. Salah satu kendala utama adalah ketimpangan akses digital, terutama di wilayah pedesaan dan terpencil yang belum memiliki infrastruktur teknologi informasi dan komunikasi (TIK) yang memadai. Sekitar 32% populasi Amerika Latin dan Karibia (sekitar 224 juta orang) masih tidak memiliki akses internet yang stabil dan terjangkau [243]. Laporan lain [244, 245] menegaskan adanya kesenjangan signifikan antara area urban dan rural, di mana hanya 35,8% rumah tangga di daerah pedesaan yang memiliki akses internet tetap, dibandingkan 74,8% di perkotaan. Bahkan, menurut *GSMA Intelligence*, hampir separuh populasi di wilayah Karibia belum terkoneksi [246]. Beberapa hal tersebut menegaskan kesenjangan yang signifikan antara wilayah urban dan rural. Ketimpangan ini tidak hanya membatasi peluang ekonomi dan pendidikan, tetapi juga menghambat pemerataan kepercayaan digital di seluruh lapisan masyarakat.

Selain kesenjangan akses, rendahnya literasi digital [247, 248] dan ketidakpercayaan masyarakat terhadap keamanan serta penggunaan data pribadi turut menjadi tantangan. Hal ini diperparah oleh ketidakpercayaan masyarakat terhadap keamanan serta penggunaan data pribadi, ditambah dengan maraknya serangan siber dan lemahnya kebijakan perlindungan data di sejumlah negara. Meskipun beberapa negara seperti Brasil, Meksiko, dan Argentina telah mengadopsi kerangka hukum perlindungan data yang serupa dengan GDPR, tingkat implementasi dan kapasitas pengawasan masih sangat bervariasi [249].

Analisis terhadap pendekatan kebijakan yang diterapkan menunjukkan bahwa meskipun terdapat kemajuan dalam penyusunan regulasi dan penguatan infrastruktur, koordinasi antaraktor (pemerintah, sektor swasta, dan masyarakat sipil) masih perlu ditingkatkan. Pendekatan *multi-stakeholder* menjadi prasyarat penting bagi pembangunan kepercayaan digital yang menyeluruh dan berkelanjutan. Keterlibatan aktif lembaga internasional seperti OECD dan OEA dalam penguatan kapasitas

dan harmonisasi kebijakan digital telah berkontribusi positif, tetapi pelaksanaannya di tingkat lokal tetap bergantung pada komitmen politik, stabilitas kelembagaan, dan partisipasi masyarakat.

Selain itu, tekanan ekonomi pascapandemi dan stagnasi produktivitas tenaga kerja sejak 2011 menjadi faktor yang menghambat alokasi sumber daya untuk inisiatif digital yang berorientasi pada kepercayaan [250]. Rendahnya kepuasan terhadap layanan publik dan tingginya angka ketimpangan pendapatan di beberapa negara LAC turut memperlemah persepsi publik terhadap efektivitas kebijakan digital yang ada.

Dengan demikian, keberhasilan penerapan kepercayaan digital di Amerika Latin sangat bergantung pada kemampuan negara untuk mengatasi kesenjangan digital, meningkatkan literasi digital, memperkuat kerangka hukum dan kelembagaan, serta membangun sinergi antaraktor dalam ekosistem digital. Investasi dalam infrastruktur, pendidikan, dan tata kelola digital yang transparan menjadi kunci untuk memastikan bahwa transformasi digital tidak hanya bersifat elitis atau eksklusif, melainkan kolaboratif dengan memberdayakan seluruh lapisan masyarakat.

3.1.5 Turki

Kebijakan nasional Turki, *Twelfth Development Plan* (2024-2028) [251], disusun dalam kerangka visi 2053, yang menandai abad baru Republik. Kebijakan ini sejalan dengan visi "Turki yang stabil, kuat, dan makmur di Abad Turki", yang berfokus pada pembangunan ramah lingkungan, ketangguhan terhadap bencana, peningkatan nilai tambah berbasis teknologi canggih, serta alokasi pendapatan yang adil. Langkah-langkah dalam Twelfth Development Plan diimplementasikan melalui Program Tahunan Presiden. Salah satu fokus utama dalam rencana ini adalah transformasi digital, dengan "pemerintahan digital" menjadi topik khusus yang menekankan pengalaman pengguna dan partisipasi elektronik.

Mengapa Kepercayaan Digital Penting (*Why*)

Strategi kepercayaan digital Turki merupakan bagian dari rencana transformasi digital nasional yang lebih luas, yang bertujuan menjadikan negara Turki sebagai pemimpin dalam teknologi digital dan layanan publik berbasis data [252]. Beberapa sasaran utama yang ditetapkan pemerintah Turki melalui Kantor Transformasi Digital (Dijital Dönüşüm Ofisi, DTO) dapat dijelaskan sebagai berikut:

1. Memperkuat infrastruktur digital
   DTO berperan dalam memperkuat infrastruktur digital, mendorong inovasi, dan meningkatkan keterampilan digital masyarakat sebagai bagian dari agenda nasional transformasi digital [253, 254].

2. Transformasi Digital Sektor Publik
   DTO didirikan melalui Keputusan Presiden No. 1 (2018) sebagai lembaga

di bawah Presiden Republik Turki yang bertugas mengonsolidasikan upaya transformasi digital, khususnya pada sektor publik [255, 256].

3. Teknologi Digital sebagai Pendorong Daya Saing
   Teknologi digital dan TIK menjadi faktor penting dalam meningkatkan daya saing ekonomi Turki. DTO berfokus agar layanan publik berbasis digital dapat diakses secara merata oleh masyarakat [252, 253].

4. Ekspektasi Pelanggan dan Keamanan Data
   Pasar *e-commerce* Turki berkembang pesat dan menimbulkan tuntutan pengguna terkait keamanan data pribadi dan keuangan. Pelanggaran data berdampak pada kerugian finansial serta merusak reputasi dan loyalitas pengguna. Oleh karena itu tuntutan terhadap transparansi, manajemen risiko, dan tata kelola merupakan keniscayaan. Regulasi perlindungan data (KVKK) dan regulasi *e-commerce* memperkuat aspek kepercayaan digital dalam transaksi *online* [257, 258].

5. Transformasi Berbasis Data
   Pemerintah menekankan pentingnya tata kelola data nasional melalui inisiatif seperti *National Data Strategy* dan proyek *National Data Dictionary*. Upaya ini bertujuan mengoordinasikan pemangku kepentingan lintas sektor untuk mengoptimalkan pemanfaatan data [259, 254].

6. Transparansi dan Akuntabilitas
   OECD menekankan bahwa data publik penting untuk meningkatkan akuntabilitas dan kepercayaan masyarakat terhadap pemerintah. DTO didorong untuk memperluas praktik keterbukaan data dan evaluasi berbasis kinerja [252, 255].

Tujuan Pengenalan Kepercayaan Digital (*What*)

Kepercayaan digital diberikan kepada perusahaan yang telah menunjukkan kepada penggunanya bahwa mereka dapat memberikan keamanan, privasi, keamanan, keandalan, dan etika data dengan program atau perangkat *online* mereka. Ketika pengguna memutuskan untuk menggunakan produk suatu perusahaan, pengguna tersebut menegaskan kepercayaan digital terhadap perusahaan tersebut. Pada tahun 2018, pemerintah Turki meluncurkan "Inisiatif Teknologi Nasional" dan strategi "Digital Türkiye" [260] yang bertujuan untuk untuk meningkatkan infrastruktur digital, mendorong inovasi, dan menumbuhkan keterampilan digital bagi warga negaranya.

Siapa yang Bertanggung Jawab (*Who*)

Sistem pemerintahan presidensial di Turki menuntut tata kelola yang cepat, transparan, dan efisien. Untuk mendukung hal ini, langkah strategis telah diambil dengan mengintegrasikan koordinasi Digital Türkiye (*e-government*) dan keamanan siber dalam satu struktur yang terpusat [261].

Pada 10 Juli 2018, Pemerintah Turki mendirikan Kantor Transformasi Digital (Dijital Dönüşüm Ofisi, DTO) Kepresidenan Republik Türkiye berdasarkan Keputusan Presiden No. 1 yang tercatat dalam Lembaran Negara No. 30474 [262]. Kantor ini bertanggung jawab menyatukan berbagai inisiatif yang sebelumnya terfragmentasi dalam bidang transformasi digital, keamanan siber, teknologi nasional, big data, dan kecerdasan artifisial [262]. Dengan pendekatan ini, DTO memastikan bahwa kebijakan dan implementasi digital di Turki sejalan dengan kemajuan teknologi, kebutuhan masyarakat, serta tren reformasi sektor publik.

Sebagai bagian dari misi "Digital Türkiye", Kantor Transformasi Digital bertujuan mewujudkan transformasi digital secara menyeluruh melalui kolaborasi antara lembaga pemerintah, sektor swasta/industri, universitas, dan organisasi nonpemerintah [263]. Dengan koordinasi yang lebih baik, Turki berharap dapat mempercepat inovasi digital dan meningkatkan keamanan serta efisiensi di pelayanan publik.

Waktu dan Tahapan Implementasi (*When*)

Pemerintah Turki mulai merancang *National Data Strategy* pada tahun 2022 melalui penugasan kepada Digital Transformation Office (DTO) sebagaimana tertuang dalam *Annual Presidential Program 2022* [264]. Strategi ini bertujuan untuk membangun kebijakan komprehensif dan nyata mencakup tata kelola, pengelolaan, pembagian, penggunaan, serta perlindungan dan privasi data [252].

Dalam *Medium-Term Program 2024–2026*, Secara eksplisit DTO ditugaskan memimpin penyusunan strategi data nasional dan rencana aksi [264]. Lebih lanjut, *Twelfth Development Plan 2024–2028* juga menekankan penguatan tata kelola data, termasuk melalui Kebijakan No. 584 tentang penyusunan “Strategi Data Nasional dan Rencana Aksi” serta Kebijakan No. 967 mengenai penguatan tata kelola data di lembaga publik [264, 265].

Sebagai langkah awal, pemerintah Turki meluncurkan proyek pada April 2023 bersama United Nations Development Programme (UNDP) untuk membangun kerangka tata kelola data yang mengatur akses, penggunaan, dan pembagian data [259]. Dalam prosesnya, UNDP melakukan tinjauan internasional dengan mengacu pada praktik terbaik PBB, OECD, Uni Eropa, Bank Dunia, dan ASEAN [266]. Proyek ini melibatkan lebih dari 40 konsultasi multipemangku kepentingan yang terdiri atas lembaga pemerintah, organisasi masyarakat sipil, sektor swasta, dan universitas. Konsultasi dilakukan secara daring dan luring untuk memastikan partisipasi luas dalam perumusan strategi data nasional [259].

Bagaimana Kepercayaan Digital Diterapkan (*How*)

Otoritas Perlindungan Data Pribadi (*Kişisel Verileri Koruma Kurumu*, KVKK) merupakan lembaga independen yang dibentuk oleh pemerintah Turki berdasarkan Undang-Undang Perlindungan Data Pribadi No. 6698 [267]. Lembaga ini memiliki tanggung jawab sebagai badan pengatur yang mengawasi dan menegakkan regulasi perlindungan data, serta menjalankan fungsi koordinatif dengan berbagai institusi

pemerintahan terkait.

Tata kelola data yang baik dipandang sebagai faktor utama dalam peningkatan kualitas kebijakan publik dan pelayanan kepada masyarakat. Selain itu, penguatan kepercayaan publik juga sangat bergantung pada efektivitas pengelolaan data. Sebaliknya, kegagalan dalam mengelola data berpotensi menimbulkan dampak negatif yang signifikan terhadap persepsi dan kepercayaan masyarakat. Kompetensi dalam tata kelola data, disertai langkah strategis untuk mempertahankan, memelihara, dan memulihkan kepercayaan publik, menjadi aspek krusial dalam ekosistem digital.

Upaya penguatan ini mencakup penerapan prinsip-prinsip etika, transparansi, perlindungan privasi, kejelasan persetujuan, serta standar keamanan data yang ketat. Melalui pendekatan tersebut, keberlangsungan ekosistem kepercayaan digital dapat terjaga dengan baik, mendukung kepentingan warga negara, dan menjamin keseimbangan antara kemajuan teknologi dan perlindungan hak individu.

1. Etika
   Peningkatan penggunaan, ketersediaan, dan akses terhadap data pribadi maupun nonpribadi menimbulkan berbagai pertanyaan etis terkait proses pengumpulan, pengelolaan, dan penyimpanan data. Permasalahan ini mencakup tanggung jawab, akuntabilitas, keadilan, serta kepatuhan terhadap hak asasi manusia dan regulasi yang berlaku. Dalam konteks tersebut, penerapan prinsip dan budaya penggunaan data yang etis menjadi langkah fundamental untuk memastikan bahwa praktik berbasis data dapat memberikan manfaat maksimal tanpa mengorbankan nilai-nilai kemanusiaan dan kepercayaan publik [208].

   Pengalaman organisasi publik di Turki menunjukkan bahwa kepercayaan masyarakat terhadap tata kelola data pemerintah berperan penting dalam meningkatkan kualitas layanan publik dan kesejahteraan warga negara. Kepercayaan ini hanya dapat dibangun melalui penerapan prinsip etika yang kuat, seperti transparansi, akuntabilitas, dan tanggung jawab dalam setiap tahap pengelolaan data. Dengan demikian, etika bukan sekadar pelengkap, melainkan fondasi utama dalam membangun tata kelola data yang tepercaya.

   Untuk mewujudkan hal tersebut, pemerintah perlu menerapkan seperangkat pedoman etika yang komprehensif dalam pengelolaan data pribadi maupun nonpribadi. Pedoman ini berfungsi sebagai mekanisme pengaturan mandiri yang memberikan arahan tentang perilaku, kebijakan, dan pendekatan yang sesuai untuk mencapai standar etika yang lebih tinggi. Selain itu, kerangka etika juga berperan dalam memperkuat pemahaman bersama di antara pemangku kepentingan serta membantu mengantisipasi dan menyelesaikan tantangan etis yang muncul dalam praktik pengelolaan data publik.

2. Transparansi, privasi dan persetujuan
   Privasi, transparansi, dan persetujuan merupakan tiga pilar utama dalam tata kelola data yang bertanggung jawab. Privasi berkaitan dengan perlindungan terhadap hak individu sebagai subjek data, sedangkan kerahasiaan berfokus pada pengamanan dan pengendalian akses terhadap data itu sendiri. Dalam

konteks perlindungan data pribadi, konsep persetujuan berdasarkan informasi (informed consent) menjadi prinsip mendasar yang memastikan bahwa individu memahami secara jelas tujuan pengumpulan, pemrosesan, dan penggunaan data mereka sebelum memberikan izin atas penggunaannya untuk kepentingan tertentu [267].

Transparansi menjadi unsur penting dalam memperkuat kepercayaan publik terhadap tata kelola data, khususnya di sektor pemerintahan berbasis data. Dalam konteks ini, transparansi memiliki dua dimensi utama. Pertama, keterbukaan pemerintah dalam membagikan data yang menjadi dasar pengambilan kebijakan serta menjelaskan penggunaan algoritma yang digunakan dalam proses tersebut. Kedua, pemberian akses yang memadai bagi warga negara untuk mengetahui bagaimana data pribadi mereka dikumpulkan, digunakan, dan disebarluaskan, serta untuk mengelola persetujuan atas pemrosesannya. Dengan demikian, setiap proses pengelolaan data dapat berlangsung secara terbuka, akuntabel, dan tidak melanggar hak individu.

Sebagai bagian dari komitmennya terhadap prinsip-prinsip tersebut, Turki berupaya menyelaraskan Personal Data Protection Law No. 6698 dengan General Data Protection Regulation (GDPR) yang diterapkan di Uni Eropa. Salah satu bentuk harmonisasi yang dilakukan adalah penyesuaian jangka waktu pelaporan pelanggaran data menjadi 72 jam, sebagaimana ditetapkan dalam Keputusan Dewan KVKK [268]. Penyesuaian ini tidak hanya memperkuat posisi Turki dalam proses aksesi ke Uni Eropa, tetapi juga meningkatkan kepercayaan internasional terhadap komitmen negara tersebut dalam melindungi data pribadi dan mendukung aliran data lintas batas yang aman.

Selain itu, Turki juga memperkuat transparansi dan akuntabilitas melalui penerapan Sistem Informasi Registri Pengendali Data atau Veri Sorumluları Sicil Bilgi Sistemi (VERBİS), yang dikelola oleh Otoritas Perlindungan Data Pribadi [269]. Sistem berbasis notifikasi ini memungkinkan publik untuk mengakses informasi mengenai identitas pengendali data, tujuan pemrosesan data, kelompok subjek data, serta kategori data yang dikumpulkan dan digunakan. Melalui VERBİS, warga negara memperoleh kendali yang lebih besar atas data pribadi mereka, sementara pemerintah menunjukkan komitmen nyata terhadap keterbukaan dan perlindungan hak privasi individu.

3. Keamanan
   Keamanan digital merupakan elemen krusial dalam tata kelola data modern yang berfokus pada upaya mencegah akses, penggunaan, atau penyebaran data secara tidak sah. Pemerintah Turki menaruh perhatian besar terhadap aspek ini melalui Personal Data Protection Law (KVKK), yang mengatur perlindungan data pribadi, persetujuan pengguna, serta kewajiban pengendali data untuk menerapkan langkah-langkah keamanan yang memadai. Untuk mendukung implementasinya, Otoritas Perlindungan Data Pribadi telah menerbitkan Guideline on Data Security Obligations [270], yang memberikan pedoman administratif dan teknis bagi organisasi publik dalam memastikan perlindungan data yang efektif serta mencegah kebocoran informasi.

Sebagai bagian dari strategi penguatan ekosistem keamanan siber nasional, Badan Industri Pertahanan (Savunma Sanayii Başkanlığı, SSB) membentuk Turkish Cyber Security Cluster (Türkiye Siber Güvenlik Kümelenmesi) [271]. Platform ini berfungsi sebagai wadah kolaborasi antara pemerintah, industri, dan akademisi dalam mengembangkan inovasi serta strategi keamanan siber nasional. Dalam kerangka kelembagaan, Cyber Security Department of the Defence Technologies Office (DTO) bertanggung jawab atas perumusan, pemantauan, dan implementasi kebijakan keamanan siber, sedangkan Directorate for Security and Foreign Policy berperan dalam merancang rekomendasi kebijakan strategis di tingkat nasional.

Dari sisi inovasi dan pengembangan teknologi, Kementerian Perindustrian dan Teknologi memiliki peran penting dalam menetapkan kebijakan, mekanisme insentif, serta strategi riset dan pengembangan (R&D) untuk memperkuat kapabilitas nasional di bidang keamanan siber. Tujuan utamanya adalah mendorong kemandirian teknologi, memperkuat kemampuan sumber daya manusia, serta menciptakan ekosistem yang mendukung pengembangan solusi keamanan digital lokal. Selain itu, Electronic Communications Law No. 5809 menetapkan tanggung jawab bagi Kementerian Transportasi dan Infrastruktur bersama Information and Communication Technologies Authority (BTK) dalam pelaksanaan kebijakan keamanan siber nasional. Tugas operasional ini dijalankan oleh BTK melalui Turkish Computer Emergency Response Team (TR-CERT/USOM) [272], yang berperan dalam deteksi, respons, dan mitigasi insiden siber di tingkat nasional.

Meskipun berbagai kebijakan dan inisiatif telah diterapkan, tantangan utama yang dihadapi adalah menemukan keseimbangan antara keamanan digital dan optimalisasi pemanfaatan data. Penekanan berlebihan pada keamanan dan kerahasiaan berpotensi membatasi inovasi serta pemanfaatan data untuk kebijakan publik berbasis bukti. Pemerintah Turki melalui Information and Communication Security Guide berupaya mengatasi tantangan tersebut dengan mendorong penerapan keamanan data yang adaptif dan proporsional. Pendekatan ini bertujuan menjaga keseimbangan antara perlindungan data, transparansi, dan pemanfaatan informasi untuk mendukung penyelenggaraan layanan publik yang aman, efisien, dan tepercaya.

Inisiatif Kepercayaan Digital Turki

Turki telah mengambil berbagai inisiatif untuk membangun kepercayaan digital sebagai bagian dari upayanya untuk memperkuat ekonomi digital, melindungi privasi warga, dan meningkatkan keamanan siber. Berikut adalah penjelasan rinci tentang inisiatif-inisiatif yang dilakukan oleh Turki dalam konteks kepercayaan digital :

1. *Cybersecurity* (Keamanan Siber)
    - Strategi Keamanan Siber Nasional:
      Pada tahun 2016, Turki meluncurkan *National Cyber Security Strategy and Action Plan* untuk melindungi infrastruktur kritis, mencegah

serangan siber, dan meningkatkan kesadaran publik tentang risiko siber. Strategi ini mencakup pembentukan badan-badan khusus seperti Information and Communication Technologies Authority (BTK) dan Presidency of Defense Industries (SSB) untuk mengelola keamanan siber.

- Pusat Operasi Keamanan Siber (SOC):
  Turki mendirikan pusat operasi keamanan siber untuk memantau ancaman siber secara *real-time* dan merespons insiden dengan cepat. SOC juga berfungsi sebagai pusat koordinasi antara pemerintah, sektor swasta/industri, dan institusi akademik.
- Regulasi Keamanan Siber:
  Pemerintah Turki menerapkan regulasi yang mewajibkan organisasi untuk melindungi data sensitif dan melaporkan insiden keamanan siber kepada otoritas terkait.

2. Perlindungan Data dan Privasi

   - Undang-Undang Perlindungan Data Pribadi (KVKK):
     Pada tahun 2016, Turki mengesahkan Law on Protection of Personal Data (KVKK), yang mirip dengan *General Data Protection Regulation* (GDPR) Uni Eropa. KVKK bertujuan untuk melindungi privasi individu dengan mengatur pengumpulan, pemrosesan, dan penyimpanan data pribadi. Organisasi yang melanggar aturan dapat dikenai sanksi administratif atau hukum.
   - Peningkatan Kesadaran Privasi:
     Pemerintah dan lembaga swasta/industri aktif menyebarkan informasi tentang pentingnya perlindungan data pribadi kepada masyarakat melalui kampanye edukasi.

3. *Digital Identity* (Identitas Digital)

   - Sistem Identitas Digital Terpusat:
     Turki mengembangkan sistem identitas digital yang terintegrasi untuk memberikan akses aman ke layanan pemerintah dan swasta/industri. Sistem ini menggunakan teknologi autentikasi dua faktor (2FA) dan enkripsi untuk memastikan keamanan.
   - *E-Government Services*:
     Platform *e-government* seperti e-Devlet memungkinkan warga untuk mengakses lebih dari 100 layanan publik secara *online* dengan aman. Penggunaan identitas digital yang terverifikasi meminimalkan risiko penyalahgunaan data.

4. Transformasi Digital dan AI Governance

   - Strategi AI Nasional:
     Pada tahun 2021, Turki meluncurkan *Artificial Intelligence Strategy Document*, yang menekankan pentingnya transparansi, akuntabilitas, dan

etika dalam pengembangan AI. Dokumen ini bertujuan untuk memastikan bahwa teknologi AI digunakan secara bertanggung jawab dan tidak merugikan masyarakat.

- *Blockchain* untuk Kepercayaan Digital:
  Turki mulai menjajaki penggunaan teknologi *blockchain* untuk meningkatkan transparansi dalam sektor publik, seperti pelacakan rantai pasokan, manajemen dokumen, dan pemungutan suara elektronik.

5. Kolaborasi Internasional

   - Kemitraan Global:
     Turki bekerja sama dengan organisasi internasional seperti International Telecommunication Union (ITU) dan World Economic Forum (WEF) untuk berbagi praktik terbaik dalam membangun kepercayaan digital. Turki juga menjadi anggota *Global Cyber Security Agenda* (GCA) untuk berkolaborasi dalam isu-isu keamanan siber global.
   - Perjanjian Bilateral:
     Turki menandatangani perjanjian bilateral dengan negara-negara lain untuk memperkuat kerja sama dalam keamanan siber dan pertukaran informasi intelijen.

6. Edukasi dan Kesadaran Publik

   - Program Pelatihan Keamanan Siber:
     Pemerintah Turki meluncurkan program pelatihan untuk meningkatkan kemampuan tenaga kerja dalam bidang keamanan siber. Program ini mencakup pelatihan bagi mahasiswa, profesional TI, dan pejabat pemerintah.
   - Kampanye Kesadaran Publik:
     Kampanye seperti "*Safe Internet*" bertujuan untuk meningkatkan kesadaran masyarakat tentang risiko *online*, seperti *phishing*, *malware*, dan penipuan digital.

7. Infrastruktur Teknologi

   - Pengembangan Infrastruktur *Cloud*:
     Turki mendorong pengembangan layanan *cloud* lokal untuk mengurangi ketergantungan pada penyedia asing dan meningkatkan kontrol atas data nasional. Contohnya, proyek *Turkcell Cloud* yang menyediakan solusi *cloud* aman untuk bisnis dan pemerintah.
   - Investasi dalam R&D:
     Pemerintah Turki menginvestasikan dana besar dalam penelitian dan pengembangan teknologi baru, termasuk keamanan siber, AI, dan IoT.

8. Tanggap Darurat Insiden Siber

   - Tim Tanggap Darurat Keamanan Komputer (CERT):
     Turki membentuk TR-CERT (*Turkish Computer Emergency Response*

Team) untuk menangani insiden keamanan siber secara cepat dan efektif. TR-CERT bekerja sama dengan organisasi internasional seperti FIRST (*Forum of Incident Response and Security Teams*).

- Simulasi Serangan Siber:
  Pemerintah secara rutin melakukan simulasi serangan siber berskala besar untuk menguji kesiapan nasional dan meningkatkan kapasitas respons.

Analisis Penerapan Kepercayaan Digital Turki

Turki menunjukkan komitmen kuat dalam mengintegrasikan teknologi digital sebagai bagian dari transformasi pemerintahan dan peningkatan kualitas layanan publik. Inisiatif strategis seperti *Digital Government Strategy* serta pembentukan *Digital Transformation Office* (DTO) menjadi langkah konkret untuk memastikan pemanfaatan teknologi dan data dalam memperkuat transparansi, efisiensi, dan ketahanan institusi negara. Pendekatan ini menegaskan orientasi Turki terhadap tata kelola pemerintahan yang adaptif dan berbasis bukti. Namun, dinamika kebijakan digital di Turki tidak lepas dari tantangan keseimbangan antara keamanan, kepercayaan digital, dan kebebasan sipil. Upaya memperkuat pengawasan ruang digital terkadang menimbulkan kekhawatiran akan potensi pembatasan terhadap kebebasan berekspresi dan akses informasi. Oleh karena itu, diperlukan pendekatan regulatif yang proporsional, yakni yang mampu melindungi integritas ruang digital tanpa mengorbankan hak-hak fundamental pengguna. Keseimbangan ini menjadi kunci untuk menjaga kepercayaan publik terhadap transformasi digital yang aman dan berkelanjutan.

Dalam konteks regulasi, Undang-Undang No. 5651 menjadi salah satu instrumen utama dalam pengaturan media digital di Turki. Regulasi ini mewajibkan penyedia layanan digital asing untuk memiliki kantor perwakilan di dalam negeri serta menyimpan data pengguna secara lokal. Meskipun bertujuan memperkuat kedaulatan data dan akuntabilitas platform, kebijakan tersebut memunculkan kekhawatiran akan potensi kontrol berlebihan terhadap konten daring. Kekhawatiran ini terbukti melalui tindakan otoritas penyiaran Turki (RTUK) yang memblokir akses terhadap *Voice of America* dan *Deutsche Welle* [273], yang menimbulkan perdebatan mengenai batas antara regulasi dan pembatasan kebebasan pers digital.

Selain isu tata kelola informasi, Turki juga menghadapi tantangan dalam sektor keuangan digital. Sejak 2021, Turki masuk dalam "*grey list*" *Financial Action Task Force* (FATF), yang menandakan perlunya peningkatan kepatuhan terhadap standar internasional terkait *anti-money laundering* (AML) dan *counter-terrorist financing* (CTF). Dalam konteks ini, kebijakan terhadap aset kripto menjadi salah satu area sensitif. Pemerintah melarang penggunaan mata uang kripto sebagai alat pembayaran untuk barang dan jasa, dengan alasan tingginya risiko spekulatif serta potensi kerugian yang sulit dipulihkan. Langkah ini mencerminkan sikap kehati-hatian pemerintah sambil menunggu tersusunnya kerangka regulasi kripto yang lebih komprehensif dan selaras dengan praktik global.

Secara keseluruhan, pendekatan digital Turki memperlihatkan dualitas antara ambisi modernisasi dan kebutuhan kontrol negara. Tantangan ke depan terletak pada kemampuan pemerintah menyeimbangkan inovasi dengan perlindungan hak-hak digital warga, agar transformasi digital dapat berlangsung secara beretika, transparan, dan berorientasi pada kepentingan publik.

3.2 Analisis Komparatif Praktik Terbaik Kepercayaan Digital Negara

Kepercayaan digital merupakan elemen kunci dalam era transformasi digital, ketika interaksi antara masyarakat, dunia usaha, dan pemerintah semakin bergantung pada teknologi. Keberhasilan transformasi ini tidak hanya ditentukan oleh ketersediaan infrastruktur digital, tetapi juga oleh tingkat kepercayaan terhadap sistem, data, dan tata kelola digital yang mendasarinya.

Analisis sebelumnya menelaah penerapan praktik terbaik kepercayaan digital di lima kawasan atau negara, yaitu Singapura, Malaysia, Uni Eropa, Amerika Latin, dan Turki, dengan menggunakan lima indikator tematik: *Why*, *What*, *Who*, *When*, dan *How*. Pendekatan ini memungkinkan penilaian yang komprehensif terhadap motivasi, kebijakan, aktor, tahapan implementasi, serta mekanisme pelaksanaan di masing-masing konteks nasional.

Tabel 3.1 merangkum hasil analisis komparatif tersebut berdasarkan kelima indikator tematik. Melalui perbandingan ini, terlihat bahwa setiap negara mengembangkan strategi kepercayaan digital yang disesuaikan dengan prioritas, kapasitas institusional, dan tantangan domestiknya. Pemahaman terhadap berbagai pendekatan ini memberikan dasar yang kuat untuk mengidentifikasi peluang sinergi, serta merumuskan langkah-langkah strategis guna memperkuat ekosistem kepercayaan digital di tingkat nasional maupun global.

Kepercayaan digital merupakan elemen kunci dalam ekosistem digital modern, di mana setiap negara menerapkan pendekatan yang berbeda dalam membangunnya. Analisis komparatif terhadap kebijakan kepercayaan digital di Singapura, Malaysia, Uni Eropa, Amerika Latin, dan Turki menunjukkan bahwa meskipun terdapat perbedaan dalam konteks sosial, ekonomi, dan regulasi, semua negara dan kawasan tersebut memiliki tujuan yang sama, yaitu membangun ekosistem digital yang aman, transparan, dan tepercaya.

Tabel 3.1: Analisis Komparatif Kepercayaan Digital Negara

Aspek	Singapura	Malaysia	Uni Eropa	Amerika Latin	Turki
***Why*: Mengapa kerangka kepercayaan digital menjadi hal penting bagi negara atau wilayah tersebut?**	Menjaga posisinya sebagai pusat digital global dan mengamankan kepercayaan warga terhadap layanan *e-government*.	Meningkatkan postur keamanan siber nasional dan membangun kepercayaan dalam perlindungan data berdasarkan Akta PDPA No 709.	Menjaga kebebasan sipil dan memperkuat otonomi strategis di pasar tunggal digital.	Menjembatani kesenjangan kepercayaan yang diperburuk oleh misinformasi dan ancaman siber.	Memperkuat kepercayaan publik terhadap *e-government* dan memastikan keamanan serta kerja sama dalam transformasi digital.
***What*: Apa saja yang menjadi tujuan dan ruang lingkup kerangka kerja kepercayaan digital?**	Memastikan infrastruktur tangguh, meningkatkan keamanan siber, dan mendorong transparansi tata kelola.	Mendorong platform digital yang aman dan teknologi yang bertanggung jawab.	Menciptakan pasar digital tepercaya dengan menyelaraskan regulasi seperti eIDAS dan NIS2.	Mendorong adopsi digital yang aman dengan melindungi data pengguna dan nilai sosial.	Menyediakan layanan publik yang berpusat pada warga dan membangun kerangka tata kelola data yang kuat.
***Who*: Siapa saja aktor yang terlibat dalam perencanaan, penerapan, dan pengendalian kepercayaan digital?**	Pemerintah (IMDA, GovTech) dan pihak swasta/industri; warga negara melalui literasi digital.	Pemerintah (Komisaris PDPA), bisnis, serta individu melalui kepatuhan dan praktik aman.	Komisi Eropa, negara anggota, sektor swasta/industri, dan masyarakat sipil.	Pemerintah dan sektor swasta/industri dengan peran aktif masyarakat sipil.	Digital Transformation Office (DTO) dengan dukungan pemangku kepentingan publik dan swasta/industri.
***When*: Kapan target implementasi kepercayaan digital tercapai berdasarkan lini masanya?**	Pembaruan rutin undang-undang dan inisiatif seperti Safer Cyberspace Masterplan.	Menargetkan 2030 dalam peta jalan transformasi digital nasional.	Progresif, dengan tonggak sejarah pada 2024, menuju cakupan penuh pada 2030.	Bervariasi di setiap negara, dengan peningkatan sejak 2022 berdasarkan strategi regional.	Mengikuti rekomendasi OECD, dengan target kematangan digital tingkat lanjut pada 2030.
***How*: Bagaimana strategi penerapan kerangka kepercayaan digital untuk mencapai tujuan?**	Membangun sistem tangguh, kampanye kesadaran publik, dan kolaborasi internasional.	Menerapkan PDPA 709, mempromosikan edukasi keamanan data, dan adopsi Model Kepercayaan Digital.	Perundang-undangan (eIDAS, Undang-Undang Ketahanan Siber), kemitraan publik-swasta/industri, dan investasi dalam keamanan siber.	Mengadopsi standar internasional dan membuat strategi keamanan siber lokal.	Mengintegrasikan layanan publik berbasis data, meningkatkan keterampilan digital, dan menerapkan kerangka OECD.

Tabel 3.1 memperlihatkan variasi dalam praktik terbaik kepercayaan digital di masing-masing negara, termasuk alasan penerapan, tujuan utama, pemangku kepentingan yang terlibat, jadwal implementasi, serta strategi yang digunakan. Perbedaan ini mencerminkan bagaimana setiap negara menyesuaikan kebijakan mereka dengan kebutuhan lokal serta dinamika global dalam memastikan kepercayaan digital tetap terjaga.

1. Perbedaan dan Persamaan dalam Alasan Membangun Kepercayaan Digital
   Setiap negara memiliki motivasi yang berbeda dalam membangun kepercayaan digital, bergantung pada kebutuhan dan tantangan yang dihadapi. Singapura berusaha mempertahankan posisinya sebagai pusat digital global dengan memastikan kepercayaan warga terhadap layanan *e-government*. Malaysia fokus pada peningkatan keamanan siber nasional dan kepatuhan terhadap regulasi perlindungan data, seperti Akta PDPA No. 709. Uni Eropa menekankan perlindungan kebebasan sipil dan otonomi strategis di pasar digital tunggal, sementara negara-negara di Amerika Latin berupaya menjembatani kesenjangan kepercayaan akibat meningkatnya misinformasi dan ancaman siber. Turki, di sisi lain, berfokus pada memperkuat kepercayaan publik terhadap *e-government* serta memastikan keamanan dalam transformasi digital.

2. Tujuan Implementasi Kepercayaan Digital
   Negara-negara tersebut memiliki kesamaan dalam upaya membangun infrastruktur digital yang tangguh dan transparan. Singapura berupaya meningkatkan keamanan siber dan tata kelola yang lebih transparan. Malaysia menargetkan ekosistem digital yang aman dengan adopsi teknologi yang bertanggung jawab. Uni Eropa memanfaatkan regulasi seperti eIDAS dan NIS2 untuk menciptakan pasar digital yang lebih tepercaya. Sementara itu, Amerika Latin berfokus pada adopsi digital yang lebih aman dengan menjaga perlindungan data dan nilai sosial. Turki berorientasi pada pembangunan layanan publik berbasis data serta tata kelola yang kuat.

3. Pemangku Kepentingan dalam Kepercayaan Digital
   Implementasi kepercayaan digital melibatkan berbagai pemangku kepentingan di masing-masing negara. Singapura dan Malaysia menempatkan pemerintah sebagai aktor utama yang didukung oleh sektor swasta/industri dan masyarakat dalam membangun kepercayaan digital. Uni Eropa memiliki struktur lebih kompleks dengan Komisi Eropa sebagai pengarah kebijakan, negara anggota yang mengimplementasikan regulasi, serta peran signifikan sektor swasta/industri dan masyarakat sipil. Di Amerika Latin, pendekatan kolaboratif antara pemerintah, sektor swasta/industri, dan masyarakat sipil semakin ditekankan. Turki mengandalkan Digital Transformation Office (DTO) sebagai pengelola utama dengan dukungan pemangku kepentingan publik dan swasta/industri.

4. Jadwal Implementasi Kepercayaan Digital
   Dalam hal jadwal implementasi, negara-negara ini memiliki target yang berbeda. Singapura terus memperbarui regulasi dan inisiatif keamanan sibernya

melalui program seperti Safer Cyberspace Masterplan. Malaysia menetapkan tahun 2030 sebagai target utama dalam peta jalan transformasi digitalnya. Uni Eropa menerapkan pendekatan progresif dengan tonggak sejarah pada tahun 2024 untuk menuju cakupan penuh pada 2030. Sementara itu, di Amerika Latin, implementasi kepercayaan digital berlangsung secara bertahap sejak 2022, tergantung pada strategi masing-masing negara. Turki mengikuti rekomendasi OECD dengan tujuan mencapai tingkat kematangan digital yang lebih tinggi pada tahun 2030.

5. Strategi untuk Memajukan Kepercayaan Digital
   Negara-negara ini mengadopsi berbagai strategi dalam membangun kepercayaan digital. Singapura mengandalkan sistem keamanan siber yang kuat, kampanye kesadaran publik, dan kolaborasi internasional. Malaysia menerapkan regulasi PDPA 709 serta mempromosikan edukasi keamanan data dan adopsi *Digital Trust Model*. Uni Eropa menekankan pada regulasi yang kuat, seperti eIDAS dan Undang-Undang Ketahanan Siber, serta investasi dalam keamanan siber melalui kemitraan publik-swasta/industri. Amerika Latin berfokus pada adopsi standar internasional dan strategi keamanan siber lokal. Sementara itu, Turki mengintegrasikan layanan publik berbasis data, meningkatkan literasi digital, dan mengadopsi kerangka kebijakan dari OECD.

6. Implikasi dan Tantangan di Masa Depan
   Meskipun setiap negara memiliki tantangan dan pendekatan yang berbeda dalam membangun kepercayaan digital, terdapat pola yang serupa dalam aspek regulasi, peran pemerintah dan sektor swasta/industri, serta strategi keamanan siber. Dari analisis ini, dapat disimpulkan bahwa negara-negara dengan regulasi yang lebih matang, seperti Singapura dan Uni Eropa, lebih siap menghadapi tantangan dalam membangun kepercayaan digital. Mereka memiliki kebijakan yang lebih terstruktur serta kolaborasi erat antara sektor publik dan swasta/industri. Di sisi lain, negara-negara berkembang seperti Malaysia, Amerika Latin, dan Turki masih menghadapi tantangan dalam membangun ekosistem digital yang aman dan tepercaya, terutama dalam hal literasi digital, infrastruktur teknologi, serta kepercayaan publik terhadap sistem digital yang baru diadopsi.
   Selain itu, ancaman keamanan siber yang terus berkembang serta tantangan dalam penegakan regulasi dan kepatuhan terhadap standar internasional tetap menjadi hambatan yang harus diatasi oleh semua negara. Kerja sama internasional, peningkatan kapasitas teknologi, serta edukasi digital bagi masyarakat menjadi faktor kunci dalam memastikan kepercayaan digital dapat diimplementasikan secara efektif dan berkelanjutan.
   Dengan adanya komitmen yang kuat dari pemerintah, sektor swasta/industri, dan masyarakat, kepercayaan digital dapat menjadi landasan utama bagi transformasi digital yang sukses di berbagai negara, memungkinkan pertumbuhan ekonomi digital yang berkelanjutan serta memberikan manfaat yang lebih luas bagi masyarakat.

3.3 Praktik Terbaik Kepercayaan Digital Komunitas

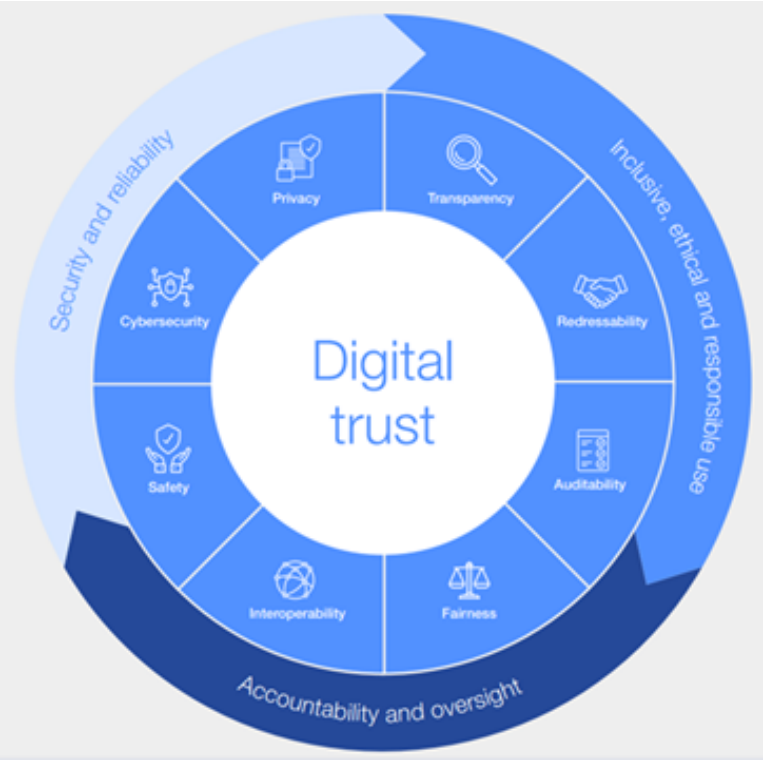
Kepercayaan digital tidak hanya menjadi tanggung jawab pemerintah, tetapi juga tanggung jawab komunitas global yang terdiri atas organisasi internasional, perusahaan konsultan, dan asosiasi profesional. Berbagai lembaga telah mengembangkan kerangka kerja kepercayaan digital yang memberikan panduan bagi organisasi dalam membangun sistem digital yang aman, transparan, dan dapat diandalkan. Beberapa komunitas terkemuka yang menjadi referensi global meliputi: World Economic Forum (WEF), PricewaterhouseCoopers (PwC), dan Information Systems Audit and Control Association (ISACA). Bagian ini membahas bagaimana masing-masing komunitas atau organisasi tersebut mendefinisikan kepercayaan digital dan bagaimana prinsip-prinsip yang mereka kembangkan dapat diterapkan dalam berbagai sektor industri. Sama halnya dengan bahasan sebelumnya, hasil analisis kerangka kerja kepercayaan digital yang ditawarkan oleh organisasi internasional ini disajikan dengan pendekatan pertanyaan tematik 5W1H (*Where, Why, What, Who, When, How*).

3.3.1 World Economic Forum (WEF)

Digital Trust Initiative dari World Economic Forum (WEF) menjelaskan bahwa kepercayaan digital adalah kepercayaan orang terhadap teknologi dan layanan digital, serta organisasi yang menyediakannya, untuk melindungi kepentingan semua pihak dan mematuhi nilai-nilai masyarakat [77]. Berdasarkan definisi ini, WEF telah membuat panduan untuk membantu organisasi mengambil keputusan, merencanakan langkah implementasi, memulai penerapan, dan mengukur tingkat kepercayaan digital. Dokumen ini melanjutkan upaya tersebut dengan menegaskan bahwa manusia harus menjadi pusat perhatian dalam pengembangan teknologi. Dokumen ini juga memberikan panduan bagi pemimpin bisnis, pemerintah, dan masyarakat agar lebih memahami pentingnya peran manusia dalam membangun kepercayaan digital. Dengan teknologi baru seperti *generative AI* yang berkembang pesat, fokus pada teknologi yang memprioritaskan manusia menjadi semakin penting. Kepercayaan terhadap teknologi, khususnya teknologi baru dan yang sedang berkembang seperti kecerdasan artifisial (AI) harus diperoleh melalui pengambilan keputusan yang bertanggung jawab dan menekankan bahwa individu dan masyarakat memiliki wewenang atas masa depan teknologi.

Pada tahun 2022, World Economic Forum (WEF) telah menerbitkan kerangka kerja tentang kepercayaan digital (*digital trust*) yang telah dibuat dengan berkolaborasi bersama tiga perusahaan besar, yaitu Accenture, KPMG, dan PWC. Kerangka kerja kepercayaan digital tersebut mendefinisikan tiga buah tujuan (*goals*) atau nilai bersama yang dapat merepresentasikan konsep kepercayaan digital, serta delapan buah dimensi (*dimensions*) yang dapat digunakan untuk mengoperasionalkan dan mengevaluasi kepercayaan terhadap teknologi digital, sebagaimana tampak pada Gambar 3.6. Kerangka kerja tersebut direkomendasikan untuk digunakan sebagai

panduan dalam pengambilan keputusan bagi para pemimpin di tingkat tertinggi.



Gambar 3.6: Kerangka Kerja Kepercayaan Digital WEF [77]

Dalam membangun kepercayaan digital, perancangan teknologi perlu mempertimbangkan tujuan-tujuan tertentu yang mencerminkan harapan masyarakat, norma dan nilai yang berlaku, serta kebiasaan lokal di mana teknologi tersebut diterapkan. Pendekatan ini penting agar masyarakat merasa yakin dan percaya untuk menggunakan teknologi tersebut. Dalam kerangka kerjanya, World Economic Forum (WEF) mendefinisikan tiga tujuan utama (*goals*), yaitu:

1. Keamanan dan keandalan (*Security and reliability*);
2. Akuntabilitas dan pengawasan (*Accountability and oversight*); dan
3. Penggunaan yang aman,berkelanjutan, etis, dan bertanggung jawab (*secure,reliable, ethical and responsible use*).

Terdapat delapan faktor penting yang dapat mendukung agar ketiga tujuan tersebut dapat dipenuhi, sehingga kepercayaan digital dapat dicapai, yaitu:

1. Keamanan siber (*cybersecurity*);

2. Keselamatan (*safety*);
3. Transparansi (*transparency*);
4. Interoperabilitas (*interoperability*);
5. Kemampuan diaudit (*auditability*);
6. Kemampuan memperbaiki kesalahan (*redressability*);
7. Keadilan (*fairness*); dan
8. Privasi (*privacy*).

Pada tahun 2024, dua tahun setelah kerangka kerja tersebut diterbitkan, WEF kembali merilis *white paper* dengan judul "*Digital Trust: Supporting Individual Agency*". Dalam *white paper* tersebut, WEF menekankan bahwa dari 8 (delapan) dimensi yang terdapat pada kerangka kerja yang dirilis sebelumnya, terdapat 3 (tiga) aspek atau dimensi utama yang sangat berperan dalam keberhasilan untuk mencapai kepercayaan digital, yaitu transparansi, privasi, dan penyelesaian masalah, baik dari sudut pandang organisasi, pemerintah, dan individu. Fokus utamanya adalah mendukung kendali dan hak individu.

Para pemimpin bisnis dan pemerintah didorong untuk selalu mempertimbangkan sudut pandang individu di setiap tahap pengembangan teknologi, dengan memastikan transparansi dan privasi sudah menjadi bagian utama sejak awal. Jika semua pihak menjalankan perannya, diharapkan manfaat dari teknologi baru dapat dimaksimalkan sambil membangun kepercayaan di antara semua pihak yang terlibat.

Mengapa Kepercayaan Digital Penting (*Why*)

Kepercayaan digital berperan penting dalam mendorong adopsi teknologi baru dan memastikan manfaatnya dapat dirasakan secara adil oleh semua pemangku kepentingan. Harapan bahwa teknologi digital, serta organisasi di belakangnya, akan melindungi kepentingan masyarakat dan menjunjung tinggi nilai-nilai fundamental menjadi dasar dari kepercayaan ini. Ketika individu dan pemerintah semakin menuntut agar perusahaan menghormati nilai-nilai sosial, kegagalan memenuhi ekspektasi tersebut dapat menyebabkan penurunan dukungan terhadap organisasi yang bersangkutan. Selain itu, kepercayaan digital turut menjaga stabilitas lembaga sosial dengan mempromosikan keadilan serta meminimalkan potensi risiko, yang pada akhirnya memperkuat kohesi sosial.

Di era ketika teknologi digital mendukung hampir seluruh transaksi ekonomi, hubungan sosial, dan lembaga masyarakat, kepercayaan digital menjadi lebih krusial dari sebelumnya. Sayangnya, kepercayaan terhadap teknologi, inovasi, dan ilmu pengetahuan mengalami penurunan di berbagai belahan dunia. Menanggapi tantangan ini, WEF meluncurkan *Digital Trust Initiative* sebagai upaya membangun kembali kepercayaan melalui kebijakan yang memastikan teknologi dapat diandalkan.

Secara umum, kepercayaan digital mengacu pada harapan bahwa teknologi dan layanan digital, beserta organisasi yang menyediakannya, akan melindungi kepentingan publik serta mematuhi nilai-nilai dan harapan masyarakat. Pendekatan ini tidak hanya menekankan manfaat teknis, tetapi juga aspek etika dan keadilan dalam penggunaan teknologi.

Menjaga hak individu, menghormati pilihan mereka, serta mengutamakan nilai-nilai kemanusiaan menjadi prinsip utama dalam membangun kembali kepercayaan terhadap teknologi digital. Individual *agency by design*, yaitu pendekatan yang menempatkan kendali pengguna sebagai inti dari desain teknologi, perlu diterapkan dalam pengembangan inovasi maupun kebijakan regulasi guna memastikan kepercayaan digital tetap terjaga.

Tujuan Pengenalan Kepercayaan Digital (*What*)

Kepercayaan digital menjadi sangat penting di era ketika teknologi digital mendukung hampir seluruh aspek kehidupan, mulai dari transaksi ekonomi hingga hubungan sosial dan tata kelola kelembagaan. Meskipun demikian, kepercayaan terhadap teknologi, inovasi, dan ilmu pengetahuan menunjukkan tren penurunan di berbagai belahan dunia. Untuk merespons tantangan ini, WEF meluncurkan *Digital Trust Initiative* yang bertujuan membangun kembali kepercayaan publik melalui pengambilan keputusan yang mendukung pengembangan teknologi yang dapat dipercaya.

Kepercayaan digital didefinisikan sebagai harapan bahwa teknologi dan layanan digital, beserta organisasi yang menyediakannya, akan melindungi kepentingan seluruh pemangku kepentingan serta mematuhi nilai-nilai dan harapan masyarakat. Definisi ini menekankan bahwa teknologi tidak hanya harus bermanfaat secara teknis, tetapi juga harus dikembangkan secara etis dan adil.

Dalam kerangka kerjanya, WEF menekankan pentingnya perlindungan hak individu, penghormatan terhadap pilihan pengguna, serta penempatan nilai-nilai kemanusiaan sebagai dasar dalam membangun kepercayaan digital. Pendekatan ini dikenal sebagai *individual agency by design*, yakni prinsip bahwa teknologi harus dirancang untuk memperkuat kendali pengguna. Prinsip ini perlu menjadi inti dari strategi pengembangan teknologi maupun kebijakan regulasi guna memperoleh dan mempertahankan kepercayaan masyarakat terhadap ekosistem digital.

Siapa yang Bertanggung Jawab (*Who*)

Pihak yang terlibat dalam pembentukan kepercayaan digital meliputi perusahaan teknologi, pemerintah, pembuat kebijakan, masyarakat, dan organisasi nirlaba. WEF menekankan bahwa kepercayaan digital adalah tanggung jawab bersama yang melibatkan semua pemangku kepentingan, mulai dari penyedia teknologi hingga pengguna, dalam memastikan keamanan dan tanggung jawab dalam penggunaan teknologi digital.

Waktu dan Tahapan Implementasi (*When*)

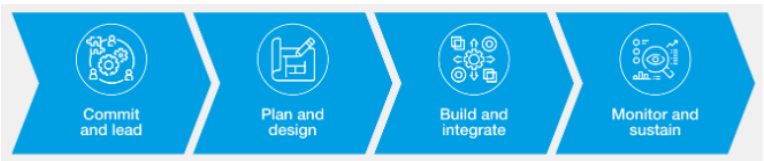
Kerangka kerja ini merupakan pedoman strategis bagi para pengambil keputusan dalam upaya memenuhi harapan individu dan masyarakat, sekaligus membangun kepercayaan digital secara berkelanjutan. Pendekatan kolaboratif menjadi prinsip utama dalam proses pengambilan keputusan terkait teknologi, menggantikan pola kerja yang terfragmentasi. Cakupan panduan meliputi proses perancangan, pengembangan, pembangunan, hingga pemeliharaan dimensi-dimensi utama dari kepercayaan digital.

Struktur panduan dirancang untuk mendukung pengambilan keputusan secara menyeluruh. Fokus tidak hanya diarahkan pada satu aspek kepercayaan digital, melainkan juga mencakup instrumen implementasi operasional yang dapat diadopsi oleh organisasi secara sistematis dan terukur.

Melalui penerapan panduan ini, organisasi memperoleh dukungan dalam:

1. Integrasi nilai-nilai etis dan kepentingan publik dalam pengembangan teknologi;
2. Peningkatan konsistensi dan efektivitas kebijakan yang mendukung kepercayaan digital;
3. Pemeliharaan kepercayaan dari berbagai pemangku kepentingan melalui prinsip transparansi dan akuntabilitas;
4. Pengelolaan risiko serta dampak sosial dari adopsi teknologi secara terukur dan bertanggung jawab.

Panduan ini berfungsi sebagai arahan strategis bagi para pemimpin organisasi dalam pelaksanaan langkah-langkah yang diperlukan guna memastikan penerapan kerangka kerja kepercayaan digital secara efektif. Penekanan diberikan pada pentingnya pendekatan yang sistematis, terstruktur, dan berorientasi pada nilai, sehingga organisasi mampu menjawab ekspektasi publik serta tantangan etis dan teknologi secara seimbang dan berkelanjutan.



Gambar 3.7: Peta Jalan Kepercayaan Digital WEF [77]

Upaya yang dijelaskan dalam *white paper* bertujuan untuk mendukung *individual agency*, namun bukan merupakan solusi tunggal. Pendekatan ini hanya merupakan bagian dari elemen yang lebih luas dalam kerangka perlindungan dan dukungan organisasi. Urutan intervensi yang disampaikan tidak dimaksudkan sebagai hierarki preferensi atau tahapan penerapan, melainkan menggambarkan pendekatan yang

mengedepankan kerja sama dan upaya pencegahan terlebih dahulu, kemudian dilanjutkan dengan mekanisme penyelesaian masalah secara responsif.

Bagaimana Kepercayaan Digital Diterapkan (*How*)

Kendali individu (*individual agency*), penghormatan terhadap hak asasi manusia, serta pengakuan terhadap pilihan dan nilai-nilai pengguna merupakan unsur penting dalam membangun kembali kepercayaan terhadap teknologi digital. Dalam kerangka kerja yang dikembangkan oleh WEF, prinsip *individual agency by design* ditempatkan sebagai prinsip utama untuk memastikan bahwa teknologi dirancang sejak awal guna melindungi hak dan kendali individu. WEF menekankan bahwa pendekatan ini bukan hanya aspek teknis, melainkan strategi etis yang menempatkan nilai-nilai kemanusiaan sebagai pusat pengambilan keputusan teknologi dan kebijakan. Dengan demikian, kepercayaan digital tidak hanya dibangun melalui keamanan dan transparansi, tetapi juga melalui komitmen terhadap partisipasi, perlindungan hak, dan pemberdayaan pengguna.

Prinsip ini berfokus pada tiga aspek utama: transparansi, privasi, dan mekanisme penyelesaian masalah (*redressability*).

- Transparansi
  Pengguna harus dapat memahami dan mengendalikan cara teknologi bekerja agar hanya berfungsi sesuai harapan mereka. Transparansi dapat diterapkan melalui:
  - Penyediaan informasi yang jelas mengenai produk dan layanan digital.
  - Program literasi digital yang efektif.
  - Alat transparansi yang mudah diakses dan digunakan.
- Privasi
  Perlindungan data pribadi dan keamanan interaksi *online* menjadi prioritas utama dalam menjaga privasi pengguna. Upaya yang dapat dilakukan meliputi:
  - Kepatuhan terhadap aturan privasi yang ketat dan menyeluruh.
  - Penyediaan mekanisme persetujuan yang jelas serta alat pendukung untuk mengontrol data pribadi.
- Mekanisme Penyelesaian Masalah (*redressability*)
  Tidak semua risiko teknologi dapat dihindari, sehingga perlu ada mekanisme yang memastikan hak pengguna tetap terlindungi. Beberapa langkah yang dapat diambil antara lain:
  - Penerapan aturan yang memungkinkan individu menegakkan hak mereka sebagai pengguna atau konsumen.
  - Prosedur penyelesaian yang memungkinkan komunikasi langsung antara individu dan pengembang atau pemilik teknologi.

- Pengawasan pihak ketiga untuk memastikan penyelesaian masalah dilakukan secara adil.

Kepercayaan digital menjadi isu global, terutama bagi negara-negara yang telah atau sedang mengadopsi teknologi digital secara luas. WEF mendorong penerapan konsep ini melalui berbagai forum internasional, termasuk pertemuan tahunan yang melibatkan pemangku kepentingan dari berbagai sektor. Pada akhirnya, membangun kepercayaan digital bukan hanya tanggung jawab perusahaan atau pemerintah, tetapi juga masyarakat sipil dan individu. Prinsip-prinsip ini menjadi dasar bagi upaya kolektif dalam menciptakan ekosistem digital yang lebih aman dan dapat dipercaya.

3.3.2 PricewaterhouseCoopers (PwC)

Kerangka kerja kepercayaan digital yang diajukan oleh PricewaterhouseCoopers (PwC) adalah pendekatan yang digunakan untuk membangun dan mempertahankan kepercayaan dalam ekosistem digital, terutama di dunia yang semakin terhubung dengan teknologi dan data [78]. Kerangka kerja ini berfokus pada bagaimana perusahaan dapat memelihara kepercayaan pelanggan, mitra, dan pemangku kepentingan lainnya dengan menjaga aspek-aspek penting seperti keamanan, transparansi, dan tanggung jawab dalam penggunaan data.

Mengapa Kepercayaan Digital Penting (*Why*)

Kepercayaan digital menjadi elemen kunci dalam era modern, di mana perusahaan dan organisasi semakin mengandalkan teknologi untuk operasional dan interaksi. Peningkatan volume data pribadi, transaksi digital, dan interaksi *online* membawa tantangan baru terkait privasi, keamanan, dan transparansi. Dalam ekosistem yang saling terhubung, kepercayaan memungkinkan bisnis mengelola risiko, memanfaatkan peluang digital, serta menjaga keyakinan pelanggan, mitra, dan pemangku kepentingan terhadap sistem dan integritas data mereka. Tanpa kepercayaan yang kuat, perusahaan menghadapi kesulitan dalam berkembang dan mempertahankan hubungan jangka panjang, terutama di tengah ancaman seperti kebocoran data, serangan siber, dan penyalahgunaan informasi.

Peran krusial kepercayaan digital tidak hanya terbatas pada keamanan data, tetapi juga menjadi faktor penentu keberhasilan transformasi digital. Organisasi yang mampu membangun kepercayaan yang solid akan lebih siap menghadapi era digital dan membuka peluang pertumbuhan yang lebih luas. Pertumbuhan ekonomi digital tidak hanya ditentukan oleh inovasi dan kemajuan teknologi, tetapi juga oleh tingkat kepercayaan yang tertanam dalam setiap aspek operasional.

Integrasi kepercayaan digital dalam strategi nasional memperkuat ketahanan sistem dan proses suatu negara. Pendekatan ini memungkinkan pengelolaan risiko yang lebih efektif, mendukung pengambilan keputusan yang lebih baik, serta berkontribusi pada stabilitas ekonomi dan pertumbuhan berkelanjutan.

Sebagai dasar ekonomi digital, kepercayaan digital juga berperan dalam meningkatkan daya saing suatu negara di tingkat global. Ekosistem digital yang aman dan tepercaya menarik lebih banyak investasi, mendorong inovasi, serta mempercepat adopsi teknologi baru, menciptakan lingkungan yang kondusif bagi perkembangan ekonomi digital.

Tujuan Pengenalan Kepercayaan Digital (*What*)

Risiko digital dan kebutuhan untuk membangun kepercayaan harus dianggap sebagai isu perusahaan yang memerlukan dewan direksi untuk mengembangkan pemahaman yang jelas tentang profil risiko yang sesuai dengan kondisi bisnis mereka. Selain itu, perlu ada rencana tindakan yang tegas serta pemantauan dan jaminan berkala untuk memastikan risiko dikelola dengan baik. Kerangka kerja ini mengidentifikasi elemen-elemen kunci dalam membangun kepercayaan digital, yang mencakup hal-hal berikut.

- Keamanan siber dan perlindungan data: Melindungi data pribadi dan informasi sensitif dari ancaman baik dari dalam maupun luar organisasi.
- Kepercayaan pada sistem bisnis dan manajemen risiko TI: Menjamin bahwa sistem yang digunakan aman dan dapat diandalkan.
- Tata kelola data untuk keunggulan kompetitif: Mengelola data dengan bijaksana untuk mendapatkan nilai lebih, sembari tetap menjaga keamanan dan privasi.
- Kepastian dalam transformasi berbasis teknologi: Menjamin bahwa penerapan teknologi baru dilakukan secara aman dan sesuai standar yang berlaku.

Selain itu, penting juga untuk memperhatikan aspek transparansi, yang memastikan visibilitas yang jelas bagi pelanggan dan pemangku kepentingan mengenai penggunaan dan perlindungan data mereka, serta etika dan tanggung jawab, yang menjamin penggunaan teknologi, termasuk kecerdasan artifisial, secara etis dan bertanggung jawab. Kepatuhan terhadap regulasi yang berlaku, terutama terkait perlindungan data dan privasi, juga menjadi aspek yang tidak kalah penting dalam kerangka ini.

Siapa yang Bertanggung Jawab (*Who*)

Kerangka kerja kepercayaan digital ini melibatkan beberapa aktor utama, di antaranya:

- Perusahaan/Organisasi: Sebagai pihak yang bertanggung jawab dalam mengelola data dan teknologi. Mereka perlu memastikan bahwa mereka memenuhi standar keamanan dan privasi yang tinggi.

- Konsumen/Pengguna: Pihak yang harus diberi kepercayaan melalui perlindungan data yang tepat, transparansi tentang bagaimana data mereka digunakan, dan hak mereka untuk mengontrol informasi pribadi.
- Regulator: Badan yang menetapkan dan menegakkan peraturan yang berkaitan dengan perlindungan data dan kepercayaan digital.
- Pemangku Kepentingan lainnya: Misalnya, mitra bisnis, penyedia layanan pihak ketiga, atau pengembang teknologi yang turut terlibat dalam pengelolaan dan penggunaan data.

Waktu dan Tahapan Implementasi (*When*)

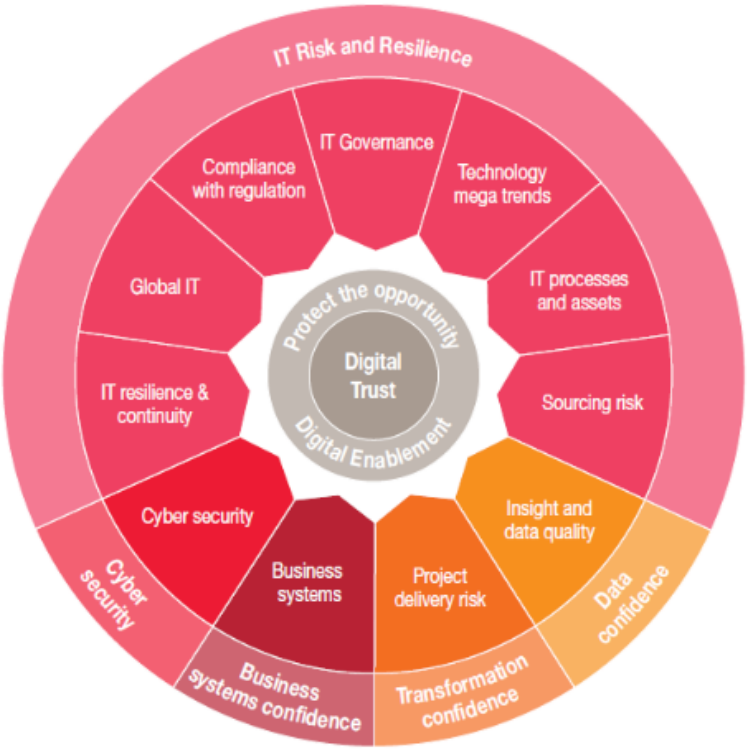
Kerangka kerja kepercayaan digital ini berfokus pada transformasi bisnis yang cepat dan terus berkembang, yang didorong oleh teknologi digital, dengan menekankan pentingnya penerapan strategi kepercayaan digital. Tren seperti hiper-konektivitas, perangkat seluler, adopsi *cloud*, dan *big data* telah mengubah dinamika kepercayaan dan risiko. Oleh karena itu, kepercayaan digital perlu dijaga secara konsisten, bukan hanya sebagai isu kepatuhan yang sesekali diterapkan, tetapi sebagai bagian integral dari operasi harian organisasi. Beberapa momen penting yang terkait dengan kepercayaan digital meliputi:

- Pengumpulan data: Organisasi harus memastikan transparansi dan memperoleh izin eksplisit dari pelanggan atau pengguna saat mengumpulkan data.
- Penggunaan data: Saat data diproses, penting untuk memberikan kejelasan dan kontrol mengenai bagaimana data tersebut digunakan.
- Pelanggaran atau insiden keamanan: Ketika terjadi kebocoran data atau serangan siber, organisasi harus segera merespons dan memberi tahu pihak terkait dengan cara yang transparan dan jujur.

Bagaimana Kepercayaan Digital Diterapkan (*How*)

Kepercayaan digital menjadi elemen mendasar dalam strategi organisasi, mencerminkan komitmen untuk memanfaatkan peluang digital secara efektif. Untuk mendukung hal ini, organisasi menerapkan pendekatan komprehensif dalam mengelola kontrol sistem bisnis, terutama dalam transisi pengguna antara sistem internal dan layanan berbasis *cloud*. Pendekatan ini meningkatkan keandalan serta kematangan lingkungan kontrol.

Dengan mengintegrasikan kepercayaan digital ke seluruh siklus hidup kontrol, desain sistem menjadi lebih kuat, dan keberlanjutan lingkungan kontrol semakin terjamin. Optimalisasi kontrol sistem juga berkontribusi pada peningkatan manajemen risiko serta pengambilan keputusan yang lebih baik, yang keduanya merupakan faktor utama dalam mempertahankan kepercayaan digital.



Gambar 3.8: Kerangka Kepercayaan Digital PwC [78]

Secara keseluruhan, kepercayaan digital bukan sekadar bagian dari strategi, tetapi juga terintegrasi dalam perencanaan dan operasional organisasi. Pendekatan ini memastikan adanya kerangka kerja yang kokoh untuk mengelola risiko dan kontrol secara efektif.

PwC menyediakan langkah-langkah konkret melalui kerangka kerja mereka, yang mencakup beberapa aspek utama (lihat Gambar 3.8):

1. Sistem Bisnis
   Perusahaan semakin bergantung pada sistem yang terintegrasi secara global, baik untuk operasi internal maupun interaksi dengan pelanggan dan pemasok. Meskipun banyak yang telah berinvestasi dalam teknologi ini, belum semuanya memanfaatkan praktik terbaik dalam standarisasi dan kontrol. Keamanan dan kontrol harus menjadi bagian integral dari sistem ini dan terus dipantau. Seiring berkembangnya teknologi, sistem tradisional akan semakin berinteraksi dengan aplikasi berbasis cloud, membawa risiko baru yang perlu dikelola.

2. Keamanan Siber
   Serangan siber terus berkembang, sementara banyak bisnis kesulitan mengimbangi ancaman ini. Meskipun pemerintah telah meningkatkan kesadaran

akan pentingnya keamanan siber, pendekatan baru tetap diperlukan untuk menghadapi ancaman yang terus berubah. Pelanggaran data tidak hanya berdampak finansial tetapi juga dapat merusak reputasi perusahaan secara signifikan.

3. Ketahanan dan Keberlanjutan Teknologi Informasi (TI)
   Layanan TI semakin kompleks dengan ketergantungan pada berbagai infrastruktur, sistem lama, teknologi seluler, dan vendor pihak ketiga. Kompleksitas ini dapat menyebabkan pemadaman TI yang berdampak besar. Selain itu, penggunaan *cloud* menambah dimensi risiko baru yang perlu diantisipasi.

4. Pengelolaan TI Global
   Pengoperasian sistem TI global menambah tantangan dalam hal kompleksitas dan risiko. Perbedaan pendekatan dan regulasi di berbagai wilayah dapat menciptakan kerentanan yang mengganggu stabilitas sistem global. Dukungan global yang tidak memadai dapat menyebabkan waktu henti yang tinggi dan efektivitas yang menurun. Selain itu, regulasi perlindungan data global yang semakin ketat menjadi faktor penting dalam pengelolaan TI global.

5. Kepatuhan terhadap Regulasi
   Banyak persyaratan kepatuhan saling terkait, sehingga pendekatan terpadu diperlukan untuk menghindari tumpang tindih kontrol atau celah yang dapat menyebabkan ketidakpatuhan. Kepatuhan yang efektif memastikan kelangsungan bisnis dan mengurangi risiko hukum.

6. Tata Kelola TI
   Struktur dan kerangka kerja TI memengaruhi kinerja keseluruhan perusahaan. Studi yang dilakukan Massachusetts Institute of Technology (MIT) menunjukkan bahwa bisnis dengan tata kelola TI yang baik memiliki laba 25% lebih tinggi dibandingkan perusahaan dengan tata kelola TI yang buruk. Oleh karena itu, tata kelola yang kuat menjadi faktor penting dalam efektivitas bisnis.

7. Tren Teknologi Mega
   Teknologi seperti big data, analitik, seluler, media sosial, dan cloud menjadi kekuatan utama yang memengaruhi bisnis dan menuntut peningkatan kepercayaan digital. Strategi bisnis yang tepat dalam era digital menjadi krusial untuk mempertahankan daya saing. Investasi dalam teknologi memang membawa risiko, tetapi mengabaikannya dapat menyebabkan kehilangan keunggulan kompetitif.

8. Proses dan Aset TI
   Proses TI yang kuat dan konsisten sangat penting untuk menjaga kebersihan TI. Inventaris aset TI yang tidak lengkap dapat menimbulkan masalah keamanan dan mengganggu investasi. Misalnya, 90% tinjauan lisensi perangkat lunak yang dilakukan oleh PwC menemukan adanya ketidakpatuhan, yang dapat berdampak pada reputasi dan keuangan perusahaan.

9. Risiko Sumber Daya Komputasi awan menawarkan penghematan biaya yang signifikan tetapi juga menghadirkan risiko terkait penyimpanan dan pengamanan data. Pengalihdayaan sering kali tidak berjalan sesuai harapan, memaksa perusahaan mengevaluasi ulang pendekatan mereka. Beberapa kegagalan TI besar dalam beberapa tahun terakhir disebabkan oleh pengelolaan alih daya yang buruk, sehingga perlindungan data harus menjadi prioritas dalam pengaturan ini.

10. Risiko Penyampaian Proyek
    Volume, biaya, dan kompleksitas proyek TI terus meningkat. Namun, seperempat dari semua proyek gagal total dan setengahnya terlambat diselesaikan atau melebihi anggaran. Di era digital, keberhasilan bisnis akan semakin bergantung pada transformasi yang didorong oleh teknologi dan kecepatan perubahan akan meningkat.

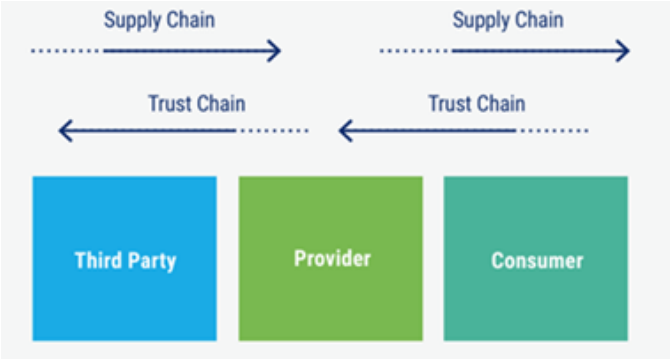
11. Wawasan dan Kualitas Data
    Data adalah elemen vital dalam suatu organisasi. Dengan data, individu dapat mengevaluasi kinerja dan menentukan langkah strategis selanjutnya. Pengelolaan data yang baik tidak hanya meningkatkan efisiensi, tetapi juga menciptakan proses yang transparan. Transparansi ini memperkuat reputasi organisasi dan membangun kepercayaan di antara pelanggan, pemasok, serta pegawai.

Kerangka kerja kepercayaan digital yang dikembangkan oleh PwC memberikan panduan bagi organisasi dalam membangun dan mempertahankan kepercayaan di era digital. Aspek utama dari kerangka ini meliputi perlindungan data, transparansi, etika, kepatuhan terhadap regulasi, dan penerapan praktik terbaik dalam mitigasi risiko digital. Dengan kepercayaan yang terjaga, perusahaan dapat memastikan kesuksesan jangka panjang dalam menghadapi tantangan digital yang terus berkembang.

3.3.3 Information Systems Audit and Control Association (ISACA)

Information Systems Audit and Control Association (ISACA) adalah organisasi profesi internasional yang berfokus pada tata kelola teknologi informasi. Sejak 2008, singkatan ISACA tidak lagi digunakan secara resmi, dan nama tersebut langsung merujuk pada organisasi itu sendiri. Sebagai organisasi profesi, ISACA menyediakan sertifikasi, pelatihan, panduan praktik terbaik, serta berbagai sumber daya bagi para profesional di bidang audit TI, pengendalian, keamanan, serta manajemen dan tata kelola TI. Salah satu sertifikasi paling terkenal yang dikeluarkan adalah *Certified Information Systems Auditor* (CISA). Selain itu, ISACA dikenal sebagai penerbit kerangka kerja COBIT (*Control Objectives for Information and Related Technologies*), yang banyak digunakan secara global untuk membantu organisasi dalam mengelola dan mengendalikan TI secara efektif.

Sejak 2020, ISACA mulai membahas kepercayaan digital, terutama di tengah pandemi COVID-19 yang mempercepat transformasi digital di berbagai aspek kehidupan. Kepercayaan digital, menurut ISACA, merujuk pada keyakinan terhadap integritas hubungan, interaksi, dan transaksi antara penyedia dan konsumen dalam ekosistem digital [93]. Konsep ini mencakup kemampuan individu, organisasi, proses, informasi, dan teknologi dalam menciptakan serta mempertahankan dunia digital yang dapat dipercaya.



Gambar 3.9: Rantai pasok hubungan oleh ISACA [93]

Mengapa Kepercayaan Digital Penting (*Why*)

Kepercayaan digital memainkan peran krusial dalam membangun hubungan yang transparan dan mengurangi dampak negatif dari pelanggaran serta insiden keamanan. Dengan membangun nilai dan kepercayaan sejak awal, suatu negara dapat memperkuat reputasinya serta memitigasi potensi krisis yang dapat timbul di dunia digital. Selain itu, organisasi dapat terhubung dan menjalankan bisnis secara lebih efektif dalam ekosistem digital yang semakin berkembang. Jejak digital yang tepercaya menjadi elemen utama dalam menjaga kepercayaan konsumen, karyawan, dan mitra bisnis. Kepercayaan ini tidak hanya mendukung pencapaian tujuan nasional, tetapi juga memastikan relevansi dalam lanskap digital yang terus berubah.

Seiring dengan percepatan transformasi digital, peningkatan kepercayaan digital menghadirkan peluang besar bagi pertumbuhan ekonomi. Studi menunjukkan bahwa stabilitas dan keamanan digital dapat memberikan kontribusi signifikan terhadap perekonomian global, dengan potensi peningkatan hingga triliunan dolar pada tahun 2025. Stabilitas ekonomi, keamanan nasional, serta kelangsungan operasional suatu negara di era digital sangat bergantung pada keberlanjutan kepercayaan digital.

Dalam konteks ekonomi digital, kepercayaan dalam transaksi dan interaksi *online* mendorong pertumbuhan sektor *e-commerce*, berbagi data, serta kolaborasi lintas batas. Individu dan bisnis lebih cenderung berpartisipasi dalam ekosistem digital ketika mereka yakin akan keamanan dan privasi sistem yang digunakan. Kepercayaan ini menjadi dasar bagi inovasi, peningkatan produktivitas, dan ekspansi

peluang bisnis di berbagai sektor.

Namun, ancaman siber dapat mengikis kepercayaan terhadap sistem digital. Serangan siber yang merusak data atau mengancam privasi berpotensi menurunkan kredibilitas suatu organisasi, bahkan mempengaruhi nilai pasar modalnya. Keamanan siber harus menjadi prioritas utama untuk menjaga dan meningkatkan kepercayaan digital. Penerapan langkah-langkah keamanan yang ketat serta kepatuhan terhadap praktik terbaik memungkinkan organisasi mengurangi risiko, melindungi informasi sensitif, serta memperkuat hubungan dengan para pemangku kepentingan.

Selain aspek ekonomi dan keamanan, kepercayaan digital juga berdampak langsung pada kepuasan pelanggan. Pengguna lebih cenderung berinteraksi dan menggunakan layanan digital dari organisasi yang mereka anggap aman dan tepercaya. Organisasi yang berkomitmen pada kepercayaan digital tidak hanya membangun hubungan jangka panjang dengan pelanggan, tetapi juga meningkatkan loyalitas, memperkuat reputasi melalui promosi dari mulut ke mulut, dan memastikan pertumbuhan bisnis yang berkelanjutan.

Tujuan Pengenalan Kepercayaan Digital (*What*)

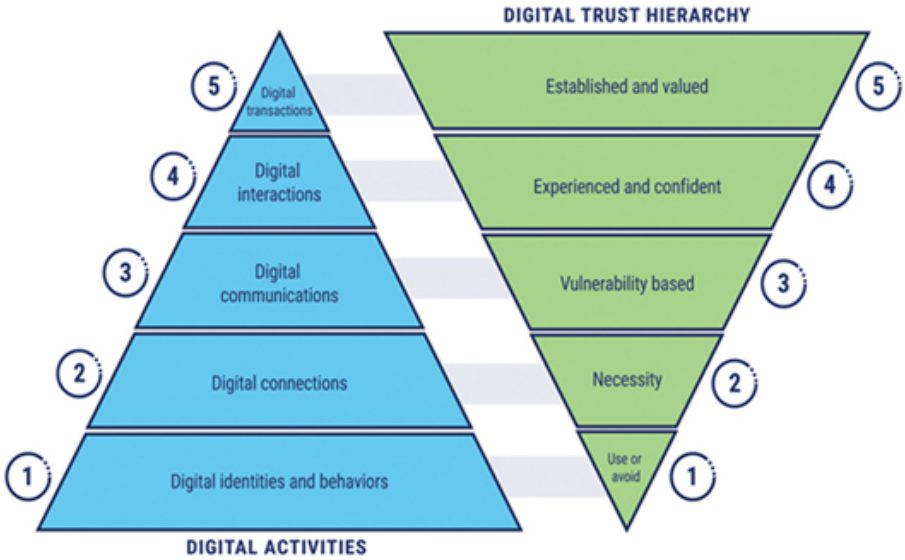
Pengenalan kepercayaan digital oleh negara bertujuan untuk memastikan bahwa organisasi memiliki jejak digital yang dapat dipercaya dan transparan. Kepercayaan ini menjadi faktor kunci dalam menjalankan bisnis di era digital, terutama karena transaksi *online* telah mengubah model bisnis tradisional dan menciptakan kebutuhan mendesak akan lingkungan yang aman dan tepercaya.

Dalam ekosistem digital, kepercayaan berperan dalam membangun nilai, memperkuat hubungan bisnis, meningkatkan pendapatan, serta mengurangi risiko dari pelanggaran dan insiden keamanan. Oleh karena itu, strategi kepercayaan digital perlu selaras dengan inisiatif transformasi digital agar organisasi siap menghadapi tantangan baru yang muncul akibat perkembangan teknologi seperti kecerdasan artifisial. Dengan demikian, upaya negara dalam membangun kepercayaan digital menjadi landasan penting bagi terciptanya lingkungan bisnis yang stabil dan aman di era digital.

Beberapa komponen utama yang mendukung kepercayaan digital mencakup *Quality, Resiliency, Transparency and Honesty, Ethics and Integrity, Availability, Security and Privacy. Quality* memastikan bahwa produk dan layanan memenuhi atau melampaui ekspektasi. *Resiliency* menjamin ketangguhan entitas terhadap gangguan eksternal. *Transparency and Honesty* menekankan kejujuran dalam penggunaan informasi dan mitigasi terhadap potensi penyalahgunaannya. *Ethics and Integrity* mencerminkan kepatuhan terhadap klaim yang telah dipublikasikan. *Availability* berkaitan dengan ketersediaan informasi dan layanan setiap saat, sementara *Security and Privacy* memastikan perlindungan serta kerahasiaan data.

Aktivitas dalam kepercayaan digital dapat digambarkan sebagai proses bertahap. Perjalanan ini dimulai dari transformasi digital, seperti identitas digital dan perubah-

an dari sistem manual ke representasi digital. Pada tahap awal, tingkat kepercayaan masih rendah, hanya sebatas penggunaan atau tidak. Seiring perkembangan, keterhubungan digital mulai tumbuh, meningkatkan kebutuhan akan kepercayaan digital (lihat Gambar 3.10).



Gambar 3.10: Korelasi aktivitas digital dengan derajat kepercayaan [93]

Langkah berikutnya melibatkan komunikasi digital, yang memerlukan perlindungan siber lebih dalam berdasarkan praktik terbaik dan analisis berbasis data. Pada tingkat lebih lanjut, interaksi digital semakin matang, memungkinkan penyedia layanan membangun ekosistem yang teruji dan andal. Tahapan tertinggi adalah transaksi digital, yang menjadi dasar dari ekonomi digital. Ekonomi digital inilah yang menciptakan nilai tambah serta memastikan kestabilan ekosistem digital secara keseluruhan.

Siapa yang Bertanggung Jawab (*Who*)

Peran *Chief Trust Officer* (CTO) menjadi krusial dalam mendukung kerja *Digital Trust Committee*, khususnya dalam mengawasi dan memastikan efektivitas inisiatif kepercayaan digital di seluruh organisasi. Keberadaan peran ini membawa manfaat strategis jangka panjang, seperti peningkatan pendapatan, penguatan keamanan dan privasi, loyalitas pelanggan, serta penguatan ekuitas merek melalui penerapan kepercayaan digital yang terukur dan berkelanjutan.

MATT CHIODI, CTO di Cerby sekaligus anggota *Digital Trust Advisory Board* ISACA, menekankan bahwa kepercayaan digital harus menjadi prioritas utama organisasi. Menurutnya, fokus pada kepercayaan digital tidak hanya mendorong pertumbuhan pendapatan, tetapi juga secara signifikan mengurangi risiko pelanggaran

data dan meningkatkan kepatuhan terhadap regulasi [274, 275].

Dalam konteks ini, organisasi disarankan untuk mengintegrasikan kepercayaan digital sebagai bagian dari strategi transformasi digital mereka. Tim kepemimpinan, termasuk dewan direksi, memiliki tanggung jawab utama untuk memastikan bahwa strategi kepercayaan digital selaras dengan visi, nilai, dan tujuan bisnis organisasi. Pada akhirnya, tanggung jawab utama atas tata kelola dan keberlanjutan kepercayaan digital berada pada CTO bersama jajaran pimpinan eksekutif.

Selain kepemimpinan strategis, keberhasilan pembangunan kepercayaan digital juga memerlukan komitmen bersama dari seluruh pemangku kepentingan dalam ekosistem digital. Setiap pihak memiliki peran dan tanggung jawab yang saling melengkapi:

- *Providers* bertanggung jawab memastikan layanan dan produk yang mereka tawarkan aman, bermanfaat, serta sesuai dengan standar etika dan regulasi. Keamanan dan privasi data pengguna menjadi aspek utama dalam komitmen ini.
- *Consumers* memiliki peran dalam menjaga informasi pribadi, menggunakan teknologi secara bijaksana, dan memahami risiko yang muncul dalam interaksi digital.
- *Third parties*, seperti pemasok atau mitra bisnis, harus menjalin kerja sama yang mengedepankan integritas dan transparansi dalam setiap transaksi dan interaksi digital.
- *Proxy technologies*, termasuk perangkat lunak dan perangkat keras yang menghubungkan pengguna dengan layanan, perlu dirancang dan dikelola dengan standar keamanan serta privasi yang tinggi.
- *Digital peers*, sebagai pihak yang berinteraksi dalam ekosistem digital, harus membangun kepercayaan melalui kerja sama yang mendukung lingkungan digital yang aman dan andal.

Dengan definisi peran yang jelas bagi setiap pemangku kepentingan, ISACA menegaskan bahwa kepercayaan digital dapat dipertahankan dan ditingkatkan melalui pengukuran level kepercayaan digital hingga sertifikasi untuk personel yang terlibat dalam ekosistem. Kerangka DTEF dengan pengelompokan peran membantu organisasi mengintegrasikan tata kelola, etika, manajemen risiko, dan landasan teknologi dalam membina dan mempertahankan kepercayaan digital secara tepat dan efektif.

Waktu dan Tahapan Implementasi (*When*)

Sejak tahun 2022, ISACA mulai memperkuat komunikasi dan pertemuan intensif dengan lebih dari 180 ribu anggota di 225 *chapter* di seluruh dunia. Pada periode tersebut, konsep kepercayaan digital diperkenalkan untuk menekankan pentingnya

kepercayaan dalam interaksi dan transaksi digital. Sebagai langkah konkret, ISACA meluncurkan Kerangka Kerja Ekosistem Kepercayaan Digital (*Digital Trust Ecosystem Framework* - DTEF) pada awal 2023, yang memberikan pendekatan bagi organisasi dalam membangun struktur yang selaras dengan prinsip-prinsip kepercayaan digital.

DTEF dirancang dengan fokus pada komponen utama seperti integritas, aksesibilitas, keberlanjutan, keamanan siber, perlindungan data, kualitas, transparansi, dan kejujuran. Selain itu, kerangka kerja ini mengintegrasikan berbagai praktik, aktivitas, output, kontrol, serta indikator kinerja utama (*Key Performance Indicator* - KPI) dan indikator risiko utama (*Key Risk Indicator* - KRI), sehingga menyediakan perangkat yang komprehensif untuk implementasi dan evaluasi capaian.

Sebagai kelanjutan dari inisiatif tersebut, ISACA merilis Sertifikat *Digital Trust Ecosystem Framework Foundation* pada pertengahan 2023 untuk menandai kompetensi dalam mengadopsi dan mengintegrasikan praktik kepercayaan digital di seluruh organisasi. Kemudian, pada akhir tahun yang sama, panduan implementasi DTEF diterbitkan guna memberikan arahan lebih rinci dalam menerapkan strategi kepercayaan digital secara menyeluruh.

Pada tahun 2024, ISACA memperkenalkan *Digital Trust Board Briefing*, sebuah dokumen yang dapat diunduh dalam format PDF, yang menjelaskan cara memanfaatkan DTEF untuk membangun ekosistem digital yang dapat dipercaya. Secara keseluruhan, tahapan dalam DTEF dikembangkan secara paralel dengan perhatian khusus pada domain-domain utama yang menjadi prioritas dalam penerapannya.

Bagaimana Kepercayaan Digital Diterapkan (*How*)

Kepercayaan digital diwujudkan melalui DTEF, yang menyediakan struktur untuk mendukung kepercayaan di seluruh ekosistem digital. Kerangka ini mempertimbangkan bagaimana hubungan antarpemangku kepentingan memengaruhi keterlibatan dengan konsumen, pelanggan, dan pengguna.

DTEF mengelompokkan faktor kepercayaan dalam berbagai domain yang krusial bagi keberhasilan integrasi teknologi AI dan pengiriman layanan digital. Peningkatan kepercayaan dilakukan secara berkelanjutan melalui umpan balik dan mekanisme evaluasi, memungkinkan interaksi manusia dengan aktor AI menjadi lebih dapat diandalkan.

Arsitektur kepercayaan digital menghubungkan data, manusia, proses, dan teknologi, menuntut pendekatan strategis untuk mengidentifikasi serta mengatasi kesenjangan antara kondisi saat ini dan yang diharapkan. Faktor manusia memiliki peran sentral dalam membangun kepercayaan digital, terutama dalam mengantisipasi kebutuhan sumber daya serta memastikan pemantauan yang ketat terhadap model AI agar tetap berfungsi sesuai tujuan.

Selain aspek teknis, kepercayaan digital juga bertumpu pada prinsip etika dan integritas, di mana individu diharapkan untuk menepati komitmen mereka guna menciptakan lingkungan interaksi yang dapat diandalkan. Transparansi dan keju-

juran menjadi elemen penting, termasuk keterbukaan dalam penggunaan data serta pengakuan terhadap potensi kompromi informasi.

Standar etika ini dipandang sebagai dasar dalam membangun dan mempertahankan kepercayaan digital di berbagai sektor. Secara keseluruhan, penerapan kepercayaan digital berakar pada perilaku etis dan komunikasi yang transparan, yang menjadi kunci dalam menciptakan interaksi digital yang aman dan dapat dipercaya.

3.4 Analisis Komparatif Praktik Terbaik Kepercayaan Digital Komunitas

Kepercayaan digital telah menjadi isu krusial dalam menghadapi tantangan dan peluang di era digital. Sebagai respons terhadap kompleksitas ini, berbagai organisasi dan komunitas global telah mengembangkan kerangka kerja, standar, dan praktik terbaik untuk membangun dan memelihara kepercayaan digital. Analisis ini akan membandingkan praktik terbaik kepercayaan digital dari tiga komunitas terkemuka, yaitu World Economic Forum (WEF), PricewaterhouseCoopers (PwC), dan Information Systems Audit and Control Association (ISACA), dengan menggunakan pendekatan kontekstual yang mencakup lima pertanyaan kunci: *Why*, *What*, *Who*, *When*, dan *How*.

- *Why* (Mengapa): Menjelaskan motivasi dan urgensi di balik upaya masing-masing komunitas dalam mempromosikan kepercayaan digital, termasuk tantangan global seperti keamanan siber, privasi data, dan etika teknologi.
- *What* (Apa): Mengidentifikasi kerangka kerja, inisiatif, atau rekomendasi utama yang dikembangkan oleh WEF, PwC, dan ISACA untuk meningkatkan kepercayaan digital.
- *Who* (Siapa): Menganalisis peran dan kolaborasi antara berbagai pemangku kepentingan, termasuk pemerintah, perusahaan, dan masyarakat sipil, yang terlibat dalam inisiatif ini.
- *When* (Kapan): Meninjau *timeline* perkembangan dan implementasi inisiatif kepercayaan digital oleh masing-masing komunitas.
- *How* (Bagaimana): Menjelaskan metode, alat, atau pendekatan yang digunakan oleh WEF, PwC, dan ISACA untuk mengimplementasikan dan memantau efektivitas praktik kepercayaan digital.

Dengan membandingkan kontribusi dan pendekatan dari ketiga komunitas tersebut, analisis ini diharapkan dapat memberikan pemahaman yang mendalam tentang bagaimana praktik terbaik kepercayaan digital komunitas dapat diadopsi, diadaptasi, atau diperluas untuk menghadapi tantangan digital yang terus berkembang. Hasil analisis ini diharapkan dapat menjadi referensi bagi organisasi dan negara dalam merancang strategi kepercayaan digital yang lebih efektif dan berkelanjutan.

Untuk memperoleh informasi yang lebih komprehensif, lima pertanyaan tematik diuraikan lebih lanjut menjadi sejumlah aspek yang dijadikan indikator komparasi antarketiga kerangka kerja kepercayaan digital yang dikembangkan oleh WEF, PwC, dan ISACA. Tabel 3.2 menyajikan keterkaitan antara pertanyaan tematik dengan aspek-aspek indikator tersebut.

Tabel 3.2: Aspek Pertanyaan Tematik Penerapan Kepercayaan Digital oleh Komunitas

Pertanyaan Tematik	**Penjelasan**	**Indikator Komparasi**
Mengapa kepercayaan digital penting	Menjelaskan motivasi dan urgensi di balik upaya komunitas dalam mempromosikan kepercayaan digital, termasuk isu global seperti keamanan siber, privasi, dan etika teknologi.	Peran Kepercayaan Digital Dampak terhadap Ekonomi Keamanan dan Risiko Strategi Implementasi Dampak pada Konsumen dan Bisnis
Apa tujuan memperkenalkan kepercayaan digital?	Mengidentifikasi kerangka kerja dan inisiatif dari WEF, PwC, dan ISACA untuk meningkatkan kepercayaan digital.	Tujuan Utama Fokus Kepercayaan Digital Strategi Implementasi Dampak terhadap Bisnis dan Masyarakat
Siapa yang bertanggung jawab atas kepercayaan digital?	Menganalisis peran dan kolaborasi antarpemangku kepentingan seperti pemerintah, perusahaan, dan masyarakat sipil.	Tanggung Jawab Utama Peran Perusahaan/Organisasi Peran Pemerintah/Regulator Peran Konsumen/Pengguna Peran Pihak Ketiga & Ekosistem Digital
Kapan waktu dan tahapan implementasi kepercayaan digital?	Meninjau tahapan dan waktu implementasi inisiatif kepercayaan digital masing-masing komunitas.	Fokus Utama Tahapan Implementasi Prinsip Utama Pendekatan
Bagaimana kepercayaan digital dapat diterapkan	Menjelaskan metode, alat, atau pendekatan yang digunakan untuk implementasi dan pemantauan kepercayaan digital.	Pendekatan Utama Fokus Implementasi Prinsip Pendukung Elemen Kunci

Tabel 3.3: Kepercayaan Digital menurut WEF, PwC, dan ISACA

Aspek	**WEF**	**PwC**	**ISACA**
Peran Kepercayaan Digital	Mendorong adopsi teknologi baru serta memastikan manfaat yang adil bagi semua pihak.	Elemen kunci dalam operasional bisnis dan interaksi digital yang aman.	Memperkuat transparansi dan mengurangi dampak negatif insiden keamanan.

Aspek	WEF	PwC	ISACA
Dampak terhadap Ekonomi	Menjaga stabilitas lembaga sosial dan memperkuat kohesi masyarakat.	Menentukan keberhasilan transformasi digital serta meningkatkan daya saing global.	Berkontribusi pada pertumbuhan ekonomi global hingga triliunan dolar.
Keamanan dan Risiko	Penurunan kepercayaan terhadap teknologi dapat menghambat inovasi dan adopsi digital.	Kepercayaan digital memungkinkan mitigasi risiko kebocoran data dan serangan siber.	Ancaman siber dapat mengikis kepercayaan dan memengaruhi nilai pasar organisasi.
Strategi Implementasi	Pendekatan berbasis kebijakan untuk memastikan teknologi dapat diandalkan.	Integrasi kepercayaan digital dalam strategi nasional guna mendukung stabilitas ekonomi.	Membangun kepercayaan sejak awal untuk memperkuat reputasi dan relevansi di era digital.
Dampak pada Konsumen & Bisnis	Mengutamakan hak individu dan prinsip *individual agency by design* dalam inovasi teknologi.	Meningkatkan loyalitas pelanggan serta menjaga hubungan jangka panjang dengan pemangku kepentingan.	Memastikan kepercayaan dalam transaksi dan interaksi *online*, mendukung pertumbuhan *e-commerce* dan bisnis digital.

Tabel 3.4: Tujuan Pengenalan Kepercayaan Digital menurut WEF, PwC, dan ISACA

Aspek	WEF	PwC	ISACA
Tujuan Utama	Mengembalikan kepercayaan terhadap teknologi dan inovasi melalui *Digital Trust Initiative*.	Mengelola risiko digital dengan pendekatan sistematis untuk membangun kepercayaan dalam bisnis.	Membangun jejak digital yang tepercaya dan transparan, mendukung lingkungan bisnis yang aman dan stabil.
Fokus Kepercayaan Digital	Menekankan pentingnya etika dan keadilan dalam penerapan teknologi serta *individual agency by design* untuk melindungi hak pengguna.	Mengintegrasikan keamanan siber, kepercayaan pada sistem bisnis, tata kelola data, dan transparansi untuk menjamin kepercayaan digital.	Menjamin kualitas, ketahanan, transparansi, kejujuran, etika, integritas, keamanan, dan privasi dalam ekosistem digital.
Strategi Implementasi	Membentuk kebijakan dan regulasi yang memastikan teknologi dapat dipercaya serta melindungi kepentingan publik.	Menerapkan pemantauan dan evaluasi berkala untuk memastikan pengelolaan risiko yang efektif.	Bertahap dari transformasi digital (identitas digital, perubahan sistem manual), hingga transaksi digital sebagai dasar dari ekonomi digital.

Aspek	WEF	PwC	ISACA
Dampak terhadap Bisnis dan Masyarakat	Menjaga keseimbangan antara manfaat teknologi dan perlindungan hak individu, menciptakan keadilan digital.	Meningkatkan transparansi, menjaga kepatuhan terhadap regulasi, serta membangun keunggulan kompetitif melalui tata kelola data yang baik.	Memperkuat hubungan bisnis, meningkatkan pendapatan, dan mengurangi risiko pelanggaran keamanan.

Tabel 3.5: Peran dan Tanggung Jawab Kepercayaan Digital menurut WEF, PwC, dan ISACA

Aspek	WEF	PwC	ISACA
Tanggung Jawab Utama	Kepercayaan digital adalah tanggung jawab bersama antara perusahaan teknologi, pemerintah, pembuat kebijakan, masyarakat, dan organisasi nirlaba.	Perusahaan, pengguna, *regulator*, dan pemangku kepentingan lainnya bekerja sama dalam membangun kepercayaan digital.	Chief Trust Officer (CTO) dan kepemimpinan organisasi bertanggung jawab dalam strategi kepercayaan digital.
Peran Perusahaan/Organisasi	Perusahaan teknologi harus memastikan keamanan dan tanggung jawab dalam penggunaan teknologi digital.	Perusahaan bertanggung jawab mengelola data dan teknologi dengan standar keamanan dan privasi tinggi.	Penyedia layanan (*providers*) harus memastikan layanan dan produk aman, bermanfaat, serta sesuai standar etika dan regulasi.
Peran Pemerintah & Regulator	Pemerintah dan pembuat kebijakan bertugas memastikan regulasi untuk penggunaan teknologi yang aman dan bertanggung jawab.	Regulator menetapkan dan menegakkan peraturan terkait perlindungan data serta kepercayaan digital.	Dewan direksi dan kepemimpinan organisasi harus menyelaraskan strategi kepercayaan digital dengan tujuan bisnis dan persyaratan regulasi.
Peran Konsumen/Pengguna	Masyarakat sebagai pengguna teknologi turut berperan dalam menjaga kepercayaan digital.	Pengguna harus mendapatkan perlindungan data yang tepat serta memiliki kontrol atas informasi pribadinya.	Konsumen bertanggung jawab menjaga informasi pribadi, menggunakan teknologi secara bijak, dan memahami risiko digital.

Lanjutan dari Tabel 3.5

Aspek	WEF	PwC	ISACA
Peran Pihak Ketiga & Ekosistem Digital	Organisasi nirlaba dan komunitas digital turut berperan dalam memastikan nilai-nilai kepercayaan digital ditegakkan.	Penyedia layanan pihak ketiga dan mitra bisnis bertanggung jawab atas pengelolaan data dan keamanan digital.	Mitra bisnis (*third parties*) harus bekerja dengan transparansi dan integritas. Teknologi perantara (*proxy technologies*) serta komunitas digital (*digital peers*) perlu memastikan keamanan layanan.

Tabel 3.6: Waktu dan Tahapan Implementasi Kepercayaan Digital menurut WEF, PwC, dan ISACA

Aspek	WEF	PwC	ISACA
Fokus Utama	Mendorong organisasi untuk menerapkan *kerangka kerja kepercayaan digital* yang komprehensif, tidak hanya untuk kepatuhan tetapi juga untuk membangun kepercayaan jangka panjang.	Kepercayaan digital harus menjadi bagian *integral dari operasi bisnis sehari-hari*, bukan hanya sekadar kepatuhan.	Membangun ekosistem kepercayaan digital dengan pendekatan berbasis *Digital Trust Ecosystem Framework (DTEF).*
Tahapan Implementasi	*Mengadopsi* program kepercayaan digital. *Berkomitmen* menjalankan program secara konsisten. *Memastikan keberlanjutan* program kepercayaan digital dalam operasional organisasi.	*Pengumpulan data*: Memastikan transparansi dan izin eksplisit dari pengguna. *Penggunaan data*: Menjamin kejelasan dan kontrol atas data yang digunakan. *Pelanggaran atau insiden keamanan*: Respons cepat dan transparan saat terjadi kebocoran data atau serangan siber.	2022: Pengenalan konsep kepercayaan digital dan komunikasi dengan anggota ISACA. Awal 2023: Peluncuran *Digital Trust Ecosystem Framework (DTEF).* Pertengahan 2023: Peluncuran *Sertifikat DTEF Foundation.* Akhir 2023: Publikasi *Panduan Implementasi DTEF.* 2024: Rilis *Digital Trust Board Briefing* sebagai pedoman implementasi bagi organisasi.

Aspek	WEF	PwC	ISACA
Prinsip Utama	Kepercayaan digital dipandang sebagai *proses kolaboratif* dalam pengambilan keputusan teknologi, bukan sekadar aturan kepatuhan.	Menyesuaikan dengan *tren teknologi digital* seperti hiperkonektivitas, adopsi *cloud*, dan big data.	Berbasis pada komponen *integritas, aksesibilitas, keberlanjutan, keamanan siber, perlindungan data, transparansi, dan kejujuran* dalam ekosistem digital.
Pendekatan	*Panduan strategis* bagi pengambil keputusan agar kepercayaan digital diterapkan secara holistik dan operasional.	*Transformasi bisnis berbasis risiko*, memastikan kepercayaan digital selalu diperbarui mengikuti perkembangan teknologi.	*Framework berbasis evaluasi* dengan KPI dan KRI untuk mengukur efektivitas implementasi.

Tabel 3.7: Pendekatan Penerapan Kepercayaan Digital menurut WEF, PwC, dan ISACA

Aspek	WEF	PwC	ISACA
Pendekatan Utama	Mengutamakan *individual agency by design*, yang berfokus pada transparansi, privasi, dan mekanisme penyelesaian masalah.	Mengintegrasikan kepercayaan digital dalam *sistem kontrol bisnis* dan manajemen risiko organisasi.	Menggunakan *Digital Trust Ecosystem Framework (DTEF)* untuk mengelola kepercayaan digital secara menyeluruh.
Fokus Implementasi	*Transparansi*: Memberikan informasi jelas tentang layanan digital dan menyediakan alat literasi digital. *Privasi*: Menjaga keamanan data dengan persetujuan pengguna dan kepatuhan terhadap regulasi. *Mekanisme Penyelesaian Masalah*: Menyediakan prosedur pengaduan dan pengawasan pihak ketiga.	*Optimalisasi kontrol sistem* untuk meningkatkan keandalan dan keamanan. *Pengelolaan risiko digital* yang efektif dalam seluruh siklus hidup sistem. Integrasi dalam perencanaan dan operasional organisasi untuk memastikan keberlanjutan kepercayaan digital.	Memastikan interaksi manusia dengan AI dan sistem digital lebih dapat dipercaya. Menghubungkan *data, manusia, proses, dan teknologi* dalam ekosistem digital. Mengelola *kesenjangan kepercayaan* antara kondisi saat ini dan yang diharapkan.
Prinsip Pendukung	*Menghormati hak individu* dalam penggunaan teknologi. Mendorong *kolaborasi multi-stakeholder* dalam membangun ekosistem digital yang tepercaya.	*Kepercayaan digital sebagai bagian dari strategi bisnis.* Memastikan sistem keamanan tetap relevan dalam menghadapi ancaman baru.	Berbasis pada *standar etika dan transparansi.* Menggunakan umpan balik dan evaluasi terukur untuk peningkatan berkelanjutan.

Aspek	WEF	PwC	ISACA
Elemen Kunci	*Transparansi & edukasi digital* bagi pengguna. Regulasi ketat untuk menjaga privasi dan keamanan data.	*Sistem kontrol yang matang* untuk mendukung pengambilan keputusan yang lebih baik.	Evaluasi *kinerja AI dan keamanan digital.* Penguatan aspek *etika, transparansi, dan integritas.*

Berdasarkan analisis terhadap pandangan WEF, PwC, dan ISACA mengenai kepercayaan digital (lihat Tabel 3.3, 3.4, 3.5, 3.6, dan 3.7), dapat disimpulkan bahwa ketiga komunitas sepakat akan pentingnya kepercayaan digital sebagai landasan dari transformasi teknologi yang berkelanjutan. Meskipun memiliki penekanan berbeda, berikut poin kunci yang teridentifikasi:

1. Peran Kepercayaan Digital
   Ketiga organisasi sepakat bahwa kepercayaan digital merupakan elemen kunci dalam ekosistem digital modern. WEF menekankan adopsi teknologi yang adil dan etis, PwC menggarisbawahi integrasi kepercayaan digital dalam bisnis serta interaksi digital yang aman, sementara ISACA menyoroti pentingnya menjaga akuntabilitas dan transparansi serta bertanggung jawab untuk mewujudkan kepercayaan digital.

2. Dampak terhadap Ekonomi dan Masyarakat
   Kepercayaan digital berperan besar dalam ekonomi digital. WEF menekankan stabilitas sosial sebagai dampak positifnya, PwC melihatnya sebagai faktor peningkatan daya saing dan keberhasilan transformasi digital, sedangkan ISACA menghubungkannya dengan pertumbuhan ekonomi digital.

3. Keamanan dan Risiko
   Ancaman siber menjadi faktor utama yang dapat menghambat kepercayaan digital. WEF mengaitkannya dengan hambatan inovasi, PwC menekankan kepercayaan digital sebagai alat mitigasi terhadap kebocoran data dan serangan siber, sementara ISACA menyoroti dampaknya pada kepercayaan konsumen dan ekosistem secara umum.

4. Strategi Implementasi
   WEF berfokus pada kebijakan dan regulasi untuk menciptakan lingkungan digital yang adil, PwC mengusulkan integrasi kepercayaan digital dalam strategi nasional guna memastikan stabilitas ekonomi dan keberlanjutan bisnis, sedangkan ISACA menekankan pentingnya membangun kepercayaan sejak perancangan dan pengembangan sistem agar selaras dengan strategi bisnis dan persyaratan kepatuhan Kepercayaan digital mendorong pertumbuhan bisnis dan perlindungan konsumen. WEF berorientasi pada perlindungan hak individu dalam penggunaan teknologi, PwC menekankan peningkatan loyalitas pelanggan serta hubungan jangka panjang dengan pemangku kepentingan, sementara ISACA melihatnya sebagai faktor pendukung *e-commerce* dan ekonomi digital.

5. Tujuan Pengenalan Kepercayaan Digital
   Ketiga organisasi memiliki fokus berbeda dalam pengenalan kepercayaan digital. WEF bertujuan mengembalikan kepercayaan publik terhadap teknologi, PwC menitikberatkan pada pengelolaan risiko digital dalam bisnis, sedangkan ISACA menekankan transparansi dan stabilitas dalam lingkungan digital.

6. Peran dan Tanggung Jawab dalam Kepercayaan Digital
   Kepercayaan digital merupakan tanggung jawab kolektif berbagai pemangku kepentingan. WEF menyoroti kolaborasi antara pemerintah, perusahaan, dan masyarakat, PwC menekankan kerja sama antara regulator dan dunia usaha, sementara ISACA menggarisbawahi peran *Digital Trust Committee* yang menjalankan peran evaluasi, pengarah, dan monitor strategi, serta didukung oleh *Chief Trust Officer* (CTO) dan kepemimpinan organisasi dalam memastikan implementasi yang efektif.

7. Tahapan Implementasi Kepercayaan Digital
   Masing-masing organisasi menawarkan pendekatan berbeda dalam implementasi kepercayaan digital. WEF mengusulkan tahapan adopsi, komitmen, dan keberlanjutan, PwC menitikberatkan pada pengelolaan dan pemanfaatan data serta respons terhadap insiden keamanan, sedangkan ISACA mengembangkan *Digital Trust Ecosystem Framework* (DTEF) yang memiliki metrik ukur untuk penilaian pencapaian serta didukung oleh sertifikasi kompetensi personil.

8. Pendekatan Penerapan Kepercayaan Digital
   WEF mengadopsi pendekatan "*individual agency by design*" yang menekankan transparansi dan perlindungan hak individu. PwC mengintegrasikan kepercayaan digital dalam sistem kontrol bisnis dan manajemen risiko. Sementara itu, ISACA menerapkan DTEF untuk memastikan pengelolaan kepercayaan digital secara menyeluruh dan sistematis.

Secara keseluruhan, WEF, PwC, dan ISACA sepakat bahwa kepercayaan digital adalah faktor penting bagi bisnis dan masyarakat digital. Namun, masing-masing organisasi memiliki fokus berbeda dalam implementasinya:

- WEF mengedepankan kebijakan regulasi, etika, dan perlindungan hak individu dalam inovasi teknologi.
- PwC mengintegrasikan kepercayaan digital dalam strategi bisnis, manajemen risiko, serta loyalitas pelanggan.
- ISACA menitikberatkan pada pencapaian transparansi, akuntabilitas dan tanggung jawab dari seluruh pemangku kepentingan dalam ekosistem digital.

Kepercayaan digital bukan hanya masalah kepatuhan terhadap regulasi, tetapi juga faktor fundamental dalam menciptakan ekosistem digital yang aman, stabil, dan berkelanjutan.

4

Regulasi dan Referensi

> Digital trust is the foundation for a safe, secure, and inclusive digital future.
>
> — World Economic Forum

Transformasi digital menjadi langkah yang ditempuh oleh Indonesia dalam menghadapi globalisasi teknologi. Beberapa regulasi telah disusun dan ditetapkan. Menurut Hive Five [276], transformasi digital adalah proses perubahan mendasar dalam cara individu, organisasi, dan pemerintah beroperasi dengan memanfaatkan teknologi digital. Proses ini mencakup adopsi sistem berbasis teknologi, peningkatan literasi digital, serta inovasi di berbagai sektor guna meningkatkan produktivitas, efisiensi, dan keterlibatan masyarakat dalam ekosistem digital.

Adapun tujuan utama transformasi digital di Indonesia meliputi:

1. Meningkatkan Efisiensi dan Transparansi Layanan Publik.
   Salah satu tujuan utama transformasi digital adalah meningkatkan aksesibilitas dan kualitas layanan publik. Melalui penerapan ekosistem digital seperti SPBE yang mengintegrasikan layanan kependudukan dan perpajakan (*e-tax*), pemerintah dapat memangkas birokrasi, mempercepat proses pelayanan, serta meningkatkan transparansi untuk mencegah korupsi. Efektivitas ini terlihat nyata pada layanan *e-filing*, yang tidak hanya mempermudah masya-

rakat dalam pelaporan pajak, tetapi juga meningkatkan efisiensi administrasi negara.

2. Mendorong Pertumbuhan Ekonomi Digital.
   Indonesia memiliki potensi besar dalam sektor ini, didukung oleh populasi pengguna internet yang terus bertumbuh secara signifikan. Transformasi digital diarahkan untuk mematangkan ekosistem ekonomi melalui inovasi teknologi di bidang strategis, seperti *e-commerce*, *fintech*, dan *startup* digital. Akselerasi ini tidak hanya bertujuan memperluas pasar, tetapi secara konkret diproyeksikan untuk meningkatkan kontribusi terhadap Produk Domestik Bruto (PDB) nasional serta menciptakan lapangan kerja baru yang berkualitas di sektor teknologi.

3. Keadilan Sosial dan Inklusi Keuangan.
   Transformasi digital dirancang untuk menciptakan kesetaraan peluang dengan memperluas akses terhadap teknologi, literasi, dan layanan finansial bagi masyarakat di wilayah tertinggal (*last-mile*).
   Program Strategis: Akselerasi digitalisasi UMKM yang terintegrasi dengan sistem pembayaran digital dan akses permodalan (*fintech*), guna memperluas jangkauan pasar serta meningkatkan ketahanan ekonomi pelaku usaha kecil.

4. Meningkatkan Daya Saing Global.
   Dalam lanskap ekonomi yang semakin terinterkoneksi, penguasaan teknologi digital menjadi faktor determinan untuk memenangkan persaingan di pasar internasional. Transformasi digital memampukan Indonesia untuk mengakselerasi produktivitas industri melalui adopsi manufaktur cerdas berbasis *Internet of Things* (IoT) dan kecerdasan buatan (AI). Kesiapan ekosistem digital ini tidak hanya memperkuat kapasitas produksi nasional, tetapi juga menjadi katalis utama dalam menarik investasi asing langsung (*Foreign Direct Investment*).

5. Meningkatkan Literasi Digital Masyarakat.
   Peningkatan literasi digital ditempatkan sebagai pilar fundamental dalam agenda transformasi nasional Indonesia. Pemerintah berupaya membangun masyarakat yang cakap teknologi, dengan penekanan tidak hanya pada kecakapan teknis, tetapi juga pemahaman mendalam mengenai keamanan siber (*digital safety*) dan pemanfaatan internet yang produktif.
   Program Terkait: Gerakan Nasional Literasi Digital (GNLD) oleh Kementerian Kominfo, yang telah menjangkau jutaan peserta di berbagai wilayah untuk menutup kesenjangan keterampilan digital.

6. Mendukung Pembangunan Berkelanjutan.
   Digitalisasi berfungsi sebagai katalis vital dalam mewujudkan tujuan pembangunan berkelanjutan (*Sustainable Development Goals*/SDGs). Integrasi teknologi cerdas memungkinkan pengelolaan sumber daya alam berbasis data, menekan jejak karbon melalui efisiensi energi, serta memperkuat mitigasi dampak lingkungan yang lebih responsif.

Selain tujuan-tujuan tersebut, pemerintah juga telah menyusun berbagai regulasi untuk mengatur dan mempercepat transformasi digital di Indonesia. Regulasi ini memiliki tingkatan berbeda, mulai dari peraturan dengan kekuatan hukum mengikat hingga kebijakan yang bersifat imbauan. Beberapa produk hukum dan inisiatif tingkat kementerian/lembaga (K/L) yang telah dikembangkan juga didorong menjadi gerakan nasional guna mempercepat implementasi transformasi digital di seluruh sektor.

4.1 Undang-Undang (UU)

Undang-undang memiliki peran yang sangat penting sebagai perangkat regulasi tertinggi setelah Undang-Undang Dasar (UUD) 1945. Kehadiran undang-undang berfungsi sebagai landasan normatif yang mengatur kehidupan berbangsa dan bernegara, termasuk dalam konteks perkembangan teknologi dan digitalisasi. Penyusunannya umumnya dirancang dalam cakupan yang lebih umum dan tidak terlalu rinci, sebab aspek teknis maupun operasional akan diturunkan ke dalam peraturan pelaksana, seperti peraturan pemerintah, peraturan presiden, maupun peraturan menteri. Dengan demikian, undang-undang dapat menjaga sifatnya yang fleksibel sekaligus memberikan ruang adaptasi terhadap dinamika yang terus berkembang.

Dalam menghadapi tantangan era transformasi digital, regulasi ini tidak hanya mencakup aspek hukum konvensional, tetapi juga merambah ke berbagai isu strategis, seperti keamanan siber, pelindungan data pribadi, transaksi elektronik, serta penguatan ekonomi digital. Regulasi yang kuat dan adaptif diperlukan agar inovasi digital dapat berkembang tanpa menimbulkan risiko yang merugikan masyarakat, baik dari sisi keamanan maupun etika penggunaan teknologi.

Kerangka hukum yang jelas akan memberikan kepastian bagi semua pemangku kepentingan, pemerintah, pelaku usaha, maupun masyarakat luas. Bagi pemerintah, regulasi menjadi instrumen untuk mengarahkan pembangunan digital nasional agar berjalan sesuai dengan prinsip keberlanjutan, kedaulatan, dan perlindungan kepentingan publik. Bagi pelaku usaha, kejelasan hukum memberikan kepastian berinvestasi dan berinovasi di bidang teknologi, sekaligus mendorong persaingan yang sehat. Sedangkan bagi masyarakat, adanya perlindungan hukum menjamin hak-hak mereka tetap terjaga dalam memanfaatkan layanan digital.

Dengan demikian, undang-undang berfungsi tidak hanya sebagai perangkat pengatur, tetapi juga sebagai katalisator yang mendorong terciptanya ekosistem digital yang aman, andal, dan berkeadilan. Pada akhirnya, regulasi yang baik akan melahirkan lingkungan yang kondusif bagi pertumbuhan ekonomi berbasis teknologi sekaligus memperkuat daya saing bangsa di tingkat global.

4.1.1 UU Nomor 17 Tahun 2007 tentang Rencana Pembangunan Jangka Panjang Nasional (RPJP Nasional) tahun 2005-2025

Undang-Undang ini merupakan dokumen perencanaan pembangunan nasional untuk jangka waktu 20 tahun [277]. Meskipun tidak secara eksplisit menyebutkan transformasi digital, beberapa pasalnya menunjukkan arah kebijakan yang mendukung pengembangan teknologi dan inovasi.

Pasal 4 menetapkan visi, misi, dan arah pembangunan nasional, termasuk penguatan sumber daya manusia serta penguasaan ilmu pengetahuan dan teknologi. Penguasaan teknologi ini diposisikan sebagai pendorong inovasi, yang merupakan faktor penting bagi transformasi digital. Dalam Pasal 4 huruf (e), pengembangan infrastruktur juga diarahkan untuk memperkuat konektivitas nasional, meliputi transportasi, energi, serta teknologi informasi dan komunikasi (TIK).

Komitmen terhadap peran strategis teknologi semakin ditegaskan dalam Pasal 5 ayat (1) huruf (g), yang menyebutkan teknologi sebagai salah satu faktor utama dalam membangun masyarakat mandiri dan berdaya saing. Pemerintah bertanggung jawab atas penyediaan infrastruktur pendukung, sebagaimana diatur dalam Pasal 5 ayat (1), serta pengelolaannya sebagaimana tercantum dalam Pasal 10 ayat (2).

Pengembangan dan penguasaan ilmu pengetahuan dan teknologi (IPTEK) menjadi prioritas nasional, sebagaimana tercantum dalam Pasal 8 ayat (1) huruf (b). Dukungan terhadap IPTEK juga diwujudkan melalui penguatan riset dan kerja sama antarlembaga, seperti yang ditegaskan dalam Pasal 9. Dalam hal penguatan sumber daya manusia, Pasal 7 ayat (2) menekankan pentingnya pengembangan SDM di bidang teknologi, sementara Pasal 10 ayat (1) mendorong penyelenggaraan pendidikan dan pelatihan berbasis IPTEK untuk menciptakan tenaga kerja yang kompeten dan inovatif.

Di sisi regulasi, pemerintah memberikan dukungan melalui perlindungan Hak Kekayaan Intelektual (HKI) sebagaimana diatur dalam Pasal 6 ayat (2), serta menciptakan ekosistem yang kondusif bagi inovasi dan pengembangan teknologi nasional sesuai Pasal 8 ayat (2).

Keterkaitan dengan Kerangka Kerja Kepercayaan Digital di Indonesia

Penyusunan kerangka kerja kepercayaan digital di Indonesia perlu merujuk pada arah dan kebijakan pembangunan nasional yang telah ditetapkan dalam undang-undang ini. Meskipun transformasi digital tidak disebutkan secara eksplisit, berbagai pasal dalam regulasi ini menunjukkan dukungan yang kuat terhadap pengembangan teknologi, inovasi, dan infrastruktur digital, unsur-unsur kunci dalam membangun kepercayaan digital. Visi pembangunan nasional yang menekankan penguatan sumber daya manusia, penguasaan IPTEK, serta pengembangan infrastruktur TIK menjadi landasan strategis bagi upaya menciptakan ekosistem digital yang andal, aman, kolaboratif dan berkeadilan. Dengan demikian, kerangka kerja kepercayaan

digital tidak dapat dilepaskan dari konteks kebijakan jangka panjang negara yang tercermin dalam dokumen ini.

1. Pembangunan Infrastruktur TIK
   Infrastruktur adalah salah satu aspek penting untuk mendukung kepercayaan digital. Infrastruktur yang stabil, aman, dan terkelola dengan baik memastikan layanan digital dapat berjalan tanpa gangguan, melindungi data pengguna, dan memenuhi standar keamanan yang diperlukan. Organisasi yang ingin membangun dan mempertahankan kepercayaan digital harus berinvestasi dalam penguatan, pemantauan, dan inovasi infrastruktur TIK mereka.

2. Pengembangan SDM
   Pengembangan SDM yang kompeten di bidang TIK sangat penting dalam membangun kepercayaan digital. Manusia adalah penggerak utama dalam implementasi dan pengelolaan teknologi yang tepercaya.

3. Regulasi dan Kebijakan
   RPJP Nasional mencakup pengembangan regulasi dan kebijakan yang mendukung penggunaan teknologi secara aman dan bertanggung jawab.

4. Peningkatan Kesadaran dan Literasi Digital
   Regulasi ini menekankan pentingnya peningkatan kesadaran dan literasi digital di kalangan masyarakat. Literasi digital yang baik akan membantu masyarakat memahami pentingnya kepercayaan digital dan bagaimana cara menjaga keamanan dan privasi mereka saat menggunakan teknologi.

5. Kolaborasi dan Kemitraan
   Kolaborasi dan kemitraan antara pemerintah, sektor swasta/industri, dan masyarakat dalam pembangunan TIK diperlukan untuk membangun ekosistem kepercayaan digital yang kuat.

4.1.2 UU Nomor 59 Tahun 2024 tentang Rencana Pembangunan Jangka Panjang Nasional (RPJPN) 2025-2045

Undang-Undang Nomor 59 Tahun 2024 tentang Rencana Pembangunan Jangka Panjang Nasional (RPJPN) 2025–2045 merupakan kelanjutan dari UU No. 17 Tahun 2007 dan menetapkan visi pembangunan Indonesia dalam 20 tahun ke depan [8]. Salah satu prioritas utama dalam visi ini adalah transformasi digital sebagai pendorong pertumbuhan ekonomi, peningkatan daya saing, dan perbaikan layanan publik.

Transformasi digital ditegaskan dalam berbagai pasal. Pasal 6 ayat 1 menekankan pentingnya pengembangan teknologi informasi dan komunikasi (TIK) untuk memperkuat daya saing dan efisiensi ekonomi. Ayat 2 huruf e menambahkan bahwa modernisasi sektor pemerintahan dan pelayanan publik berbasis digital bertujuan

meningkatkan transparansi dan efisiensi birokrasi. Selanjutnya, Pasal 7 menyebutkan bahwa teknologi berperan strategis dalam mempercepat transformasi ekonomi nasional.

Dari sisi infrastruktur, Pasal 9 ayat 1 mengamanatkan pembangunan dan perluasan jaringan digital, termasuk pemerataan akses internet hingga ke daerah terpencil. Ayat 2 menambahkan pentingnya peningkatan kapasitas pusat data nasional serta penguatan keamanan siber sebagai bagian integral dari transformasi digital.

Sumber daya manusia juga menjadi perhatian. Pasal 10 menugaskan pemerintah untuk memastikan peningkatan keterampilan masyarakat di bidang digital, guna menciptakan talenta yang kompetitif di era Industri 4.0. Hal ini diperkuat oleh Pasal 11 ayat 2, yang memberi arah bagi dunia usaha dan industri untuk mendukung penerapan teknologi dan inovasi.

Di sektor ekonomi, Pasal 11 ayat 1 menetapkan pengembangan ekonomi digital sebagai salah satu pilar utama pertumbuhan nasional. Untuk memperkuat ekosistem ini, Pasal 13 mengatur dua hal penting: ayat 1 menggarisbawahi perlindungan data dan privasi, sedangkan ayat 2 menugaskan pemerintah menyusun kebijakan inovatif, termasuk perlindungan Hak Kekayaan Intelektual (HKI).

Sebagai langkah pengawasan dan penyesuaian, regulasi ini juga memperkenalkan mekanisme evaluasi pelaksanaan transformasi digital. Pemerintah diwajibkan memantau implementasi kebijakan, mengukur dampaknya terhadap sektor-sektor strategis, dan menyesuaikan arah kebijakan sesuai dengan perkembangan global dan kebutuhan nasional. Evaluasi berkelanjutan ini diharapkan memastikan transformasi digital berjalan efektif dan berkontribusi nyata pada pertumbuhan ekonomi, peningkatan daya saing, dan kualitas layanan publik.

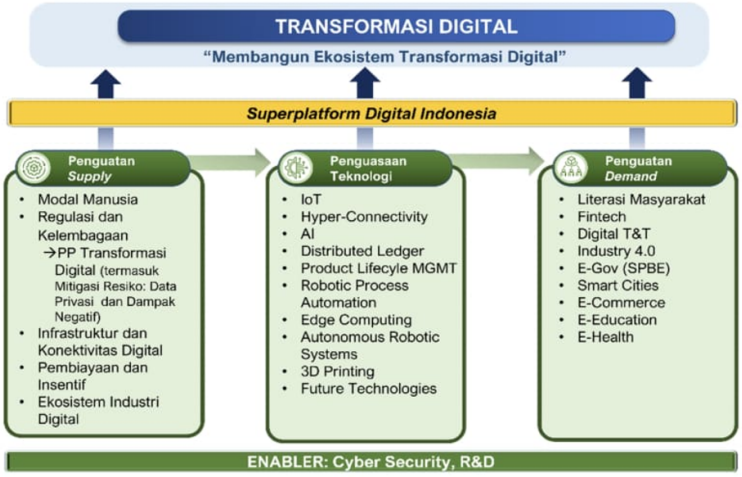
Garis besar arah kebijakan ini tergambar secara visual dalam Gambar 4.1, yang mengilustrasikan ekosistem transformasi digital Indonesia melalui pendekatan holistik yang terbagi dalam tiga pilar utama: penguatan sisi *Supply*, penguasaan *Teknologi*, dan penguatan sisi *Demand*. Ketiganya bertumpu pada pengembangan *Superplatform Digital Indonesia* sebagai simpul integrasi antaraktor dan antarlevel digitalisasi nasional.

Pilar *Supply* menitikberatkan pada penguatan kelembagaan, kebijakan mitigasi risiko (termasuk privasi data dan dampak negatif digital), pembangunan infrastruktur digital, serta penciptaan ekosistem industri digital yang kompetitif. Hal ini sejalan dengan amanat Pasal 9 dan 10 yang memadukan penguatan infrastruktur dan kapasitas SDM digital.

Sementara itu, pilar *Penguasaan Teknologi* mencakup adopsi berbagai teknologi mutakhir, seperti Internet of Things (IoT), *Artificial Intelligence* (AI), *distributed ledger*, automasi, dan teknologi masa depan lainnya. Hal ini mengaktualisasikan arahan Pasal 6 dan 7 yang mengedepankan peran teknologi sebagai penggerak transformasi ekonomi dan layanan publik.

Adapun pilar *Demand* berfokus pada literasi digital masyarakat dan pemanfaatan teknologi dalam sektor-sektor utama seperti *fintech*, *e-Government*, *e-Commerce*, *e-Education*, dan *e-Health*. Fokus ini selaras dengan Pasal 11 dan 13 yang mengede-

pankan penguatan ekosistem ekonomi digital serta perlindungan hak digital warga negara. Keseluruhan proses transformasi ini ditopang oleh dua *enabler* utama, yaitu keamanan siber dan riset serta pengembangan (R&D). Keduanya memainkan peran krusial dalam membangun kerangka kepercayaan digital yang menyeluruh, baik melalui perlindungan teknis maupun dukungan kebijakan berbasis inovasi, guna menjamin keberlanjutan dan resiliensi digital Indonesia ke depan.



Gambar 4.1: Korelasi aktivitas digital dengan derajat kepercayaan

Keterkaitan dengan Kerangka Kerja Kepercayaan Digital di Indonesia

Salah satu pilar utama dalam RPJPN 2025-2045 adalah Transformasi Digital, yang bertujuan meningkatkan efisiensi, inovasi, dan daya saing nasional. Pilar ini tercantum dalam misi kedua dari delapan misi pembangunan, yaitu mewujudkan transformasi ekonomi untuk meningkatkan produktivitas melalui inovasi iptek, penguatan ekonomi produktif (termasuk industri manufaktur, ekonomi dan keuangan syariah, pertanian, ekonomi biru dan bioekonomi, pariwisata, ekonomi kreatif, UMKM dan koperasi, tenaga kerja, serta BUMN), penerapan ekonomi hijau, transformasi digital, integrasi ekonomi domestik dan global, serta pembangunan perkotaan dan perdesaan sebagai pusat pertumbuhan ekonomi.

Dalam mewujudkan transformasi digital yang aman dan berkelanjutan, kepercayaan digital menjadi elemen krusial. Keamanan data, perlindungan privasi pengguna, serta keandalan transaksi elektronik berperan penting dalam menciptakan lingkungan digital yang aman dan tepercaya. Menurut laporan Champions Needed: Building Digital Trust in a Dangerous World (Oxford Economics), kepercayaan digital tidak hanya bergantung pada regulasi, tetapi juga pada peran aktif individu dan organisasi. Sejalan dengan hal ini, regulasi yang ada menekankan pentingnya pengembangan sumber daya manusia yang melek digital dan berdaya saing tinggi. Dengan meningkatkan literasi digital serta kesadaran akan keamanan siber, ma-

syarakat Indonesia diharapkan dapat berkontribusi dalam membangun ekosistem digital yang lebih aman dan tepercaya.

4.1.3 UU Nomor 11 Tahun 2008 juncto Nomor 19 Tahun 2019 juncto Nomor 1 Tahun 2024 tentang Informasi dan Transaksi Elektronik (ITE)

Undang-Undang Informasi dan Transaksi Elektronik (UU ITE) adalah regulasi utama yang mengatur pemanfaatan teknologi informasi di Indonesia [278]. Sebagai pijakan hukum tertinggi dalam interaksi digital, UU ini telah mengalami dua kali revisi, yaitu pada 2019 dan 2024, untuk menyesuaikan dengan perkembangan teknologi dan kebutuhan hukum di era digital.

UU ITE menjadi landasan transformasi digital dengan mengakui keberadaan dan kekuatan hukum informasi serta transaksi elektronik. Pasal 1 ayat 1 mengakui informasi elektronik, sementara ayat 2 memberikan legalitas pada transaksi elektronik. Pasal 5 ayat 1 menegaskan bahwa dokumen digital memiliki kekuatan hukum yang setara dengan dokumen fisik. Pasal 11 memperkuat hal ini dengan menyatakan bahwa tanda tangan elektronik memiliki validitas yang sama dengan tanda tangan manual, memungkinkan transaksi tanpa batasan jarak dan waktu.

Regulasi ini juga memperhatikan aspek keamanan sistem informasi. Pasal 15 ayat 1 mewajibkan Penyelenggara Sistem Elektronik (PSE) menjamin keamanan informasi sesuai standar. Pasal 16 memberi kewenangan kepada pemerintah untuk mengatur sistem keamanan tersebut. Perlindungan privasi ditegaskan dalam Pasal 26 ayat 1, sedangkan Pasal 30 dan 31 melarang akses ilegal serta penyadapan tanpa izin, menegaskan komitmen terhadap keamanan digital yang beretika dan bertanggung jawab.

Dalam hal kenyamanan dan perlindungan pengguna, UU ITE menetapkan sanksi terhadap pelanggaran di ruang digital. Pasal 27 mengatur penyebaran konten negatif, Pasal 29 mengatur ancaman kekerasan, Pasal 32 menangani pencemaran nama baik, dan Pasal 45 melarang penyebaran kebencian dan permusuhan.

Di sisi ekonomi, UU ini mendukung pertumbuhan ekosistem digital. Pasal 9 ayat 1 mengatur transaksi digital, sementara Pasal 10 menegaskan peran penting tanda tangan elektronik dalam mendukung efisiensi dan kepercayaan dalam aktivitas ekonomi digital. Secara keseluruhan, UU ITE tidak hanya menjadi kerangka hukum transformasi digital, tetapi juga menjamin keamanan, kenyamanan, dan kepercayaan dalam ekosistem digital Indonesia.

Poin-Poin Utama dalam UU ITE:

1. Pengakuan Informasi dan Transaksi Elektronik
   Informasi dan dokumen elektronik dinyatakan sah setara dengan dokumen fisik dan memiliki kekuatan pembuktian dalam proses hukum, sehingga dapat digunakan sebagai alat bukti yang diakui secara yuridis. Selaras dengan itu, tanda tangan elektronik juga memperoleh kedudukan hukum yang sama

dengan tanda tangan manual sehingga menjamin kepastian hukum atas transaksi digital yang dilakukan. Ketentuan ini tidak hanya memperkuat validitas dokumen dan transaksi elektronik, tetapi juga menjadi dasar penting dalam membangun kepercayaan terhadap ekosistem digital nasional.

2. Keamanan dan Perlindungan Data
   Keamanan dan perlindungan data merupakan aspek fundamental dalam membangun kepercayaan digital. Setiap PSE memiliki kewajiban untuk menjamin keamanan data dan menjaga privasi pengguna melalui penerapan standar teknis serta kebijakan yang ketat. Perlindungan ini tidak hanya berfokus pada menjaga kerahasiaan data, tetapi juga memastikan bahwa hak pribadi individu dalam penggunaan data elektronik terlindungi dari potensi penyalahgunaan. Dengan adanya regulasi yang jelas dan pengawasan yang konsisten, mekanisme perlindungan data mampu memperkuat akuntabilitas PSE sekaligus meningkatkan kepercayaan masyarakat terhadap layanan digital yang mereka gunakan.

3. Tindak Pidana Siber dan Sanksi
   Tindak pidana diperluas mencakup berbagai bentuk kejahatan digital, antara lain akses ilegal terhadap sistem elektronik, manipulasi dan pencurian data, penyebaran hoaks, hingga pencemaran nama baik di ruang digital. Untuk menanggulangi kejahatan ini, aparat penegak hukum memiliki kewenangan melakukan penyidikan, penindakan, serta membawa kasus ke ranah peradilan. Sanksi yang dikenakan bagi pelaku tindak pidana siber bervariasi, mulai dari pidana penjara hingga denda, sesuai dengan ketentuan yang berlaku dalam peraturan perundang-undangan. Pendekatan ini bertujuan tidak hanya memberikan efek jera, tetapi juga memastikan adanya kepastian hukum serta perlindungan bagi masyarakat di ruang digital.

4. Peran Pemerintah dan Masyarakat
   Pemerintah memiliki tanggung jawab utama dalam memfasilitasi keamanan siber dan melindungi kepentingan nasional. Peran ini mencakup penyusunan regulasi, pembangunan infrastruktur, serta penguatan kapasitas institusi agar ekosistem digital dapat berkembang secara aman dan berkelanjutan. Di sisi lain, masyarakat juga memiliki kontribusi penting melalui partisipasi aktif dalam pengawasan serta pemanfaatan sistem elektronik secara bertanggung jawab. Dengan adanya sinergi antara pemerintah sebagai pembuat kebijakan dan masyarakat sebagai pengguna sekaligus pengawas, kepercayaan digital dapat dibangun secara lebih kokoh dan bertanggungjawab.

Keterkaitan dengan Kerangka Kerja Kepercayaan Digital di Indonesia

Kerangka kerja kepercayaan digital disusun untuk menjawab arah kebijakan nasional dalam mendukung transformasi digital yang aman dan bertanggung jawab. Hal ini sejalan dengan Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik beserta perubahan-perubahannya, yang menegaskan pentingnya perlindungan data, keamanan informasi, dan kepastian hukum dalam ruang

digital. RPJPN 2025–2045 turut menekankan pilar-pilar strategis yang mendasari kepercayaan digital, sebagaimana dijabarkan dalam poin-poin berikut:

1. Keamanan Siber dan Pelindungan Data Pribadi
   RPJPN menekankan pentingnya keamanan siber dan pelindungan data pribadi dalam setiap inisiatif digital. Hal ini untuk memastikan bahwa masyarakat merasa aman dalam menggunakan layanan digital, yang pada gilirannya membangun kepercayaan terhadap sistem digital nasional.

2. Transparansi dan Akuntabilitas Layanan Digital
   Pemerintah berkomitmen untuk meningkatkan transparansi dan akuntabilitas dalam penyelenggaraan layanan digital. Dengan demikian, masyarakat dapat memantau dan menilai kinerja layanan tersebut, yang akan meningkatkan kepercayaan publik terhadap layanan digital pemerintah.

3. Peningkatan Literasi Digital
   RPJPN juga menargetkan peningkatan literasi digital masyarakat. Dengan pemahaman yang lebih baik tentang teknologi digital, masyarakat akan lebih percaya dan mampu menggunakan layanan digital dengan bijak dan aman.

4. Pengembangan Infrastruktur Digital yang Andal
   Pembangunan infrastruktur digital yang andal dan aman menjadi prioritas. Infrastruktur yang baik akan memastikan layanan digital beroperasi dengan lancar dan aman, yang merupakan dasar dari kepercayaan digital.

4.1.4 UU Nomor 27 Tahun 2022 tentang Pelindungan Data Pribadi

Undang-Undang Nomor 27 Tahun 2022 tentang Pelindungan Data Pribadi (UU PDP) merupakan tonggak penting dalam perkembangan regulasi pelindungan data di Indonesia [279]. Kehadirannya menjadi dasar hukum utama yang mengatur bagaimana data pribadi dikelola, baik dalam bentuk fisik maupun digital, sekaligus menjadi payung hukum yang melindungi hak-hak privasi warga negara. UU ini disusun dengan tujuan memastikan bahwa setiap aktivitas pengumpulan, penyimpanan, pemrosesan, hingga penyebaran data dilakukan secara hati-hati, transparan, dan bertanggung jawab. Melalui kerangka hukum yang komprehensif, UU PDP mengatur secara jelas definisi data pribadi, hak-hak yang dimiliki oleh subjek data, kewajiban yang harus dipatuhi oleh pengendali data, serta sanksi administratif maupun pidana yang dikenakan terhadap pihak-pihak yang melanggar ketentuan.

Ruang lingkup UU PDP berlaku luas, mencakup seluruh pihak yang terlibat dalam pengelolaan data pribadi, baik individu maupun badan hukum. Pihak-pihak tersebut antara lain:

1. Subjek Data Pribadi, yakni individu yang data pribadinya dikumpulkan, disimpan, atau diproses, yang sekaligus memiliki hak penuh untuk melindungi dan mengontrol penggunaan datanya.

2. Pengendali Data, yaitu entitas yang menentukan tujuan serta sarana pemrosesan data pribadi, sehingga bertanggung jawab atas tata kelola data sesuai dengan prinsip-prinsip perlindungan yang ditetapkan.

3. Prosesor Data, yakni pihak yang melakukan pemrosesan data pribadi atas instruksi atau untuk kepentingan pengendali data, sehingga tetap berada dalam lingkup kewajiban hukum yang melekat pada pengendali.

UU PDP resmi diundangkan pada 17 Oktober 2022. Meskipun telah ditetapkan, pelaksanaan penuh undang-undang ini tidak berlaku serta-merta. Pemerintah memberikan masa transisi selama dua tahun, yang bertujuan untuk memberikan ruang bagi para pengendali maupun prosesor data untuk menyesuaikan kebijakan, infrastruktur, serta prosedur internal mereka agar selaras dengan ketentuan yang diatur. Dengan demikian, UU PDP mulai berlaku penuh sejak 17 Oktober 2024.

Cakupan penerapan UU PDP tidak hanya terbatas pada yurisdiksi nasional, melainkan juga memiliki dimensi ekstrateritorial. Artinya, undang-undang ini berlaku pula terhadap pengelolaan data pribadi yang dilakukan oleh pihak di luar negeri, sepanjang data tersebut berkaitan dengan warga negara Indonesia atau diproses di wilayah Indonesia. Dengan pendekatan ini, UU PDP menegaskan kedaulatan hukum Indonesia dalam melindungi data pribadi warganya di tengah arus globalisasi dan interkoneksi lintas batas.

Secara substansial, penerapan UU PDP diarahkan untuk mencapai sejumlah tujuan strategis, antara lain:

1. Memberikan perlindungan yang optimal terhadap hak privasi setiap individu, terutama di era digital yang semakin kompleks dan rentan penyalahgunaan data.

2. Meningkatkan tingkat keamanan sekaligus membangun kepercayaan masyarakat terhadap praktik pengumpulan dan pemrosesan data pribadi.

3. Mendorong terciptanya tata kelola data yang baik, transparan, dan akuntabel pada perusahaan maupun lembaga yang memanfaatkan data pribadi dalam aktivitasnya.

4. Mengharmonisasikan regulasi domestik dengan standar dan praktik terbaik internasional, sehingga Indonesia dapat bersaing sekaligus berkolaborasi dalam ekosistem digital global.

5. Menyediakan dasar hukum yang kuat untuk menindak tegas berbagai pelanggaran, seperti kebocoran data, pemrosesan tanpa persetujuan, atau bentuk penyalahgunaan data lainnya.

Dengan demikian, UU PDP bukan hanya sekadar instrumen hukum, melainkan juga representasi komitmen negara dalam melindungi hak asasi digital warga negara, meningkatkan kepercayaan publik, serta memperkuat daya saing Indonesia dalam ekonomi digital global.

Keterkaitan dengan Kerangka Kerja Kepercayaan Digital di Indonesia

Sebagai salah satu pilar utama dalam ekosistem digital yang aman dan bertanggung jawab, pelindungan data pribadi memiliki peran krusial dalam membangun kepercayaan masyarakat terhadap pemanfaatan teknologi digital. UU PDP hadir sebagai instrumen hukum yang komprehensif dalam mengatur hak, kewajiban, dan tanggung jawab seluruh pihak yang terlibat dalam pemrosesan data pribadi di Indonesia.

Kerangka kerja kepercayaan digital nasional menempatkan UU PDP sebagai referensi normatif yang mengatur prinsip-prinsip dasar dalam tata kelola data pribadi secara adil, aman, dan transparan. Sejalan dengan tujuan untuk menciptakan ruang digital yang tepercaya dan aman, UU PDP tidak hanya mempertegas posisi data pribadi sebagai bagian dari hak asasi manusia, tetapi juga menetapkan parameter etis dan teknis yang harus diikuti oleh pengendali maupun prosesor data.

Beberapa prinsip utama yang diatur dalam UU PDP, seperti privasi, keamanan, transparansi, akuntabilitas, persetujuan, dan keadilan, menjadi landasan penting dalam perancangan kerangka kepercayaan digital Indonesia. Dengan mengintegrasikan prinsip-prinsip tersebut, kerangka kerja kepercayaan digital dapat memberikan panduan praktis bagi pemerintah, pelaku usaha, dan masyarakat dalam membangun sistem digital yang menjunjung tinggi hak individu, memperkuat integritas informasi, dan menjaga keberlangsungan transformasi digital nasional.

1. Aspek Kerahasiaan (*Privacy*)
   UU PDP secara komprehensif mengatur aspek kerahasiaan dalam kerangka kerja kepercayaan digital. UU ini menegaskan bahwa pelindungan data pribadi merupakan bagian dari hak asasi manusia yang harus dihormati dan dilindungi. Beberapa cara yang dilakukan dalam penegakan aspek privasi ini di antaranya adalah sebagai berikut:
   - Mengklasifikasikan data pribadi menjadi data spesifik dan data umum;
   - Mengatur hak-hak subjek data pribadi, termasuk hak untuk mengakses, mengoreksi, menghapus, dan menarik persetujuan atas pemrosesan data pribadi;
   - Menetapkan kewajiban bagi pengendali data pribadi, seperti memastikan dasar hukum pemrosesan, menjaga kerahasiaan, dan memastikan keamanan data pribadi yang diproses;
   - Menerapkan sanksi bagi para pelanggar.
2. Aspek Keamanan (*Security*)
   Pada aspek keamanan, langkah yang dapat diterapkan di antaranya adalah penerapan sistem pengamanan untuk mencegah kebocoran atau penyalahgunaan data dan menetapkan sanksi bagi pihak yang melakukan pembocoran, penyalahgunaan, atau peretasan data pribadi. Keamanan yang kuat meningkatkan kepercayaan pengguna terhadap sistem digital, mencegah kebocoran data, dan menjaga integritas data.

3. Aspek Transparansi (*Transparency*)
   Pada aspek transparansi ditegaskan bahwa pemrosesan data pribadi harus dilakukan secara transparan, termasuk pemberitahuan kepada pemilik data mengenai tujuan pengumpulan dan penggunaannya. Di samping itu juga diatur kewajiban pemberitahuan kepada subjek data jika terjadi kebocoran data pribadi. Transparansi meningkatkan kredibilitas organisasi dan mencegah praktik pemrosesan data yang tidak etis.

4. Aspek Akuntabilitas (*Accountability*)
   Pada aspek akuntabilitas, UU PDP mewajibkan adanya penunjukkan Petugas yang melaksanakan fungsi Pelindungan Data Pribadi. Langkah ini memastikan adanya mekanisme pertanggungjawaban bagi perusahaan atau institusi yang memproses data pribadi.

5. Aspek Persetujuan dan Kontrol Pengguna (*Consent and Control*)
   Aspek persetujuan dan kontrol pengguna ini diwujudkan dalam pengaturan hak-hak individu terkait data pribadi mereka, seperti hak untuk mengakses, mengoreksi, menarik persetujuan, dan menghapus data. Penerapan aspek ini dapat meningkatkan rasa aman dan kepercayaan individu dalam menggunakan layanan digital.

6. Aspek Etika dan Keadilan (*Ethics and Fairness*)
   Pada aspek etika dan keadilan, UU PDP mewajibkan pengendali data untuk mengelola data secara adil dan sesuai hukum, termasuk larangan penyalahgunaan data untuk kepentingan yang melanggar hak asasi manusia. Praktik pemrosesan data yang etis menciptakan lingkungan digital yang adil dan dapat dipercaya.

UU PDP tidak hanya berfokus pada kerahasiaan, tetapi juga mencakup keamanan, transparansi, akuntabilitas, kontrol pengguna, serta etika dalam pengelolaan data pribadi. Semua aspek ini berkontribusi dalam membangun kerangka kerja kepercayaan digital di Indonesia, yang sangat penting dalam mendorong transformasi digital yang aman dan berkelanjutan.

4.1.5 UU Nomor 8 Tahun 1999 tentang Perlindungan Konsumen

UU Nomor 8 Tahun 1999 tentang Perlindungan Konsumen merupakan tonggak penting dalam sistem perlindungan hukum di Indonesia dalam menciptakan keseimbangan antara hak dan kewajiban konsumen serta pelaku usaha [280]. Undang-undang ini tidak hanya memberi jaminan atas hak-hak konsumen, tetapi juga mengatur standar perilaku yang harus dipatuhi oleh pelaku usaha agar tercipta ekosistem perdagangan yang adil, transparan, dan bertanggung jawab.

Kehadiran UU ini menjadi sangat relevan dalam konteks digital saat ini, di mana transaksi berbasis teknologi informasi semakin dominan. Prinsip-prinsip dalam UU

ini dapat dijadikan dasar adaptif untuk pengembangan regulasi kepercayaan digital yang lebih luas.

Poin-poin utama dalam UU No.8 tentang perlindungan konsumen, yaitu:

1. Asas dan Tujuan
   Perlindungan konsumen didasarkan pada asas manfaat, keadilan, keseimbangan, keamanan, keselamatan, dan kepastian hukum. Tujuan utamanya adalah menjamin hak-hak konsumen, meningkatkan kesadaran masyarakat, serta mendorong pertanggungjawaban pelaku usaha.

2. Hak dan Kewajiban Konsumen dan Pelaku Usaha
   Konsumen berhak atas kenyamanan, keamanan, dan keselamatan dalam mengonsumsi barang dan/atau jasa, serta berhak memperoleh informasi yang benar. Di sisi lain, pelaku usaha berkewajiban memberikan informasi yang jujur, menjamin mutu dan keamanan produk, serta memberikan ganti rugi atas kerugian yang dialami konsumen.

3. Larangan dan Sanksi
   UU ini memuat larangan terhadap praktik usaha yang menyesatkan, membahayakan konsumen, atau bertentangan dengan prinsip etika bisnis. Pelanggaran atas ketentuan ini dapat dikenai sanksi administratif maupun pidana, termasuk denda dan hukuman penjara.

4. Penyelesaian Sengketa
   Sengketa antara konsumen dan pelaku usaha dapat diselesaikan secara nonlitigasi melalui Badan Penyelesaian Sengketa Konsumen (BPSK) atau melalui pengadilan. Mekanisme ini dirancang untuk menjamin akses keadilan yang cepat dan efektif bagi konsumen.

5. Kelembagaan dan Pengawasan
   Pemerintah membentuk Badan Perlindungan Konsumen Nasional (BPKN) yang berfungsi memberikan saran dan kebijakan perlindungan konsumen kepada pemerintah, serta mendukung peran Lembaga Perlindungan Konsumen Swadaya Masyarakat (LPKSM) dalam edukasi dan advokasi konsumen.

Keterkaitan dengan Kerangka Kerja Kepercayaan Digital

Dalam era transformasi digital, substansi UU No. 8 Tahun 1999 memberikan landasan awal yang kuat bagi pengembangan kerangka kerja kepercayaan digital. Kepercayaan digital mencakup keandalan sistem, perlindungan data, serta kepastian hukum dalam ruang siber, yang secara prinsipil sejalan dengan perlindungan terhadap hak-hak konsumen digital. Secara umum keterkaitan tersebut dapat diuraikan sebagai berikut:

1. Penguatan Hak Konsumen Digital
   Perlindungan terhadap informasi yang akurat, layanan yang aman, serta

mekanisme kompensasi atas kerugian menjadi aspek krusial dalam membangun kepercayaan masyarakat terhadap transaksi digital.

2. Tanggung Jawab Pelaku Usaha Digital
   Pelaku usaha digital, termasuk penyedia platform *e-commerce* dan layanan *online* lainnya, diwajibkan menerapkan prinsip transparansi dan akuntabilitas sebagaimana diatur dalam UU Perlindungan Konsumen.

3. Mekanisme Penyelesaian Sengketa Digital
   Perluasan peran BPSK atau pembentukan unit khusus dalam menangani sengketa digital dapat memperkuat rasa aman konsumen dalam melakukan transaksi elektronik.

4. Dasar Etika Bisnis Digital
   UU ini menjadi acuan dalam menumbuhkan etika bisnis digital yang berlandaskan kejujuran, keterbukaan, dan tanggung jawab sosial, yang merupakan fondasi dari ekosistem digital yang sehat dan tepercaya.

4.2 Peraturan Pemerintah (PP)

Peraturan Pemerintah merupakan peraturan pelaksana yang disusun untuk menjabarkan ketentuan-ketentuan dalam undang-undang. PP berfungsi sebagai jembatan antara norma hukum yang bersifat umum dengan kebutuhan implementasi yang lebih teknis dan operasional. Dalam konteks transformasi digital, PP menjadi instrumen penting untuk mengatur pelaksanaan kebijakan digital nasional, termasuk penguatan sistem keamanan informasi, tata kelola data, dan pelayanan publik berbasis elektronik. Keberadaan PP memastikan agar implementasi kebijakan digital berjalan konsisten, terarah, dan selaras dengan tujuan pembangunan nasional berbasis teknologi.

4.2.1 PP Nomor 71 tentang Penyelenggaraan Sistem dan Transaksi Elektronik

Peraturan Pemerintah (PP) No. 71 Tahun 2019 mengatur penyelenggaraan sistem dan transaksi elektronik di Indonesia. Regulasi ini hadir untuk menggantikan PP No. 82 Tahun 2012 dengan tujuan memperkuat kepastian hukum, meningkatkan keamanan layanan digital, serta melindungi kepentingan masyarakat dalam pemanfaatan teknologi informasi [281]. Substansi utama dari PP ini dapat dirangkum sebagai berikut:

1. Latar Belakang dan Tujuan
   PP No. 71/2019 memberikan landasan hukum yang lebih tegas terkait penyelenggaraan sistem elektronik dan transaksi elektronik. Tujuannya meliputi peningkatan keamanan, kepastian hukum bagi semua pihak, serta perlindungan masyarakat dari risiko penyalahgunaan teknologi informasi.

2. Ruang Lingkup dan Kategori PSE
   Peraturan ini berlaku bagi PSE baik di lingkup publik maupun privat. Setiap PSE diwajibkan melakukan pendaftaran, menyelenggarakan sistem secara andal, mengelola data dengan baik, serta memenuhi standar keamanan yang ditetapkan. Untuk memastikan pengelolaan risiko yang proporsional, sistem elektronik kemudian dikategorikan ke dalam tiga tingkat, yaitu strategis, tinggi, atau rendah, sesuai dengan potensi dampak dan tingkat risikonya.

3. Lokasi dan Pengelolaan Data
   Peraturan ini menegaskan bahwa data strategis wajib ditempatkan di wilayah Indonesia, kecuali bagi PSE tertentu yang memperoleh izin khusus dari pemerintah. Ketentuan ini bertujuan menjaga kedaulatan data sekaligus memastikan kendali negara atas informasi yang bernilai tinggi bagi kepentingan nasional. Selain itu, PSE berkewajiban menjaga kerahasiaan, integritas, dan ketersediaan data yang dikelola, termasuk melaporkan setiap insiden kebocoran atau kegagalan sistem kepada pihak berwenang.

4. Keamanan Sistem dan Sertifikasi
   PSE diwajibkan menerapkan sistem manajemen keamanan informasi sesuai standar yang berlaku, seperti SNI ISO/IEC 27001. Penerapan standar ini diperkuat dengan kewajiban melakukan audit keamanan secara berkala untuk memastikan kepatuhan dan efektivitas pengendalian yang diterapkan. Bagi PSE yang dikategorikan strategis, regulasi menekankan pentingnya memiliki pusat data dan pusat pemulihan bencana di wilayah Indonesia sebagai upaya menjaga ketersediaan layanan dan melindungi kepentingan nasional.

5. Pelindungan Data Pribadi
   Peraturan ini menegaskan kewajiban PSE untuk memperoleh persetujuan dari pengguna sebelum melakukan pengumpulan, pengolahan, maupun pemanfaatan data pribadi. Persetujuan tersebut menjadi dasar hukum agar setiap pemrosesan data berlangsung secara sah dan dapat dipertanggungjawabkan. Selain itu, data pribadi hanya boleh digunakan sesuai dengan tujuan yang telah disepakati bersama, sehingga hak pengguna tetap terlindungi dan risiko penyalahgunaan dapat diminimalkan.

6. Tata Kelola dan Pengawasan
   Pemerintah berperan sebagai regulator sekaligus pengawas dalam penyelenggaraan sistem elektronik. Untuk menjamin kepatuhan, setiap PSE diwajibkan memberikan akses audit kepada pemerintah sebagai bentuk transparansi dan akuntabilitas. Pelanggaran dapat dikenai sanksi administratif, mulai dari teguran hingga pencabutan izin, untuk menegakkan kepatuhan dan menjaga kepercayaan publik.

7. Sanksi
   Pelanggaran terhadap kewajiban penyelenggara sistem elektronik dapat dikenai berbagai bentuk sanksi administratif. Sanksi tersebut meliputi teguran tertulis sebagai peringatan awal, penghentian sementara sebagian atau seluruh layanan, pemblokiran akses terhadap sistem, hingga pencabutan izin

usaha bagi pelanggaran yang bersifat serius atau berulang. Mekanisme ini dimaksudkan untuk menegakkan kepatuhan sekaligus memberikan efek jera, sehingga penyelenggara lebih konsisten dalam menjaga keamanan dan keandalan layanan digital.

Keterkaitan dengan Kerangka Kerja Kepercayaan Digital di Indonesia

PP No. 71/2019 berperan penting dalam membangun ekosistem digital yang tepercaya di Indonesia. Regulasi ini tidak hanya menetapkan kewajiban teknis dan administratif bagi PSE, tetapi juga memperkenalkan prinsip-prinsip dasar yang mendukung tumbuhnya kepercayaan digital dari sisi pengguna, penyedia layanan, maupun pemerintah.

Dalam konteks penyusunan kerangka kerja kepercayaan digital nasional, ketentuan dalam PP No. 71/2019 menjadi landasan awal yang mengarahkan bagaimana sistem dan layanan digital harus dirancang, dioperasikan, dan diawasi. Regulasi ini menekankan aspek pelindungan data pribadi, transparansi, interoperabilitas sistem, pengendalian risiko siber, serta kepatuhan bagi PSE domestik maupun asing. Keseluruhan aspek tersebut mendukung terwujudnya lingkungan digital yang aman, andal, dan berdaulat. Poin-poin berikut merangkum keterkaitan PP No. 71/2019 dengan komponen utama kerangka kepercayaan digital Indonesia:

1. Keamanan dan Ketahanan Siber
   Kewajiban penerapan standar keamanan informasi dan pelaksanaan audit secara berkala menjadi langkah penting untuk memperkuat resiliensi digital. Dengan mekanisme ini, potensi kerentanan dapat terdeteksi lebih awal dan sistem mampu beradaptasi terhadap ancaman siber yang terus berkembang.

2. Perlindungan Data dan Privasi
   Aturan mengenai persetujuan pemilik data sebelum digunakan, pembatasan pemanfaatan hanya sesuai dengan tujuan yang disepakati, serta kewajiban pelindungan data pribadi memastikan hak pengguna tetap terjaga. Ketentuan ini menegaskan bahwa data pribadi dipandang sebagai aset penting yang harus dikelola secara hati-hati.

3. Akuntabilitas dan Tata Kelola
   Meskipun dapat melibatkan pihak ketiga dalam penyelenggaraan sistem, PSE tetap memegang tanggung jawab penuh atas pengelolaan data dan keamanan sistem. Hal ini menunjukkan bahwa akuntabilitas tidak dapat dialihkan, sehingga penyelenggara harus memastikan tata kelola yang baik dari awal hingga akhir rantai layanan.

4. Transparansi dan Kepatuhan
   Kewajiban pendaftaran PSE, pelaporan insiden yang terjadi, serta penyediaan akses audit kepada pemerintah mencerminkan keterbukaan yang terukur. Transparansi ini memungkinkan regulator melakukan pengawasan secara efektif sekaligus memberi jaminan kepada masyarakat bahwa penyelenggaraan

layanan digital diawasi dengan baik. Dengan demikian, kepatuhan tidak hanya bersifat administratif, tetapi juga membangun kepercayaan publik.

5. Kedaulatan Digital dan Kepentingan Nasional
   Ketentuan mengenai penempatan data strategis di wilayah Indonesia menegaskan perlindungan terhadap kepentingan nasional. Dengan memastikan data vital tetap berada dalam yurisdiksi negara, pemerintah dapat menjaga kedaulatan digital sekaligus memperkuat kepercayaan masyarakat terhadap pengelolaan data yang bernilai strategis.

6. Kolaborasi Multi-Pihak
   Implementasi regulasi ini memerlukan kerja sama erat antara pemerintah, PSE publik maupun privat, serta lembaga sertifikasi keamanan. Kolaborasi tersebut menciptakan ekosistem digital yang lebih kuat karena setiap pihak membawa peran dan tanggung jawabnya masing-masing. Pendekatan multipihak ini sejalan dengan semangat membangun ekosistem digital yang aman, kolaboratif, dan berkelanjutan.

PP No. 71/2019 menjadi pijakan penting dalam membangun kepercayaan digital nasional karena mengatur tidak hanya aspek teknis, seperti keamanan sistem dan pengelolaan data, tetapi juga nilai dasar yang mendukung terciptanya ekosistem digital yang tepercaya. Melalui ketentuan tentang pelindungan data pribadi, kewajiban transparansi, pengawasan pemerintah, hingga penempatan data strategis di Indonesia, regulasi ini menunjukkan komitmen negara untuk menjaga kedaulatan digital sekaligus melindungi hak pengguna. Lebih dari itu, penerapannya juga mendorong kerja sama antara pemerintah, PSE, dan berbagai pemangku kepentingan, sehingga kerangka kerja kepercayaan digital benar-benar dapat dijalankan secara nyata dan dirasakan manfaatnya oleh masyarakat.

4.3 Peraturan Presiden (Perpres)

Peraturan Presiden (Perpres) dibentuk untuk mendukung pelaksanaan kewenangan presiden dalam menyelenggarakan pemerintahan. Perpres kerap digunakan untuk menetapkan arah strategis dan kebijakan lintas sektor, termasuk di dalamnya agenda percepatan transformasi digital. Dalam era digital saat ini, Perpres berperan dalam mengoordinasikan berbagai lembaga dan pemangku kepentingan, memperkuat infrastruktur digital nasional, serta memastikan integrasi kebijakan digital dalam berbagai bidang pembangunan. Dengan demikian, Perpres menjadi kunci dalam mendorong sinergi antarinstansi dan mempercepat implementasi inisiatif strategis di bidang teknologi dan keamanan siber.

4.3.1 Perpres Nomor 95 Tahun 2018 tentang Sistem Pemerintahan Berbasis Elektronik (SPBE)

Perpres No. 95 Tahun 2018 bertujuan mewujudkan tata kelola pemerintahan yang bersih, efektif, transparan, dan akuntabel, sekaligus meningkatkan kualitas serta kepercayaan publik terhadap layanan pemerintahan melalui penerapan SPBE [282]. Regulasi ini juga mendorong keterpaduan dan efisiensi sistem SPBE secara nasional. Namun, perkembangan aplikasi digital yang pesat menimbulkan tantangan baru, khususnya dalam hal interoperabilitas [283]. Substansi utama Perpres ini dapat dirangkum sebagai berikut:

1. Tujuan Utama
   Peraturan ini bertujuan mewujudkan tata kelola pemerintahan yang bersih, efektif, transparan, dan akuntabel, sekaligus menghadirkan pelayanan publik yang berkualitas dan dapat dipercaya. Untuk mencapai hal tersebut, penyelenggaraan SPBE diatur secara nasional agar berjalan terpadu, efisien, dan berkesinambungan.

2. Prinsip SPBE
   Prinsip penyelenggaraan SPBE mencakup efektivitas, keterpaduan, kesinambungan, efisiensi, akuntabilitas, interoperabilitas, dan keamanan. Efektivitas menekankan pada pencapaian tujuan pemerintahan yang terukur. Keterpaduan dan interoperabilitas memastikan berbagai sistem dapat saling terhubung. Kesinambungan dan efisiensi berfokus pada keberlanjutan serta optimalisasi sumber daya. Sementara itu, akuntabilitas dan keamanan menjadi pilar untuk menjaga kepercayaan publik terhadap layanan digital pemerintah.

3. Ruang Lingkup
   Ruang lingkup SPBE meliputi tata kelola, manajemen, audit TIK, penyelenggaraan layanan, percepatan implementasi, serta pemantauan dan evaluasi. Hal ini mencerminkan pendekatan menyeluruh, mulai dari perencanaan, pelaksanaan, hingga pengawasan agar transformasi digital berjalan terarah dan konsisten.

4. Arsitektur dan Peta Rencana SPBE
   Arsitektur SPBE disusun secara berlapis, meliputi arsitektur nasional, arsitektur instansi pusat, dan arsitektur pemerintah daerah. Penyusunan ini bertujuan memastikan keterpaduan penerapan SPBE di seluruh tingkatan pemerintahan. Untuk mendukung implementasinya, ditetapkan peta rencana lima tahunan yang berfungsi sebagai panduan strategis. Peta rencana tersebut mencakup aspek tata kelola, manajemen, infrastruktur, aplikasi, keamanan, layanan, serta audit, sehingga arah pembangunan SPBE dapat berlangsung konsisten, terukur, dan berkesinambungan.

5. Infrastruktur dan Data
   Penguatan infrastruktur digital pemerintah diwujudkan melalui penyediaan Pusat Data Nasional, jaringan intra pemerintah, serta sistem penghubung

layanan pemerintah yang memungkinkan integrasi lintas instansi. Setiap instansi pusat maupun daerah diwajibkan memanfaatkan data bersama dengan mengacu pada standar interoperabilitas. Dengan cara ini, pengelolaan data menjadi lebih konsisten, efisien, dan saling terhubung, sehingga mendukung terciptanya layanan pemerintahan yang terpadu dan dapat dipercaya.

6. Keamanan SPBE
   Aspek keamanan dalam SPBE menekankan perlindungan menyeluruh terhadap kerahasiaan, integritas, ketersediaan, keaslian, dan nirsangkal data serta layanan digital pemerintah. Untuk mencapai hal tersebut, diatur mekanisme klasifikasi keamanan, pembatasan akses sesuai otorisasi, dan pemulihan data jika terjadi gangguan atau insiden. Selain itu, penerapan tanda tangan digital dan sertifikat digital menjadi instrumen penting guna memastikan keabsahan identitas serta mencegah penyalahgunaan informasi dalam transaksi elektronik.

7. Manajemen SPBE
   Manajemen SPBE mencakup pengelolaan risiko, keamanan informasi, data, aset TIK, sumber daya manusia, pengetahuan, perubahan, dan layanan. Setiap aspek ini menjadi dasar penting dalam menjaga kualitas layanan digital. Misalnya, pengelolaan risiko dan keamanan informasi memastikan resiliensi, sementara manajemen SDM dan pengetahuan mendukung penguatan kapasitas aparatur dalam menjalankan transformasi digital.

8. Audit TIK
   Audit dalam SPBE mencakup infrastruktur, aplikasi, dan aspek keamanan yang dilakukan secara berkala dengan standar tertentu. Tujuannya adalah untuk memastikan sistem yang digunakan tetap andal, aman, dan sesuai dengan kebutuhan organisasi serta regulasi yang berlaku.

9. Layanan SPBE
   Layanan SPBE terbagi menjadi dua kategori utama. Pertama, layanan administrasi pemerintahan yang mendukung proses internal birokrasi. Kedua, layanan publik yang mencakup sektor strategis seperti pendidikan, kesehatan, keuangan, transportasi, dan lain-lain, yang secara langsung dirasakan manfaatnya oleh masyarakat.

10. Kelembagaan
    Untuk menjamin implementasi SPBE berjalan efektif, dibentuk Tim Koordinasi SPBE Nasional yang berada langsung di bawah Presiden. Tim ini melibatkan kementerian dan lembaga utama, termasuk Badan Siber dan Sandi Negara (BSSN), yang berperan dalam mengoordinasikan, mengawasi, dan mengawal penerapan SPBE secara nasional.

Keterkaitan dengan Kerangka Kerja Kepercayaan Digital di Indonesia

Kepercayaan digital merupakan prasyarat utama dalam pembangunan layanan pemerintahan yang transparan, akuntabel, dan berorientasi pada masyarakat. Da-

lam konteks ini, Perpres No. 95 Tahun 2018 menjadi landasan penting untuk membangun sistem pemerintahan digital yang aman dan tepercaya.

Perpres ini menekankan layanan publik berbasis elektronik yang andal, aman, dan terintegrasi. Aspek keamanan informasi, perlindungan data, interoperabilitas sistem, serta akuntabilitas instansi pemerintah merupakan faktor yang secara langsung mendukung kepercayaan digital.

Oleh karena itu, penyusunan kerangka kerja kepercayaan digital di Indonesia perlu diselaraskan dengan amanat SPBE agar transformasi digital tidak hanya efisien dan inovatif, tetapi juga mampu menumbuhkan kepercayaan publik melalui tata kelola yang transparan, sistem yang aman, serta perlindungan data yang kuat. Keterkaitan tersebut dapat dilihat pada poin-poin berikut:

1. Akuntabilitas dan Transparansi
   Prinsip akuntabilitas dalam SPBE tercermin melalui kewajiban audit TIK dan mekanisme pelaporan yang terstruktur. Hal ini memastikan setiap instansi pemerintah mempertanggungjawabkan pengelolaan sistemnya secara terbuka, sehingga publik dapat menilai tingkat kepatuhan dan kinerja layanan digital yang diberikan.

2. Keamanan dan Privasi
   Regulasi terkait keamanan SPBE menekankan penerapan sertifikat digital, tanda tangan digital, serta pengendalian akses. Langkah-langkah ini dirancang untuk menjaga kerahasiaan, integritas, dan keaslian data, sekaligus memberikan perlindungan terhadap privasi pengguna dalam setiap interaksi digital dengan pemerintah.

3. Interoperabilitas dan Keterpaduan
   Pemanfaatan pusat data nasional, sistem penghubung layanan, dan standar interoperabilitas menjadi fondasi untuk menciptakan layanan digital yang efisien. Dengan keterpaduan ini, proses pertukaran data antarinstansi menjadi lebih lancar, mengurangi duplikasi sistem, serta meningkatkan konsistensi informasi publik.

4. Kedaulatan Digital
   Pengelolaan data nasional melalui Pusat Data Nasional menegaskan kontrol negara terhadap aset digital strategis. Kebijakan ini memperkuat posisi Indonesia dalam menjaga kedaulatan digital dan mengurangi ketergantungan pada infrastruktur asing.

5. Kolaborasi Multi-Pihak
   Pelaksanaan SPBE melibatkan kementerian, pemerintah daerah, dan BSSN, yang bekerja sama untuk membangun ekosistem digital yang aman dan andal. Kolaborasi lintas sektor ini memastikan kebijakan dan implementasi digital tidak berjalan sendiri-sendiri, melainkan saling melengkapi.

6. Pelayanan Publik yang Tepercaya
   Transformasi digital pemerintah diarahkan untuk menghasilkan layanan publik

berbasis elektronik yang berkualitas dan mudah diakses. Dengan layanan yang lebih cepat, transparan, dan responsif, kepercayaan masyarakat terhadap pemerintahan digital dapat terus meningkat.

Kepercayaan digital menjadi kunci dalam menghadirkan layanan pemerintahan yang transparan, akuntabel, dan berfokus pada kebutuhan masyarakat. Perpres No. 95 Tahun 2018 tentang SPBE menegaskan bahwa transformasi digital pemerintah tidak hanya soal efisiensi dan inovasi, tetapi juga tentang membangun sistem yang aman, terintegrasi, dan dapat dipercaya oleh publik. Dengan prinsip akuntabilitas, transparansi, interoperabilitas, serta perlindungan data dan privasi, regulasi ini memastikan bahwa setiap layanan digital dijalankan secara konsisten dan dapat dipertanggungjawabkan. Pengelolaan data nasional melalui Pusat Data Nasional, didukung oleh kolaborasi antarkementerian, pemerintah daerah, dan BSSN, memperkuat kedaulatan digital sekaligus menciptakan ekosistem layanan publik yang andal. Dengan demikian, penerapan SPBE memungkinkan masyarakat untuk berinteraksi dengan layanan pemerintah secara elektronik dengan aman, nyaman, dan percaya diri.

4.3.2 Perpres Nomor 82 Tahun 2022 tentang Pelindungan Infrastruktur Informasi Vital

Perpres Nomor 82 Tahun 2022 tentang Pelindungan Infrastruktur Informasi Vital (IIV) merupakan landasan strategis dalam sistem tata kelola keamanan siber di Indonesia, khususnya dalam melindungi sektor-sektor vital dari ancaman digital yang semakin kompleks [284]. Regulasi ini tidak hanya menekankan perlunya penguatan keamanan pada infrastruktur kritis, tetapi juga menetapkan prinsip tata kelola, manajemen risiko, serta koordinasi lintas sektor untuk menciptakan ekosistem digital yang aman dan tepercaya.

Kehadiran Perpres ini menjadi sangat relevan dalam konteks transformasi digital Indonesia, di mana layanan publik dan aktivitas ekonomi berbasis teknologi informasi semakin terintegrasi dengan infrastruktur vital. Prinsip-prinsip yang terkandung di dalamnya dapat dijadikan acuan adaptif dalam menyusun kerangka kerja kepercayaan digital nasional yang lebih komprehensif. Untuk memahami lebih jauh substansi dan cakupan Perpres ini, berikut disajikan poin-poin utama yang terkandung di dalamnya:

1. Tujuan Pelindungan IIV (Pasal 2)
   Regulasi ini menetapkan tujuan pelindungan IIV untuk menjamin keberlangsungan infrastruktur vital agar beroperasi secara aman, andal, dan tepercaya. Selain itu, ditegaskan pula upaya pencegahan terhadap serangan siber yang berpotensi merusak sistem, serta peningkatan kesiapan menghadapi insiden melalui percepatan proses pemulihan.

2. Ruang Lingkup (Pasal 3–6)
   Pelindungan mencakup identifikasi sektor dan sistem yang dikategorikan sebagai IIV, seperti administrasi pemerintahan, energi, transportasi, keuangan,

kesehatan, teknologi informasi dan komunikasi, pangan, pertahanan, dan sektor strategis lainnya. Penyelenggara sistem diwajibkan melakukan identifikasi secara berkala dan menyampaikan laporan sesuai prosedur.

3. Kerangka Kerja dan Peta Jalan Pelindungan IIV (Pasal 7–8)
   BSSN bertugas menyusun kerangka kerja serta peta jalan lima tahunan sebagai pedoman teknis dan regulatif. Dokumen ini mencakup standar keamanan, pembinaan, pengawasan, serta arah strategis dalam memperkuat IIV secara berkelanjutan.

4. Standar Keamanan Siber dan Manajemen Risiko (Pasal 9–10)
   Setiap penyelenggara IIV wajib menerapkan standar keamanan informasi dan keamanan siber yang sesuai dengan sektor masing-masing. Selain itu, regulasi ini mengatur kewajiban penerapan manajemen risiko keamanan siber untuk mengidentifikasi, menganalisis, dan memitigasi ancaman secara sistematis.

5. Penanganan Insiden Siber (Pasal 11–17)
   Perpres ini mengatur pembentukan Tim Tanggap Insiden Siber di tingkat nasional, sektoral, dan organisasi. Mekanisme penanganan mencakup pelaporan insiden, pemulihan, hingga manajemen krisis siber agar respons dapat dilakukan secara cepat, terkoordinasi, dan efektif.

6. Pembinaan dan Pengawasan (Pasal 18–22)
   Upaya pembinaan dan pengawasan difokuskan pada peningkatan kapasitas sumber daya manusia melalui pelatihan dan sertifikasi, penguatan kerja sama nasional maupun internasional, serta pengukuran tingkat kematangan keamanan siber setiap tahun untuk mendukung perbaikan berkelanjutan.

7. Koordinasi Nasional (Pasal 23–25)
   BSSN berperan sebagai koordinator utama pelindungan IIV. Rapat koordinasi nasional wajib dilaksanakan sedikitnya sekali dalam setahun dengan melibatkan seluruh pemangku kepentingan, dan hasilnya dilaporkan langsung kepada Presiden sebagai bentuk akuntabilitas.

Keterkaitan dengan Kerangka Kerja Kepercayaan Digital di Indonesia

Keterkaitan antara Perpres Nomor 82 Tahun 2022 dan penyusunan kerangka kerja kepercayaan digital di Indonesia dapat dilihat dari kesesuaian prinsip, tujuan, serta mekanisme yang diatur dalam peraturan tersebut dengan kebutuhan ekosistem digital yang aman, transparan, dan tepercaya. Regulasi ini tidak hanya menetapkan standar keamanan bagi infrastruktur informasi vital, tetapi juga menyediakan kerangka koordinasi, akuntabilitas, dan pengawasan yang dapat diintegrasikan ke dalam model kepercayaan digital nasional. Dengan demikian, Perpres 82/2022 menjadi acuan penting dalam memperkuat aspek regulasi, kelembagaan, dan teknis pada kerangka kerja kepercayaan digital Indonesia.

1. Keamanan sebagai Dasar Kepercayaan Digital
   Perpres menekankan pelindungan IIV melalui penerapan standar keamanan

siber yang kuat. Hal ini sejalan dengan prinsip kepercayaan digital yang mengharuskan setiap layanan elektronik andal, aman, dan tepercaya.

2. Manajemen Risiko dan *Trust by Design*
   Kewajiban penerapan manajemen risiko serta standar keamanan (Pasal 9–10) menjadi dasar bagi implementasi prinsip *trust by design* dalam kerangka kerja kepercayaan digital.

3. Respon Insiden dan Resiliensi Ekosistem Digital
   Pembentukan Tim Tanggap Insiden Siber dan mekanisme manajemen krisis memperkuat pilar resiliensi dan pemulihan cepat. Hal ini penting agar masyarakat tetap memiliki kepercayaan terhadap sistem digital meskipun terjadi serangan.

4. Peningkatan SDM dan Literasi Digital
   Ketentuan mengenai pembinaan Sumber Daya Manusia melalui pelatihan dan sertifikasi memperkuat aspek *human capital* dalam kerangka kepercayaan digital, sekaligus mendukung peningkatan literasi keamanan siber di masyarakat.

5. Kerja Sama *Multi-Stakeholder* dan Diplomasi Digital
   Kolaborasi dalam dan luar negeri (Pasal 21) mendukung pembentukan *trust framework* baik di tingkat nasional maupun regional, serta memperkuat posisi Indonesia dalam diplomasi digital global.

6. Pengukuran Kematangan Keamanan Siber
   Proses audit dan pengukuran tingkat kematangan keamanan siber (Pasal 22) dapat dijadikan indikator objektif untuk menilai tingkat maturitas kepercayaan digital di berbagai sektor.

7. Koordinasi Nasional
   Penetapan BSSN sebagai koordinator pelindungan IIV sejalan dengan kebutuhan adanya otoritas nasional kepercayaan digital. Peran ini memayungi kebijakan lintas sektor sekaligus menjaga konsistensi regulasi.

Perpres Nomor 82 Tahun 2022 secara substansial menyediakan landasan regulasi keamanan siber yang erat kaitannya dengan pembangunan kerangka kepercayaan digital Indonesia. Perlindungan terhadap IIV berfungsi sebagai basis utama yang menjamin fondasi digital nasional tetap kuat dan andal. Dalam konteks ini, keamanan dan kepercayaan memiliki hubungan yang saling terkait, di mana kepercayaan digital tidak mungkin tumbuh tanpa adanya sistem keamanan siber yang kokoh. Dengan demikian, kerangka kerja kepercayaan digital di Indonesia dapat menjadikan Perpres ini sebagai referensi utama, terutama pada aspek keamanan, resiliensi ekosistem, tata kelola, penguatan sumber daya manusia, serta kerja sama lintas sektor dan tingkat nasional.

4.3.3 Perpres Nomor 132 Tahun 2022 tentang Arsitektur Sistem Pemerintahan Berbasis Elektronik (SPBE) Nasional

Perpres No. 132 Tahun 2022 ditetapkan untuk memperkuat arsitektur Sistem Pemerintahan Berbasis Elektronik (SPBE) di Indonesia, dengan tujuan memastikan penerapan sistem digital pemerintah berjalan terpadu, konsisten, dan dapat mendukung transformasi layanan publik secara efektif [285]. Regulasi ini menekankan penyusunan arsitektur SPBE secara nasional, instansi pusat, dan pemerintah daerah, sehingga seluruh implementasi sistem digital dapat saling terhubung dan terstandarisasi. Dengan hadirnya Perpres ini, diharapkan pengelolaan data, aplikasi, infrastruktur, dan keamanan informasi dapat berlangsung lebih efisien dan terarah, sekaligus meningkatkan kemampuan pemerintah dalam menghadapi tantangan teknologi informasi yang terus berkembang. Substansi utama Perpres ini dapat dirangkum sebagai berikut:

1. Latar Belakang
   Perpres 132/2022 merupakan kelanjutan dari Perpres 95/2018 tentang SPBE dan diterbitkan untuk memperkuat penerapan sistem pemerintahan berbasis elektronik di seluruh tingkat pemerintahan. Regulasi ini lahir sebagai respons terhadap ketimpangan implementasi SPBE antara instansi pusat dan pemerintah daerah, yang selama ini masih berjalan secara terpisah atau "silo". Kondisi ini tercermin dari rata-rata capaian indeks SPBE nasional yang baru berada pada level "cukup", sehingga dibutuhkan pedoman arsitektur dan standar yang lebih jelas untuk mendorong keterpaduan, efisiensi, dan konsistensi dalam transformasi digital pemerintahan.

2. Tujuan
   Perpres No. 132 Tahun 2022 bertujuan memberikan panduan yang jelas untuk mengintegrasikan seluruh aspek SPBE, mulai dari proses bisnis, data dan informasi, aplikasi, hingga infrastruktur dan keamanan. Dengan kerangka yang terstruktur ini, pemerintah diharapkan mampu menghadirkan layanan yang lebih terpadu, efisien, dan berorientasi pada kebutuhan pengguna, sehingga transformasi digital tidak hanya meningkatkan efektivitas internal, tetapi juga menghadirkan pengalaman layanan publik yang lebih baik dan dapat diandalkan.

3. Ruang Lingkup Arsitektur SPBE Nasional (2020–2024)
   Ruang lingkup Arsitektur SPBE Nasional untuk periode 2020–2024 dirancang agar sejalan dengan RPJMN, transformasi digital pemerintah, serta kebijakan *Satu Data Indonesia*. Arsitektur ini mengacu pada standar baku SPBE yang berlaku di seluruh domain, sehingga setiap pengembangan sistem dan layanan digital pemerintah memiliki pedoman yang konsisten. Domain arsitektur mencakup proses bisnis, data dan informasi, aplikasi, infrastruktur, layanan, serta keamanan, yang saling terkait untuk mendukung penyelenggaraan pemerintahan berbasis elektronik secara terpadu. Untuk mencapai tujuan

tersebut, beberapa inisiatif strategis dijalankan, antara lain penguatan tata kelola SPBE, peningkatan kualitas layanan, integrasi TIK, dan pengembangan kapasitas SDM SPBE. Dengan pendekatan ini, implementasi Arsitektur SPBE Nasional dapat berlangsung terarah, efisien, dan responsif terhadap kebutuhan pemerintah maupun masyarakat.

4. Pengelolaan dan Implementasi
   Dalam pengelolaan dan implementasi SPBE, setiap instansi pusat maupun pemerintah daerah diwajibkan menyusun arsitektur SPBE yang mengacu pada arsitektur nasional, sehingga penerapan sistem digital pemerintah berjalan terpadu dan konsisten. Untuk menjamin kelancaran layanan, Wali Layanan ditunjuk sebagai pengelola SPBE pada masing-masing tingkat instansi, bertanggung jawab atas pengelolaan dan pemantauan operasional layanan digital. Selain itu, pengembangan infrastruktur dan layanan SPBE harus diselesaikan dalam jangka waktu tertentu, yakni maksimal dua tahun sejak penetapan, agar transformasi digital dapat segera memberikan manfaat bagi proses pemerintahan dan pelayanan publik.

5. Fokus Strategis
   Fokus strategis Perpres ini menekankan penguatan layanan publik digital di berbagai sektor, mulai dari kesehatan, pendidikan, bantuan sosial, hukum, hingga administrasi pemerintahan, dengan tujuan menghadirkan layanan yang lebih cepat, transparan, dan mudah diakses masyarakat. Selain itu, regulasi ini mendorong integrasi *Satu Data Indonesia*, sehingga seluruh data pemerintah dapat dikelola secara konsisten, saling terhubung, dan mendukung pengambilan kebijakan yang berbasis bukti. Pemanfaatan teknologi baru seperti *Big Data*, AI, dan layanan berbagi pakai menjadi pendorong utama transformasi digital, memungkinkan inovasi layanan yang lebih adaptif dan efisien. Di sisi lain, pengembangan talenta digital ASN dan pembentukan forum kolaborasi lintas pihak bertujuan memperkuat kapasitas sumber daya manusia dan memperluas kerja sama antarinstansi, sehingga implementasi SPBE dapat berjalan secara terarah dan berkelanjutan.

Keterkaitan dengan Kerangka Kerja Kepercayaan Digital di Indonesia

Perpres No. 132 Tahun 2022 menjadi penguatan lanjutan bagi pembangunan layanan pemerintahan digital yang terintegrasi dan dapat dipercaya. Regulasi ini menekankan pentingnya penyusunan arsitektur SPBE secara nasional, termasuk integrasi data, standar interoperabilitas, dan pemanfaatan teknologi baru, sehingga layanan publik dapat berjalan lebih efisien, konsisten, dan aman. Dengan kerangka arsitektur yang jelas, pengelolaan data yang terstandarisasi, serta koordinasi lintas instansi yang lebih terstruktur, Perpres ini secara langsung mendukung prinsip kepercayaan digital. Oleh karena itu, implementasi SPBE perlu diselaraskan dengan amanat Perpres 132 agar transformasi digital tidak hanya menghadirkan layanan inovatif, tetapi juga memperkuat kepercayaan masyarakat melalui sistem yang andal, terintegrasi, dan terlindungi dengan baik.Keterkaitan tersebut dapat dilihat

pada poin-poin berikut:

1. Akuntabilitas dan Tata Kelola
   Kewajiban instansi pusat dan daerah untuk menyusun arsitektur SPBE sesuai standar nasional mencerminkan praktik tata kelola yang akuntabel. Hal ini memastikan setiap instansi dapat dipertanggungjawabkan dalam pengelolaan sistem digital, termasuk perencanaan, implementasi, dan pemeliharaan layanan.

2. Transparansi dan Kepatuhan
   Evaluasi SPBE secara nasional, pemantauan berkala, serta sinkronisasi dengan *Satu Data Indonesia* mendukung prinsip transparansi dan keterbukaan. Masyarakat dan pemangku kepentingan dapat memperoleh informasi yang jelas mengenai kinerja sistem digital pemerintah, sekaligus memastikan instansi mematuhi regulasi yang berlaku.

3. Keamanan dan Resiliensi Digital
   Domain arsitektur keamanan SPBE menekankan perlindungan data, integritas layanan, dan mitigasi risiko siber. Pendekatan ini menjadi pilar utama dalam membangun kepercayaan digital, sekaligus menjaga keberlanjutan operasional layanan publik di tengah potensi ancaman teknologi informasi.

4. Kolaborasi Multi-Pihak
   Pelibatan instansi pusat, pemerintah daerah, BSSN, serta sektor nonpemerintah melalui forum kolaborasi SPBE menunjukkan pendekatan ekosistem yang terintegrasi. Kolaborasi ini memastikan pengembangan dan implementasi SPBE berjalan lebih efisien, responsif, dan saling melengkapi antarpemangku kepentingan.

5. Kedaulatan Digital
   Pusat Data Nasional, integrasi *Satu Data Indonesia*, dan pengelolaan infrastruktur SPBE di dalam negeri memperkuat kedaulatan digital. Langkah ini memastikan kontrol nasional terhadap data publik, mengurangi ketergantungan pada infrastruktur asing, dan mendukung keamanan serta privasi informasi.

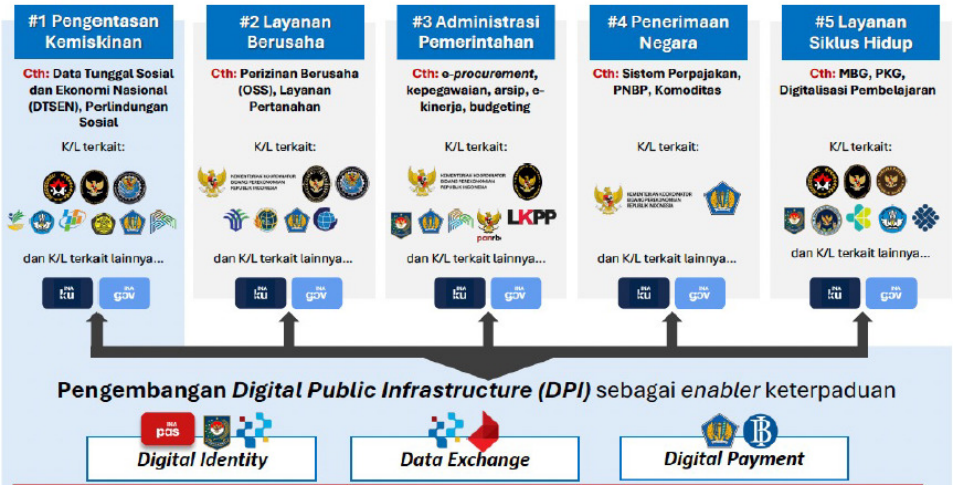
6. Pelayanan Publik yang Andal
   Fokus pada peningkatan kualitas layanan publik digital yang terintegrasi, G2C, G2B, G2G, dan G2E, membantu membangun kepercayaan masyarakat terhadap layanan pemerintah. Layanan yang cepat, konsisten, dan mudah diakses meningkatkan kepuasan publik sekaligus memperkuat legitimasi digital pemerintah.

Perpres No. 132 Tahun 2022 memberikan arah strategis dalam memperkuat arsitektur SPBE di Indonesia. Regulasi ini mendorong integrasi data, pemanfaatan teknologi baru, dan penyusunan arsitektur SPBE yang konsisten di seluruh instansi pemerintah, sehingga mendukung pembangunan layanan publik digital yang aman,

andal, dan terintegrasi. Dengan memperkuat koordinasi antarinstansi, meningkatkan kapasitas talenta digital ASN, serta membangun forum kolaborasi lintas pihak, Perpres ini menjadi dasar penting bagi pengembangan ekosistem pemerintahan digital yang efisien, transparan, dan dapat dipercaya oleh masyarakat.

4.3.4 Perpres Nomor 82 Tahun 2023 tentang Percepatan Transformasi Digital dan Keterpaduan Layanan Digital Nasional

Perpres Nomor 82 Tahun 2023 mengatur tentang Percepatan Transformasi Digital dan Keterpaduan Layanan Digital Nasional [286]. Regulasi ini bertujuan untuk meningkatkan kualitas pelayanan publik, efisiensi birokrasi, keamanan siber, serta pencegahan korupsi melalui digitalisasi sistem pemerintahan.



Gambar 4.2: Kerangka Kerja Proyek Strategis Nasional

Gambar 4.2 menggambarkan kerangka kerja Proyek Strategis Nasional (PSN) yang dikoordinasikan oleh Kementerian PANRB, dengan fokus utama pada *Pengembangan Layanan Digital Pemerintah Terpadu*. Inisiatif ini merupakan bagian dari Program Prioritas Nasional 7, Kegiatan Prioritas Utama #78, yaitu *Transformasi Digital Layanan Publik Prioritas*. Pendekatan strategis ini menitikberatkan pada penguatan ekosistem layanan publik digital melalui lima klaster layanan prioritas, yang masing-masing mencerminkan kebutuhan esensial masyarakat dan tata kelola pemerintahan yang efektif.

1. Pengentasan Kemiskinan
   Fokus pada penguatan basis data sosial dan layanan perlindungan sosial, seperti *Data Tunggal Sosial dan Ekonomi Nasional (DTSEN)*. Kementerian/Lembaga (K/L) seperti Kementerian Sosial, Bappenas, dan lembaga terkait lainnya terlibat aktif dalam klaster ini.

2. Layanan Berusaha
   Transformasi layanan perizinan dan pertanahan, seperti *Online Single Submission* (OSS) dan digitalisasi layanan ATR/BPN, menjadi pendorong kemudahan berusaha. Kementerian Investasi/BKPM, ATR/BPN, serta K/L ekonomi lainnya menjadi pemangku kepentingan utama.

3. Administrasi Pemerintahan
   Digitalisasi birokrasi difokuskan pada layanan seperti *e-procurement*, pengelolaan kepegawaian, kearsipan, e-kinerja, dan penganggaran. LKPP, BKN, Arsip Nasional, dan Kementerian Keuangan memainkan peran penting dalam implementasinya.

4. Penerimaan Negara
   Transformasi sistem perpajakan dan manajemen komoditas, termasuk PNBP, difokuskan pada efektivitas penerimaan negara. Ditjen Pajak, Kementerian Keuangan, dan lembaga pendapatan lainnya bertanggung jawab dalam klaster ini.

5. Layanan Siklus Hidup
   Meliputi layanan dari lahir hingga akhir hayat warga negara, seperti *Manajemen Berbasis Gugus (MBG)*, *Pengelolaan Kependudukan dan Keluarga (PKG)*, dan digitalisasi pembelajaran. Kementerian Pendidikan, Kesehatan, dan instansi layanan dasar terlibat secara kolaboratif.

Kelima klaster tersebut didukung oleh pengembangan *Digital Public Infrastructure (DPI)* sebagai *enabler* keterpaduan sistem layanan. Tiga pilar utama DPI yang dikembangkan meliputi:

- *Digital Identity*, untuk menjamin identitas digital warga secara aman [287]. Pengembangan identitas digital ini mengikuti praktik global untuk meningkatkan interoperabilitas dan mempercepat proses layanan publik.

- *Data Exchange*, guna memastikan pertukaran data antarsistem yang efisien dan tepercaya. Setelah disahkannya UU PDP [279], ekosistem pertukaran data menjadi lebih berpihak kepada kedaulatan data. Kedaulatan data tercermin dari kewajiban penyimpanan data strategis yang harus disimpan dan diproses di dalam negeri.

- *Digital Payment*, untuk mendukung transaksi keuangan digital lintas layanan. Seperti telah dicanangkan dalam Blueprint Sistem Pembayaran RI [288], digital payment di Indonesia akan semakin aman melalui *Payment ID*.

Pengembangan DPI dilakukan secara terintegrasi oleh lembaga-lembaga strategis seperti Perum Peruri sebagai penyelenggara utama aplikasi SPBE Prioritas termasuk pengembangan dan pemeliharaan sistem [289, 290] dan juga BSSN, Dukcapil serta Bank Indonesia, dengan penguatan prinsip-prinsip *Data Protection*, *Security by Design* hingga *Security Awareness*.

Keterkaitan dengan Kerangka Kerja Kepercayaan Digital di Indonesia

Perpres Nomor 82 Tahun 2023 menjadi salah satu landasan strategis dalam pembangunan ekosistem digital nasional yang aman dan tepercaya. Regulasi ini tidak hanya memperkuat interoperabilitas infrastruktur dan layanan digital pemerintah, tetapi juga menegaskan pentingnya tata kelola digital yang akuntabel dan berbasis kepercayaan.

Dalam konteks penyusunan Kerangka Kerja Kepercayaan Digital, Perpres ini memperkuat landasan kebijakan yang menempatkan kepercayaan sebagai prasyarat utama untuk adopsi teknologi digital yang berkelanjutan. Berbagai inisiatif seperti SPBE, *Satu Data Indonesia*, Identitas Digital dan Identitas Pembayaran Digital, yang diamanatkan dalam Perpres tersebut, secara langsung mendukung dimensi-dimensi utama kepercayaan digital. Hal tersebut dimulai dari transparansi, keamanan informasi, hingga kepatuhan terhadap regulasi pelindungan data pribadi. Poin-poin berikut merangkum bagaimana Perpres ini berkontribusi pada pembentukan arsitektur kepercayaan digital nasional:

1. Meningkatkan Transparansi dan Akuntabilitas
   Transformasi digital melalui SPBE dan *Satu Data Indonesia* menciptakan transparansi dalam layanan publik, yang merupakan pilar utama kepercayaan digital.

2. Memperkuat Keamanan Siber dan Perlindungan Data
   Dengan menekankan interoperabilitas sistem, perlindungan data, serta kendali mutu keamanan siber, Perpres ini mendukung kebijakan kepercayaan digital yang mengutamakan integritas, keandalan, dan keamanan informasi.

3. Mendorong Partisipasi dan Kemudahan Akses Layanan Digital
   Dengan adanya Identitas Digital Terpadu dan *Single Sign-On* Nasional, kepercayaan pengguna dalam mengakses layanan digital akan meningkat karena adanya keamanan, kemudahan, dan kepastian hukum dalam setiap transaksi [287].

4. Memastikan Kepatuhan Regulasi dan Tata Kelola Digital
   Regulasi ini sejalan dengan UU PDP serta standar keamanan informasi global, menciptakan ekosistem digital yang aman dan tepercaya bagi masyarakat dan pelaku usaha.

4.3.5 Perpres Nomor 17 Tahun 2023 tentang Percepatan Transformasi Digital di Bidang Pengadaan Barang/Jasa Pemerintah

PerPres Nomor 17 Tahun 2023 tentang Percepatan Transformasi Digital di Bidang Pengadaan Barang/Jasa Pemerintah diterbitkan sebagai langkah strategis untuk memperkuat kemandirian ekonomi nasional melalui digitalisasi sistem pengadaan pemerintah. Tujuan utamanya adalah meningkatkan penggunaan produk dalam

negeri serta memberdayakan UMKM dan koperasi dalam ekosistem pengadaan barang/jasa pemerintah. Melalui transformasi digital, regulasi ini diharapkan dapat mempercepat penyerapan anggaran, meningkatkan efisiensi, serta mendorong pemerataan ekonomi nasional melalui sistem pengadaan yang terintegrasi dan sepenuhnya digital [291].

Secara umum, Perpres ini dirancang untuk mempercepat digitalisasi proses pengadaan barang/jasa pemerintah guna mewujudkan efisiensi, transparansi, akuntabilitas, dan keterpaduan antarsistem pengelolaan [291]. Di dalamnya diatur penugasan, pembagian peran, serta mekanisme dukungan lintas kementerian dan lembaga untuk menjamin keberhasilan transformasi tersebut. Substansi utama dari Perpres ini dapat dijabarkan sebagai berikut:

1. Penugasan kepada BUMN PT Telekomunikasi Indonesia (Persero) atau Telkom
   Berdasarkan Pasal 2 dan Pasal 3, pemerintah menugaskan Telkom untuk menyelenggarakan *Sistem Pengadaan Secara Elektronik* (SPSE) beserta seluruh sistem pendukungnya. Penugasan ini mencakup pendanaan, perencanaan, pembangunan, pengembangan, pengintegrasian, pengoperasian, serta pemeliharaan sistem secara menyeluruh. Pendekatan ini dimaksudkan agar pengelolaan SPSE memiliki kesinambungan teknis dan operasional dalam satu entitas yang memiliki kapasitas digital nasional yang kuat.

2. Integrasi dengan kebijakan nasional digital
   Sejalan dengan arah kebijakan *Satu Data Indonesia* dan SPBE, Perpres ini menegaskan pentingnya interoperabilitas antarsistem pengelolaan data pemerintah. Integrasi ini bertujuan untuk menciptakan tata kelola digital yang terpadu, efisien, dan konsisten antarkementerian/lembaga.

3. Penetapan kepemilikan hak kekayaan intelektual (HKI)
   Perpres menetapkan bahwa hak kekayaan intelektual atas SPSE ditetapkan menjadi milik negara dan dikelola oleh *Lembaga Kebijakan Pengadaan Barang/Jasa Pemerintah* (LKPP). Hal ini memperkuat prinsip kedaulatan data dan pengendalian infrastruktur digital oleh negara.

4. Pembagian peran lintas kementerian dan lembaga
   Pengaturan peran diatur secara terperinci untuk memastikan tata kelola berjalan efektif, antara lain:

   - LKPP berperan sebagai pengawas dan pengelola SPSE;
   - Kementerian BUMN melakukan pembinaan terhadap Telkom selaku pelaksana teknis;
   - Kementerian Keuangan mendukung pengelolaan barang milik negara serta penerimaan negara bukan pajak (PNBP);
   - Kementerian Komunikasi dan Informatika (Kemenkominfo) memastikan kepatuhan terhadap kebijakan SPBE, *Satu Data Indonesia*, serta keamanan informasi.

5. Peningkatan penggunaan produk dalam negeri dan pemberdayaan UMKM
   Sesuai Pasal 4, pengadaan melalui SPSE wajib mengutamakan produk dalam negeri serta melibatkan UMKM dan koperasi. Ketentuan ini diharapkan dapat mendorong inovasi lokal, memperkuat rantai pasok nasional, dan meningkatkan daya saing produk Indonesia di pasar domestik.

6. Dukungan lintas kementerian dan pengawasan
   Berdasarkan Pasal 8, seluruh kementerian dan lembaga diwajibkan memberikan dukungan terhadap pelaksanaan transformasi digital pengadaan barang/jasa. Untuk menjamin akuntabilitas dan transparansi, Perpres ini juga mewajibkan pelaporan berkala kepada Presiden dan lembaga terkait, dengan pengawasan langsung oleh BPKP.

Dengan demikian, Perpres Nomor 17 Tahun 2023 tidak hanya mengatur aspek teknis digitalisasi pengadaan, tetapi juga menegaskan komitmen pemerintah terhadap penguatan ekonomi nasional, tata kelola digital yang terpadu, serta prinsip akuntabilitas dalam pengelolaan anggaran negara.

Keterkaitan dengan Kerangka Kerja Kepercayaan Digital di Indonesia

Perpres Nomor 17 Tahun 2023 memiliki relevansi strategis dalam pembangunan kerangka kerja kepercayaan digital di Indonesia, khususnya dalam memperkuat tata kelola digital di sektor publik. Regulasi ini tidak hanya berfokus pada transformasi pengadaan barang/jasa pemerintah, tetapi juga membentuk dasar kepercayaan digital melalui penerapan prinsip keamanan, transparansi, integritas data, kolaborasi lintas lembaga, serta pemberdayaan ekonomi digital nasional.

Transformasi digital dalam sistem pengadaan pemerintah melalui integrasi SPSE menjadi salah satu pilar utama dalam mewujudkan ekosistem digital yang tepercaya. Keterkaitan antara substansi Perpres No. 17 Tahun 2023 dan elemen-elemen kepercayaan digital dapat dijelaskan melalui aspek berikut:

1. Keamanan dan Reliabilitas Sistem
   Pengaturan peran Kementerian Kominfo serta penerapan kebijakan SPBE dan *Satu Data Indonesia* memastikan keamanan, interoperabilitas, dan keandalan sistem pengadaan digital. Penerapan standar keamanan dan mekanisme perlindungan data transaksi memperkuat integritas sistem serta mencegah penyalahgunaan atau kebocoran informasi. Keandalan sistem menjadi dasar utama dalam membangun kepercayaan masyarakat dan pelaku usaha terhadap layanan digital pemerintah.

2. Transparansi dan Akuntabilitas Pengadaan Digital
   Melalui mekanisme pelaporan berkala dan pengawasan oleh BPKP, serta penetapan SPSE sebagai aset negara, Perpres ini memperkuat keterbukaan dan tanggung jawab lembaga penyelenggara pengadaan. Masyarakat dan pelaku usaha dapat memantau proses pengadaan secara *online*, sehingga peluang korupsi dan kolusi dapat ditekan. Transparansi ini menjadi faktor

penting dalam membangun kepercayaan publik terhadap tata kelola digital pemerintah.

3. Integritas Data dan Kedaulatan Digital
   Ketentuan mengenai kepemilikan hak kekayaan intelektual (HKI) oleh negara serta pengelolaan data oleh LKPP memperkuat kontrol negara atas data strategis dan menjamin integritas informasi. Hal ini memastikan pengelolaan sistem pengadaan tetap berada dalam kerangka kedaulatan digital nasional.

4. Kolaborasi Multi-Pemangku Kepentingan
   Implementasi Perpres No. 17 Tahun 2023 melibatkan sinergi antara LKPP, Kementerian Kominfo, Kementerian Keuangan, BUMN, dan berbagai lembaga lainnya. Kolaborasi lintas sektor ini mencerminkan model tata kelola digital yang partisipatif, di mana setiap pemangku kepentingan berperan dalam menjaga transparansi, keamanan, dan efisiensi sistem pengadaan nasional. Pendekatan kolaboratif ini sejalan dengan prinsip kepercayaan digital yang menempatkan koordinasi antarinstansi sebagai pilar utama.

5. Pemberdayaan Ekonomi Digital Nasional
   Perpres ini juga mendorong penggunaan produk dalam negeri serta pelibatan UMKM dalam proses pengadaan digital. Dengan memperluas partisipasi pelaku usaha lokal, kebijakan ini memperkuat daya saing nasional sekaligus menumbuhkan rasa memiliki dan kepercayaan terhadap ekosistem digital yang menyeluruh. Integrasi antara ekonomi digital dan tata kelola pengadaan yang transparan menciptakan dasar kepercayaan bersama antara pemerintah, masyarakat, dan dunia usaha.

6. Pengawasan dan Evaluasi Berkala
   Keberlanjutan kepercayaan digital tidak dapat dilepaskan dari mekanisme pengawasan dan evaluasi yang sistematis. Melalui pemantauan rutin terhadap kinerja SPSE dan audit kelembagaan, pemerintah dapat memastikan bahwa sistem tetap relevan, aman, dan efisien seiring perkembangan teknologi. Pengawasan berkelanjutan menjadi jaminan atas konsistensi dan kredibilitas sistem pengadaan digital nasional.

Secara keseluruhan, Perpres No. 17 Tahun 2023 berperan sebagai instrumen penting dalam memperkuat kepercayaan digital di sektor publik. Melalui penerapan prinsip keamanan, transparansi, integritas data, kolaborasi, dan inklusivitas ekonomi, regulasi ini mendukung terwujudnya kepercayaan digital Indonesia yang berdaulat, berintegritas, dan berkelanjutan.

4.3.6 Perpres Nomor 47 Tahun 2023 tentang Strategi Keamanan Siber Nasional dan Manajemen Krisis Siber

Perpres Nomor 47 Tahun 2023 mengatur Strategi Keamanan Siber Nasional dan Manajemen Krisis Siber untuk melindungi kepentingan nasional dari ancaman siber serta memastikan kesiapsiagaan dalam menghadapi insiden siber [50]. Strategi

Keamanan Siber Nasional (SKSN) dan Manajemen Krisis Siber (MKS) memiliki tujuan, yaitu mewujudkan keamanan siber, melindungi ekosistem perekonomian digital nasional, meningkatkan kekuatan dan kapabilitas keamanan siber yang andal dan berdaya tangkal, dan mengutamakan kepentingan nasional dan mendukung terciptanya ruang siber global yang terbuka, aman, stabil, dan bertanggung jawab. Regulasi ini mencakup hal-hal sebagai berikut.

1. Strategi Keamanan Siber Nasional
   Strategi Keamanan Siber Nasional disusun untuk mengarahkan kebijakan negara dalam pemanfaatan sumber daya siber demi menjaga kepentingan nasional. Strategi ini menekankan pentingnya tata kelola yang baik, pengelolaan risiko, peningkatan kesiapsiagaan, serta perlindungan terhadap infrastruktur informasi vital. Selain itu, strategi ini juga berfokus pada pengembangan kapabilitas nasional di bidang keamanan siber agar Indonesia mampu menghadapi ancaman yang semakin kompleks. Di sisi lain, kerja sama internasional turut menjadi prioritas guna membangun ruang siber yang aman, stabil, dan berkelanjutan melalui kolaborasi dengan berbagai negara serta forum global.

2. Manajemen Krisis Siber
   Manajemen krisis siber mencakup penyusunan langkah-langkah penanganan insiden baik sebelum, saat, maupun setelah krisis terjadi, sehingga respons dapat dilakukan secara terstruktur dan efektif. Proses ini melibatkan berbagai pemangku kepentingan, termasuk Tim Tanggap Insiden Siber serta BSSN sebagai otoritas utama dalam ketahanan siber nasional. Dalam situasi tertentu, penetapan status Krisis Siber dilakukan melalui mekanisme formal, yakni berdasarkan usulan Kepala BSSN kepada Presiden, sehingga langkah penanganan dapat segera dilaksanakan secara terkoordinasi di tingkat nasional.

3. Koordinasi dan Pelaksanaan
   Koordinasi dan pelaksanaan strategi kepercayaan digital dijalankan secara terpusat dengan BSSN sebagai koordinator utama. Implementasi strategi ini dilakukan oleh instansi pemerintah dan sektor privat melalui rencana aksi nasional yang dirancang secara komprehensif dan ditinjau setiap lima tahun untuk memastikan relevansi terhadap dinamika perkembangan teknologi serta ancaman siber yang terus berubah. Dari sisi pendanaan, pelaksanaan strategi didukung oleh APBN, APBD, serta sumber lain yang sah sesuai dengan ketentuan perundang-undangan.

SKSN memiliki 8 (delapan) fokus area dalam peningkatan kualitas keamanan siber, yaitu tata kelola; manajemen risiko; kesiapsiagaan dan ketahanan; penguatan pelindungan infrastruktur informasi vital; kemandirian kriptografi nasional; peningkatan kapabilitas, kapasitas, dan kualitas; kebijakan keamanan siber; dan kerja sama internasional. Beberapa hal yang perlu digarisbawahi berkaitan dengan penjelasan kedelapan fokus area tersebut, antara lain:

1. Perlunya penguatan ekosistem keamanan siber, mencakup Sumber Daya Manusia (SDM), proses, dan teknologi;
2. Perlunya peningkatan sinergi dan kolaborasi antarpemangku kepentingan dalam pelaksanaan keamanan siber;
3. Perlunya pembangunan kapabilitas tanggap insiden siber yang efektif dan efisien;
4. Perlunya penguatan pelindungan Infrastruktur Informasi Vital (IIV);
5. Perlunya peningkatan riset, pengembangan, dan inovasi ilmu pengetahuan dan teknologi;
6. Perlunya penegakan hukum di bidang keamanan siber secara terpadu;
7. Peningkatan kerja sama praktis, berbagi informasi, dan praktik terbaik dalam menghadapi krisis siber.

Adapun delapan fokus area tersebut diperjelas kembali dengan Rencana Aksi Nasional (RAN) yang berisi upaya terencana dan terukur untuk menjabarkan dan mengimplementasikan fokus area SKSN, baik oleh kementerian/lembaga terkait maupun beserta pemangku kepentingan. RAN dibuat untuk jangka waktu 5 (lima) tahun, namun dapat ditinjau sewaktu-waktu. Dalam perumusannya memperhatikan rencana pembangunan nasional, perkembangan ilmu pengetahuan dan teknologi, dan perkembangan lingkungan strategis.

Keterkaitan dengan Kerangka Kerja Kepercayaan Digital di Indonesia

Perpres Nomor 47 Tahun 2023 tentang Strategi Keamanan Siber Nasional dan Manajemen Krisis Siber memiliki peran krusial dalam membentuk landasan strategis bagi penguatan kepercayaan digital di Indonesia. Strategi yang tertuang dalam regulasi ini tidak hanya berorientasi pada penguatan ketahanan siber secara teknis, namun juga memberikan arah kebijakan yang menyeluruh bagi tata kelola ekosistem digital yang aman, adaptif, dan berkelanjutan.

Dalam konteks penyusunan kerangka kerja kepercayaan digital, Perpres ini menjadi rujukan penting karena menekankan integrasi antara perlindungan infrastruktur digital, penjaminan hak-hak pengguna, peningkatan literasi, dan adopsi pendekatan berbasis risiko. Setiap elemen dalam strategi tersebut mendukung pembangunan sistem digital nasional yang dapat dipercaya oleh masyarakat, sektor swasta/industri, dan pemerintah. Dengan demikian, sinergi antara kebijakan keamanan siber dan kepercayaan digital menjadi kunci untuk menciptakan ruang digital nasional yang resilien.

1. Meningkatkan Keamanan dan Kepercayaan dalam Ekosistem Digital
   Keamanan siber yang kuat adalah elemen kunci dalam membangun kepercayaan digital. Dengan strategi ini, Indonesia dapat meningkatkan perlindungan terhadap infrastruktur digital, layanan publik, dan sektor swasta/industri.

2. Perlindungan Data dan Privasi
   Strategi ini mendukung implementasi kebijakan kepercayaan digital dengan memperkuat perlindungan data dan kesiapsiagaan terhadap serangan siber yang berpotensi mengancam hak-hak pengguna digital.

3. Meningkatkan Kapasitas dan Kesadaran Siber
   Pendidikan dan pelatihan terkait keamanan siber yang diatur dalam Perpres ini akan meningkatkan literasi digital masyarakat dan sektor bisnis, mendukung ekosistem digital yang lebih aman dan tepercaya.

4. Mendukung Regulasi Digital yang Berbasis Risiko
   Dengan mengadopsi pendekatan berbasis risiko dalam manajemen siber, strategi ini memastikan bahwa PSE dan pemerintah memiliki mekanisme mitigasi yang sesuai untuk menjaga integritas sistem digital.

Perpres 47/2023 menjadi landasan penting dalam membangun kepercayaan digital di Indonesia melalui keamanan, kesiapsiagaan, dan tata kelola risiko siber yang lebih kuat.

4.4 Instruksi Presiden (Inpres)

Instruksi Presiden (Inpres) merupakan bentuk pengaturan yang bersifat internal dalam pemerintahan dan digunakan untuk memberikan arahan langsung dari Presiden kepada para menteri, kepala lembaga, atau kepala daerah. Inpres berperan sebagai mekanisme percepatan pelaksanaan kebijakan atau program prioritas nasional, termasuk di bidang transformasi digital. Dalam hal ini, Inpres memungkinkan respons cepat terhadap dinamika teknologi dengan menetapkan langkah-langkah konkret, mempercepat koordinasi antarinstansi, dan memastikan pelaksanaan program digital yang bersifat lintas sektor dapat segera diimplementasikan secara efektif dan efisien.

4.4.1 Inpres Nomor 4 Tahun 2025 tentang Data Tunggal Sosial dan Ekonomi Nasional

Inpres Nomor 4 Tahun 2025 merupakan langkah strategis pemerintah dalam mewujudkan konsistensi dan integrasi data sosial dan ekonomi di tingkat nasional melalui penyelenggaraan *Data Tunggal Sosial dan Ekonomi Nasional* (DT-SEN). Inpres ini menekankan pentingnya keselarasan data antarlembaga negara sebagai dasar pengambilan kebijakan berbasis bukti (*evidence-based policy*) dan penguatan tata kelola data nasional.

Beberapa kementerian dan lembaga diberikan mandat khusus dalam implementasi kebijakan ini. Kementerian Perencanaan Pembangunan Nasional/Bappenas bertugas melakukan koordinasi perencanaan, penyusunan, serta pemutakhiran data.

Kementerian Komunikasi dan Digital bertanggung jawab atas penyediaan infrastruktur digital yang menunjang interoperabilitas dan aksesibilitas data. Badan Pusat Statistik (BPS) memainkan peran penting dalam menjamin kualitas, akurasi, dan konsistensi data. Sementara itu, Kementerian Dalam Negeri bertanggung jawab atas ketersediaan data kependudukan yang valid dan terkini, serta Kementerian Sosial menyediakan data penerima manfaat program-program sosial. Selain itu, kementerian/lembaga lainnya diwajibkan menggunakan data tunggal ini sebagai referensi utama dalam perencanaan dan pelaksanaan kegiatan mereka.

Data Tunggal Sosial dan Ekonomi Nasional mencakup beragam dimensi data strategis, antara lain: data kependudukan dan demografi, data kemiskinan dan kesejahteraan sosial, data pendidikan dan kesehatan, serta data ketenagakerjaan dan ekonomi. Keseluruhan data ini menjadi dasar penting dalam mewujudkan ekosistem tata kelola data nasional yang andal, terbuka, dan berkelanjutan.

Keterkaitan dengan Kerangka Kerja Kepercayaan Digital di Indonesia

Kebijakan DT-SEN sebagaimana diamanatkan dalam Inpres No. 4 Tahun 2025 memiliki keterkaitan langsung dengan upaya membangun kerangka kerja kepercayaan digital di Indonesia. Beberapa aspek kunci yang relevan antara lain:

1. Data Publik Tepercaya
   Inpres ini menunjukkan komitmen pemerintah dalam menjamin kualitas data publik yang terpadu, akurat, dan diperbarui secara berkala. Prinsip-prinsip ini sejalan dengan kebutuhan akan data yang valid sebagai dasar layanan digital yang tepercaya.

2. Perlindungan Data
   Penugasan khusus kepada BSSN untuk menjaga keamanan dan perlindungan atas Data Tunggal memperkuat kepercayaan masyarakat terhadap keterlibatan pemerintah dalam menjamin kerahasiaan dan integritas data pribadi. Hal ini menjadi elemen penting dalam membangun sistem kepercayaan digital nasional.

3. Akses dan Interoperabilitas antar-Lembaga
   Instruksi ini menuntut terbangunnya sistem data yang interoperabel di antara berbagai kementerian dan lembaga, yang hanya mungkin dicapai dengan infrastruktur digital yang memadai serta tata kelola akses data yang transparan dan terkontrol.

4. Kolaborasi Partisipatif dengan Masyarakat
   Pemutakhiran data secara partisipatif melalui pelibatan aktif masyarakat di tingkat desa dan daerah memperkuat kualitas data sekaligus mendorong kepercayaan publik terhadap proses pendataan. Model ini menciptakan relasi timbal balik antara negara dan masyarakat dalam membangun ekosistem data.

5. *Government-as-a-Platform* (GaaP)
   Integrasi seluruh data dalam satu sistem tunggal membuka jalan bagi implementasi *Government-as-a-Platform*, di mana kebijakan publik, seperti bantuan sosial, subsidi, hingga pembangunan daerah, disusun berdasarkan referensi data yang sama. Hal ini mengurangi redundansi, meminimalkan kesalahan kebijakan, dan meningkatkan efisiensi layanan pemerintah berbasis data.

4.5 Peraturan dan Kebijakan Lainnya

Selain perangkat hukum formal seperti undang-undang, Peraturan Pemerintah (PP), Peraturan Presiden (Perpres), dan Instruksi Presiden (Inpres), terdapat pula berbagai regulasi dan kebijakan turunan yang secara nyata memperkuat ekosistem transformasi digital nasional. Regulasi ini tidak hanya berbentuk peraturan menteri, surat edaran, maupun pedoman teknis, tetapi juga mencakup strategi nasional yang dirancang untuk menjawab kebutuhan sektoral serta merespons isu-isu spesifik, misalnya keamanan siber, kriptografi, tata kelola data, perlindungan konsumen digital, hingga pengembangan ekonomi berbasis teknologi.

Kebijakan-kebijakan tersebut memiliki peran penting sebagai jembatan antara kerangka hukum makro dengan kebutuhan operasional di lapangan. Di tengah kompleksitas dan kecepatan perubahan teknologi, regulasi turunan memberikan ruang fleksibilitas dalam implementasi, sekaligus mempercepat adopsi standar baru yang diperlukan oleh industri maupun masyarakat. Dengan mekanisme ini, pemerintah dapat lebih responsif terhadap tantangan baru seperti munculnya model bisnis digital, serangan siber yang semakin canggih, serta tuntutan interoperabilitas sistem lintas sektor.

Lebih jauh, keberadaan regulasi dan kebijakan operasional ini berfungsi sebagai katalisator inovasi. Di satu sisi, ia membuka peluang bagi sektor publik maupun swasta untuk bereksperimen dengan teknologi baru tanpa harus menunggu perubahan undang-undang yang bersifat lebih rigid. Di sisi lain, ia memastikan adanya koridor pengawasan dan perlindungan, terutama dalam hal pelindungan data pribadi, transparansi pemanfaatan teknologi, serta penegakan akuntabilitas. Dengan demikian, kebijakan yang adaptif tidak hanya memperkuat kepercayaan digital masyarakat, tetapi juga mendorong daya saing Indonesia dalam ekosistem digital global secara berkelanjutan.

4.5.1 Peraturan Menteri Komunikasi dan Informatika Nomor 5 Tahun 2020 juncto Nomor 10 Tahun 2021 tentang Penyelenggara Sistem Elektronik Lingkup Privat

Peraturan Menteri ini mengatur Penyelenggara Sistem Elektronik (PSE) Lingkup Privat, yang mencakup pendaftaran, tata kelola, serta kewajiban keamanan dan perlindungan data [292]. Peraturan ini bertujuan untuk memastikan sistem elektronik

yang digunakan oleh sektor privat di Indonesia beroperasi dengan transparan, aman, dan sesuai dengan regulasi. Beberapa poin utama dari peraturan ini meliputi:

1. Definisi dan Ruang Lingkup PSE Lingkup Privat
   Definisi dan ruang lingkup PSE lingkup privat mencakup berbagai penyedia layanan digital yang beroperasi di Indonesia. PSE privat ini meliputi platform *e-commerce*, layanan keuangan digital, media sosial, mesin pencari, hingga layanan penyimpanan data yang digunakan secara luas oleh masyarakat. Untuk menjamin kepastian hukum dan tata kelola yang transparan, setiap PSE wajib melakukan pendaftaran sebelum beroperasi, termasuk perusahaan asing yang menyediakan layanan digital bagi pengguna di Indonesia. Kewajiban ini dimaksudkan untuk memperkuat pengawasan, meningkatkan akuntabilitas, serta memastikan bahwa seluruh layanan digital yang beroperasi di Indonesia mematuhi regulasi yang berlaku dan mendukung terciptanya ekosistem digital yang aman dan tepercaya.

2. Kewajiban Keamanan dan Perlindungan Data
   Kewajiban keamanan dan perlindungan data menempatkan PSE sebagai aktor utama dalam menjaga keandalan ekosistem digital. PSE dituntut untuk memastikan sistem yang mereka kelola terlindungi dari berbagai bentuk ancaman siber sekaligus menjamin keamanan serta kerahasiaan data pribadi pengguna. Selain itu, PSE juga berkewajiban memberikan akses kepada pemerintah untuk kepentingan pengawasan dan penegakan hukum. Dengan mekanisme ini, keberlangsungan layanan digital dapat berjalan secara aman, transparan, dan tetap berada dalam koridor hukum yang berlaku.

3. Moderasi Konten dan Pengawasan
   Moderasi konten dan pengawasan merupakan salah satu elemen penting dalam menjaga kepercayaan digital di Indonesia. PSE memiliki tanggung jawab utama untuk memastikan bahwa platform atau layanan yang mereka kelola tidak digunakan sebagai sarana penyebaran konten yang melanggar hukum, meresahkan masyarakat, maupun mengganggu ketertiban umum. Kewajiban ini tidak hanya melindungi pengguna dari paparan informasi yang berbahaya atau menyesatkan, tetapi juga berfungsi sebagai instrumen untuk menjaga stabilitas ruang digital nasional.
   Apabila PSE lalai atau tidak memenuhi ketentuan tersebut, mekanisme penegakan hukum dapat diberlakukan dalam bentuk sanksi administratif. Sanksi ini dapat berupa pemutusan akses (*blocking*) terhadap layanan tertentu, hingga pencabutan izin operasional penyelenggaraan sistem elektronik. Pendekatan ini menegaskan bahwa kepatuhan terhadap regulasi moderasi konten merupakan prasyarat bagi keberlangsungan ekosistem digital yang sehat, aman, dan tepercaya.

4. Sanksi dan Tindakan Penegakan Hukum
   Sanksi dan tindakan penegakan hukum merupakan instrumen yang dirancang untuk menjamin kepatuhan PSE terhadap kerangka regulasi yang berlaku. Pelanggaran oleh PSE dapat dikenai sanksi administratif dengan mekanisme

bertingkat, mulai dari pemberian teguran hingga pemutusan akses terhadap layanan yang disediakan. Pendekatan ini mencerminkan prinsip proporsionalitas dalam penegakan hukum, di mana tingkat sanksi disesuaikan dengan beratnya pelanggaran serta dampaknya terhadap ekosistem digital.
Selain itu, regulasi mewajibkan setiap PSE untuk menunjuk narahubung resmi di wilayah Indonesia. Ketentuan ini berfungsi memperkuat mekanisme akuntabilitas dan memastikan adanya saluran komunikasi langsung antara PSE dan otoritas pengawas. Kehadiran narahubung memungkinkan koordinasi yang lebih cepat dalam konteks penanganan insiden siber, klarifikasi regulasi, maupun penyelesaian sengketa hukum. Dengan demikian, kombinasi antara sanksi administratif dan kewajiban penunjukan narahubung tidak hanya meningkatkan kepatuhan regulatif, tetapi juga memperkuat tata kelola dan transparansi dalam penyelenggaraan sistem elektronik di Indonesia.

Keterkaitan dengan Kerangka Kerja Kepercayaan Digital di Indonesia

Dalam era transformasi digital yang kian pesat, kepercayaan digital menjadi prasyarat mutlak bagi terselenggaranya layanan digital yang aman, bertanggung jawab, dan berkelanjutan. Pemerintah Indonesia, melalui berbagai regulasi strategis, berupaya menciptakan ekosistem digital yang mengutamakan perlindungan hak pengguna sekaligus mendukung pertumbuhan inovasi. Salah satu instrumen penting dalam hal ini adalah Peraturan Menteri Komunikasi dan Informatika Nomor 5 Tahun 2020 sebagaimana telah diubah dengan Peraturan Nomor 10 Tahun 2021 tentang Penyelenggara Sistem Elektronik (PSE) Lingkup Privat, yang turut mengatur aspek Manajemen Krisis Siber.

Regulasi ini tidak hanya menetapkan kewajiban administratif bagi PSE, tetapi juga memperkuat prinsip tata kelola yang selaras dengan agenda nasional kepercayaan digital. Sejumlah aspek penting seperti pelindungan data pribadi, keamanan sistem elektronik, transparansi layanan, akuntabilitas, serta kepatuhan hukum menjadi pilar dalam mengarahkan operasional digital yang kredibel. Ketentuan tersebut secara langsung memperkuat elemen-elemen kunci dalam kerangka kerja kepercayaan digital Indonesia, sekaligus menciptakan ruang kolaboratif antara pemerintah, industri, dan masyarakat.

Penjabaran berikut menggambarkan bagaimana regulasi ini berkontribusi secara konkret dalam membentuk kerangka kerja kepercayaan digital nasional, melalui pendekatan menyeluruh terhadap perlindungan pengguna, kepastian hukum, serta keberlanjutan layanan digital yang aman dan tepercaya.

1. Pelindungan Data Pribadi dan Keamanan Sistem Elektronik
   Pelindungan data pribadi dan keamanan sistem elektronik menjadi prioritas utama untuk mewujudkan kepercayaan digital. Regulasi yang menekankan pentingnya pelindungan data pribadi serta kewajiban penyimpanan data transaksi elektronik sesuai standar berperan besar dalam mendukung kredibilitas sistem digital. Dengan adanya kepastian hukum bagi pengguna layanan digital, masyarakat dapat merasa lebih aman karena penyedia layanan bertanggung

jawab penuh terhadap pengelolaan sistem elektronik mereka.
Sejalan dengan upaya memperkuat pelindungan data pribadi dan keamanan sistem elektronik, regulasi ini mendukung implementasi UU PDP. Pilar-pilar ini menjadi landasan bagi transformasi digital yang berkelanjutan. Dengan mewajibkan pendaftaran dan kepatuhan terhadap regulasi, PSE diharapkan dapat menjalankan operasionalnya secara bertanggung jawab. Prinsip tata kelola digital yang baik ini tidak hanya meningkatkan kepercayaan publik tetapi juga mendukung inovasi dalam ekonomi digital.

2. Transparansi dan Akuntabilitas
   Transparansi dan akuntabilitas menjadi elemen penting dalam membangun kepercayaan publik. Mekanisme pengaduan pengguna, informasi yang jelas dan tidak menyesatkan, serta edukasi kepada masyarakat mencerminkan komitmen terhadap prinsip-prinsip tersebut. Dengan adanya transparansi, masyarakat semakin percaya untuk berpartisipasi dalam ekonomi digital tanpa khawatir terhadap penyalahgunaan data atau praktik penipuan. Selain itu, peraturan yang mewajibkan evaluasi risiko sebelum izin operasi diberikan memastikan bahwa semua PSE mematuhi standar kepatuhan dan legalitas yang jelas. Hal ini memberikan kejelasan bagi pengguna dan pemangku kepentingan mengenai status operasional PSE.
   Pengawasan oleh instansi pemerintah juga memainkan peran krusial dalam memastikan kepatuhan terhadap regulasi dan standar yang berlaku. Mekanisme pengawasan ini membantu menjaga integritas sistem elektronik yang beroperasi di Indonesia, sehingga menciptakan lingkungan digital yang lebih terjamin. Regulasi ini secara keseluruhan berkontribusi pada pembentukan kerangka kerja kepercayaan digital dengan menjamin transparansi dan keamanan dalam penyelenggaraan layanan digital.

3. Regulasi dan Penegakan Hukum
   Regulasi ini memastikan bahwa perkembangan ekonomi digital tetap berada dalam kendali hukum yang jelas. Dengan demikian, inovasi dapat berkembang pesat tanpa mengorbankan perlindungan pengguna dan stabilitas nasional. Melalui pendekatan yang terstruktur dan berbasis regulasi, Indonesia berupaya membangun ekosistem digital yang aman, andal, dan dipercaya oleh semua pihak.

Peraturan Menteri Komunikasi dan Informatika Nomor 5 Tahun 2020 Juncto Nomor 10 Tahun 2021 merupakan bagian penting dari kerangka kerja kepercayaan digital di Indonesia, dengan fokus pada keamanan, transparansi, dan kepatuhan regulasi dalam sistem elektronik sektor privat.

4.5.2 Peraturan Menteri Komunikasi dan Digital Nomor 6 Tahun 2025 tentang Standar Teknis dan Prosedur Pembangunan dan Pengembangan Aplikasi Sistem Pemerintahan Berbasis Elektronik

Peraturan Menteri Komunikasi dan Digital (Permenkomdigi) Nomor 6 Tahun 2025 mengatur standar teknis dan prosedur pembangunan serta pengembangan aplikasi Sistem Pemerintahan Berbasis Elektronik (SPBE) [293]. Regulasi ini bertujuan untuk memastikan seluruh instansi pemerintah, baik di tingkat pusat maupun daerah, membangun dan mengelola aplikasi pemerintahan secara terpadu, aman, efisien, serta sesuai dengan standar nasional dan internasional. Secara substansial, peraturan ini mencakup beberapa aspek utama sebagai berikut:

1. Penerapan Standar Teknis SPBE, meliputi pemenuhan persyaratan umum, penyediaan infrastruktur, pengelolaan siklus hidup pengembangan aplikasi, interoperabilitas data, keberlangsungan layanan, manajemen SPBE, serta dokumentasi aplikasi.
2. Keamanan Informasi dan Pelindungan Data Pribadi, melalui penerapan manajemen keamanan informasi SPBE, audit keamanan aplikasi, serta kepatuhan terhadap regulasi pelindungan data pribadi.
3. Pemanfaatan Infrastruktur SPBE Nasional, termasuk penggunaan pusat data nasional, jaringan intra-pemerintah, dan sistem penghubung layanan antarinstansi.
4. Interoperabilitas dan *Satu Data Indonesia*, untuk menjamin integrasi data dan layanan lintas instansi secara efisien, transparan, dan konsisten.
5. Pengelolaan Kode Sumber dan Repositori Aplikasi SPBE, yang diwajibkan disimpan secara aman dengan arsitektur *microservices* agar mudah diintegrasikan, dipelihara, dan dikembangkan lebih lanjut.
6. Kewajiban Penggunaan Perangkat Lunak Sumber Terbuka (*Open Source*) serta Audit TIK, sebagai upaya meningkatkan kemandirian digital, efisiensi biaya, dan keamanan sistem.
7. Larangan Pengembangan Aplikasi Sejenis, untuk menghindari duplikasi sistem dan mendorong pemanfaatan aplikasi umum SPBE secara bersama oleh berbagai instansi.

Melalui pengaturan tersebut, Permenkomdigi Nomor 6 Tahun 2025 menegaskan tujuan utama pembangunan dan pengembangan aplikasi SPBE, yaitu:

- Mewujudkan layanan publik yang efisien, terpadu, dan aman.
- Meningkatkan interoperabilitas antaraplikasi dan sistem pemerintahan.
- Mendorong tata kelola digital yang akuntabel, transparan, dan berkelanjutan.

Ruang lingkup regulasi ini mencakup seluruh tahapan siklus hidup pengembangan aplikasi, mulai dari perencanaan, analisis, desain, pengembangan, pengujian, implementasi, pemeliharaan, hingga evaluasi. Salah satu aspek penting yang ditekankan adalah penerapan kode sumber terbuka (*open source*) untuk mengurangi

ketergantungan terhadap lisensi perangkat lunak komersial.

Pendekatan *open source* memberikan fleksibilitas bagi pemerintah sebagai pemilik sistem untuk memodifikasi, menyesuaikan, dan mengembangkan solusi secara mandiri tanpa bergantung pada vendor tertentu (*vendor lock-in*). Selain itu, keterbukaan kode sumber juga mendorong kolaborasi lintas instansi dan komunitas dalam memperkuat keamanan aplikasi, meningkatkan interoperabilitas, serta mempercepat adopsi sistem.

Keterkaitan dengan Kerangka Kerja Kepercayaan Digital di Indonesia

Dalam upaya memperkuat dasar kepercayaan digital nasional, Pemerintah Indonesia terus menyelaraskan kebijakan teknis dengan prinsip tata kelola digital yang aman, transparan, dan berkelanjutan. Salah satu regulasi strategis dalam konteks tersebut adalah Peraturan Menteri Komunikasi dan Informatika Nomor 6 Tahun 2025 tentang Standar Teknis dan Prosedur Pembangunan dan Pengembangan Aplikasi SPBE.

Peraturan ini berperan penting dalam memperkuat pilar kepercayaan digital di sektor pemerintahan dengan memastikan bahwa setiap pengembangan aplikasi SPBE memenuhi standar keamanan, interoperabilitas, dan integritas data yang tinggi. Lebih dari sekadar pedoman teknis, regulasi ini menjadi instrumen tata kelola yang mendukung integrasi identitas digital, perlindungan data, serta kolaborasi antarinstansi dalam mewujudkan ekosistem digital yang tepercaya dan berdaulat.

Penjabaran berikut menggambarkan kontribusi konkret Permenkomdigi No. 6 Tahun 2025 terhadap penyusunan kerangka kerja kepercayaan digital nasional melalui penerapan prinsip keamanan, identitas digital terverifikasi, dan tata kelola yang kolaboratif.

1. Keamanan dan Integritas Sistem Pemerintahan Digital Regulasi ini menetapkan penerapan manajemen keamanan informasi dalam SPBE yang sejalan dengan standar internasional seperti SNI ISO/IEC 12207, 25000, dan 29119. Melalui penerapan audit keamanan aplikasi dan pengujian mutu perangkat lunak, pemerintah memastikan bahwa setiap sistem digital yang digunakan memiliki tingkat keamanan dan integritas yang tinggi. Langkah ini berkontribusi langsung terhadap peningkatan kepercayaan publik terhadap layanan digital pemerintah, sekaligus mencegah risiko kebocoran data dan serangan siber.

2. Identitas Digital dan Tata Kelola Data Terverifikasi
   Salah satu aspek strategis dari regulasi ini adalah penguatan identitas digital dalam sistem pemerintahan. Dengan mengatur penerapan identitas digital terintegrasi lintas instansi, Permenkomdigi No. 6 Tahun 2025 mendorong terbentuknya sistem autentikasi elektronik yang andal dan konsisten. Identitas digital ini menjadi landasan dalam membangun kepercayaan antara pengguna dan penyedia layanan, memastikan bahwa setiap transaksi dan pertukaran data dilakukan secara aman, terverifikasi, dan berjejak digital yang jelas. Kebijakan ini juga mendukung implementasi *trust framework* nasional yang

menekankan prinsip *accountability* dan *traceability* dalam tata kelola data publik.

3. Kolaborasi dan Peran Lembaga Pendukung
   Regulasi ini menekankan pentingnya kolaborasi lintas lembaga untuk memperkuat kepercayaan digital. Pelibatan entitas seperti Peruri dan BSSN menunjukkan pendekatan ekosistem dalam tata kelola digital nasional. Peruri berperan dalam formulasi teknis identitas digital dan penerapan standar autentikasi, sedangkan BSSN berfungsi sebagai *broker ID* yang memverifikasi serta membangun perimeter kepercayaan dalam pertukaran data elektronik antarinstansi. Sinergi ini menciptakan dasar tata kelola kepercayaan digital yang adaptif, akuntabel, dan selaras dengan prinsip *zero trust architecture*.

4. Kedaulatan dan Kemandirian Teknologi
   Penerapan penggunaan kode sumber terbuka (*open source*) dan pemanfaatan pusat data nasional dalam Permenkomdigi ini turut memperkuat kedaulatan digital Indonesia. Langkah tersebut memastikan bahwa sistem pemerintahan digital tidak bergantung pada teknologi asing, sekaligus memperkuat kontrol negara atas infrastruktur dan data publik yang strategis. Dengan demikian, regulasi ini tidak hanya meningkatkan efisiensi dan keamanan, tetapi juga menegaskan komitmen terhadap kemandirian teknologi nasional.

Secara keseluruhan, Permenkomdigi Nomor 6 Tahun 2025 berkontribusi signifikan terhadap penyusunan dan implementasi kerangka kerja kepercayaan digital di Indonesia. Melalui penekanan pada keamanan, integritas data, identitas digital, kolaborasi antarlembaga, dan kedaulatan teknologi, regulasi ini memperkuat ekosistem SPBE yang kredibel dan tepercaya. Pendekatan yang menyeluruh ini memastikan bahwa transformasi digital pemerintahan berjalan sejalan dengan nilai-nilai transparansi, akuntabilitas, dan kepercayaan publik yang menjadi inti dari agenda digital nasional.

4.5.3 Visi Indonesia Digital

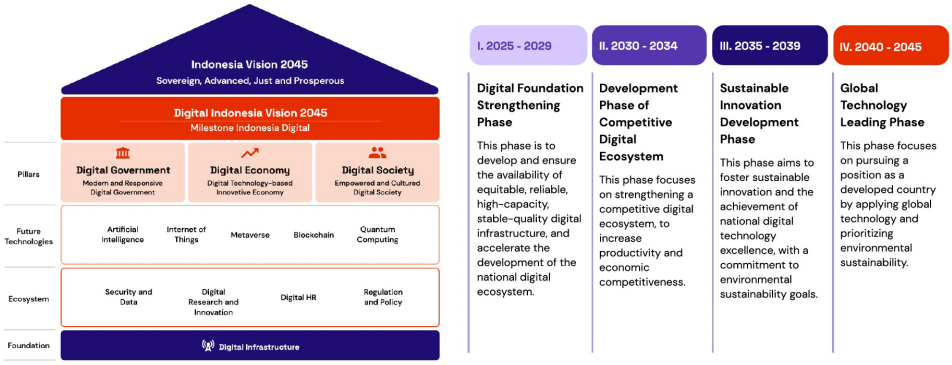
Visi Indonesia Digital 2045 disusun oleh Kementerian Komunikasi dan Informatika (Kemenkominfo) dengan melibatkan berbagai pemangku kepentingan, termasuk perwakilan pemerintah, sektor swasta/industri, asosiasi, akademisi, dan institusi terkait lainnya [294]. Visi ini secara resmi diluncurkan pada 13 Desember 2023 dan bertujuan untuk memastikan perencanaan transformasi digital yang kolaboratif, komprehensif, dan aman guna mendukung pencapaian visi besar *Indonesia Emas 2045*.

Melalui visi ini, Indonesia diharapkan mampu meningkatkan daya saing di tingkat global dengan mendorong inovasi digital, tata kelola pemerintahan berbasis teknologi, serta pembentukan masyarakat digital yang cerdas dan partisipatif. Untuk mewujudkannya, dirancang tiga pendekatan utama: pendekatan berbasis ekosistem yang membangun dasar kuat bagi ekosistem digital yang aman dan kolaboratif;

pendekatan sektoral yang mendorong transformasi digital lintas sektor, baik ekonomi maupun sosial; serta pendekatan kewilayahan yang menjamin pemerataan akses dan manfaat transformasi digital di seluruh wilayah Indonesia.

Transformasi digital menjadi salah satu dasar strategis dalam mewujudkan cita-cita Indonesia sebagai negara berdaulat, maju, adil, dan makmur pada tahun 2045. Dalam konteks ini, Visi Indonesia Digital 2045 ditetapkan sebagai kerangka jangka panjang untuk mengarahkan kebijakan dan pengembangan ekosistem digital secara bertahap, terintegrasi, dan berkelanjutan. Visi ini tidak hanya menekankan pada pentingnya adopsi teknologi mutakhir, tetapi juga pada penguatan pilar-pilar utama seperti pemerintahan digital, ekonomi digital, dan masyarakat digital yang berdaya.

Kerangka tersebut dibangun di atas dasar infrastruktur digital yang andal, dan diperkuat oleh ekosistem pendukung yang mencakup keamanan data, riset dan inovasi digital, pengembangan sumber daya manusia digital, serta regulasi yang adaptif. Pelaksanaan visi ini dibagi ke dalam empat fase strategis, mulai dari penguatan fondasi digital hingga pencapaian posisi sebagai pemimpin teknologi global. Setiap fase dirancang untuk membentuk lingkungan digital yang kompetitif, inovatif, dan berkelanjutan.



Gambar 4.3: Kerangka Visi Indonesia Digital 2045 [294]

Gambaran menyeluruh mengenai kerangka visi ini disajikan pada Gambar 4.3, yang memetakan tahapan pembangunan, pilar strategis, serta komponen utama pendukung transformasi digital nasional. Gambar tersebut merepresentasikan *Digital Indonesia Vision 2045*, yang menjadi bagian integral dari pencapaian Visi Indonesia 2045: *Berdaulat, Maju, Adil, dan Makmur*. Visualisasi ini menyajikan rangkaian pengembangan ekosistem digital Indonesia secara bertahap, sekaligus menunjukkan pilar strategis dan elemen pendukung yang menopangnya. Penjelasan berikut menguraikan keterkaitan antara isi gambar dengan Visi Indonesia Digital 2045 serta urgensi penguatan kepercayaan digital sebagai landasan utama transformasi digital nasional.

1. Struktur Visi Digital Indonesia 2045

Visi Digital Indonesia 2045 dirancang dalam empat fase pengembangan yang berkesinambungan hingga tahun 2045:

- Fase I (2025–2029): *Digital Foundation Strengthening*
  Tahap awal pembangunan ekosistem digital nasional difokuskan pada penguatan fondasi melalui penyediaan infrastruktur yang merata, andal, dan berkapasitas tinggi. Keberadaan jaringan yang stabil dan aman akan menjadi dasar bagi terselenggaranya aktivitas digital, baik di tingkat masyarakat maupun pemerintahan. Selain itu, fase ini juga menekankan percepatan pengembangan ekosistem digital secara menyeluruh agar kepercayaan digital dapat mulai terbangun sejak dini, terutama dengan menghadirkan layanan yang konsisten, transparan, dan terjamin keamanannya.
- Fase II (2030–2034): *Development Phase of Competitive Digital Ecosystem*
  Setelah fondasi kuat terbentuk, fokus bergeser pada penguatan daya saing ekosistem digital nasional. Tujuannya adalah menjadikan ekosistem ini sebagai pendorong utama produktivitas dan peningkatan daya saing ekonomi. Kepercayaan digital dibangun melalui penerapan regulasi yang semakin matang, pelindungan data pribadi yang lebih kokoh, serta pemanfaatan teknologi yang aman dan dapat diawasi. Dengan demikian, fase ini diharapkan mampu menciptakan iklim digital yang sehat, kompetitif, dan tetap selaras dengan kepentingan masyarakat luas.
- Fase III (2035–2039): *Sustainable Innovation Development*
  Memasuki fase ini, pembangunan digital diarahkan pada penguatan inovasi berkelanjutan yang tidak hanya mengejar kemajuan teknologi, tetapi juga memperhatikan aspek keberlanjutan lingkungan dan sosial. Kepercayaan digital berperan sebagai pengikat antara inovasi dan penerimaan masyarakat, memastikan bahwa setiap terobosan baru sesuai dengan prinsip etika, tata kelola kolaboratif, serta menjaga keseimbangan antara pertumbuhan ekonomi dan keberlanjutan. Dengan demikian, inovasi yang lahir pada fase ini tidak hanya relevan secara global, tetapi juga bermanfaat bagi generasi mendatang.
- Fase IV (2040–2045): *Global Technology Leading Phase*
  Pada tahap akhir, Indonesia menargetkan diri untuk tampil sebagai salah satu pemimpin global dalam pengembangan dan penerapan teknologi. Orientasi pembangunan digital bukan lagi sebatas adaptasi, tetapi juga penciptaan standar baru dalam teknologi global yang berpihak pada keberlanjutan. Kepercayaan digital menjadi prasyarat mutlak agar Indonesia mampu bersaing di kancah internasional, terutama di tengah meningkatnya kompleksitas ancaman siber, tuntutan transparansi, dan ekspektasi akuntabilitas publik. Dengan dasar yang kokoh dari fase sebelumnya, Indonesia berpeluang menjadi pusat inovasi dan referensi global dalam transformasi digital berkelanjutan.

Keempat fase tersebut saling terkait dan membentuk jalur strategis menuju Indonesia Digital 2045. Namun, visi jangka panjang ini tidak dapat dicapai tanpa fondasi

yang lebih mendalam. Oleh karena itu, penting untuk menelaah pilar-pilar utama yang menjadi arah transformasi digital sekaligus membangun kepercayaan digital sebagai dasar interaksi di ruang siber.

2. Pilar transformasi digital

Pilar transformasi digital berfungsi sebagai kerangka strategis yang memastikan pemanfaatan teknologi berlangsung terarah, aman, kolaboratif, dan berkelanjutan. Pilar-pilar ini saling melengkapi dan menjadi penggerak utama terbentuknya ekosistem digital yang tepercaya.

- *Digital Government*: Sasaran utama dari pemerintahan digital adalah terwujudnya tata kelola pemerintahan yang modern dan responsif. Hal ini mencakup pengembangan ekosistem layanan publik yang inovatif melalui pemanfaatan teknologi canggih, perumusan kebijakan berbasis data nasional (*data-policy-making*), serta peningkatan efisiensi dan transparansi dalam penyelenggaraan layanan. Dalam proses ini, keamanan dan perlindungan data seluruh warga negara tetap menjadi prioritas utama. Kepercayaan digital pun dibangun melalui layanan publik yang tidak hanya aman dan transparan, tetapi juga andal dan berpihak pada kepentingan masyarakat.
- *Digital Economy*: Sasaran utama pengembangan ekonomi digital adalah mewujudkan pertumbuhan ekonomi yang inovatif dan berkelanjutan, berbasis pemanfaatan teknologi digital. Hal ini didorong melalui pengembangan dan penerapan inovasi digital yang memberikan dampak positif bagi sektor sosial dan ekonomi. Untuk menciptakan ekonomi yang berdaya saing, diperlukan penguatan ekosistem digital nasional, peningkatan kapasitas riset dan inovasi, serta pembangunan kemitraan lintas sektor guna mempercepat adopsi teknologi di seluruh sektor ekonomi. Dalam konteks ini, kepercayaan digital memegang peran krusial dengan memperkuat transaksi elektronik, melindungi data konsumen, dan memastikan kepastian hukum.
- *Digital Society*: Sasaran dari pembangunan masyarakat digital adalah terwujudnya masyarakat Indonesia yang berdaya dan berbudaya. Hal ini mencakup pengembangan sumber daya manusia digital yang terampil dan mampu bersaing melalui penguasaan teknologi, serta pembentukan masyarakat yang produktif dalam memanfaatkan teknologi digital. Di saat yang sama, nilai-nilai Pancasila, budaya lokal, dan norma sosial tetap dijaga sebagai pijakan dalam menghadapi transformasi digital yang semakin cepat.
  Pemanfaatan teknologi digital diharapkan dapat meningkatkan produktivitas masyarakat, namun tetap memperhatikan keseimbangan antara kemajuan teknologi dan pelestarian kearifan lokal. Dalam ekosistem ini, kepercayaan digital menjadi dasar utama, agar setiap masyarakat dapat berpartisipasi secara aktif, aman, dan bertanggung jawab di ruang digital.

Pilar-pilar ini memberikan arah yang jelas bagi pembangunan ekosistem digital nasional. Namun, agar berjalan efektif, diperlukan komponen pendukung yang

menjamin kesiapan teknis, regulasi, serta kapasitas sumber daya. Tanpa hal tersebut, pilar transformasi akan sulit diwujudkan secara menyeluruh.

3. Komponen pendukung visi digital dan relevansinya terhadap kepercayaan digital

Komponen pendukung memiliki peran krusial dalam memastikan visi dan pilar transformasi digital dapat diimplementasikan secara nyata. Beberapa di antaranya meliputi:

- *Future Technologies*, seperti *Artificial Intelligence*, *Internet of Things*, *Blockchain*, hingga *Quantum Computing*, terus berkembang dengan cepat dan memberikan peluang besar bagi inovasi. Namun, di balik peluang tersebut terdapat tantangan serius yang berkaitan dengan privasi, etika, serta keamanan sistem. Apabila aspek ini tidak ditangani secara tepat, maka risiko penyalahgunaan teknologi akan semakin besar. Oleh karena itu, membangun kepercayaan digital menjadi prasyarat penting agar masyarakat tidak hanya merasa aman, tetapi juga yakin dalam memanfaatkan teknologi masa depan secara berkelanjutan.
- *Ecosystem Elements* yang mencakup keamanan dan perlindungan data, penelitian digital, pengembangan sumber daya manusia, serta kerangka regulasi, merupakan komponen kunci dalam mewujudkan ekosistem digital yang dapat dipercaya. Keempat elemen ini tidak dapat berdiri sendiri, melainkan saling melengkapi satu sama lain. Kolaborasi antara aspek teknis, sumber daya manusia yang kompeten, serta regulasi yang adaptif akan menghasilkan *trustworthy digital environment* yang memberi kepastian dan kenyamanan, baik bagi masyarakat umum, dunia usaha, maupun pemerintah.
- *Foundation – Digital Infrastructure*: Infrastruktur digital yang kuat, andal, dan aman adalah fondasi utama terciptanya kepercayaan digital. Infrastruktur ini bukan hanya menyangkut ketersediaan jaringan dan pusat data, tetapi juga mencakup integritas sistem, perlindungan privasi, serta keandalan layanan. Tanpa adanya fondasi yang kokoh, seluruh upaya membangun ekosistem digital yang tepercaya akan sulit terwujud, karena tidak ada jaminan keberlangsungan layanan, perlindungan informasi, maupun kenyamanan bagi para pengguna.

Secara keseluruhan, struktur visi, pilar transformasi, dan komponen pendukung membentuk kerangka yang utuh dalam mewujudkan Visi Digital Indonesia 2045. Struktur visi menetapkan arah jangka panjang, pilar transformasi memandu pembangunan sektor-sektor utama, sedangkan komponen pendukung memastikan kesiapan infrastruktur, regulasi, teknologi, dan SDM. Integrasi dari ketiganya memungkinkan terbentuknya kepercayaan digital yang berkelanjutan, sehingga Indonesia mampu menjawab tantangan global sekaligus mengoptimalkan peluang dari ekonomi dan masyarakat digital di masa depan.

Sebagai tindak lanjut dari kerangka Visi Indonesia Digital 2045, telah disusun Peta Jalan Indonesia Digital (lihat Gambar 4.4) yang berfungsi sebagai panduan strategis dalam mempercepat transformasi digital di berbagai sektor. Peta jalan untuk periode 2021–2024 ini mencakup sepuluh sektor prioritas, yaitu transportasi dan pariwisata digital, perdagangan digital, jasa keuangan digital, media dan hiburan digital, pertanian dan perikanan digital, *real estate* dan perkotaan digital, pendidikan digital, kesehatan digital, digitalisasi perindustrian, serta digitalisasi pemerintahan.

Gambar 4.4: Visi Indonesia Digital 2045 [294]

Keterkaitan dengan Kerangka Kerja Kepercayaan Digital di Indonesia

Dalam rangka mewujudkan Visi Indonesia Digital yang aman, merata dan berkelanjutan, kepercayaan digital memegang peran sentral sebagai prasyarat utama. Tanpa adanya kepercayaan terhadap sistem, layanan, dan teknologi digital, transformasi nasional ke arah digitalisasi tidak akan mampu memberikan manfaat optimal bagi masyarakat, pemerintah, maupun sektor swasta/industri.

Penyusunan Kerangka Kerja Kepercayaan Digital menjadi langkah strategis untuk menjawab kebutuhan tersebut. Kerangka ini tidak hanya mendefinisikan prinsip dan standar kepercayaan, tetapi juga mengaitkannya secara langsung dengan lima pilar utama pembangunan digital nasional, yaitu:

1. Ekonomi Digital yang Tangguh
   Tanpa kepercayaan terhadap transaksi digital, perlindungan data konsumen, dan sistem pembayaran elektronik, transformasi ekonomi tidak akan berkelanjutan.

2. Pemerintahan Digital
   SPBE hanya efektif jika masyarakat percaya bahwa data mereka aman serta layanan publik transparan dan akuntabel.

3. Masyarakat Digital
   Literasi tidak hanya mencakup *cyber hygiene*, namun juga harus mencakup

perubahan perilaku dan tingkat intelektual dalam menghadapi ancaman siber, sehingga kepercayaan digital, baik dari maupun ke pengguna, dapat terjaga.

4. Inovasi Teknologi (AI, IoT, *Cloud*)
   Pemanfaatan AI dan IoT memerlukan regulasi dan etika penggunaan agar tidak melanggar privasi atau bersifat diskriminatif. Kepercayaan digital hadir melalui auditabilitas dan standar.

5. Infrastruktur dan Keamanan Siber
   Tanpa sistem yang tahan serangan (*resilient*), risiko kebocoran data dan serangan siber akan meruntuhkan kepercayaan masyarakat.

4.5.4 Gerakan Nasional Literasi Digital

Program ini merupakan inisiatif Kementerian Komunikasi dan Informatika yang bertujuan untuk meningkatkan literasi digital masyarakat Indonesia guna mengurangi kesenjangan antara sumber daya manusia, terutama di kalangan generasi muda dan kelompok masyarakat rentan yang selama ini kurang terlayani. Secara sederhana, literasi digital merujuk pada pengetahuan dan kemampuan dalam menggunakan media digital, alat komunikasi, serta jaringan secara efektif. Literasi digital yang baik memungkinkan masyarakat untuk memanfaatkan teknologi dan media sosial secara bijak serta bertanggung jawab. Berbagai metode pelaksanaan dilakukan, mulai dari pembelajaran daring dan luring, *workshop*, serta kolaborasi dengan komunitas dan lembaga pendidikan untuk memperluas akses dan efektivitas program. Berdasarkan siaran pers Kemenkominfo, sejak 2017 hingga 2024, sebanyak 24.640.451 orang telah mengikuti program Gerakan Nasional Literasi Digital [295].

Gerakan Nasional Literasi Digital juga berkontribusi pada tujuan *Sustainable Development Goals* (SDGs) 2030, khususnya dalam pengentasan kemiskinan, pendidikan berkualitas, dan pengurangan kesenjangan sosial. Namun, transformasi digital di Indonesia masih menghadapi berbagai tantangan, di antaranya:

- Kesenjangan infrastruktur digital antara daerah perkotaan, pedesaan, hingga pedalaman. Indonesia adalah negara kepulauan dengan tantangan pemerataan pembangunan yang besar. Seperti yang diketahui, Indonesia mempunyai lebih dari 17 ribu pulau. Keterbatasan transportasi dan akses, seperti jalan, menjadi penghambat distribusi pembangunan yang merata. Kajian ERIA dan Kementerian Keuangan menyoroti bahwa peningkatan kualitas infrastruktur di daerah pedesaan mampu menurunkan biaya logistik hingga 30% dan mempercepat integrasi pasar [296].

- Rendahnya tingkat literasi digital di sebagian besar masyarakat. Menurut survei *World Digital Competitiveness Index* (WDCR) oleh Institute for Management Development (IMD) pada 2023 [297], Indonesia berada di peringkat ke-45 dari 64 negara dan mengalami kenaikan enam peringkat dari posisi sebelumnya. Namun, Indonesia masih memiliki tingkat literasi digital sebesar

62% yang merupakan angka terendah jika dibandingkan dengan negara-negara di ASEAN lainnya, yang rata-rata mencapai 70% [298].

- Ancaman keamanan siber yang terus meningkat. Berdasarkan laporan dari National Security Operation Center (NSOC) yang dimiliki BSSN, pada tahun 2025 terdapat anomali trafik mencapai 3,6 miliar yang merupakan angka terbesar melebihi aktivitas anomali dalam lima tahun ke sebelumnya [299].
- Tingginya biaya investasi teknologi bagi Usaha Mikro, Kecil, dan Menengah (UMKM) serta sektor kecil lainnya.

4.5.5 Peraturan Bank Indonesia Nomor 9/15/PBI/2007 tentang Penerapan Manajemen Risiko dalam Penggunaan Teknologi Informasi oleh Bank Umum

Peraturan ini dikeluarkan oleh Bank Indonesia untuk memastikan penerapan manajemen risiko secara efektif dalam penggunaan teknologi informasi oleh bank umum [300]. Peraturan ini bertujuan untuk menjaga kerahasiaan, integritas, dan ketersediaan data, serta mendukung keberlangsungan operasional perbankan melalui tata kelola teknologi informasi yang baik. Beberapa poin penting pada peraturan ini adalah sebagai berikut:

1. Latar Belakang
   Perkembangan teknologi informasi (TI) telah memberikan peluang besar bagi perbankan untuk meningkatkan efisiensi operasional sekaligus memperbaiki kualitas layanan kepada nasabah. Namun, pemanfaatan TI juga membawa konsekuensi berupa meningkatnya potensi risiko yang dapat mengganggu stabilitas dan keberlangsungan kegiatan usaha bank. Oleh karena itu, Bank Indonesia menegaskan perlunya penerapan manajemen risiko yang efektif dan menyeluruh pada setiap aspek penggunaan TI. Selain itu, keberadaan infrastruktur TI yang andal menjadi syarat mutlak agar perbankan nasional mampu memenuhi standar internasional, termasuk implementasi Basel II, yang menekankan pentingnya tata kelola risiko secara komprehensif.

2. Prinsip Utama
   Prinsip utama dalam penerapan manajemen risiko teknologi informasi menekankan pentingnya keterlibatan aktif dewan komisaris dan direksi dalam mengarahkan, memantau, serta mengevaluasi kebijakan penggunaan teknologi informasi di perbankan. Prinsip ini kemudian diwujudkan melalui penyusunan kebijakan dan prosedur yang komprehensif, mencakup aspek keamanan informasi, rencana kesinambungan usaha (*Business Continuity Plan*/BCP), hingga pengelolaan layanan perbankan elektronik. Untuk menjamin efektivitasnya, bank wajib menjalankan proses manajemen risiko yang meliputi identifikasi, pengukuran, pemantauan, dan pengendalian terhadap berbagai potensi risiko yang muncul dalam pemanfaatan teknologi informasi. Seluruh mekanisme tersebut diperkuat dengan penerapan sistem pengendalian internal yang solid

serta pelaksanaan audit teknologi informasi secara berkala, sehingga tercipta tata kelola yang transparan, akuntabel, dan berkesinambungan.

3. Penggunaan Pihak Ketiga
   Dalam penerapan teknologi informasi, bank diperbolehkan bekerja sama dengan pihak ketiga atau vendor TI. Namun demikian, tanggung jawab penuh atas penerapan manajemen risiko tetap berada pada pihak bank. Oleh karena itu, vendor diwajibkan mematuhi standar keamanan yang berlaku, termasuk penyediaan *Disaster Recovery Center* (DRC), pelaporan setiap kejadian kritis, serta pemberian akses audit baik kepada bank, auditor independen, maupun Bank Indonesia. Selain itu, untuk menjaga kedaulatan data dan efektivitas pengawasan, pusat data dan DRC pada prinsipnya harus berlokasi di dalam negeri, kecuali apabila bank telah memperoleh izin khusus dari Bank Indonesia untuk menyelenggarakannya di luar negeri.

4. *Electronic Banking*
   Dalam konteks *electronic banking*, Bank Indonesia mewajibkan setiap bank untuk secara berkesinambungan memberikan edukasi kepada nasabah mengenai keamanan penggunaan layanan perbankan elektronik. Edukasi ini penting agar nasabah memahami risiko yang melekat, sekaligus mampu melindungi diri dari potensi ancaman siber. Selain itu, setiap rencana penerbitan produk *e-banking* baru harus melalui proses pelaporan kepada Bank Indonesia serta pengujian menyeluruh. Pengujian tersebut tidak hanya menilai aspek bisnis, tetapi juga mencakup dimensi hukum dan keamanan, termasuk pemenuhan prinsip kerahasiaan (*confidentiality*), integritas (*integrity*), ketersediaan (*availability*), keaslian (*authentication*), serta *non-repudiation* sebagai pilar kepercayaan dalam transaksi digital.

5. Pelaporan dan Sanksi
   Dalam peraturan ini, bank diwajibkan untuk menyampaikan laporan terkait penggunaan teknologi informasi secara berkala, termasuk laporan atas perubahan mendasar, hasil audit, maupun kejadian insiden kritis yang berpotensi mengganggu operasional. Kewajiban pelaporan ini bertujuan memastikan adanya transparansi, akuntabilitas, serta kesiapan bank dalam mengelola risiko teknologi informasi. Apabila kewajiban tersebut tidak dipenuhi atau terdapat pelanggaran lain terhadap ketentuan yang berlaku, Bank Indonesia berwenang menjatuhkan sanksi administratif. Sanksi dapat berupa teguran tertulis, denda, pembekuan sebagian kegiatan usaha, hingga pencantuman pengurus dalam daftar tidak lulus uji kepatutan dan kelayakan (*fit and proper test*)

Keterkaitan dengan Kerangka Kerja Kepercayaan Digital di Indonesia

Keterkaitan substansi Peraturan Bank Indonesia No. 9/15/PBI/2007 dengan penyusunan kerangka kerja kepercayaan digital di Indonesia terletak pada prinsip-prinsip dasar yang diatur dalam peraturan tersebut. Meskipun ditujukan khusus untuk sektor perbankan, ketentuan mengenai manajemen risiko teknologi informasi, tata

kelola, perlindungan data, serta mekanisme pelaporan dan sanksi memiliki relevansi yang lebih luas. Prinsip-prinsip ini dapat diadopsi dan diperluas untuk membentuk dasar kepercayaan digital yang mencakup berbagai sektor, tidak hanya perbankan. Dengan demikian, peraturan ini dapat dilihat sebagai salah satu rujukan penting dalam merancang kebijakan nasional yang menekankan keamanan, transparansi, akuntabilitas, dan perlindungan data dalam ekosistem digital Indonesia.

1. Keamanan (*Security and Risk Management*)
   Aspek keamanan dalam Peraturan Bank Indonesia No. 9/15/PBI/2007 menekankan pentingnya penerapan prinsip *confidentiality*, *integrity*, dan *availability* (CIA Triad) yang menjadi standar internasional dalam membangun kepercayaan digital. Peraturan ini tidak hanya mengatur perlindungan informasi secara teknis, tetapi juga menuntut adanya tata kelola risiko yang menyeluruh, mulai dari tahap perencanaan, operasional, hingga penghentian penggunaan sistem. Dengan pendekatan *end-to-end* tersebut, regulasi ini dapat dijadikan model tata kelola nasional yang mampu memperkuat dasar keamanan siber sekaligus mendukung pembangunan ekosistem digital yang tepercaya dan berkelanjutan.

2. Transparansi dan Akuntabilitas
   Kewajiban pelaporan rutin yang disertai audit independen tidak hanya memperkuat akuntabilitas lembaga, tetapi juga menjadi instrumen penting untuk menjamin keterbukaan dalam pengelolaan data. Mekanisme ini relevan bagi ekosistem digital Indonesia, karena mendorong terciptanya standar transparansi yang konsisten sekaligus meningkatkan kepercayaan publik terhadap integritas sistem digital.

3. Perlindungan Data dan Privasi
   Peraturan ini menekankan bahwa vendor teknologi informasi memiliki kewajiban untuk menjaga kerahasiaan bank dan data nasabah. Ketentuan ini sejalan dengan prinsip pelindungan data pribadi sebagaimana diatur dalam UU PDP. Dengan demikian, penerapan aturan tersebut tidak hanya memperkuat aspek keamanan perbankan, tetapi juga mendukung terbentuknya ekosistem digital yang berlandaskan kepercayaan, di mana data pribadi dilindungi secara konsisten dan akuntabel.

4. *Business Continuity and Resilience*
   Kewajiban bagi bank untuk memiliki *Business Continuity Plan* (BCP) dan *Disaster Recovery Center* (DRC) menunjukkan bahwa aspek ketahanan dan keberlangsungan layanan merupakan bagian esensial dari tata kelola teknologi informasi. Langkah ini memastikan bahwa gangguan serius pada sistem tidak serta-merta menghentikan layanan kepada nasabah, sehingga kepercayaan terhadap institusi tetap terjaga. Prinsip *resiliency* semacam ini tidak hanya relevan bagi sektor perbankan, tetapi juga dapat diperluas ke berbagai sektor nonperbankan dalam kerangka kerja kepercayaan digital nasional, guna menjamin kontinuitas layanan publik dan ekosistem digital secara menyeluruh.

5. Kolaborasi Multi-Pihak
   Peraturan ini menegaskan bahwa bank tetap memegang tanggung jawab penuh atas penerapan manajemen risiko, meskipun sebagian layanan teknologi informasi diselenggarakan oleh pihak ketiga. Prinsip ini menekankan bahwa penggunaan penyedia jasa eksternal tidak boleh mengurangi kewajiban bank dalam menjaga keamanan, integritas, dan ketersediaan data serta layanan. Dalam konteks kerangka kerja kepercayaan digital nasional, pendekatan serupa sangat relevan untuk pengaturan layanan berbasis *cloud*, perusahaan *fintech*, dan berbagai penyedia platform digital lainnya. Dengan demikian, kolaborasi multipihak dapat berjalan secara produktif tanpa mengurangi akuntabilitas utama penyelenggara layanan terhadap keamanan dan kepercayaan publik.

6. Edukasi Publik
   Kewajiban bank mengedukasi nasabah tentang keamanan *e-banking* dapat diadaptasi menjadi program literasi keamanan digital untuk masyarakat luas.

PBI No. 9/15/PBI/2007 dapat dipandang sebagai *blueprint* awal kepercayaan digital di sektor keuangan. Substansinya, yang mencakup manajemen risiko, perlindungan data, transparansi, *resiliency*, dan edukasi publik, sangat relevan untuk diintegrasikan ke dalam kerangka kerja kepercayaan digital Indonesia yang lebih luas, mencakup sektor perbankan, pemerintahan, hingga layanan publik berbasis digital.

4.5.6 Peraturan Bank Indonesia Nomor 2 Tahun 2024 tentang Keamanan Sistem Informasi Dan Ketahanan Siber Bagi Penyelenggara Sistem Pembayaran, Pelaku Pasar Uang Dan Pasar Valuta Asing, Serta Pihak Lain Yang Diatur Dan Diawasi Bank Indonesia

Peraturan ini diterbitkan oleh Bank Indonesia (BI) sebagai langkah strategis untuk memperkuat keamanan sistem informasi dan ketahanan siber pada penyelenggara sistem pembayaran, pelaku pasar uang, pelaku pasar valuta asing, serta pihak lain yang berada di bawah pengawasan BI [301]. Tujuannya adalah memastikan stabilitas sistem keuangan nasional melalui perlindungan terhadap infrastruktur digital dan data keuangan yang vital. Beberapa poin penting pada peraturan ini adalah sebagai berikut:

1. Tujuan Utama
   Untuk menjamin stabilitas sistem pembayaran dan keuangan, diperlukan langkah strategis berupa penguatan keamanan siber yang menyeluruh. Hal ini mencakup perlindungan terhadap infrastruktur digital dan data keuangan yang vital. Selain itu, upaya pencegahan dan penanganan insiden siber yang dapat mengganggu stabilitas keuangan menjadi prioritas utama, guna memastikan bahwa setiap ancaman atau serangan siber tidak berujung pada

gangguan terhadap layanan keuangan yang esensial bagi masyarakat dan perekonomian.

2. Prinsip Dasar Keamanan dan Ketahanan Siber (KKS)
   Penting untuk memiliki kejelasan peran dan tanggung jawab dalam setiap aspek pengelolaan keamanan siber, sehingga setiap pihak memahami tugas mereka dengan jelas dan dapat bertindak secara efektif. Kejelasan ini harus didukung oleh strategi komprehensif yang berbasis pada manajemen risiko siber, dengan pendekatan sistematis untuk mengidentifikasi, menilai, dan mengatasi ancaman yang berpotensi mengganggu sistem. Selain itu, keamanan siber harus terintegrasi ke dalam budaya organisasi, mencakup pelatihan berkelanjutan dan kesadaran akan pentingnya menjaga keamanan. Hal ini perlu dilengkapi dengan kesiapan menghadapi insiden siber melalui pengembangan rencana tanggap darurat yang teruji, serta memastikan kemampuan untuk merespons dan memitigasi dampak dari setiap ancaman yang muncul.

3. Ruang Lingkup Pengaturan dan Pengawasan
   Tata kelola, pencegahan, penanganan, pengawasan, dan kolaborasi merupakan elemen kunci dalam menciptakan ekosistem keamanan siber yang efektif sekaligus berkelanjutan. Penyelenggara sistem diharuskan untuk memiliki strategi yang terstruktur, kebijakan yang jelas, serta prosedur operasional yang komprehensif guna mengantisipasi dan menghadapi ancaman siber. Langkah ini bertujuan untuk memastikan perlindungan terhadap aset digital, menjaga integritas data, serta meningkatkan kepercayaan pengguna dalam lingkungan digital yang semakin kompleks.

4. Pendekatan Pengawasan
   Bank Indonesia menerapkan pendekatan pengawasan berbasis risiko yang mencakup pengawasan langsung dan tidak langsung. Dalam pelaksanaannya, pendekatan ini juga didukung oleh pemanfaatan pelaporan data yang disampaikan oleh penyelenggara, sehingga memungkinkan pengawasan yang lebih efektif dan terfokus pada area dengan tingkat risiko yang lebih tinggi.

5. Kolaborasi Antar-Pemangku Kepentingan
   Pertukaran informasi terkait ancaman dan serangan siber menjadi langkah penting dalam memperkuat keamanan digital di tengah meningkatnya risiko serangan. Hal ini mencakup berbagi data dan wawasan tentang pola serangan, teknik mitigasi, serta kerentanan yang ditemukan, sehingga semua pihak yang terlibat dapat lebih siap menghadapi ancaman. Selain itu, kerja sama yang erat antara pihak internal, eksternal, dan lembaga-lembaga lain yang relevan juga memainkan peran krusial. Kolaborasi ini memungkinkan terciptanya ekosistem keamanan siber yang lebih terintegrasi dan responsif terhadap berbagai ancaman, dengan memanfaatkan keahlian dan sumber daya dari berbagai pihak untuk melindungi infrastruktur digital secara menyeluruh.

Keterkaitan dengan Kerangka Kerja Kepercayaan Digital di Indonesia

Kerangka kerja kepercayaan digital berfokus pada pengembangan ekosistem digital yang andal melalui prinsip keamanan, transparansi, dan kepatuhan. Peraturan BI Nomor 2 Tahun 2024 memiliki keterkaitan erat dengan kerangka kerja ini, terutama dalam empat aspek utama berikut:

1. Keamanan Siber sebagai Pilar Kepercayaan Digital
   Peraturan ini bertujuan untuk memperkuat kepercayaan publik terhadap layanan keuangan digital dengan memastikan tiga aspek utama keamanan informasi, yaitu kerahasiaan, integritas, dan ketersediaan data. Dalam pelaksanaannya, penerapan Kerangka Keamanan dan Ketahanan Siber (KKS) berkontribusi secara signifikan terhadap pilar utama *security* dan *privacy* dalam kerangka kerja kepercayaan digital, sehingga menciptakan ekosistem digital yang lebih andal dan aman bagi pengguna.

2. Transparansi dan Kepatuhan
   Penyelenggara sistem pembayaran dan pelaku pasar keuangan diwajibkan untuk melaporkan tingkat kematangan keamanan siber serta insiden siber yang terjadi kepada Bank Indonesia. Kewajiban ini bertujuan untuk meningkatkan transparansi operasional dan memberikan gambaran yang lebih jelas terkait kesiapan penyelenggara dalam menghadapi ancaman siber. Selain itu, pemberlakuan sanksi administratif dan mekanisme pengawasan yang ketat menjadi langkah strategis untuk memastikan bahwa setiap penyelenggara mematuhi standar keamanan yang telah ditetapkan. Pendekatan ini diharapkan dapat menciptakan ekosistem keuangan yang lebih aman dan andal.

3. Kolaborasi sebagai Elemen Kunci
   Kolaborasi antara penyelenggara, asosiasi, dan otoritas berperan penting dalam mendukung pendekatan berbasis ekosistem yang menjadi elemen fundamental dalam kerangka kerja kepercayaan digital. Melalui kerja sama yang erat, berbagai pemangku kepentingan dapat berbagi informasi, sumber daya, dan keahlian untuk menciptakan lingkungan digital yang lebih aman, transparan, dan tepercaya. Pendekatan ini memungkinkan terciptanya sinergi yang efektif dalam mengatasi tantangan keamanan, meningkatkan perlindungan data, dan memastikan kepatuhan terhadap regulasi, sehingga memperkuat kepercayaan pengguna terhadap layanan digital.

4. Fokus pada Risiko dan Resiliensi
   Peraturan ini mencerminkan pendekatan berbasis risiko yang menjadi inti dari kerangka kerja kepercayaan digital. Dengan mengadopsi pendekatan ini, peraturan tersebut dirancang untuk mendeteksi, mencegah, dan memitigasi berbagai ancaman yang muncul di ruang digital. Hal ini bertujuan untuk menciptakan lingkungan digital yang lebih aman, andal, dan dapat dipercaya oleh seluruh pemangku kepentingan.

Secara keseluruhan, Peraturan Bank Indonesia Nomor 2 Tahun 2024 memberikan landasan yang kuat bagi pengembangan kerangka kerja kepercayaan digital di Indo-

nesia, khususnya di sektor keuangan. Melalui tata kelola yang ketat, transparansi, pengawasan berbasis risiko, serta kolaborasi lintas lembaga, peraturan ini memperkuat kepercayaan publik terhadap stabilitas dan keamanan layanan keuangan digital. Dengan demikian, BI berperan strategis dalam mendukung terciptanya ekosistem ekonomi digital yang stabil, tangguh, dan tepercaya.

4.5.7 Buku Putih Strategi Nasional Pengembangan Ekonomi Digital Indonesia 2030

Buku putih ini merupakan dokumen strategis yang dirancang untuk memandu pengembangan ekonomi digital Indonesia menuju visi menjadi salah satu negara dengan ekonomi terbesar pada tahun 2045 [302]. Poin-poin utama dari dokumen ini adalah:

1. Urgensi Ekonomi Digital
   Ekonomi digital telah menjadi katalisator utama dalam mendorong pertumbuhan ekonomi yang resilien dan berkelanjutan di berbagai negara, termasuk Indonesia. Dengan potensi besar yang dimiliki, Indonesia memiliki peluang untuk menjadi pemimpin regional dalam ekonomi digital. Hal ini didukung oleh pertumbuhan ekonomi digital yang terus meningkat, yang berkontribusi secara signifikan terhadap Produk Domestik Bruto (PDB) nasional dan membuka peluang untuk memperkuat daya saing Indonesia di kancah global.

2. Pilar Utama Pengembangan Ekonomi Digital
   Pembangunan ekonomi digital di Indonesia berfokus pada beberapa aspek strategis yang saling mendukung. Infrastruktur menjadi prioritas utama, dengan perhatian pada peningkatan konektivitas, pembangunan pusat data, serta pengembangan layanan digital yang andal dan terjangkau. Selain itu, sumber daya manusia (SDM) berperan penting melalui pengembangan keterampilan digital dan peningkatan literasi digital, sehingga masyarakat dapat beradaptasi dengan transformasi teknologi yang terus berkembang. Dalam mendukung ekosistem digital, iklim bisnis dan keamanan siber ditingkatkan melalui adopsi teknologi yang lebih luas serta penguatan sistem keamanan siber untuk melindungi data dan informasi vital. Aspek penelitian, inovasi, dan pengembangan usaha juga didorong oleh investasi pada riset dan pengembangan (R&D) serta inovasi teknologi, guna menciptakan solusi yang relevan bagi tantangan di sektor digital. Untuk mempercepat pertumbuhan, pendanaan dan investasi diarahkan pada upaya menarik investasi lokal dan asing ke sektor digital, termasuk mendukung *startup* dan perusahaan teknologi. Semua langkah ini dilengkapi dengan kebijakan dan regulasi yang dirancang untuk mendorong inklusi digital, menciptakan lingkungan yang mendukung inovasi, serta memastikan bahwa transformasi digital berlangsung secara adil dan berkelanjutan.

3. Strategi Implementasi
   Kerangka regulasi yang resilien dan adaptif sangat penting dalam mencipta-

kan ekosistem digital yang kondusif bagi pertumbuhan ekonomi. Regulasi ini harus mampu mengakomodasi kebutuhan berbagai pihak, mulai dari pemerintah, sektor swasta/industri, hingga masyarakat, sehingga tercipta lingkungan yang mendukung inovasi dan inklusi digital. Untuk mewujudkannya, kolaborasi yang erat antara pemerintah, sektor swasta/industri, dan masyarakat menjadi kunci utama. Kolaborasi ini dapat mempercepat adopsi teknologi baru, meningkatkan kepercayaan publik, serta memperkuat sinergi dalam menghadapi tantangan era digital. Selain itu, fokus utama harus diarahkan pada pembangunan ekosistem digital yang tidak hanya aman dari ancaman siber, tetapi juga kompetitif dan inovatif, sehingga mampu mendorong daya saing nasional di tingkat global.

4. Target 2045 Indonesia memiliki aspirasi untuk menjadi salah satu dari 20 negara teratas dalam peringkat daya saing digital global, sebuah langkah ambisius yang mencerminkan komitmen terhadap transformasi digital yang menyeluruh. Selain itu, target lain yang ingin dicapai adalah peningkatan kontribusi ekonomi digital hingga 20% terhadap PDB nasional. Pencapaian ini diharapkan tidak hanya memperkuat posisi Indonesia di kancah global, tetapi juga memberikan dampak signifikan terhadap pertumbuhan ekonomi yang andal dan berkelanjutan.

Keterkaitan dengan Kerangka Kerja Kepercayaan Digital di Indonesia

Kerangka kerja kepercayaan digital bertujuan membangun kepercayaan dalam ekosistem digital melalui peningkatan keamanan, transparansi, dan kepatuhan. Buku Putih ini memberikan landasan konseptual dan strategis bagi penyusunan kerangka kerja melalui beberapa aspek berikut:

1. Keamanan Siber dan Data
   Penegasan bahwa keamanan siber merupakan faktor krusial dalam menciptakan ekosistem ekonomi digital yang aman dan tepercaya. Keamanan siber serta perlindungan data menjadi dasar utama untuk membangun kepercayaan di kalangan pengguna dan investor. Pilar keamanan siber yang diuraikan dalam dokumen ini menitikberatkan pada penguatan perlindungan data, sertifikasi keamanan produk digital, dan pelaporan insiden siber. Upaya ini sejalan dengan elemen keamanan dalam kerangka kerja kepercayaan digital yang bertujuan untuk memastikan kerahasiaan, integritas, dan ketersediaan data. Lebih lanjut, pilar ini juga mendukung pengembangan Undang-Undang Keamanan Siber, yang menurut kajian dalam buku ini masih sangat dibutuhkan di Indonesia. Penyusunan undang-undang yang komprehensif diharapkan dapat memberikan landasan hukum yang lebih jelas dan mendukung pertukaran data lintas batas secara aman. Dengan demikian, kerangka kerja kepercayaan digital harus mengadopsi prinsip-prinsip keamanan siber, termasuk regulasi dan standar yang kuat terkait pelindungan data pribadi dan identitas digital.

2. Transparansi dan Kepatuhan
   Rekomendasi perumusan kebijakan yang mendukung ekosistem digital yang aman, dengan memberikan fokus pada regulasi yang pro-pertumbuhan, namun tetap mengutamakan perlindungan terhadap kepentingan konsumen dan keberlanjutan ekosistem. Dalam konteks ini, kerangka kerja kepercayaan digital harus dirancang untuk mencakup kebijakan yang mampu menjaga keseimbangan antara kemajuan teknologi dan perlindungan privasi serta keamanan data. Strategi pengembangan regulasi juga perlu mengedepankan transparansi dalam pengambilan keputusan, yang merupakan elemen kunci dalam membangun kepercayaan publik terhadap DTF. Selain itu, kolaborasi antarlembaga dalam mengadopsi standar global turut berkontribusi pada terciptanya kepatuhan yang mendukung ekosistem digital yang tepercaya dan aman.

3. Penguatan Infrastruktur Digital
   Ketersediaan infrastruktur digital yang memadai dan sumber daya manusia (SDM) yang terampil dalam bidang teknologi informasi dan komunikasi (TIK) merupakan elemen penting dalam mendukung kepercayaan digital. Tanpa infrastruktur yang andal dan tenaga kerja yang terlatih, kepercayaan pengguna maupun pelaku bisnis terhadap layanan digital dapat terganggu. Oleh karena itu, kerangka kerja kepercayaan digital harus mencakup strategi untuk meningkatkan kapasitas SDM, terutama dalam literasi digital dan penguasaan keterampilan teknis yang relevan. Selain itu, fokus pada pengembangan infrastruktur digital, seperti konektivitas yang luas dan pusat data yang kuat, sangat penting untuk menciptakan ekosistem yang mendukung kelangsungan operasional ekonomi digital. Hal ini sejalan dengan elemen kepercayaan teknis dalam kerangka kerja kepercayaan digital.

4. Pengembangan SDM dan Literasi Digital
   Upaya untuk memperkuat keterampilan digital dan literasi masyarakat memiliki peran penting dalam mendukung penggunaan teknologi secara bertanggung jawab. Langkah ini tidak hanya membantu individu memahami cara memanfaatkan teknologi secara efektif, tetapi juga mendorong perilaku yang sesuai dengan prinsip keamanan dan etika digital. Dengan peningkatan literasi digital, kepercayaan pengguna terhadap ekosistem digital juga akan meningkat, menciptakan lingkungan yang lebih aman dan tepercaya bagi seluruh pihak yang terlibat.

5. Kolaborasi Multi-Pemangku Kepentingan
   Pentingnya sinergi antara pemerintah, sektor swasta/industri, akademisi, dan masyarakat dalam membangun ekosistem ekonomi digital yang kolaboratif dan berkelanjutan. Pendekatan kolaboratif ini tidak hanya memperkuat koordinasi antarpemangku kepentingan, tetapi juga sejalan dengan prinsip dasar kerangka kerja kepercayaan digital, yang memerlukan dukungan lintas sektor untuk menciptakan kepercayaan digital. Kolaborasi ini menjadi kunci dalam mengintegrasikan berbagai perspektif dan sumber daya untuk memastikan bahwa transformasi digital berjalan secara harmonis dan tepercaya.

Secara keseluruhan, Buku Putih Strategi Nasional Pengembangan Ekonomi Digital Indonesia 2030 memberikan landasan strategis bagi pembentukan kerangka kerja kepercayaan digital nasional. Dengan fokus pada keamanan siber, regulasi adaptif, penguatan SDM, dan kolaborasi lintas sektor, dokumen ini mendukung terciptanya ekosistem digital yang aman, andal, dan tepercaya untuk mempercepat transformasi digital menuju visi Indonesia Emas 2045.

4.5.8 Peraturan Otoritas Jasa Keuangan Nomor 11 Tahun 2022 tentang Penyelenggaraan Teknologi Informasi oleh Bank Umum

Peraturan Otoritas Jasa Keuangan (POJK) Nomor 11 Tahun 2022 tentang Penyelenggaraan Teknologi Informasi oleh Bank Umum mengatur tata kelola, pengelolaan risiko, serta penerapan keamanan dalam penggunaan teknologi informasi oleh bank umum. Peraturan ini bertujuan untuk memastikan bahwa pemanfaatan teknologi informasi mendukung operasional perbankan yang andal, aman, efisien, dan berkelanjutan, sekaligus melindungi kepentingan nasabah dan stabilitas sistem keuangan [303]. Beberapa poin utama yang diatur adalah:

1. Tata Kelola TI
   Bank memiliki kewajiban untuk menerapkan tata kelola teknologi informasi (TI) yang baik, yang disesuaikan dengan strategi bisnis, kompleksitas organisasi, dan risiko yang terkait dengan teknologi yang digunakan. Dalam hal ini, Direksi dan Dewan Komisaris memegang tanggung jawab khusus untuk memastikan bahwa penyelenggaraan TI berjalan secara efektif dan mendukung pencapaian tujuan bisnis bank secara optimal. Keputusan-keputusan yang diambil di tingkat manajerial harus selalu mempertimbangkan peran TI dalam mendukung operasional dan pertumbuhan jangka panjang, serta menjaga keberlanjutan bisnis di tengah perkembangan teknologi yang pesat.

2. Keamanan dan Ketahanan Siber
   Bank memiliki kewajiban untuk menjaga ketahanan siber dengan melakukan berbagai langkah penting. Proses ini dimulai dengan identifikasi aset yang dimiliki, diikuti dengan analisis terhadap potensi ancaman yang mungkin timbul. Setelah itu, bank harus mengambil langkah-langkah perlindungan terhadap aset-aset tersebut untuk mengurangi risiko yang ada. Deteksi insiden juga merupakan bagian krusial dari upaya ini untuk memastikan bahwa setiap ancaman dapat terdeteksi dengan cepat. Jika terjadi insiden, pemulihan yang cepat dan efektif sangat penting untuk meminimalkan dampaknya. Selain itu, pengujian keamanan siber dilakukan secara berkala untuk menilai tingkat risiko yang ada serta efektivitas langkah-langkah mitigasi yang telah diambil.

3. Manajemen Risiko TI
   Bank harus melakukan identifikasi, pengukuran, pemantauan, dan pengendalian risiko di setiap tahapan penyelenggaraan TI. Proses ini dimulai dengan

mengidentifikasi berbagai potensi risiko yang mungkin terjadi selama operasional TI. Setelah itu, bank perlu mengukur tingkat dampak dan kemungkinan terjadinya risiko-risiko tersebut. Selanjutnya, pemantauan terus-menerus dilakukan untuk memastikan bahwa risiko tersebut tetap terkendali dan sesuai dengan kebijakan yang telah ditetapkan. Terakhir, pengendalian risiko diterapkan untuk mengurangi dampak yang dapat ditimbulkan serta memastikan keberlanjutan dan keamanan operasional TI di bank tersebut.

4. Pengelolaan Data dan Pelindungan Data Pribadi
   Bank harus mengelola data dengan cara yang efektif dan efisien, serta memastikan pelindungan data pribadi sesuai dengan ketentuan peraturan perundang-undangan yang berlaku. Dalam hal pertukaran data pribadi, bank harus mendapatkan persetujuan terlebih dahulu dari pemilik data, dan proses pertukaran tersebut harus dilakukan dengan cara yang aman untuk mencegah terjadinya kebocoran atau penyalahgunaan data. Dengan langkah-langkah ini, bank tidak hanya mematuhi regulasi yang ada, tetapi juga membangun kepercayaan dari para pemilik data.

5. Kolaborasi dengan Penyedia Layanan TI
   Penggunaan jasa pihak ketiga dalam penyelenggaraan TI harus dilakukan dengan mengutamakan prinsip kehati-hatian. Hal ini penting untuk memastikan bahwa seluruh proses berjalan dengan baik, aman, dan terhindar dari potensi risiko yang dapat merugikan organisasi. Oleh karena itu, manajemen risiko yang memadai perlu diterapkan, mulai dari pemilihan pihak ketiga yang tepat hingga pemantauan berkelanjutan terhadap layanan yang diberikan. Pendekatan yang hati-hati dan terkelola dengan baik akan membantu meminimalkan potensi masalah dan memastikan bahwa TI yang diselenggarakan sesuai dengan standar yang ditetapkan.

6. Pelaporan dan Kepatuhan
   Bank diwajibkan untuk secara berkala melaporkan rencana strategis TI, insiden terkait TI, serta realisasi penyelenggaraan TI kepada Otoritas Jasa Keuangan (OJK). Pelaporan ini bertujuan untuk memastikan bahwa bank mematuhi regulasi yang ditetapkan dan dapat menjaga keamanan serta kestabilan sistem informasi yang digunakan dalam operasional mereka. OJK, sebagai lembaga pengawas, akan mengevaluasi laporan tersebut untuk memastikan bahwa bank terus menerapkan praktik TI yang baik dan sesuai dengan standar yang berlaku, serta siap mengatasi potensi risiko yang mungkin muncul.

7. Sanksi
   Bank yang melanggar ketentuan yang berlaku akan dikenakan sanksi administratif sesuai dengan tingkat pelanggaran yang dilakukan. Sanksi tersebut dapat berupa teguran tertulis sebagai peringatan pertama, namun, jika pelanggaran terus berlanjut, sanksi yang lebih berat dapat diberikan, termasuk pembekuan kegiatan usaha tertentu. Pembekuan ini dimaksudkan untuk menegakkan kepatuhan dan menjaga integritas sektor perbankan.

Keterkaitan dengan Kerangka Kerja Kepercayaan Digital di Indonesia

Peraturan ini memiliki relevansi yang kuat dengan kerangka kerja kepercayaan digital, yang bertujuan untuk membangun kepercayaan dalam ekosistem digital. Keterkaitannya mencakup hal-hal berikut:

1. Keamanan Siber sebagai Pilar Utama
   Ketentuan mengenai ketahanan siber dan pengamanan informasi dalam peraturan ini dirancang untuk mendukung dua elemen inti dari kerangka kerja kepercayaan digital, yaitu keamanan (*security*) dan keandalan (*reliability*). Pengujian keamanan siber yang dilakukan secara rutin, bersama dengan penilaian maturitas keamanan siber, bertujuan untuk memastikan bahwa sistem perbankan digital tetap terjaga integritasnya dan dapat dipercaya oleh pengguna. Langkah-langkah ini sangat penting dalam mempertahankan kepercayaan publik terhadap sistem perbankan digital yang terus berkembang, serta memastikan bahwa data dan transaksi yang dilakukan tetap aman dari potensi ancaman siber.

2. Pengelolaan Data dan Privasi
   Aspek pelindungan data pribadi dalam peraturan ini sejalan dengan pilar privasi yang ada dalam kerangka kerja kepercayaan digital. Salah satu prinsip utamanya adalah kewajiban untuk menjaga kerahasiaan data pribadi yang dimiliki oleh individu, serta pentingnya persetujuan pengguna sebelum data mereka diproses. Kedua hal ini menjadi landasan yang kuat untuk membangun kepercayaan digital, di mana pengguna merasa aman dan dihargai hak privasinya dalam ekosistem digital.

3. Transparansi dan Akuntabilitas
   Kewajiban pelaporan insiden TI dan penyelenggaraan TI memiliki peran penting dalam menciptakan transparansi, yang pada gilirannya menjadi elemen fundamental dalam membangun kepercayaan. Transparansi ini tidak hanya bermanfaat bagi hubungan antara bank dan regulator, tetapi juga bagi masyarakat secara keseluruhan. Dengan adanya kewajiban pelaporan yang jelas dan terstruktur, berbagai pihak dapat memastikan bahwa pengelolaan TI dilakukan secara bertanggung jawab dan sesuai dengan standar yang berlaku, sehingga dapat mengurangi potensi risiko dan meningkatkan rasa aman bagi semua pihak yang terlibat.

4. Kolaborasi Ekosistem Digital
   Pengaturan mengenai kerja sama dengan pihak ketiga mencerminkan pendekatan ekosistem dalam kerangka kerja kepercayaan digital. Dalam hal ini, bank diharapkan memastikan bahwa semua penyedia layanan TI yang bekerja sama dengan mereka mematuhi standar keamanan yang telah ditetapkan. Hal ini penting untuk menjaga integritas dan kepercayaan dalam sistem digital yang lebih luas, memastikan bahwa semua pihak yang terlibat memiliki komitmen yang sama terhadap perlindungan data dan keamanan informasi.

5. Manajemen Risiko Berbasis Teknologi
   Peraturan ini mendorong penerapan pendekatan berbasis risiko dalam pengelolaan TI, yang bertujuan untuk memitigasi potensi ancaman yang dapat mengganggu keberlanjutan operasional digital. Pendekatan ini selaras dengan kerangka kerja kepercayaan digital, yang mengintegrasikan analisis risiko sebagai bagian integral dari upaya perlindungan terhadap data, transaksi, dan layanan digital. Dengan demikian, peraturan ini berperan penting dalam memastikan bahwa setiap aspek TI dikelola dengan hati-hati, sehingga membangun kepercayaan dan mengurangi kerentanannya terhadap risiko yang ada.

Peraturan OJK Nomor 11 Tahun 2022 memberikan landasan hukum dan operasional yang mendukung penyusunan kerangka kerja kepercayaan digital di Indonesia. Dengan menekankan tata kelola, keamanan, privasi, dan kolaborasi, peraturan ini membantu membangun ekosistem digital yang aman, tepercaya, dan berkelanjutan, sesuai dengan tujuan transformasi digital nasional.

4.5.9 Peraturan Otoritas Jasa Keuangan Nomor 21 Tahun 2023 tentang Layanan Digital oleh Bank Umum

Peraturan Otoritas Jasa Keuangan No. 21 Tahun 2023 tentang Layanan Digital oleh Bank Umum mengatur penyelenggaraan layanan digital berbasis teknologi informasi (TI) oleh bank umum [304]. Tujuan utama regulasi ini adalah menjamin inovasi digital perbankan yang aman, bertanggung jawab, serta memperhatikan perlindungan konsumen dan keamanan data. Poin-poin utama meliputi:

1. Definisi dan Ruang Lingkup
   Layanan digital dalam konteks perbankan mencakup berbagai produk, aktivitas, dan saluran yang memanfaatkan teknologi untuk meningkatkan efisiensi dan kualitas layanan. Agar penyelenggaraan layanan tersebut berjalan secara aman, terukur, dan berkelanjutan, bank diwajibkan menyiapkan strategi, kebijakan, serta prosedur khusus yang secara komprehensif mengatur pemanfaatan teknologi dalam setiap aspek operasional dan pengembangan layanan.

2. Tata Kelola
   Tanggung jawab utama dalam pengawasan penyelenggaraan layanan digital berada pada dewan komisaris dan direksi. Kedua organ ini harus memastikan bahwa setiap aktivitas digital bank berjalan sesuai dengan prinsip kehati-hatian serta selaras dengan tujuan strategis perusahaan. Untuk itu, bank dituntut memiliki kerangka tata kelola yang komprehensif, tidak hanya sebagai landasan pengendalian dan mitigasi risiko, tetapi juga sebagai pendorong inovasi yang aman dan berkelanjutan. Dengan tata kelola yang kuat, layanan digital dapat berkembang secara sehat sekaligus menjaga kepercayaan nasabah dan stabilitas sistem keuangan.

3. Manajemen Risiko TI
   Bank diwajibkan menerapkan pengendalian menyeluruh terhadap seluruh aspek teknologi informasi, mulai dari keamanan data dan infrastruktur hingga kerja sama dengan pihak ketiga. Pelindungan data pribadi menjadi elemen penting dalam kerangka ini, sehingga setiap potensi risiko yang muncul dapat diantisipasi sejak dini. Selain itu, bank juga harus menyiapkan *business continuity plan* dan *disaster recovery plan* agar layanan tetap berfungsi dengan baik meskipun terjadi gangguan atau bencana, sehingga kepercayaan nasabah terhadap sistem perbankan digital dapat terus terjaga.

4. Perlindungan Konsumen
   Peraturan ini menempatkan perlindungan konsumen sebagai aspek yang sangat penting dalam penyelenggaraan layanan digital perbankan. Bank diwajibkan untuk memberikan edukasi yang memadai agar nasabah memahami produk dan layanan yang digunakan, sekaligus memastikan keterbukaan informasi sehingga setiap transaksi dilakukan secara transparan. Selain itu, bank harus menyediakan mekanisme penanganan pengaduan yang efektif sebagai bentuk tanggung jawab terhadap kepentingan nasabah. Di atas semua itu, pelindungan data pribadi menjadi kewajiban utama, sehingga kerahasiaan, integritas, dan keamanan data nasabah tetap terjaga dalam setiap proses layanan digital.

5. Inovasi dan *Sandbox*
   Peraturan ini memberikan ruang bagi bank untuk mengembangkan model bisnis digital baru, namun tetap dalam kerangka pengawasan OJK. Mekanisme *sandbox* yang diatur berfungsi sebagai sarana uji coba terbatas, sehingga inovasi dapat dikembangkan secara terukur dan terkendali. Dengan demikian, bank memiliki kesempatan untuk menghadirkan layanan digital yang adaptif terhadap kebutuhan pasar, sambil memastikan bahwa setiap inovasi tetap sejalan dengan prinsip kehati-hatian serta tidak menimbulkan risiko yang dapat mengganggu stabilitas sistem keuangan maupun melanggar perlindungan konsumen.

6. Penggunaan Pihak Ketiga
   Bank diperkenankan menjalin kerja sama dengan penyedia teknologi, termasuk layanan *cloud* dan penyedia solusi *fintech enabler*, untuk mendukung pengembangan layanan digitalnya. Namun demikian, tanggung jawab penuh atas keamanan, kelancaran operasional, dan perlindungan nasabah tetap berada di tangan bank sebagai penyelenggara utama. Oleh karena itu, setiap perjanjian dengan pihak ketiga wajib mencakup ketentuan yang jelas mengenai standar keamanan, mekanisme audit, serta perlindungan konsumen. Dengan cara ini, kolaborasi dapat berjalan secara efektif tanpa mengurangi akuntabilitas dan kepercayaan publik terhadap layanan perbankan digital.

Keterkaitan dengan Kerangka Kerja Kepercayaan Digital di Indonesia

POJK ini memiliki peran strategis dalam mendukung penyusunan kerangka kepercayaan digital nasional:

1. Keamanan dan Ketahanan Siber
   Penekanan pada keamanan informasi, perlindungan data, dan rencana kesinambungan bisnis mendukung kepercayaan digital yang berbasis *resilience*.

2. Akuntabilitas dan Transparansi
   Peraturan ini menegaskan bahwa dewan komisaris, direksi, dan bank tetap memegang tanggung jawab penuh atas penyelenggaraan layanan digital, termasuk ketika melibatkan pihak ketiga. Ketentuan tersebut mencerminkan prinsip akuntabilitas, yakni tidak adanya pengalihan kewajiban utama kepada penyedia jasa eksternal. Di sisi lain, kewajiban untuk menyampaikan laporan secara berkala dan membuka akses informasi kepada regulator menunjukkan komitmen terhadap transparansi dalam tata kelola digital. Dengan demikian, akuntabilitas dan transparansi berjalan beriringan sebagai dasar yang memastikan layanan digital dikelola secara bertanggung jawab dan dapat diawasi secara efektif.

3. Perlindungan Data dan Hak Pengguna
   Perlindungan data nasabah, mekanisme pengaduan, serta edukasi konsumen merupakan pilar utama kepercayaan digital.

4. Kolaborasi Multi-Pihak
   Aturan penggunaan pihak ketiga, termasuk *cloud provider* dan *fintech*, relevan untuk membangun ekosistem digital nasional yang saling terhubung namun tetap tepercaya.

5. Inovasi yang Bertanggung Jawab
   Pemberian ruang bagi bank untuk mengembangkan layanan perbankan digital di bawah pengawasan OJK menunjukkan penerapan prinsip *responsible innovation*. Inovasi didorong untuk memperluas akses dan meningkatkan kualitas layanan, namun tetap dalam kerangka regulasi yang memastikan keamanan, perlindungan konsumen, serta stabilitas sistem keuangan.

4.5.10 Peraturan Otoritas Jasa Keuangan Nomor 40 Tahun 2024 tentang Layanan Pendanaan Bersama Berbasis Teknologi Informasi

Peraturan ini mengatur penyelenggaraan Layanan Pendanaan Bersama Berbasis Teknologi Informasi (LPBBTI), atau lebih dikenal sebagai *fintech peer-to-peer* (P2P) *lending* [305]. Regulasi ini memperbarui POJK No. 10 Tahun 2022 dan bertujuan untuk memperkuat perlindungan konsumen, tata kelola, serta integritas sistem keuangan digital.

1. Latar Belakang dan Tujuan
   Layanan Pendanaan Bersama Berbasis Teknologi Informasi (LPBBTI) merupakan model bisnis *fintech peer-to-peer lending* yang berfungsi sebagai perantara antara pemberi dana dan penerima dana, tanpa menghimpun dana masyarakat. Kehadiran model ini menawarkan alternatif pembiayaan yang masif, namun juga menimbulkan risiko yang perlu dikelola dengan baik. Untuk itu, OJK menerbitkan POJK 40 Tahun 2024 yang memperkuat pengaturan sebelumnya (POJK 10/2022), sekaligus menyesuaikan amanat Undang-Undang P2SK (UU 4/2023) dan revisi Undang-Undang ITE (UU 1/2024). Peraturan ini bertujuan meningkatkan tata kelola penyelenggara LPBBTI, memperkuat perlindungan konsumen, memastikan penerapan manajemen risiko yang memadai, serta mengoptimalkan peran LPBBTI dalam mendukung inklusi keuangan dan pertumbuhan perekonomian nasional.

2. Perlindungan Konsumen dan Data
   Penyelenggara diwajibkan menjaga kerahasiaan, integritas, dan ketersediaan seluruh data yang dikelolanya, termasuk data pribadi, data transaksi, dan data keuangan. Tanggung jawab ini mencakup kewajiban untuk segera memberitahukan pemilik data apabila terjadi kebocoran atau kegagalan perlindungan, sehingga pengguna tetap memperoleh kepastian dan transparansi atas risiko yang dihadapi. Selain itu, penyelenggara harus menyediakan mekanisme pengaduan yang mudah diakses serta memastikan penyelesaian sengketa dilakukan sesuai ketentuan perlindungan konsumen yang berlaku. Dengan cara ini, kepercayaan publik terhadap layanan digital dapat terjaga melalui perlindungan hak-hak dasar pengguna dan jaminan keamanan data.

3. Keamanan dan Teknologi Informasi
   Setiap penyelenggara diwajibkan memiliki sistem pengamanan teknologi informasi yang mampu mencegah sekaligus menanggulangi potensi serangan siber. Untuk memastikan standar keamanan yang konsisten, penyelenggara juga harus memiliki sertifikat Sistem Manajemen Keamanan Informasi (SMKI) dengan cakupan yang menyeluruh. Selain itu, rekam jejak audit (*audit trail*) wajib tersedia sebagai instrumen penting bagi keperluan pengawasan, penegakan hukum, maupun penyelesaian sengketa, sehingga keamanan dan akuntabilitas layanan digital tetap terjamin.

4. Tata Kelola dan Manajemen Risiko
   Penyelenggara layanan diwajibkan untuk menerapkan prinsip tata kelola perusahaan yang baik (*Good Corporate Governance*, GCG), yaitu keterbukaan, akuntabilitas, pertanggungjawaban, kemandirian, dan kewajaran. Prinsip ini menjadi dasar dalam menjaga kepercayaan publik sekaligus memastikan keberlanjutan usaha. Tanggung jawab pengawasan melekat pada Direksi, Dewan Komisaris, serta Dewan Pengawas Syariah, sehingga seluruh lini kepemimpinan memiliki peran dalam menjamin kepatuhan dan efektivitas pengelolaan risiko. Selain itu, penyelenggara berkewajiban menyusun laporan tahunan mengenai tata kelola kepada OJK sebagai bentuk transparansi dan akuntabilitas. Dalam aspek manajemen risiko, kewajiban yang diatur mencakup

proses identifikasi, pengukuran, pemantauan, dan pengendalian risiko yang terintegrasi dengan sistem pengendalian internal. Dengan demikian, tata kelola dan manajemen risiko berjalan beriringan untuk mendukung integritas, stabilitas, serta keandalan penyelenggaraan layanan digital.

5. Sanksi
   Pelanggaran dikenakan sanksi administratif mulai dari teguran tertulis, pembatasan/pembekuan usaha, denda, hingga pencabutan izin.

Keterkaitan dengan Kerangka Kepercayaan Digital di Indonesia

POJK 40/2024 berperan penting dalam menyusun dasar kepercayaan digital, khususnya di sektor keuangan digital:

1. Perlindungan Data dan Privasi
   Pengaturan mengenai pengelolaan data pribadi, kewajiban notifikasi ketika terjadi kebocoran, serta penyediaan *audit trail* mencerminkan penerapan prinsip kepercayaan digital yang menekankan pentingnya keamanan dan transparansi data. Ketentuan ini memastikan bahwa penyelenggara layanan digital tidak hanya bertanggung jawab menjaga kerahasiaan dan integritas informasi, tetapi juga wajib bersikap terbuka kepada pemilik data dan regulator ketika terjadi insiden.

2. Keamanan Siber dan Resiliensi
   Kewajiban memiliki sertifikasi Sistem Manajemen Keamanan Informasi (SMKI), penerapan sistem pengamanan teknologi, serta penyediaan mekanisme mitigasi risiko serangan menjadi elemen penting dalam menjaga keamanan siber. Ketentuan ini memastikan penyelenggara tidak hanya mampu mencegah ancaman, tetapi juga memiliki kesiapan untuk merespons insiden dan memulihkan layanan secara cepat.

3. Akuntabilitas dan Transparansi
   Penerapan prinsip tata kelola perusahaan yang baik (*Good Corporate Governance*, GCG), kewajiban pelaporan tahunan, serta mekanisme audit yang terstruktur menjadi wujud nyata akuntabilitas penyelenggara layanan digital. Melalui instrumen tersebut, setiap keputusan dan aktivitas dapat dipertanggungjawabkan sekaligus diawasi secara berkesinambungan. Di sisi lain, keterbukaan dalam pelaporan kepada regulator maupun publik mencerminkan transparansi yang penting untuk membangun kepercayaan. Kombinasi akuntabilitas dan transparansi ini memastikan bahwa layanan digital tidak hanya inovatif, tetapi juga dikelola dengan standar yang dapat dipercaya.

4. Perlindungan Konsumen
   Pengaturan mengenai hak-hak konsumen menempatkan kepentingan pengguna sebagai prioritas utama dalam layanan digital. Penyelenggara diwajibkan menyediakan mekanisme yang jelas untuk penanganan pengaduan dan penyelesaian sengketa, sehingga pengguna memiliki saluran yang dapat dipercaya

ketika menghadapi masalah. Selain itu, kewajiban menjaga keamanan data pribadi serta memberikan informasi yang transparan memperkuat perlindungan terhadap risiko penyalahgunaan data dan praktik yang merugikan.

5. Kolaborasi Multi-Pihak
   LPBBTI melibatkan berbagai pihak, mulai dari pemberi dana, penerima dana, penyelenggara platform, hingga regulator. Interaksi antarpemangku kepentingan ini menuntut adanya koordinasi yang jelas agar kepentingan masing-masing pihak terlindungi. Prinsip tanggung jawab penuh yang tetap melekat pada penyelenggara, meskipun sebagian fungsi didukung oleh pihak ketiga, memastikan bahwa kolaborasi tersebut tidak mengurangi akuntabilitas.

4.5.11 Peraturan BSSN Nomor 8 Tahun 2020 tentang Sistem Pengamanan dalam Penyelenggaraan Sistem Elektronik

Peraturan BSSN No. 8 Tahun 2020 ditetapkan pada 16 November 2023 berisi tentang kewajiban penyelenggara sistem elektronik (publik dan privat) menerapkan Sistem Manajemen Pengamanan Informasi (SMPI) berbasis risiko, termasuk sertifikasi SNI ISO/IEC 27001, penilaian mandiri, pelaporan, monitoring, dan sanksi [306].

1. Latar Belakang dan Tujuan
   Peraturan ini disusun sebagai tindak lanjut dari Peraturan Pemerintah Nomor 71 Tahun 2019 tentang Penyelenggaraan Sistem dan Transaksi Elektronik. Kehadirannya dimaksudkan untuk memastikan bahwa setiap PSE, baik di lingkup publik maupun privat, menerapkan sistem pengamanan informasi yang sesuai dengan standar yang berlaku.

2. Pendekatan Berbasis Risiko: sistem Elektronik dikategorikan menjadi tiga: Strategis, Tinggi, dan Rendah, berdasarkan dampak terhadap kepentingan publik dan negara.

3. Ruang Lingkup
   Ketentuan ini berlaku bagi PSE, baik di sektor publik maupun privat. PSE publik mencakup instansi pemerintah dan lembaga terkait yang menyelenggarakan layanan berbasis teknologi informasi. Sementara itu, PSE privat meliputi berbagai pelaku usaha dan platform digital, termasuk perusahaan teknologi, penyedia layanan *fintech*, *e-commerce*, media sosial, aplikasi komunikasi, serta pengelola data pribadi.

4. Sistem Manajemen Pengamanan Informasi (SMPI)
   SMPI menjadi kerangka utama dalam penyelenggaraan pengamanan sistem elektronik dengan pendekatan berbasis risiko. Melalui mekanisme ini, setiap sistem elektronik dikategorikan ke dalam tiga tingkatan, strategis, tinggi, atau rendah, berdasarkan penilaian mandiri penyelenggara yang kemudian diverifikasi oleh BSSN. Kategorisasi ini memastikan bahwa tingkat pengamanan

yang diterapkan sebanding dengan potensi dampak yang ditimbulkan. Untuk menjamin konsistensi dan mutu pengamanan, penyelenggara sistem elektronik diwajibkan menerapkan standar SNI ISO/IEC 27001 maupun standar keamanan lain yang ditetapkan oleh BSSN atau kementerian terkait.

5. Implementasi dan Sertifikasi
   Penerapan SMPI dilaksanakan secara mandiri oleh PSE. Dalam prosesnya, PSE dapat memperoleh dukungan dari tenaga ahli atau konsultan yang telah diakui oleh BSSN, namun tanggung jawab utama tetap berada pada PSE. Untuk memastikan kesesuaian dengan standar keamanan yang ditetapkan, setiap PSE wajib melalui proses sertifikasi yang dilakukan oleh Lembaga Sertifikasi Keamanan Informasi. Sertifikat SMPI yang diperoleh berlaku selama tiga tahun dan harus diperbarui melalui audit pengawasan rutin, sehingga keberlanjutan penerapan standar keamanan dapat terus terjaga.

6. Pembinaan dan Pengawasan
   BSSN menjalankan fungsi pembinaan dengan menyediakan pelatihan, bimbingan teknis, dan asistensi untuk membantu PSE meningkatkan kapasitas pengamanan informasi. Selain itu, BSSN juga melakukan pengawasan melalui kegiatan pemantauan, evaluasi, penelusuran, dan pemeriksaan guna memastikan bahwa standar keamanan diterapkan secara konsisten. Pendekatan ini tidak hanya berfokus pada penegakan aturan, tetapi juga mendorong peningkatan berkelanjutan dalam tata kelola keamanan siber.

7. Sanksi
   Setiap PSE yang tidak mematuhi ketentuan dikenai sanksi administratif sesuai dengan tingkat pelanggaran yang dilakukan. Bentuk sanksi dapat berupa teguran tertulis sebagai peringatan awal, pembekuan sertifikasi apabila pelanggaran tidak segera diperbaiki, hingga pencabutan sertifikasi bagi pelanggaran yang serius atau berulang. Mekanisme sanksi ini berfungsi sebagai instrumen penegakan kepatuhan sekaligus pendorong bagi PSE untuk menjaga standar keamanan dan tata kelola yang telah ditetapkan.

Keterkaitan dengan Kerangka Kepercayaan Digital di Indonesia

Peraturan BSSN Nomor 8 Tahun 2020 tentang Sistem Pengamanan dalam Penyelenggaraan Sistem Elektronik (SMPI) memegang peran strategis dalam mendukung penyusunan kerangka kerja kepercayaan digital di Indonesia. Peraturan ini tidak hanya mengatur aspek teknis pengamanan sistem elektronik, tetapi juga mencerminkan prinsip-prinsip tata kelola digital yang kredibel, akuntabel, dan berkelanjutan. Dalam konteks transformasi digital nasional, SMPI menjadi acuan normatif dan operasional untuk memastikan bahwa sistem elektronik yang digunakan oleh sektor publik maupun privat memenuhi standar keamanan informasi yang ketat dan selaras dengan praktik terbaik internasional.

Lebih dari sekadar pedoman teknis, SMPI menanamkan nilai-nilai fundamental kepercayaan digital, seperti pelindungan data pribadi, transparansi, interoperabilitas,

dan kedaulatan digital, yang sangat relevan dalam membangun lingkungan digital yang aman dan tepercaya. Oleh karena itu, keterkaitan antara regulasi ini dan kerangka kerja kepercayaan digital bukan hanya bersifat konseptual, melainkan juga bersifat langsung dan aplikatif, sebagaimana dijabarkan dalam poin-poin berikut.

1. Keamanan dan Resiliensi Siber
   Penerapan SMPI yang berlandaskan standar SNI ISO/IEC 27001 menjadi dasar penting dalam memperkuat keamanan digital. Melalui pendekatan berbasis risiko, sistem ini mendorong pengelolaan ancaman secara lebih terstruktur dan berkesinambungan. Selain itu, adanya kategorisasi sistem elektronik, strategis, tinggi, dan rendah, memungkinkan penetapan prioritas pengamanan yang proporsional dengan potensi dampak terhadap kepentingan publik maupun nasional.

2. Akuntabilitas dan Tata Kelola
   Peraturan ini menegaskan pentingnya akuntabilitas melalui mekanisme sertifikasi, audit, dan pengawasan yang dilakukan secara berkala. Setiap PSE wajib memastikan penerapan standar keamanan dan manajemen risiko, serta membuka diri terhadap evaluasi independen. Meskipun dapat melibatkan tenaga ahli atau konsultan pihak ketiga, tanggung jawab utama tetap berada pada PSE.

3. Perlindungan Data dan Privasi
   Aturan ini memberikan perhatian khusus pada pengelolaan data pribadi dengan menetapkan kewajiban bagi PSE untuk menjaga kerahasiaan, keutuhan, dan ketersediaan data. Ketentuan tersebut juga memastikan bahwa proses pengumpulan, penyimpanan, dan pemrosesan data dilakukan secara aman serta sesuai dengan standar yang berlaku.

4. Kolaborasi Multi-Pihak
   Keterlibatan BSSN, lembaga sertifikasi, konsultan, tenaga ahli, dan PSE membentuk ekosistem yang saling melengkapi dalam menjaga keamanan sistem elektronik. Setiap pihak memiliki peran yang jelas, mulai dari penyusunan regulasi, pelaksanaan audit, pemberian asistensi teknis, hingga implementasi langsung di lapangan. Meskipun terdapat dukungan dari berbagai pemangku kepentingan, tanggung jawab utama tetap berada pada PSE untuk memastikan sistem yang dikelola sesuai dengan standar keamanan yang ditetapkan. Pendekatan ini memungkinkan kolaborasi yang efektif sekaligus menjaga akuntabilitas.

5. Transparansi dan Kepatuhan
   Kewajiban bagi PSE untuk menyampaikan laporan penilaian mandiri, hasil audit, dan proses verifikasi oleh BSSN menjadi mekanisme penting dalam memastikan keterbukaan. Proses ini tidak hanya membantu regulator dalam memantau kesiapan dan kepatuhan PSE, tetapi juga memberikan jaminan kepada publik bahwa sistem yang digunakan telah melalui pengawasan yang terukur.

Peraturan BSSN Nomor 8 Tahun 2020 secara substansial mendukung terbentuknya kerangka kerja kepercayaan digital nasional melalui pendekatan sistematis terhadap keamanan informasi, tata kelola risiko, dan pelindungan data pribadi. Dengan penerapan peraturan ini, kepercayaan digital dapat dibangun di atas prinsip kebijakan yang kuat, terukur, dan berpihak pada kepentingan nasional.

4.5.12 Peraturan BSSN Nomor 4 Tahun 2021 tentang Pedoman Manajemen Keamanan Informasi Sistem Pemerintahan Berbasis Elektronik (SPBE)

Peraturan BSSN Nomor 4 Tahun 2021, yang ditetapkan pada 19 Mei 2021, mengatur pedoman manajemen keamanan informasi serta standar teknis dan prosedur keamanan dalam penyelenggaraan Sistem Pemerintahan Berbasis Elektronik (SPBE) di instansi pusat maupun daerah [307]. Peraturan ini merupakan pelaksanaan dari Pasal 41 ayat (4) dan Pasal 48 ayat (5) Perpres Nomor 95 Tahun 2018 tentang SPBE. Substansi pengaturannya mencakup perencanaan, dukungan operasional, evaluasi kinerja, dan perbaikan berkelanjutan dalam kerangka pengelolaan keamanan informasi yang efektif dan terukur.

1. Ruang Lingkup dan Definisi
   Peraturan ini menetapkan pedoman manajemen keamanan informasi dalam penyelenggaraan SPBE oleh instansi pusat dan pemerintahan daerah. Di dalamnya ditetapkan pula standar teknis serta prosedur yang mencakup keamanan data, aplikasi, jaringan intra, sistem penghubung layanan, dan pusat data nasional yang menjadi tulang punggung SPBE.

2. Manajemen Keamanan Informasi SPBE
   Ruang lingkup manajemen keamanan informasi meliputi penetapan penanggung jawab, perencanaan, dukungan operasional, evaluasi kinerja, serta perbaikan berkelanjutan. Tanggung jawab utama berada pada koordinator SPBE yang umumnya dijabat oleh sekretaris instansi pusat maupun daerah, sedangkan pelaksana teknis bertugas memastikan bahwa standar teknis dan prosedur keamanan benar-benar diterapkan pada aplikasi dan infrastruktur SPBE.

3. Perencanaan dan Pelaksanaan Keamanan
   Perencanaan mencakup program kerja edukasi kesadaran keamanan, penilaian kerentanan, peningkatan keamanan, penanganan insiden, serta audit keamanan SPBE. Edukasi dan pelatihan bagi sumber daya manusia ditempatkan sebagai aspek penting, sementara penilaian risiko dilakukan dengan menginventarisasi aset, mengidentifikasi kerentanan dan ancaman, serta mengukur risiko keamanan yang muncul. Hasil penilaian risiko kemudian digunakan untuk merancang langkah peningkatan keamanan, termasuk pengujian fungsi keamanan aplikasi maupun infrastruktur agar tetap andal.

4. Standar Teknis dan Prosedur Keamanan
   Standar yang ditetapkan berorientasi pada prinsip kerahasiaan, keaslian, keutuhan, kenirsangkalan, dan ketersediaan data atau informasi. Pengamanan

aplikasi SPBE berbasis web maupun mobile dilaksanakan melalui mekanisme autentikasi, manajemen sesi, validasi input, penerapan kriptografi, proteksi data, kontrol akses, dan penguatan keamanan jaringan. Selain itu, standar juga mengatur sistem penghubung layanan, termasuk keamanan interoperabilitas data, kontrol integrator, keamanan API, serta mekanisme migrasi data. Aspek keamanan jaringan intra dan pusat data nasional dijabarkan secara rinci baik secara teknis maupun manajerial, untuk mencegah akses tidak sah serta menjaga integritas dan ketersediaan layanan publik.

5. Evaluasi, Audit, dan Perbaikan Berkelanjutan
   Evaluasi kinerja SPBE dilakukan secara berkala, sekurang-kurangnya sekali dalam setahun oleh koordinator SPBE, yang juga bertanggung jawab mendukung pelaksanaan audit keamanan. Tindak lanjut dari proses ini adalah perbaikan yang dilakukan secara berkelanjutan agar standar keamanan selalu relevan dan dapat menjawab tantangan baru, sehingga tingkat keamanan SPBE terus meningkat dari waktu ke waktu.

Keterkaitan dengan Kerangka Kepercayaan Digital di Indonesia

Peraturan BSSN Nomor 4 Tahun 2021 tentang Pedoman Manajemen Keamanan Informasi Sistem Pemerintahan Berbasis Elektronik (SPBE) memberikan kontribusi strategis dalam pembangunan kerangka kepercayaan digital di Indonesia. Melalui pendekatan yang sistematis terhadap pengelolaan keamanan informasi, peraturan ini menekankan pentingnya ketahanan digital, transparansi tata kelola, serta perlindungan data dan privasi sebagai unsur integral dalam penyelenggaraan layanan publik berbasis elektronik.

Regulasi ini menggarisbawahi peran aktif pemerintah dalam memastikan keandalan sistem elektronik melalui mekanisme penunjukan penanggung jawab, pelaporan, audit, serta pengelolaan risiko yang terukur. Selain itu, penekanan pada interoperabilitas, pengendalian akses, dan penggunaan teknologi nasional mendukung terwujudnya sistem yang konsisten, tepercaya, dan mandiri secara digital.

Dengan demikian, implementasi prinsip-prinsip dalam peraturan ini bukan hanya memperkuat tata kelola SPBE, tetapi juga menjadi pilar penting dalam membangun kepercayaan masyarakat terhadap transformasi digital yang berlangsung di sektor publik. Keterkaitan ini memperkuat argumen bahwa keamanan informasi, kedaulatan teknologi, dan perlindungan hak digital merupakan komponen yang saling melengkapi dalam desain ekosistem kepercayaan digital nasional. Adapun keterkaitan tersebut meliputi :

1. Dasar Keamanan Informasi dan Perlindungan Data
   Peraturan ini menghadirkan standar teknis serta pedoman manajemen keamanan informasi yang menjadi basis utama dalam menjaga keamanan sekaligus privasi data. Aspek ini merupakan elemen esensial dalam membangun kepercayaan digital nasional. Lebih jauh, pengendalian terhadap keamanan data, aplikasi, dan jaringan berperan langsung dalam melindungi identitas digital

serta memastikan transaksi elektronik berlangsung secara aman dan andal.

2. Penguatan Tata Kelola dan Akuntabilitas
   Penetapan penanggung jawab keamanan dan pembentukan struktur manajemen yang jelas menjamin adanya tata kelola keamanan yang terorganisasi di seluruh tingkatan pemerintahan. Selain itu, kewajiban pelaporan, evaluasi, dan audit yang dilakukan secara sistematis memberikan mekanisme pemantauan yang transparan dan berkesinambungan, sehingga semakin memperkuat kepercayaan publik terhadap tata kelola digital.

3. Mendukung Implementasi Standar Keamanan Nasional dan Internasional
   Penerapan standar teknis dan prosedur yang rinci serta komprehensif memperkuat ekosistem digital nasional. Hal ini selaras dengan prinsip keamanan sebagai pilar utama dalam standar identitas digital terdesentralisasi (*Self Sovereign Identity*, SSI) maupun kerangka kepercayaan digital. Selain itu, regulasi ini juga memudahkan instansi dan penyelenggara sistem untuk memenuhi kewajiban keamanan siber sesuai ketentuan, sehingga memberikan keyakinan lebih besar kepada masyarakat sebagai pengguna layanan digital.

4. Meningkatkan Kesadaran dan Kompetensi SDM dalam Keamanan Digital
   Ketentuan mengenai edukasi dan pelatihan dalam penyelenggaraan SPBE sebagaimana diatur dalam peraturan ini menjadi instrumen penting untuk meningkatkan kapasitas sumber daya manusia. Upaya ini sangat relevan dalam kerangka kerja kepercayaan digital, karena memastikan tersedianya SDM yang kompeten dalam mengelola risiko serta menangani insiden siber dengan baik.

5. Mendukung Kontinuitas dan Resiliensi Layanan Digital Publik
   Pengaturan terkait penanganan insiden keamanan serta penyusunan rencana pemulihan berfungsi menjamin keberlangsungan pelayanan publik digital yang andal dan tidak terputus. Kontinuitas layanan ini merupakan aspek kritikal untuk mempertahankan kepercayaan masyarakat terhadap layanan pemerintah berbasis elektronik.

Peraturan BSSN Nomor 4 Tahun 2021 memberikan pedoman manajemen dan standar teknis keamanan informasi yang menyeluruh untuk sistem pemerintahan berbasis elektronik di Indonesia. Ini merupakan komponen penting dalam kerangka kerja kepercayaan digital karena memastikan perlindungan data, keamanan aplikasi, dan keberlanjutan layanan digital publik yang menjadi landasan kepercayaan pengguna dan masyarakat luas.

4.5.13 Peraturan BSSN Nomor 7 Tahun 2023 tentang Identifikasi Infrastruktur Informasi Vital (IIV)

Peraturan BSSN Nomor 7 Tahun 2023 tentang Identifikasi Infrastruktur Informasi Vital (IIV) ditetapkan pada 16 Oktober 2023, diundangkan dan mulai berlaku pada 3 November 2023 [308]. Peraturan ini merujuk pada amanat Pasal 6 ayat

(5) Perpres No. 82/2022 tentang Perlindungan Infrastruktur Informasi Vital yang mengharuskan BSSN melakukan identifikasi IIV. Untuk memahami lebih jauh substansi dan cakupan Peraturan ini, berikut disajikan poin-poin utama yang terkandung di dalamnya:

1. Tujuan dan Ruang Lingkup
   Peraturan ini menetapkan mekanisme pelaksanaan identifikasi IIV di Indonesia. Cakupannya meliputi penentuan kategori sistem elektronik, pengukuran tingkat vitalitas, pelaporan hasil identifikasi, proses verifikasi, hingga penetapan IIV beserta penyelenggaranya, serta evaluasi berkala terhadap status tersebut. Sebagai sistem elektronik yang memiliki peran strategis dalam sektor publik maupun kepentingan nasional, IIV dipandang krusial karena gangguan terhadapnya dapat menimbulkan dampak serius bagi keamanan, perekonomian, dan kepentingan umum.

2. Proses Identifikasi IIV
   Proses identifikasi dilakukan melalui klasifikasi kategori sistem elektronik strategis (tinggi atau rendah) berdasarkan potensi dampaknya. Pengukuran vitalitas mempertimbangkan aspek operasional, kerugian data, dampak finansial, kepentingan umum, pertahanan dan keamanan, serta keterkaitan antarlayanan. Penilaian awal dilaksanakan secara mandiri oleh PSE lingkup sektor IIV, yang kemudian diverifikasi oleh kementerian atau lembaga terkait. Mekanisme ini memastikan bahwa sistem yang ditetapkan sebagai IIV benar-benar memenuhi kriteria kritikalitas dan relevansi nasional.

3. Pelaporan dan Verifikasi
   Setiap PSE berkewajiban menyampaikan laporan hasil identifikasi beserta informasi pendukung kepada kementerian atau lembaga terkait, sekurang-kurangnya sekali dalam setahun. Laporan tersebut diverifikasi untuk memastikan kelengkapan dan kesesuaiannya, sebelum sistem elektronik tertentu ditetapkan secara resmi sebagai IIV dan PSE sebagai penyelenggaranya. Proses verifikasi ini berfungsi sebagai instrumen tata kelola yang menegakkan standar akuntabilitas dalam perlindungan infrastruktur digital vital.

4. Penetapan dan Evaluasi
   Penetapan IIV dilakukan dalam jangka waktu yang telah ditentukan setelah proses verifikasi selesai. Selanjutnya, evaluasi berkala dilaksanakan guna menjaga validitas data dan memastikan penyesuaian terhadap dinamika perubahan sistem elektronik. PSE juga diwajibkan melakukan identifikasi ulang apabila terjadi modifikasi signifikan pada sistem yang berpotensi mengubah tingkat vitalitasnya.

5. Dampak dan Ketergantungan
   Regulasi ini menekankan pentingnya pemetaan dampak secara rinci, baik terkait gangguan operasional, kerugian data, kerugian finansial, gangguan terhadap pelayanan publik, maupun implikasi bagi pertahanan dan keamanan. Selain itu, dipetakan pula rantai ketergantungan antarsektor, yang sering kali memperbesar risiko sistemik. Identifikasi keterkaitan lintas sektor ini menjadi

landasan kritis dalam menetapkan prioritas proteksi dan strategi mitigasi, sehingga ekosistem digital nasional dapat lebih resilien terhadap ancaman siber yang kompleks dan terintegrasi.

Peraturan BSSN Nomor 7 Tahun 2023 memiliki keterkaitan erat dengan Strategi Nasional, yang merupakan salah satu dari lima regulasi turunan Perpres Nomor 82 Tahun 2022. Regulasi turunan tersebut mencakup antara lain BSSN Nomor 8 Tahun 2023 tentang Pelindungan IIV, Nomor 9 Tahun 2023 tentang Pengembangan SDM, Nomor 10 Tahun 2023 tentang Kematangan Keamanan, serta Nomor 1 Tahun 2024 tentang Pengelolaan Insiden Siber. Kehadiran Peraturan BSSN No. 7/2023 diharapkan mampu memperkuat implementasi proteksi infrastruktur strategis secara sistematis melalui koordinasi lintas sektor, khususnya pada bidang TIK, transportasi, dan pemerintahan. Dalam menjaga keamanan nasional digital, Peraturan BSSN No. 7 Tahun 2023 merupakan landasan penting yang diharapkan :

1. Membakukan proses identifikasi infrastruktur vital.
2. Mengatur pelaporan, verifikasi, dan penetapannya.
3. Memastikan evaluasi terus-menerus agar kategori IIV selalu *up-to-date*.
4. Memperkuat perlindungan sistem kritik sesuai strategi nasional (Perpres 82/2022).

Keterkaitan dengan Kerangka Kerja Kepercayaan Digital di Indonesia

Peraturan BSSN Nomor 7 Tahun 2023 tentang Identifikasi Infrastruktur Informasi Vital (IIV) memiliki kaitan yang sangat erat dengan penyusunan Kerangka Kerja Kepercayaan Digital, hal ini dikarenakan keduanya mendukung penciptaan ekosistem digital nasional yang aman, andal, dan tepercaya. Adapun keterkaitan tersebut meliputi :

1. Keamanan sebagai pilar kepercayaan digital
   Kepercayaan digital menuntut adanya jaminan bahwa sistem elektronik yang mendukung layanan penting terlindungi dari gangguan, sabotase, maupun ancaman siber. Untuk menjawab kebutuhan ini, Peraturan ini hadir sebagai instrumen yang mengatur proses identifikasi dan klasifikasi terhadap sistem elektronik yang dianggap vital bagi keberlangsungan layanan publik dan keamanan nasional. Dengan menetapkan kewajiban bagi PSE untuk mengidentifikasi sistem vital serta mengukur potensi dampak dari gangguan, regulasi ini menjadi instrumen strategis dalam mencegah risiko sistemik akibat serangan siber. Pendekatan ini mencerminkan prinsip *security by design*, di mana kepercayaan dibangun sejak tahap perancangan sistem. Melalui identifikasi yang valid dan terverifikasi, regulasi ini diharapkan dapat meningkatkan kepercayaan publik dan pelaku ekonomi digital terhadap stabilitas serta keberlanjutan ekosistem layanan digital nasional.

2. Reliabilitas dan Ketahanan Sistem Layanan Publik
   Penilaian terhadap sistem berdasarkan skala vitalitas memungkinkan pemerintah dan sektor swasta/industri memastikan layanan digital yang esensial tetap berjalan dalam berbagai situasi darurat. Hal ini menciptakan keandalan yang menjadi dasar terbentuknya kepercayaan publik terhadap transformasi digital.

3. Menjamin Transparansi & Akuntabilitas
   Mekanisme tata kelola siber yang terstandar dan terbuka merupakan elemen krusial dalam penyusunan kerangka kerja kepercayaan digital. Peraturan ini memberikan landasan yang jelas dengan menetapkan prosedur pelaporan, verifikasi, dan evaluasi terhadap IIV. Melalui kewajiban pelaporan oleh PSE dan proses verifikasi independen oleh kementerian atau lembaga terkait, regulasi ini menjamin adanya kontrol dan akuntabilitas yang terukur. Pendekatan ini mencerminkan penerapan prinsip *trust through governance*, di mana kepercayaan dibangun melalui tata kelola yang transparan, bertanggung jawab, dan berorientasi pada perlindungan sistem yang strategis.

4. Mendorong Kepatuhan dan Akuntabilitas PSE
   Dalam kerangka kepercayaan digital, kewajiban PSE untuk melaporkan dan bekerja sama dalam identifikasi IIV menciptakan budaya akuntabilitas. Hal ini dirasa penting guna membangun kepercayaan antarlembaga, antara pemerintah dan swasta/industri, serta dengan masyarakat.

5. Interdependensi Lintas Sektor dan Kolaborasi Nasional
   Peraturan ini mengakui dan mengatur dampak keterhubungan antarsistem elektronik yang menunjang layanan vital, yang seringkali saling bergantung lintas sektor. Dalam konteks tersebut, Peraturan ini mendukung pengembangan arsitektur kepercayaan digital nasional yang berbasis kolaborasi antarsektor dan lintas tingkatan pemerintahan. Kepercayaan digital pada dasarnya memerlukan keterlibatan berbagai pihak, termasuk penyelenggara infrastruktur TIK, sektor transportasi, keuangan, pemerintahan, dan sektor-sektor strategis lainnya. Melalui mekanisme identifikasi yang sistematis, regulasi ini membantu setiap sektor memahami peran dan tanggung jawabnya dalam menjaga keamanan dan keberlangsungan ekosistem digital nasional.

6. Landasan untuk Infrastruktur Informasi Vital (IIV)
   Konsep IIV yang diatur dalam regulasi ini sejalan dengan pendekatan pengamanan infrastruktur kritikal nasional. Dengan menjadikan keamanan dan integritas layanan IIV sebagai prioritas, negara secara aktif membangun ekosistem digital yang tahan terhadap disrupsi.

Peraturan BSSN Nomor 7 Tahun 2023 tidak hanya merupakan instrumen teknokratis dalam pengelolaan sistem elektronik vital, tetapi juga memainkan peran strategis dalam menyusun dasar kepercayaan digital nasional. Melalui pendekatan berbasis risiko, penguatan koordinasi kelembagaan, dan fokus pada perlindungan layanan esensial, peraturan ini dapat dijadikan pilar utama dalam pembangunan kerangka

kerja kepercayaan digital yang aman, andal, kolaboratif dan berkelanjutan di Indonesia.

4.5.14 Peraturan BSSN Nomor 8 Tahun 2023 tentang Kerangka Kerja Pelindungan Infrastruktur Informasi Vital

Peraturan BSSN Nomor 8 Tahun 2023 ditetapkan pada 16 Oktober 2023 sebagai peraturan turunan dari Pasal 7 ayat (4) Perpres Nomor 82 Tahun 2022 tentang Pelindungan Infrastruktur Informasi Vital (IIV) [309]. Peraturan ini dirancang untuk membentuk kerangka kerja nasional dalam pelindungan IIV, dengan memberikan pedoman menyeluruh kepada sektor-sektor penyelenggara dalam menerapkan kontrol keamanan siber yang terstruktur dan berlapis. Tujuan utamanya adalah memperkuat ketahanan nasional terhadap insiden siber yang berpotensi mengganggu kepentingan publik, pertahanan, keamanan, serta stabilitas ekonomi nasional. Untuk memahami lebih jauh substansi dan cakupan Peraturan ini, berikut disajikan poin-poin utama yang terkandung di dalamnya:

1. Pengertian dan Ruang Lingkup
   Kerangka Kerja Pelindungan IIV dipahami sebagai seperangkat konsep dasar dan pedoman yang berfungsi untuk menyusun, menerapkan, dan mengomunikasikan aktivitas pengelolaan keamanan siber pada sektor-sektor yang dikategorikan sebagai IIV. Infrastruktur Informasi Vital sendiri mencakup sistem elektronik yang memiliki peran kritis dan apabila terganggu dapat menimbulkan dampak serius terhadap masyarakat, pelayanan publik, pertahanan dan keamanan negara, serta stabilitas perekonomian. Ruang lingkup kerangka kerja ini meliputi penyelenggaraan pelindungan IIV, kegiatan pembinaan dan pengawasan, serta pemanfaatan teknologi perlindungan yang relevan.

2. Domain Kerangka Kerja Pelindungan
   Pelindungan terhadap IIV dilaksanakan melalui penerapan kontrol keamanan yang dikelompokkan ke dalam empat domain utama. Domain *Identifikasi* menekankan pemahaman konteks organisasi, aset yang dimiliki, peran serta tanggung jawab, strategi yang digunakan, tingkat risiko yang dihadapi, hingga keterhubungan dalam rantai pasok. Domain *Proteksi* berfokus pada perlindungan identitas, mekanisme autentikasi dan kontrol akses, serta pengamanan aset fisik, data, aplikasi, jaringan, dan sumber daya manusia. Domain *Deteksi* menitikberatkan pada upaya pemantauan serta analisis peristiwa dan anomali siber secara tepat waktu dan berkesinambungan. Sementara itu, domain *Penanggulangan dan Pemulihan* mencakup penyusunan rencana respons, pelaksanaan mitigasi, upaya pemulihan pascainsiden, serta peningkatan keamanan secara berkelanjutan.

3. Aktivitas dan Pengelolaan
   Setiap penyelenggara IIV memiliki kewajiban untuk menetapkan serta mengomunikasikan kebijakan keamanan siber secara jelas dan konsisten. Pengelolaan

inventaris aset dan penilaian risiko keamanan siber harus dilakukan secara berkelanjutan sebagai bagian dari tata kelola. Pengaturan risiko rantai pasok dan bentuk kolaborasi dengan pihak ketiga menjadi komponen yang tidak terpisahkan dalam sistem perlindungan. Selain itu, pengelolaan identitas, kontrol akses, dan autentikasi menuntut prosedur yang ketat, berlapis, serta diaudit secara berkala. Dari sisi teknologi, berbagai perangkat dan sistem pelindung digunakan untuk memastikan integritas, keandalan, dan keamanan data maupun jaringan. Tidak kalah penting, pelatihan serta pengelolaan sumber daya manusia perlu diperkuat agar kesadaran dan kompetensi dalam keamanan siber tetap terjaga.

4. Pengawasan dan Pembinaan
   Tugas pembinaan dan pengawasan dilaksanakan oleh kementerian atau lembaga di masing-masing sektor, dengan koordinasi dan pengawasan nasional berada di bawah BSSN. Mekanisme pengawasan mencakup simulasi kesiapsiagaan insiden siber, pengujian keamanan secara terukur, serta evaluasi atas implementasi peta jalan perlindungan yang telah disusun oleh sektor terkait. Hal ini bertujuan memastikan konsistensi dan efektivitas penerapan pelindungan IIV di seluruh ekosistem digital nasional.

5. Peta Jalan Perlindungan
   Setiap sektor IIV diwajibkan menyusun peta jalan perlindungan dengan cakupan waktu lima tahun. Dokumen ini berisi analisis strategi, penetapan sasaran, target penerapan kontrol keamanan, serta rencana kerja perlindungan yang bersifat spesifik dan disesuaikan dengan karakteristik masing-masing sektor. Peta jalan tersebut menjadi acuan untuk memastikan bahwa pelindungan IIV dilakukan secara sistematis, terukur, dan berkesinambungan.

Keterkaitan dengan Kerangka Kerja Kepercayaan Digital di Indonesia

Peraturan ini merupakan komponen kunci dalam membangun dan memperkuat kerangka kepercayaan digital di Indonesia, dengan keterkaitan sebagai berikut:

1. Keamanan sebagai Dasar Kepercayaan Digital
   Peraturan ini menetapkan standar minimum bagi sistem elektronik vital, sehingga membangun fondasi kepercayaan publik terhadap layanan digital nasional. Dengan penguatan keamanan infrastruktur digital, masyarakat dan pelaku usaha dapat lebih yakin bahwa layanan berbasis elektronik terlindungi dari potensi ancaman.

2. Pendekatan Berbasis Risiko (*Risk-Based Trust*)
   Penerapan manajemen risiko dalam domain identifikasi dan proteksi mendorong setiap penyelenggara sistem elektronik untuk memahami kerentanan, ancaman, dan toleransi risiko. Pendekatan ini menjadikan kepercayaan publik tidak hanya bergantung pada keamanan teknis, tetapi juga pada pengelolaan risiko yang terdokumentasi dan terukur.

3. Transparansi dan Akuntabilitas Siber
   Kewajiban penyusunan peta jalan perlindungan, pelaporan insiden, serta audit keamanan menghadirkan transparansi dalam tata kelola keamanan siber. Hal ini membangun akuntabilitas publik terhadap pengelolaan infrastruktur digital sekaligus memperkuat legitimasi kebijakan di tingkat nasional.

4. Resiliensi dan Kesiapsiagaan Ekosistem Digital
   Regulasi ini menekankan pentingnya pembentukan rencana pengelolaan insiden, pemulihan yang sistematis, serta simulasi berkala. Dengan demikian, ekosistem digital tetap tangguh dan berfungsi meski terjadi serangan, sehingga menjaga kepercayaan masyarakat pada layanan vital.

5. Penguatan Kapabilitas SDM dan Organisasi
   Aspek pembinaan, pelatihan, serta peningkatan kompetensi sumber daya manusia merupakan bagian integral dalam regulasi ini. Kapasitas SDM yang memadai memastikan bahwa pengelolaan keamanan siber tidak hanya berbasis teknologi, tetapi juga budaya kerja yang berkesadaran tinggi.

6. Kolaborasi Lintas Sektor dan *Multi-Stakeholder*
   Koordinasi antara kementerian, lembaga, serta penyelenggara IIV diwajibkan untuk membangun ekosistem kepercayaan digital yang saling mendukung. Mekanisme peta jalan sektoral yang disusun secara partisipatif memperlihatkan bahwa keamanan digital merupakan tanggung jawab bersama, bukan hanya satu pihak.

7. Penegakan Standar dan Kepastian Regulasi
   Sertifikasi perangkat teknologi, pengawasan terpadu oleh BSSN, serta audit keamanan menciptakan kepastian regulasi bagi penyelenggara IIV. Kepastian ini menjadi unsur penting untuk membangun kepercayaan digital yang kokoh sekaligus memberikan kepastian hukum bagi para pemangku kepentingan.

8. Dasar Pengembangan Ekosistem Digital Nasional
   Sebagai pedoman implementasi Perpres No. 82 Tahun 2022, peraturan ini memperkuat strategi jangka panjang pemerintah dalam membangun ekosistem digital nasional yang aman, andal, dan tepercaya. Dengan demikian, regulasi ini berfungsi tidak hanya sebagai instrumen teknis, tetapi juga sebagai landasan strategis untuk mencapai visi Indonesia Emas 2045.

Peraturan BSSN Nomor 8 Tahun 2023 memberikan kerangka kerja komprehensif yang mengatur perlindungan Infrastruktur Informasi Vital sebagai fondasi keamanan digital nasional. Kerangka kerja ini sangat relevan dan menjadi inti dalam penyusunan kerangka kerja kepercayaan digital di Indonesia, khususnya untuk memastikan bahwa identitas digital dan layanan digital nasional dapat beroperasi dengan aman, andal, dan dapat dipercaya oleh masyarakat luas serta para pemangku kepentingan. Dengan implementasi yang konsisten dan berkelanjutan, kerangka kerja pelindungan IIV ini akan memperkuat ekosistem digital Indonesia, menegakkan prinsip kedaulatan data, menjaga privasi, dan meningkatkan ketahanan nasional terhadap ancaman siber yang kian kompleks.

4.5.15 Peraturan BSSN Nomor 9 Tahun 2023 tentang Peningkatan Kapasitas Sumber Daya Manusia di Bidang Keamanan Siber dan Sandi

Peraturan BSSN No. 9 Tahun 2023 ditetapkan pada 16 Oktober 2023 berisi tentang pedoman resmi BSSN mengenai upaya peningkatan kapasitas Sumber Daya Manusia (SDM) dalam keamanan siber dan persandian (KSS) [310]. Selain itu, peraturan ini juga menjadi acuan bagi penyelenggara IIV dalam membangun kompetensi SDM KSS sesuai kebutuhan nasional. Untuk memahami lebih jauh substansi dan cakupan Peraturan ini, berikut disajikan poin-poin utama yang terkandung di dalamnya:

1. Tujuan dan Ruang Lingkup
   Peraturan ini dirancang sebagai pedoman bagi kementerian, lembaga, serta PSE dalam upaya meningkatkan kualitas dan kuantitas SDM di bidang keamanan siber dan sandi. Fokus utamanya adalah membentuk SDM yang profesional, bertanggung jawab, dan berdaya saing, sehingga mampu menjawab tantangan ekosistem digital yang semakin kompleks.

2. Definisi Kunci
   Regulasi ini memberikan kejelasan atas istilah-istilah penting. SDM bidang keamanan siber dan sandi merujuk pada individu yang menjalankan tugas atau profesi di sektor tersebut. Peningkatan kapasitas SDM dipahami sebagai upaya yang mencakup penguatan kompetensi, penyediaan sertifikasi, alih teknologi dan keahlian, serta pembangunan budaya kesadaran keamanan informasi. PSE didefinisikan sebagai organisasi maupun perorangan yang menyediakan, mengelola, atau mengoperasikan sistem elektronik yang relevan.

3. Kewajiban dan Tanggung Jawab
   Setiap PSE memiliki kewajiban untuk menyelenggarakan program peningkatan kapasitas SDM, mulai dari penyediaan tenaga kerja hingga penguatan kompetensi, sertifikasi, alih teknologi dan keahlian, serta pembangunan budaya kesadaran keamanan informasi. Kementerian dan lembaga terkait bertanggung jawab dalam mengoordinasikan pelaksanaan program ini di lingkup sektoral, sementara BSSN memegang peran sebagai koordinator utama pada tingkat nasional.

4. Pelaksanaan Peningkatan Kapasitas
   Pelaksanaan peningkatan kapasitas SDM dilakukan secara terstruktur. Pertama, penyediaan SDM dilaksanakan melalui penghitungan kebutuhan berdasarkan karakteristik jabatan dan okupasi, kemudian dipenuhi melalui mekanisme rekrutmen dan penugasan. Kedua, peningkatan kompetensi dilakukan melalui pendidikan formal maupun nonformal dengan mengacu pada standar kompetensi nasional, termasuk SKKNI bidang keamanan siber dan sandi. Ketiga, sertifikasi kompetensi dilaksanakan berdasarkan uji kompetensi oleh lembaga sertifikasi profesi yang terdaftar, atau instansi pembina SDM aparatur sipil negara. Keempat, alih teknologi dan keahlian diprioritaskan kepada tenaga

kerja Indonesia, dengan keterlibatan tenaga kerja asing hanya bila diperlukan dan tetap disertai mekanisme pendampingan. Terakhir, peningkatan budaya kesadaran diwujudkan melalui program edukasi dan promosi yang berkelanjutan untuk membentuk perilaku aman dalam pengelolaan informasi.

5. Evaluasi dan Pelaporan
   Setiap PSE berkewajiban melaksanakan evaluasi tahunan terhadap program peningkatan kapasitas yang telah dijalankan, dan hasilnya wajib dilaporkan kepada kementerian atau lembaga terkait. Selanjutnya, kementerian atau lembaga menyampaikan hasil evaluasi sektoral tersebut kepada BSSN untuk dilakukan evaluasi di tingkat nasional. Evaluasi ini meliputi aspek-aspek seperti jenis kegiatan pelatihan, sasaran peserta, target, serta capaian yang diperoleh, sehingga implementasi dapat dipantau secara akuntabel dan konsisten.

6. Pendanaan
   Pembiayaan kegiatan peningkatan kapasitas SDM bersumber dari anggaran masing-masing PSE, kementerian atau lembaga, BSSN, maupun sumber sah lainnya sesuai ketentuan hukum. Dengan adanya skema pendanaan ini, pelaksanaan program diharapkan dapat berjalan berkesinambungan dan mendukung peningkatan kualitas keamanan siber nasional secara menyeluruh.

Keterkaitan dengan Kerangka Kerja Kepercayaan Digital di Indonesia

Peraturan BSSN Nomor 9 Tahun 2023 tentang Peningkatan Kapasitas Sumber Daya Manusia di Bidang Keamanan Siber dan Sandi memiliki peran strategis dalam mendukung terbentuknya kerangka kerja kepercayaan digital nasional. Penguatan kompetensi SDM bukan hanya menjadi kebutuhan teknis, tetapi juga menjadi elemen penting dalam membangun ekosistem digital yang andal, aman, dan tepercaya. Regulasi ini mendorong terselenggaranya program pelatihan, sertifikasi, dan pembinaan SDM yang sesuai dengan standar keamanan siber nasional maupun global, yang secara langsung memperkuat pilar-pilar utama kepercayaan digital berikut:

1. Pilar SDM Profesional untuk Kepercayaan Digital
   Kualitas sumber daya manusia menjadi fondasi utama dalam membangun ekosistem kepercayaan digital yang aman dan andal. Kapasitas SDM di bidang keamanan siber memperkuat kemampuan organisasi dalam mengelola risiko digital serta menghadapi insiden siber. Melalui sertifikasi dan penerapan standar kompetensi, lahir tenaga ahli yang tepercaya dan berkompeten dalam mengimplementasikan teknologi maupun kebijakan keamanan digital sesuai standar nasional dan internasional.

2. Mendukung Tata Kelola dan Kepatuhan Regulasi
   Peningkatan kapasitas SDM dan penguatan budaya kesadaran keamanan siber turut mendukung kelancaran penerapan regulasi, seperti Undang-Undang Pelindungan Data Pribadi, Perpres tentang Pelindungan Infrastruktur Informasi Vital, serta standar lain yang dikeluarkan BSSN. Koordinasi yang

erat antara BSSN, kementerian/lembaga, dan PSE memastikan konsistensi dan keselarasan pelaksanaan kebijakan keamanan digital di tingkat sektor maupun nasional.

3. Memperkuat Resiliensi dan Respons Insiden
   SDM yang terlatih dan tersertifikasi mampu meningkatkan efektivitas deteksi, penanggulangan, serta pemulihan insiden siber. Hal ini menjadi elemen penting dalam menjaga kepercayaan masyarakat dan pemangku kepentingan terhadap layanan maupun identitas digital nasional. Selain itu, penguatan budaya kesadaran keamanan berperan menekan risiko kebocoran data dan mengurangi kesalahan manusia yang berpotensi merusak kepercayaan digital.

4. Penyiapan Ekosistem Kepercayaan Digital yang Berkelanjutan
   Transfer pengetahuan dan alih teknologi menjadi pendorong utama dalam memperkuat ketahanan digital sekaligus mendorong inovasi. Evaluasi yang dilakukan secara berkelanjutan, disertai pelaporan yang transparan, meningkatkan akuntabilitas dalam pengelolaan kepercayaan digital di tingkat SDM maupun organisasi. Proses pelaporan dan verifikasi juga menjamin konsistensi penerapan standar keamanan siber, sehingga membangun ekosistem kepercayaan digital yang adaptif dan berkelanjutan.

Peraturan BSSN Nomor 9 Tahun 2023 ini menjadi pilar penting dalam membangun kerangka kerja kepercayaan digital Indonesia dengan menekankan pada peningkatan kapasitas SDM bidang keamanan siber dan sandi. Kualitas dan kompetensi SDM yang memadai mendukung implementasi teknologi, tata kelola, dan kebijakan yang diperlukan agar identitas digital dan layanan digital nasional dapat dipercaya, aman, dan tahan terhadap ancaman siber.

4.5.16 Peraturan BSSN Nomor 10 Tahun 2023 tentang Pengukuran Tingkat Kematangan Keamanan Siber

Peraturan yang ditetapkan pada 16 Oktober 2023 ini mengatur tentang *Pengukuran Tingkat Kematangan Keamanan Siber* bagi penyelenggara Infrastruktur Informasi Vital (IIV). Peraturan ini merupakan tindak lanjut dari Pasal 22 ayat (7) Perpres Nomor 82 Tahun 2022 tentang Pelindungan IIV, dengan tujuan untuk menilai sejauh mana penyelenggara IIV mengimplementasikan sistem keamanan siber yang efektif, terstruktur, dan berkelanjutan. Untuk memahami lebih jauh substansi dan cakupan Peraturan ini, berikut disajikan poin-poin utama yang terkandung di dalamnya:

1. Tujuan dan Definisi Utama
   Peraturan ini berfokus pada pelaksanaan pengukuran tingkat kematangan keamanan siber pada Penyelenggara IIV sebagai tindak lanjut dari Perpres No. 82 Tahun 2022. Tingkat kematangan tersebut merepresentasikan kondisi kapabilitas organisasi dalam mengimplementasikan, meningkatkan, dan menjalankan praktik keamanan siber secara efektif serta efisien.

2. Ruang Lingkup Pengukuran
   Pengukuran tingkat kematangan wajib dilakukan minimal sekali dalam setahun oleh Penyelenggara IIV secara mandiri. Domain yang diukur merujuk pada kerangka kerja pelindungan IIV, yang mencakup aspek identifikasi (peran, kebijakan, aset, dan risiko), proteksi (identitas, data, aplikasi, jaringan, dan sumber daya manusia), deteksi (monitoring serta analisis peristiwa siber), serta penanggulangan dan pemulihan (meliputi rencana tanggap, mitigasi, dan pemulihan insiden).

3. Instrumen dan Metode Penilaian
   Instrumen penilaian disusun oleh BSSN dan berisi indikator evaluasi terhadap penerapan tiap domain dalam kerangka kerja. Kementerian atau lembaga dapat menggunakan instrumen lain, sepanjang tetap mengacu pada instrumen resmi yang ditetapkan BSSN. Verifikasi hasil pengukuran dilakukan dengan berbagai metode, antara lain telaah dokumen, wawancara, observasi lapangan, serta pemeriksaan kesesuaian dokumen dengan praktik di lapangan.

4. Kategori Tingkat Kematangan
   Tingkat kematangan keamanan siber dibagi ke dalam lima level. Level Awal (indeks 0–1,5) menggambarkan kondisi penerapan yang masih informal dan belum konsisten. Level Berulang (1,51–2,5) menunjukkan penerapan mulai dilakukan secara berulang namun tetap belum konsisten. Level Terdefinisi (2,51–3,5) ditandai dengan penerapan yang jelas dan formal, disertai reviu berkala. Level Terkelola (3,51–4,5) menunjukkan bahwa penerapan sudah terorganisir dengan baik dan berorientasi pada perbaikan berkelanjutan, meskipun belum sepenuhnya otomatis. Level Inovatif (4,51–5,0) menggambarkan kondisi penerapan yang optimal, terintegrasi, otomatis, dan sudah menumbuhkan budaya keamanan siber yang melekat dalam organisasi.

5. Pelaporan dan Verifikasi
   Hasil pengukuran wajib dilaporkan kepada kementerian atau lembaga terkait, yang selanjutnya menyampaikannya kepada BSSN. Proses verifikasi dilakukan secara terstruktur oleh kementerian/lembaga bersama BSSN, dan hasil verifikasi tersebut dikomunikasikan kembali kepada Penyelenggara IIV. Dengan adanya mekanisme pelaporan dan verifikasi ini, akuntabilitas serta konsistensi penerapan keamanan siber di seluruh sektor IIV dapat terjamin.

Keterkaitan dengan Kerangka Kerja Kepercayaan Digital di Indonesia

Kerangka kerja kepercayaan digital merupakan dasar untuk menjamin interaksi digital yang aman dan tepercaya antara pemerintah, bisnis, dan masyarakat. Kerangka kerja ini mencakup aspek identitas digital, keamanan data, infrastruktur digital, dan tata kelola yang akuntabel. Kepercayaan digital tidak dapat dibangun tanpa landasan keamanan siber yang kuat. Adapun keterkaitan tersebut meliputi :

1. Mengukur Tingkat Keamanan sebagai Dasar Kepercayaan
   Pengukuran kematangan keamanan siber dipandang sebagai alat strategis yang

berfungsi menilai sejauh mana kesiapan dan efektivitas proteksi terhadap sistem, data, dan identitas digital telah tercapai dalam ekosistem digital nasional. Tingkat kematangan yang baik menggambarkan sistem digital yang andal serta aman, yang pada gilirannya meningkatkan kepercayaan pengguna maupun pemangku kepentingan.

2. Memperkuat Tata Kelola dan Standarisasi Operasi
   Sesuai Peraturan ini, penilaian tingkat kematangan dilakukan berdasarkan empat domain utama, yaitu identifikasi, proteksi, deteksi, dan penanggulangan. Keempat domain ini menjadi dasar untuk penerapan standar keamanan siber yang selaras dengan regulasi pelindungan IIV, termasuk proteksi data dan mekanisme kontrol akses dalam pengelolaan identitas digital. Standarisasi tersebut memungkinkan harmonisasi prosedur dan praktik keamanan lintas sektor, sehingga konsistensi tata kelola keamanan dapat terjaga di berbagai organisasi.

3. Mendorong Pembelajaran dan Perbaikan Berkelanjutan
   Peraturan ini mengatur agar hasil penilaian tidak berhenti pada asesmen semata, tetapi ditindaklanjuti dengan rekomendasi peningkatan kapasitas. Evaluasi berkala yang diikuti dengan proses verifikasi memberi peluang bagi organisasi untuk mengidentifikasi kelemahan yang ada sekaligus membangun strategi perbaikan yang lebih adaptif terhadap ancaman baru. Tingkat kematangan yang tinggi juga menjadi indikator bahwa budaya keamanan telah terintegrasi ke dalam organisasi, sehingga ketahanan ekosistem digital nasional semakin diperkuat.

4. Mendukung Regulasi dan Kebijakan Keamanan Digital Nasional
   Laporan hasil penilaian yang disampaikan oleh penyelenggara IIV kepada BSSN menyediakan data penting bagi regulator. Data tersebut dapat dimanfaatkan untuk merumuskan kebijakan perlindungan data, identitas digital, dan keamanan infrastruktur yang berbasis bukti. Mekanisme ini juga memastikan bahwa Penyelenggara IIV maupun penyelenggara sistem elektronik lainnya mematuhi standar keamanan yang dipantau secara konsisten, sehingga tercipta ekosistem digital yang lebih aman dan tepercaya.

Peraturan BSSN Nomor 10 Tahun 2023 dengan jelas memberikan kerangka sistematis untuk melakukan penilaian kematangan keamanan siber, melaporkan hasilnya kepada BSSN, dan menindaklanjutinya dengan langkah peningkatan berkelanjutan. Kerangka ini sangat penting dalam konteks kepercayaan digital Indonesia karena menyediakan dasar objektif untuk menilai, membina, dan mengawasi pelaksanaan keamanan siber secara nasional.

4.5.17 Peraturan BSSN Nomor 1 Tahun 2024 tentang Pengelolaan Insiden Siber

Peraturan yang ditetapkan pada 10 Januari 2024 ini mengatur tentang *Pengelolaan Insiden Siber* sebagai upaya sistematis untuk mencegah, mendeteksi, menanggula-

ngi, dan memulihkan insiden yang mengancam keamanan siber nasional. Regulasi ini merupakan tindak lanjut dari Perpres Nomor 82 Tahun 2022 tentang Pelindungan IIV, yang mengamanatkan pentingnya mekanisme tanggap insiden yang terkoordinasi di berbagai sektor. Tujuannya adalah memastikan keberlangsungan layanan sistem elektronik, memperkuat respons nasional terhadap serangan siber, serta meningkatkan resiliensi infrastruktur digital strategis. Substansi pengaturan mencakup pembentukan TTIS, standar pelaporan dan penanganan insiden, serta mekanisme pencegahan, pembelajaran, dan pemulihan secara terintegrasi [311].

1. Tujuan dan Ruang Lingkup
   Peraturan ini merupakan tindak lanjut dari sejumlah regulasi strategis siber nasional, termasuk Perpres Nomor 82 Tahun 2022 tentang Pelindungan IIV. Fokus utama dari peraturan ini adalah pembentukan, penugasan, serta tata cara kerja TTIS pada tingkat nasional, sektoral, dan organisasi. Selain itu, regulasi ini juga menekankan pentingnya standar pelaporan, penanganan, dan kesiapan menghadapi insiden siber yang dapat memengaruhi sistem elektronik kritikal.

2. Definisi Kunci
   Dalam konteks regulasi ini, keamanan siber dipahami sebagai upaya perlindungan ruang siber dari berbagai ancaman baik yang bersifat teknis maupun sosial. Insiden siber didefinisikan sebagai satu atau serangkaian kejadian yang berpotensi mengganggu atau mengancam kelangsungan operasional sistem elektronik, termasuk infrastruktur informasi vital. Adapun yang dimaksud dengan IIV adalah infrastruktur penting yang apabila terganggu dapat menimbulkan dampak besar terhadap masyarakat luas maupun negara.

3. Organisasi dan Registrasi TTIS
   Penanganan insiden siber dilaksanakan secara berjenjang melalui TTIS pada tingkat organisasi, TTIS sektoral yang berada di bawah kementerian atau lembaga, dan TTIS nasional yang dikoordinasikan oleh BSSN. Seluruh TTIS diwajibkan untuk terdaftar dan diverifikasi oleh TTIS nasional guna menjamin koordinasi, validasi, serta respons yang terintegrasi terhadap setiap insiden. Proses registrasi mencakup penilaian profil dan legalitas tim, pendataan aset elektronik, serta evaluasi kompetensi sumber daya manusia. Registrasi ini juga harus sesuai dengan kriteria yang diatur dalam RFC 2350 sebagai standar global bagi tim tanggap insiden siber.

4. Standar Pelaporan dan Penanganan Insiden Siber
   Setiap insiden siber yang memiliki tingkat risiko tinggi harus dilaporkan kepada TTIS pada tingkat yang lebih tinggi dalam waktu maksimal satu kali dua puluh empat jam. Laporan sekurang-kurangnya berisi identitas pelapor, deskripsi insiden, kronologi kejadian, serta dampak yang ditimbulkan. Penanganan insiden meliputi langkah-langkah isolasi, mitigasi, analisis forensik, eradikasi, pemulihan, serta penyusunan dokumentasi teknis. Di samping itu, komunikasi publik mengenai insiden harus dilakukan secara transparan guna

menjaga kepercayaan masyarakat. Untuk meningkatkan kesiapsiagaan, simulasi serta pembaruan rencana tanggap insiden diwajibkan dilakukan secara berkala.

5. Pencegahan dan Pembelajaran Insiden Siber
   Setiap insiden siber yang terjadi wajib dijadikan dasar pembelajaran dalam memperbaiki efektivitas kontrol keamanan, memperkuat kebijakan, serta meningkatkan keterampilan sumber daya manusia yang terlibat dalam pengelolaan keamanan siber. Proses diseminasi dan berbagi informasi mengenai insiden dilakukan dengan mengacu pada *Traffic Light Protocol* (TLP), yang mengatur tingkat kerahasiaan dan distribusi informasi. Dengan cara ini, kolaborasi baik di tingkat nasional maupun internasional dapat lebih efektif dalam mencegah kejadian serupa.

6. Ketentuan Teknis Kesiapsiagaan dan Pemulihan
   Setiap organisasi diwajibkan menyusun dan memperbarui rencana tanggap insiden serta rencana keberlangsungan layanan secara berkelanjutan. Proses pencadangan (*backup*), pemulihan data, dan pengelolaan aset informasi dilaksanakan dengan mekanisme enkripsi serta kontrol keamanan yang disesuaikan dengan tingkat risiko. Langkah ini bertujuan untuk menjamin keberlangsungan sistem elektronik meskipun menghadapi serangan atau gangguan siber yang signifikan.

Keterkaitan dengan Kerangka Kerja Kepercayaan Digital di Indonesia

Penyusunan kerangka kerja kepercayaan digital di Indonesia perlu mempertimbangkan berbagai pilar utama yang memperkuat keamanan, transparansi, dan akuntabilitas dalam ekosistem digital nasional. Regulasi terkait keamanan siber dan tata kelola respons insiden menjadi salah satu landasan penting. Berikut adalah keterkaitan pilar-pilar kepercayaan digital dengan kerangka kerja yang diusulkan:

1. Pilar Kepercayaan Digital: Keamanan Siber dan Respons Insiden
   Kerangka kerja kepercayaan digital menempatkan aspek keamanan siber dan respons insiden sebagai fondasi utama. Penetapan TTIS serta standar pelaporan dan penanganan insiden siber dalam regulasi berfungsi sebagai mekanisme untuk menjaga stabilitas dan keandalan ekosistem digital nasional. Dengan adanya prosedur yang jelas dan terstruktur, setiap potensi ancaman dapat ditangani secara sistematis sehingga mencegah meluasnya dampak serangan. Lebih jauh, kepercayaan publik dibangun melalui registrasi dan audit TTIS yang memastikan kepatuhan penyelenggara sistem terhadap standar keamanan yang berlaku. Transparansi juga diperkuat melalui komunikasi publik mengenai insiden siber, yang tidak hanya menumbuhkan akuntabilitas dalam tata kelola, tetapi juga memberikan keyakinan bahwa mekanisme perlindungan selalu berjalan. Dengan demikian, keamanan yang kuat dan tata kelola yang transparan membentuk dasar kepercayaan digital yang berkelanjutan.

2. Proses dan Standar Nasional
   Kerangka kepercayaan digital tidak dapat dilepaskan dari pentingnya proses dan standar nasional yang menjadi rujukan bersama. Standarisasi registrasi sesuai RFC 2350, mekanisme pelaporan cepat, serta forum berbagi informasi siber berperan memperkuat interoperabilitas dan koordinasi antarlembaga maupun sektor. Keberlangsungan layanan digital juga dijaga melalui perencanaan kontinuitas, *backup* berlapis, dan skema pemulihan, yang memastikan identitas dan data digital tetap terlindungi meskipun terjadi insiden. Selanjutnya, prinsip transparansi diwujudkan dalam bentuk diseminasi informasi melalui TLP, publikasi hasil forensik, serta strategi komunikasi publik yang konsisten, sehingga akuntabilitas terbangun dan kepercayaan masyarakat semakin kokoh.

3. Penguatan Regulasi dan Reputasi Digital Nasional
   Aspek regulasi memiliki peran krusial dalam memperkuat kepercayaan digital. Harmonisasi Peraturan BSSN dengan berbagai regulasi terkait, seperti UU PDP, Perpres SPBE, dan Perpres IIV, menciptakan ekosistem kebijakan yang lebih terpadu dalam keamanan siber. Selain itu, kewajiban pelaporan dan proses pembelajaran dari setiap insiden siber menambah lapisan akuntabilitas, yang tidak hanya meningkatkan kepercayaan *stakeholder* tetapi juga mencegah terulangnya kasus serupa. Di sisi lain, pemberdayaan sumber daya manusia melalui pelatihan, simulasi, dan evaluasi kinerja TTIS semakin memperkuat kemampuan respons dan adaptasi. Hal ini menjadikan kualitas SDM sebagai faktor penentu tingkat kepercayaan publik terhadap sistem digital nasional.

4. Kolaborasi Lintas Sektor dan Internasional
   Keberhasilan kerangka kerja kepercayaan digital juga ditentukan oleh sejauh mana kolaborasi lintas sektor dan dukungan internasional dapat terwujud. Keterlibatan komunitas, akademisi, dan praktisi dalam ekosistem TTIS nasional membuka ruang kontribusi inovatif yang adaptif terhadap dinamika ancaman siber. Sementara itu, penerapan standar internasional seperti TLP dan RFC tidak hanya meningkatkan interoperabilitas, tetapi juga memperkuat reputasi Indonesia di ranah global, khususnya dalam kerja sama keamanan siber kawasan ASEAN. Dengan demikian, kolaborasi domestik dan pengakuan internasional saling melengkapi dalam membangun ekosistem kepercayaan digital yang lebih tangguh.

Substansi Peraturan BSSN No. 1 Tahun 2024 ini menjadi landasan krusial dalam membangun dan mengoperasionalkan kerangka kerja kepercayaan digital Indonesia. Penguatan pilar keamanan siber, integrasi tata kelola insiden, penegakan standar respons, serta kolaborasi dan transparansi yang tercantum mampu meningkatkan kepercayaan dan kenyamanan masyarakat serta *stakeholder* dalam ekosistem digital, sekaligus mendukung ambisi Indonesia sebagai pemimpin digital regional dan global.

4.5.18 Peraturan BSSN Nomor 2 Tahun 2024 tentang Manajemen Krisis Siber

Peraturan BSSN Nomor 2 Tahun 2024 tentang Manajemen Krisis Siber merupakan turunan dari Perpres No. 47 Tahun 2023 tentang Strategi Keamanan Siber Nasional dan Manajemen Krisis Siber. Peraturan ini ditetapkan pada 10 Januari 2024, dan mulai diberlakukan pada 18 Januari 2024 [312]. Tujuan dari peraturan ini adalah mengatur tata kelola dan penanganan krisis siber secara sistemik oleh BSSN dan pihak terkait. Ruang lingkup dari Peraturan BSSN Nomor 2 Tahun 2024 meliputi :

1. Latar Belakang dan Tujuan
   Peraturan ini diterbitkan sebagai tindak lanjut dari Perpres 47 Tahun 2023 tentang Strategi Keamanan Siber Nasional dan Manajemen Krisis Siber. Fokus utamanya adalah membangun mekanisme yang terstruktur untuk memastikan kesiapsiagaan, respons cepat, serta pemulihan yang efektif dalam menghadapi krisis siber. Dengan demikian, regulasi ini bertujuan melindungi keselamatan masyarakat, menjaga keutuhan layanan publik, dan memperkuat kedaulatan negara di ruang digital.

2. Definisi dan Ruang Lingkup
   Peraturan ini memberikan kejelasan mengenai konsep insiden siber, krisis siber, dan manajemen krisis siber, yang mencakup tahapan penanganan sebelum, saat, dan setelah terjadinya krisis. Ketentuan ini berlaku bagi PSE, instansi pemerintah, serta berbagai pemangku kepentingan lain yang terlibat dalam pengelolaan dan perlindungan ekosistem digital nasional.

3. Persiapan
   Tahap persiapan dilakukan melalui penyusunan rencana kontingensi krisis siber yang disusun berdasarkan penilaian risiko, prioritas nasional, dan kondisi lanskap keamanan siber. Rencana tersebut mencakup skenario ancaman yang mungkin terjadi, pembagian peran dan tanggung jawab antarpemangku kepentingan, mekanisme penanggulangan, langkah pemulihan, kebutuhan pembiayaan, hingga prosedur pelaporan. Untuk memastikan kesiapsiagaan, BSSN bersama instansi penyelenggara negara dan pemangku kepentingan terkait diwajibkan melaksanakan simulasi krisis setidaknya satu kali dalam dua tahun.

4. Penyelenggaraan berupa tahapan pra krisis, saat krisis, dan pascakrisis dari Manajemen Krisis Siber
   - Pra Krisis: deteksi insiden, pemberian peringatan oleh National CIRT, dan deklarasi krisis oleh Presiden atas rekomendasi Kepala BSSN
   - Saat Krisis: operasional penanganan dan pemulihan, serta pelaporan krisis.
   - Pasca-Krisis: evaluasi dampak ekonomi/digital, biaya pemulihan, dan kerugian reputasi.

Dengan adanya Peraturan ini diharapkan mampu memperkuat kesiapsiagaan dan respons terhadap serangan skala besar, meningkatkan koordinasi antarlembaga dan pihak swasta/industri terkait, serta menjamin kontinuitas layanan infrastruktur esensial bagi negara dan masyarakat.

Keterkaitan dengan Kerangka Kerja Kepercayaan Digital di Indonesia

Peraturan BSSN Nomor 2 Tahun 2024 tentang Manajemen Krisis Siber memiliki kaitan yang sangat erat dengan penyusunan Kerangka Kerja Kepercayaan Digital di Indonesia karena keduanya bertujuan membangun lingkungan digital yang aman, andal, dan tepercaya. Adapun keterkaitan tersebut meliputi :

1. Keamanan sebagai pilar kepercayaan digital. Kepercayaan digital bertumpu pada jaminan keamanan siber, baik dari sisi teknis, prosedural, maupun kelembagaan. Dengan adanya Peraturan BSSN ini, diharapkan mampu memperkuat resiliensi nasional terhadap krisis siber, yang merupakan prasyarat penting dalam membangun kepercayaan publik terhadap sistem digital.

2. Menjamin Transparansi dan Akuntabilitas. Dalam kerangka kepercayaan digital, kepercayaan dibangun melalui regulasi yang transparan dan dapat dipertanggungjawabkan. Dengan adanya Peraturan ini yang mengatur tata kelola krisis, alur pelaporan, hingga evaluasi pascakrisis diharapkan mampu mendorong akuntabilitas lembaga pengelola sistem elektronik.

3. Koordinasi dan Kolaborasi Banyak Pihak (*Multistakeholder Governance*) Kolaborasi antara pemerintah, sektor privat, dan Masyarakat dalam membangun Kerangka kepercayaan digital memegang peran sangat penting. Peraturan ini mengharuskan keterlibatan aktif dari berbagai pihak, di antaranya adalah PSE, *Computer Security Incident Response Team* (CSIRT/CIRT) dan BSSN sebagai koordinator nasional.

4. Kesiapsiagaan dan Respon Kepercayaan digital tidak hanya dibangun oleh keamanan sistem saat normal, tetapi juga oleh kemampuan respon cepat saat insiden terjadi. Peraturan ini mengatur simulasi, rencana kontinjensi, dan pemulihan sistem digital yang keseluruhannya merupakan bagian dari *trust by resilience*.

4.5.19 Peraturan BSSN Nomor 5 Tahun 2024 tentang Rencana Aksi Nasional Keamanan Siber

Peraturan BSSN Nomor 5 Tahun 2024 tentang Rencana Aksi Nasional Keamanan Siber (RAN-Kamsiber) menetapkan arah kebijakan, tantangan, sasaran strategis, serta langkah-langkah yang harus diambil untuk meningkatkan ketahanan siber Indonesia [313]. Peraturan ini merupakan tindak lanjut dari Perpres Nomor 47 Tahun 2023 tentang Strategi Keamanan Siber Nasional dan Manajemen Krisis Siber,

dengan tujuan memperkuat kesiapsiagaan serta respons terhadap ancaman siber di Indonesia.

Dokumen ini menyajikan rencana aksi dalam bentuk tabel yang jelas, sehingga memudahkan setiap penanggung jawab dan instansi terkait dalam melaksanakan tugas mereka menjaga keamanan siber. Sementara itu, penyelenggaraan Manajemen Krisis Siber (MKS) dalam Perpres tersebut mencakup tiga fase utama: sebelum, saat, dan setelah krisis terjadi. Setiap fase mencakup berbagai langkah, mulai dari penyusunan rencana kontingensi, latihan, mitigasi, pemulihan, pelaporan, hingga evaluasi dampak serta pembelajaran untuk mencegah kejadian serupa di masa mendatang.

Meskipun insiden atau krisis siber tidak dapat sepenuhnya dicegah, pengelolaan yang baik dapat meminimalkan dampak kerugian dan meningkatkan kesiapan dalam menghadapi ancaman berikutnya. Dengan menerapkan pembelajaran dari insiden sebelumnya, keamanan siber di Indonesia dapat terus diperkuat.

Rencana Aksi Nasional Keamanan Siber (RAN-Kamsiber) disusun sebagai panduan strategis untuk memperkuat ketahanan siber Indonesia. Dokumen ini menetapkan langkah-langkah konkret yang harus diambil oleh berbagai pemangku kepentingan guna menghadapi tantangan siber yang semakin kompleks. Berikut adalah poin-poin utama yang menjadi fokus dalam RAN-Kamsiber:

1. *Tata Kelola Keamanan Siber*: diarahkan pada upaya penguatan ekosistem keamanan siber nasional melalui peningkatan sinergi, koordinasi, dan kolaborasi antarpemangku kepentingan. Dalam konteks ini, penyusunan standar nasional keamanan siber menjadi instrumen penting yang dapat diadopsi oleh sektor publik maupun swasta/industri, sehingga tercipta keseragaman dan kepatuhan terhadap prinsip-prinsip keamanan siber yang terukur dan berkelanjutan.

2. *Manajemen Risiko Siber*: menitikberatkan pada pengembangan sistem pemantauan, deteksi dini, dan mitigasi terhadap berbagai bentuk ancaman siber. Selain itu, dilakukan penyusunan profil risiko bagi sektor infrastruktur informasi vital serta pelaksanaan penilaian risiko siber secara nasional, guna menghasilkan pemetaan risiko yang komprehensif sebagai dasar perumusan kebijakan mitigasi yang efektif.

3. *Kesiapsiagaan dan Ketahanan Siber*: berfokus pada pembangunan kapasitas nasional dalam menghadapi insiden siber. Salah satu langkah strategis yang dilakukan adalah pembentukan tim tanggap insiden siber (*Computer Security Incident Response Team*/CSIRT) di berbagai sektor, serta penyelenggaraan simulasi pengelolaan krisis siber. Langkah tersebut dimaksudkan untuk meningkatkan kemampuan respons cepat dan koordinasi lintas lembaga dalam menghadapi situasi darurat siber.

4. *Pelindungan Infrastruktur Informasi Vital*: mencakup penyusunan peta jalan (*roadmap*) pelindungan terhadap infrastruktur informasi vital nasional, sebagai panduan dalam memperkuat ketahanan sistem yang menjadi tulang punggung

penyelenggaraan layanan publik. Selain itu, dikembangkan pula strategi keamanan siber yang terintegrasi dengan SPBE, guna memastikan keamanan, keandalan, dan keberlanjutan layanan digital pemerintah.

5. *Kemandirian Kriptografi Nasional*: menjadi pilar penting dalam memperkuat kedaulatan digital Indonesia. Upaya ini dilakukan melalui pengembangan industri kriptografi nasional yang berdaya saing, serta penyusunan kebijakan penyelenggaraan algoritma kriptografi yang aman dan sesuai dengan standar internasional. Dengan demikian, Indonesia dapat mengurangi ketergantungan pada teknologi asing sekaligus memperkuat perlindungan terhadap data dan informasi strategis nasional.

6. *Peningkatan Kapabilitas dan Literasi Keamanan Siber*: difokuskan pada pengembangan kapasitas sumber daya manusia di bidang keamanan siber melalui penyusunan kurikulum pendidikan yang relevan di berbagai jenjang. Selain itu, peningkatan literasi masyarakat dilakukan melalui kampanye nasional dan program edukasi siber yang berkelanjutan, dengan tujuan membangun budaya keamanan informasi di seluruh lapisan masyarakat.

7. *Kebijakan dan Regulasi Keamanan Siber*: berperan dalam menciptakan kerangka hukum yang mendukung upaya pelindungan data pribadi dan keamanan siber secara menyeluruh. Penyusunan regulasi dilakukan secara adaptif terhadap perkembangan teknologi dan ancaman siber yang dinamis. Di samping itu, peningkatan kapasitas aparat penegak hukum serta penguatan mekanisme penegakan hukum terhadap kejahatan siber juga menjadi prioritas utama.

8. *Kerja Sama Internasional*: merupakan elemen strategis dalam memperluas peran dan kontribusi Indonesia pada tataran global. Melalui partisipasi aktif dalam forum-forum keamanan siber internasional serta penguatan kerja sama bilateral dan multilateral, Indonesia berupaya membangun solidaritas global dalam menghadapi ancaman siber lintas negara, sekaligus memperkuat posisi diplomasi siber nasional di kancah dunia.

Keterkaitan dengan Kerangka Kerja Kepercayaan Digital di Indonesia

Kerangka kerja kepercayaan digital adalah elemen kunci dalam memastikan keberlanjutan ekonomi digital yang aman dan transparan. RAN Kamsiber 2024-2028 memiliki keterkaitan erat dengan penyusunan kerangka kerja kepercayaan digital melalui beberapa aspek berikut:

1. Keamanan dan Ketahanan Siber sebagai Pilar Kepercayaan Digital
   Kerangka kerja kepercayaan digital membutuhkan sistem keamanan siber yang kuat untuk melindungi transaksi digital dan data pengguna. RAN Kamsiber menetapkan standar keamanan siber dan strategi mitigasi ancaman yang mendukung perlindungan data dan privasi.

2. Regulasi dan Tata Kelola Digital
   RAN Kamsiber mendorong harmonisasi regulasi terkait keamanan siber,

termasuk penguatan kebijakan pelindungan data pribadi (UU PDP). Kerangka kerja kepercayaan digital memerlukan regulasi yang konsisten dan terintegrasi dengan kebijakan nasional serta standar internasional.

3. Peningkatan Kesadaran dan Literasi Digital
   RAN Kamsiber menargetkan peningkatan literasi keamanan siber melalui pendidikan dan pelatihan bagi masyarakat. Kerangka kerja kepercayaan digital menekankan pentingnya edukasi publik terkait perlindungan identitas digital dan keamanan transaksi *online*.

4. Pelindungan Infrastruktur Digital dan Data Pribadi
   Infrastruktur informasi vital memegang peran penting dalam ekosistem digital yang aman. Kerangka kerja kepercayaan digital membutuhkan mekanisme proteksi infrastruktur digital yang selaras dengan strategi RAN Kamsiber.

5. Kolaborasi *Multi-Stakeholder*
   RAN Kamsiber menggunakan pendekatan *quadhelix stakeholder* yang melibatkan pemerintah, swasta/industri, akademisi, dan komunitas. Kerangka kerja kepercayaan digital juga mengandalkan kerja sama lintas sektor untuk membangun kepercayaan digital yang berkelanjutan.

6. Peluang Ekonomi Digital dan Daya Saing Global
   Kepercayaan digital yang didukung oleh keamanan siber akan meningkatkan investasi dan pertumbuhan ekonomi berbasis digital. RAN Kamsiber berperan dalam menjaga stabilitas ekosistem digital Indonesia, yang diperkirakan akan mencapai transaksi senilai USD 90 miliar pada tahun 2024.

Peraturan BSSN Nomor 5 Tahun 2024 memberikan landasan strategis dalam membangun keamanan dan ketahanan siber nasional. Implementasi RAN Kamsiber sejalan dengan penyusunan kerangka kerja kepercayaan digital, yang bertujuan menciptakan ekosistem digital yang aman, transparan, dan tepercaya. Dengan memperkuat regulasi, meningkatkan literasi digital, serta membangun kerja sama internasional, Indonesia dapat menjadi pemimpin dalam ekonomi digital yang berkelanjutan.

4.5.20 Peraturan BSSN Nomor 7 Tahun 2024 tentang Penyelenggaraan Penilaian Kesesuaian Kriteria Umum untuk Evaluasi Keamanan Teknologi Informasi Indonesia

Peraturan BSSN Nomor 7 Tahun 2024 tentang Penyelenggaraan Penilaian Kesesuaian Kriteria Umum untuk Evaluasi Keamanan Teknologi Informasi Indonesia (*Indonesia Common Criteria for Information Technology Security Evaluation*) merupakan pembaruan dari Peraturan BSSN Nomor 15 Tahun 2019 tentang Penyelenggaraan Skema *Common Criteria* Indonesia [314]. Peraturan yang ditetapkan pada 9 September 2024 ini memberikan landasan hukum bagi pelaksanaan sertifikasi

keamanan teknologi informasi melalui Skema CC Indonesia. Tujuannya adalah meningkatkan daya saing nasional, menjamin keamanan produk teknologi informasi, serta memperkuat kepercayaan konsumen dan industri terhadap ekosistem digital Indonesia. Secara khusus, peraturan ini mengatur penyelenggaraan skema *Indonesia Common Criteria for Information Technology Security Evaluation* (Skema *Common Criteria* Indonesia, SCCI). Untuk memahami lebih jauh substansi dan cakupan Peraturan ini, berikut disajikan poin-poin utama yang terkandung di dalamnya:

1. Tujuan Regulasi
   Peraturan ini mengatur penyelenggaraan penilaian kesesuaian keamanan teknologi informasi melalui *Indonesia Common Criteria.* Tujuannya adalah memberikan jaminan keamanan bagi produk TI, meningkatkan daya saing Indonesia, serta membangun kepercayaan konsumen.

2. Skema Sertifikasi (SCCI)
   SCCI mengadopsi standar internasional *Common Criteria* (CC:2022 Rev.1) serta SNI ISO/IEC 15408 sebagai acuan utama. Skema ini diberlakukan secara wajib bagi produk teknologi yang digunakan dalam pelindungan IIV, dengan tingkat jaminan evaluasi minimal *Evaluation Assurance Level* (EAL) 3. Sementara itu, untuk produk di luar kategori IIV, penerapan SCCI bersifat sukarela, sehingga tetap memberikan fleksibilitas bagi pengembang maupun penyedia teknologi dalam meningkatkan kepercayaan terhadap keamanan produknya.

3. Proses dan Tata Kelola Sertifikasi
   Proses sertifikasi keamanan teknologi informasi dalam skema Indonesia Common Criteria diawali dengan pengujian produk oleh Laboratorium Pengujian yang telah ditunjuk dan diverifikasi oleh BSSN. Selanjutnya, hasil pengujian diverifikasi oleh Lembaga Sertifikasi Produk (LSPro) yang ditetapkan sebagai otoritas nasional sekaligus mewakili Indonesia dalam skema internasional *Common Criteria Recognition Arrangement* (CCRA). Sertifikat yang diterbitkan berlaku selama 5 hingga 10 tahun, disertai mekanisme pemeliharaan, pengawasan, serta pemberian sanksi apabila terjadi pelanggaran terhadap ketentuan yang berlaku.

4. Pengawasan dan Akuntabilitas
   BSSN melaksanakan pengawasan rutin terhadap Lembaga Sertifikasi Produk (LSPro) dan laboratorium pengujian melalui kegiatan inspeksi produksi dan pengendalian mutu. Pengawasan ini bertujuan memastikan bahwa seluruh proses sertifikasi berjalan sesuai standar yang telah ditetapkan. Selain itu, tersedia mekanisme pembekuan atau pencabutan sertifikat apabila ditemukan pelanggaran atau ketidaksesuaian yang signifikan. Langkah ini dilakukan untuk menjaga integritas dan kredibilitas sistem sertifikasi, sekaligus menjamin kepercayaan publik terhadap hasil evaluasi keamanan teknologi informasi di Indonesia.

5. Integrasi dengan Standar Nasional dan Internasional
   Produk teknologi informasi yang berhasil lulus sertifikasi berhak mengguna-

kan Tanda SNI dan Tanda SCCI/CC sebagai jaminan mutu dan keamanan. Lebih jauh, ketika Indonesia berhasil meningkatkan statusnya dari *consuming member* menjadi *authorizing member* dalam skema CCRA, pengakuan terhadap produk nasional akan meluas secara global. Hal ini berarti produk yang disertifikasi di dalam negeri tidak hanya diakui di Indonesia, tetapi juga memperoleh legitimasi internasional, sehingga mampu bersaing di pasar global dengan standar keamanan yang diakui dunia.

Keterkaitan dengan Kerangka Kerja Kepercayaan Digital di Indonesia

Peraturan BSSN Nomor 7 Tahun 2024 berperan penting dalam mendukung penyusunan Kerangka Kerja Kepercayaan Digital di Indonesia. Melalui skema sertifikasi keamanan berbasis *Common Criteria* yang diakui secara internasional, regulasi ini memperkuat aspek keamanan, akuntabilitas, dan legitimasi produk teknologi nasional dalam ekosistem digital. Adapun keterkaitan tersebut meliputi :

1. Legitimasi dan Standarisasi: Regulasi ini memberikan landasan hukum bagi Indonesia untuk mengadopsi standar internasional keamanan teknologi informasi sekaligus mengintegrasikannya dengan standar nasional (SNI). Langkah ini selaras dengan prinsip kepercayaan digital yang menuntut standarisasi, interoperabilitas, serta pengakuan global. Sertifikasi keamanan produk berbasis standar internasional, seperti Common Criteria dan SNI ISO/IEC 15408, memastikan bahwa produk yang beredar di Indonesia memiliki tingkat keamanan yang dapat dipercaya. Jaminan ini tidak hanya melindungi infrastruktur digital nasional, tetapi juga memperkuat kepercayaan masyarakat dan pelaku industri terhadap ekosistem digital. Lebih jauh, regulasi menekankan pentingnya penilaian keamanan yang terukur dan terstruktur, dengan kerangka sertifikasi yang mencakup penetapan *Target of Evaluation* (TOE), penyusunan protection profile, hingga penentuan *Evaluation Assurance Level* (EAL). Dengan mekanisme evaluasi yang konsisten, produk digital yang telah teruji dapat diintegrasikan ke dalam ekosistem Indonesia dengan risiko keamanan yang lebih rendah.

2. Akuntabilitas dan Transparansi: Mekanisme pengawasan, laporan tahunan, serta sanksi atas pelanggaran merupakan wujud penerapan akuntabilitas dalam tata kelola sertifikasi. Regulasi juga mengatur secara rinci pemilihan lembaga sertifikasi, proses audit, pengujian, hingga mekanisme pengawasan pascasertifikasi. Dengan tata kelola dan pengawasan yang ketat ini, integritas serta kepatuhan produk teknologi informasi dapat dijaga sepanjang siklus hidupnya, sehingga mampu memperkuat kepercayaan digital nasional.

3. Pelindungan Infrastruktur Vital: Pelindungan IIV merupakan pilar penting dalam kerangka kerja kepercayaan digital. Untuk memperkuat resiliensi keamanan nasional, peraturan mewajibkan setiap produk yang digunakan dalam melindungi IIV memiliki sertifikasi minimal pada level EAL 3. Ketentuan ini memastikan bahwa sistem dan infrastruktur digital yang bersifat

kritikal dikelola dengan standar keamanan yang ketat, konsisten, dan dapat diandalkan.

4. Kepercayaan Konsumen dan Industri: Dengan adanya sertifikasi resmi (SCCI/CC Indonesia), konsumen dan pelaku industri mendapat jaminan bahwa produk TI telah memenuhi standar keamanan, sehingga meningkatkan adopsi digital dengan rasa aman.

5. Posisi Global Indonesia: Partisipasi Indonesia dalam *Common Criteria Recognition Arrangement* (CCRA) memberikan pengakuan internasional terhadap sertifikat keamanan yang diterbitkan di dalam negeri. Hal ini mendukung visi Indonesia untuk menjadi bagian dari ekosistem digital global yang tepercaya. Melalui sertifikasi berbasis Common Criteria, produk dan solusi teknologi lokal memiliki peluang lebih besar untuk diterima di pasar internasional. Dengan demikian, akses terhadap pasar global semakin terbuka sekaligus memperkuat kepercayaan digital nasional, karena layanan digital Indonesia terbukti mampu memenuhi standar keamanan yang diakui secara global.

Peraturan BSSN Nomor 7 Tahun 2024 menyediakan kerangka hukum, teknis, dan operasional untuk penyelenggaraan penilaian kesesuaian keamanan teknologi informasi secara komprehensif di Indonesia. Melalui skema sertifikasi yang mengadopsi *Common Criteria* dan standar ISO, peraturan ini menjadi elemen penting dalam membangun kerangka kerja kepercayaan digital nasional. Penerapan skema tersebut diharapkan mampu menjamin keamanan produk teknologi informasi, meningkatkan kepercayaan para pemangku kepentingan terhadap penggunaan teknologi, serta memastikan interoperabilitas dan pengakuan standar di tingkat internasional. Lebih jauh, pengaturan ini juga berperan dalam mengamankan infrastruktur digital vital sehingga mendukung keandalan sistem nasional secara keseluruhan.

4.5.21 Peraturan BSSN Nomor 11 Tahun 2024 tentang Penyelenggaraan Algoritma Kriptografi Indonesia dan Penilaian Kesesuaian Keamanan Modul Kriptografi

Peraturan BSSN Nomor 11 Tahun 2024 tentang Penyelenggaraan Algoritma Kriptografi Indonesia dan Penilaian Kesesuaian Keamanan Modul Kriptografi merupakan pembaruan dari Peraturan Kepala Lemsaneg Nomor 9 Tahun 2010 tentang Algoritma Kriptografi dan Peraturan Kepala Lemsaneg Nomor 5 Tahun 2014 tentang Tata Cara Sertifikasi Modul Kriptografi [315]. Peraturan ini ditetapkan pada 19 November 2024, dan mulai berlaku sejak tanggal diundangkan. Tujuan dari peraturan ini adalah menetapkan standar algoritma kriptografi nasional serta mekanisme sertifikasi keamanan modul kriptografi guna memperkuat kedaulatan teknologi, meningkatkan kepercayaan terhadap layanan digital, dan melindungi infrastruktur informasi vital di Indonesia. Untuk memahami lebih jauh substansi dan cakupan Peraturan ini, berikut disajikan poin-poin utama yang terkandung di dalamnya:

1. Tujuan dan Latar Belakang

Peraturan ini diterbitkan untuk memperkuat standardisasi keamanan informasi, melindungi informasi elektronik, dan memberikan jaminan keamanan modul kriptografi. Peraturan ini juga menggantikan aturan lama (Perka Lemsaneg No. 9/2010 dan No. 5/2014) yang sudah tidak sesuai perkembangan.

2. Algoritma Kriptografi Indonesia
   Standar algoritma kriptografi yang ditetapkan secara nasional harus melalui mekanisme adopsi atau seleksi berdasarkan kriteria umum maupun khusus yang telah ditentukan. Algoritma yang dipilih wajib bebas dari hak royalti, dipublikasikan secara terbuka di domain publik, serta memiliki tingkat kekuatan keamanan minimal, misalnya setara dengan 128 bit. Selain itu, standar ini harus direviu secara berkala untuk memastikan relevansi dan ketahanannya terhadap perkembangan teknologi serta dinamika ancaman keamanan yang terus berubah.

3. Penilaian Kesesuaian Keamanan Modul Kriptografi (PKKMK)
   Sebagai bentuk perlindungan terhadap IIV, setiap modul kriptografi diwajibkan memenuhi standar SNI ISO/IEC 19790:2015 dengan tingkat keamanan minimal Level 2. Kepatuhan ini memastikan bahwa modul yang digunakan memiliki mekanisme keamanan yang andal dan sesuai dengan standar internasional. Proses sertifikasi dilaksanakan oleh Lembaga Sertifikasi Produk (LSPro), sementara pengujian dilakukan oleh Laboratorium Pengujian yang telah ditunjuk secara resmi oleh BSSN. Dengan mekanisme ini, jaminan keamanan modul kriptografi dapat dipastikan sejak tahap sertifikasi hingga penerapannya di lingkungan IIV. Modul kriptografi yang berhasil lulus uji berhak memperoleh dan menggunakan Tanda SNI serta Tanda KMK, sebagai bukti resmi bahwa produk tersebut memenuhi standar keamanan nasional.

4. Pengawasan dan Tata Kelola
   BSSN membentuk Komite Algoritma Kriptografi Indonesia yang melibatkan perwakilan pemerintah, akademisi, industri, dan konsumen sebagai wadah kolaborasi nasional. Komite ini berperan dalam mengawasi penerapan algoritma dan modul kriptografi, baik oleh PSE maupun penyedia modul, agar sesuai dengan standar keamanan yang berlaku. Selain itu, LSPro dan laboratorium pengujian wajib mematuhi mekanisme evaluasi yang ketat, termasuk sanksi berupa pembekuan atau pencabutan akreditasi apabila tidak memenuhi persyaratan standar.

Keterkaitan dengan Kerangka Kerja Kepercayaan Digital di Indonesia

Peraturan BSSN Nomor 11 Tahun 2024 menetapkan standar penggunaan algoritma kriptografi nasional serta mekanisme penilaian kesesuaian modul kriptografi. Regulasi ini menjadi landasan penting bagi kerangka kerja kepercayaan digital di Indonesia, karena menjamin keamanan, integritas, dan keandalan modul kriptografi yang digunakan pada sistem elektronik, termasuk infrastruktur informasi vital. Adapun keterkaitan tersebut meliputi :

1. Standarisasi Algoritma sebagai Pilar Kepercayaan Digital
   Penetapan kriteria dan seleksi algoritma kriptografi yang sesuai standar internasional merupakan langkah strategis untuk memperkuat dasar keamanan digital nasional. Dengan penggunaan Algoritma Kriptografi Indonesia yang telah diverifikasi, sistem elektronik nasional memperoleh kredibilitas lebih tinggi sekaligus menjamin perlindungan terhadap ancaman siber. Regulasi yang menetapkan standar algoritma nasional dan sertifikasi modul kriptografi juga memastikan bahwa infrastruktur digital, khususnya sistem elektronik vital, memiliki tingkat resiliensi yang memadai. Hal ini menjadi salah satu pilar utama dalam membangun kepercayaan digital Indonesia, baik di tingkat nasional maupun global.

2. Sertifikasi Modul Kriptografi untuk Infrastruktur Vital
   Keamanan IIV sangat bergantung pada keandalan modul kriptografi yang digunakan untuk melindungi sistem dan data kritikal. Oleh karena itu, sertifikasi modul kriptografi menjadi langkah penting untuk memastikan kualitas dan ketahanan terhadap ancaman siber. Regulasi menetapkan kewajiban sertifikasi serta pengawasan berkala agar modul yang digunakan selalu sesuai dengan standar keamanan terbaru. Dengan mekanisme ini, perlindungan terhadap IIV dapat dijamin secara berkelanjutan sekaligus memperkuat dasar kepercayaan digital nasional.

3. Tata Kelola, Pengawasan, dan Reviu Berkelanjutan
   Kepercayaan digital hanya dapat terjaga apabila terdapat mekanisme tata kelola yang kuat, disertai pengawasan dan reviu berkelanjutan. Melalui proses evaluasi rutin dan sistematis, tingkat keamanan dapat tetap adaptif terhadap dinamika ancaman siber yang terus berkembang. Struktur komite yang melibatkan berbagai pemangku kepentingan memastikan adanya transparansi sekaligus memperkuat akuntabilitas dalam pengelolaan keamanan digital. Kehadiran komite multipihak, mekanisme pengawasan yang terukur, serta skema sertifikasi yang terbuka menjadi wujud nyata penerapan prinsip akuntabilitas dalam tata kelola ekosistem digital nasional.

4. Penguatan Kemandirian dan Daya Saing Nasional
   Penetapan Algoritma Kriptografi Indonesia yang bebas royalti serta telah melalui proses seleksi ilmiah dan kompetisi menjadi langkah strategis dalam membangun ekosistem kriptografi nasional yang mandiri. Dengan adanya pengakuan dan rekognisi internasional, algoritma ini tidak hanya selaras dengan standar global, tetapi juga mendorong interoperabilitas lintas sistem dan batas negara, sehingga memperkuat kepercayaan digital. Lebih jauh, mekanisme seleksi yang transparan membuka ruang bagi inovasi lokal untuk diakui secara resmi sebagai Algoritma Kriptografi Indonesia. Hal ini tidak hanya menegaskan kedaulatan teknologi, tetapi juga meningkatkan daya saing nasional.

5. Dokumen dan Proses Formal untuk Implementasi Praktis
   Pengaturan prosedur administratif sertifikasi dan penilaian menyatukan prak-

tik terbaik internasional dengan konteks regulasi nasional, sehingga dapat diterapkan secara efektif dan efisien di berbagai institusi dan sektor.

6. Perlindungan Konsumen dan Industri
   Sertifikasi modul kriptografi memberi jaminan keamanan pada produk digital yang digunakan masyarakat dan industri, meningkatkan rasa aman sekaligus mendorong adopsi layanan digital.

Peraturan BSSN Nomor 11 Tahun 2024 menjadi salah satu tonggak penting dalam penyusunan kerangka kerja kepercayaan digital di Indonesia. Regulasi ini memberikan dasar hukum, teknis, dan organisatoris yang kuat untuk pengembangan serta pengawasan algoritma dan modul kriptografi, sehingga dapat menjamin tingkat keamanan yang memadai dalam sistem elektronik, khususnya pada IIV. Selain itu, peraturan ini melengkapi pilar teknis dari kerangka kerja kepercayaan digital Indonesia dengan menekankan aspek keamanan algoritma kriptografi, sertifikasi modul kriptografi, akuntabilitas tata kelola, serta pengakuan terhadap standar internasional. Dengan demikian, kepercayaan masyarakat, pemerintah, dan dunia usaha terhadap ekosistem digital nasional semakin diperkuat.

4.5.22 Strategi Nasional Kecerdasan Artifisial Indonesia

Strategi Nasional Kecerdasan Artifisial (Stranas KA) 2020-2045 merupakan pedoman kebijakan nasional untuk mengembangkan dan mengimplementasikan teknologi kecerdasan artifisial (AI) secara menyeluruh di Indonesia [316]. Disusun oleh BPPT, dokumen ini berfungsi sebagai acuan bagi kementerian, lembaga pemerintah, pemerintah daerah, dan pemangku kepentingan dalam membangun ekosistem AI yang etis, transparan, dan akuntabel. Meski belum berbentuk regulasi khusus, Stranas KA dirancang untuk menjawab tantangan strategis melalui empat pilar utama:

1. Etika dan Kebijakan – Penyusunan regulasi dan prinsip etika guna memastikan pemanfaatan AI yang bertanggung jawab.
2. Pengembangan Talenta – Peningkatan kapasitas sumber daya manusia melalui program pendidikan, pelatihan, dan literasi AI.
3. Infrastruktur dan Data – Penyediaan infrastruktur teknologi serta sistem pengelolaan data yang aman, terintegrasi, dan berkelanjutan.
4. Riset dan Inovasi Industri – Penguatan kolaborasi antara akademisi, industri, dan pemerintah untuk mendorong inovasi AI yang meningkatkan daya saing nasional.

Keempat pilar ini tidak hanya memetakan prioritas pengembangan AI di berbagai sektor tetapi juga menjadi landasan strategis dalam menyelaraskan kebijakan teknologi dengan tujuan pembangunan jangka panjang Indonesia hingga 2045. Selain itu, Stranas KA mencantumkan lima bidang prioritas utama:

- Layanan Kesehatan – Pemanfaatan AI untuk meningkatkan akses dan kualitas layanan kesehatan.
- Reformasi Birokrasi – Penerapan AI guna meningkatkan efisiensi dan transparansi dalam administrasi pemerintahan.
- Pendidikan dan Riset – Integrasi AI dalam sistem pendidikan dan penelitian untuk meningkatkan kualitas dan relevansi.
- Ketahanan Pangan – Penggunaan AI dalam sektor pertanian dan distribusi pangan guna memastikan ketersediaan dan keamanan pangan.
- Mobilitas dan Kota Pintar – Pengembangan solusi AI untuk transportasi cerdas dan manajemen kota yang lebih efisien.

Sebagai langkah konkret dalam mewujudkan ekosistem kecerdasan artifisial yang berkelanjutan, berbagai sektor telah mulai menerapkan prinsip dan strategi yang tercantum dalam Stranas KA. Implementasi ini bertujuan untuk meningkatkan efisiensi, transparansi, serta daya saing nasional melalui pemanfaatan teknologi AI yang inovatif dan bertanggung jawab. Berikut adalah beberapa sektor utama yang telah mengadopsi AI dalam upaya mendukung transformasi digital di Indonesia.

1. Layanan Kesehatan
   Pemerintah berkomitmen mendukung inovasi AI di bidang kesehatan untuk meningkatkan efisiensi pelayanan medis. Kementerian Kesehatan telah memanfaatkan AI dalam diagnosis medis, khususnya untuk meningkatkan akurasi analisis gambar seperti X-ray dan MRI. Implementasi ini membantu rumah sakit dalam proses diagnosis serta meningkatkan efisiensi layanan kesehatan. Sebagai contoh, Kementerian Kesehatan telah menandatangani Memorandum of Understanding (MoU) dengan Horrison AI, perusahaan teknologi kesehatan asal Australia, untuk penerapan AI di beberapa rumah sakit utama, termasuk Rumah Sakit Pusat Otak Nasional (RSPON) Prof. Dr. dr. Mahar Mardjono Jakarta, Rumah Sakit Kanker Dharmais, dan Rumah Sakit Dr. M. Djamil Padang [317].
   Penelitian AI dalam bidang kesehatan juga mengalami kemajuan. Manajemen Ilmu Kesehatan (MIK) Universitas Muhammadiyah Sidoarjo, misalnya, telah mengembangkan sistem berbasis AI untuk pengelolaan rekam medis dan informasi kesehatan guna meningkatkan efisiensi pengolahan data pasien [318].

2. Reformasi Birokrasi
   Dalam rangka meningkatkan efisiensi layanan publik, AI telah diterapkan dalam berbagai aspek administrasi pemerintahan. *Chatbot* berbasis AI, misalnya, telah diimplementasikan oleh Kementerian Pendayagunaan Aparatur Negara dan Reformasi Birokrasi (PANRB) untuk menjawab pertanyaan sehari-hari terkait kebijakan dan layanan publik. Salah satu contoh penerapan AI adalah Si PANDay, platform interaktif yang membantu penyebaran informasi secara efisien [319].

3. Pendidikan dan Riset
   AI juga dimanfaatkan dalam sektor pendidikan dan riset guna meningkatkan kualitas pembelajaran dan pengembangan talenta digital. Ditjen Diktiristek telah menjalin kerja sama dengan NVIDIA untuk melatih 20.000 mahasiswa dalam bidang kecerdasan artifisial. Selain itu, NVIDIA juga menyediakan infrastruktur berupa teknologi super komputer dengan daya 25 petaFLOPS guna mendukung fasilitas DIKTI AI Centre [320].

4. Mobilitas dan Kota Pintar
   Strategi implementasi AI dalam mobilitas dan kota pintar telah diterapkan di Ibu Kota Nusantara (IKN). Salah satu proyek unggulan adalah kolaborasi dengan Sergek, perusahaan asal Kazakhstan yang mengembangkan sistem transportasi cerdas berbasis AI. Proyek ini berhasil menyelesaikan *Proof of Concept* (PoC) untuk sistem lalu lintas dan mobilitas di Nusantara. Teknologi ini memungkinkan Otorita IKN memperoleh data analitik yang dapat membantu perencanaan kota dan manajemen lalu lintas yang lebih efisien [321]. Sistem AI Sergek memberikan data yang akurat mengenai pola arus lalu lintas, periode kepadatan lalu lintas, serta rute perjalanan yang paling efisien berdasarkan analitik data besar. Implementasi teknologi ini diharapkan dapat meningkatkan efektivitas perencanaan perkotaan dan optimalisasi sistem transportasi di IKN.

Stranas KA menjadi landasan utama dalam pengembangan dan implementasi AI di Indonesia. Melalui empat pilar utama dan lima bidang prioritas, strategi ini memastikan bahwa AI digunakan secara etis, transparan, dan akuntabel. Berbagai penerapan AI dalam sektor kesehatan, reformasi birokrasi, pendidikan, dan mobilitas menunjukkan komitmen pemerintah dalam membangun ekosistem AI yang dapat meningkatkan kesejahteraan masyarakat dan daya saing nasional. Dengan terus memperkuat regulasi, infrastruktur, serta pengembangan talenta digital, Indonesia dapat memanfaatkan AI secara optimal untuk mencapai visi Indonesia Emas 2045.

Keterkaitan dengan Kerangka Kerja Kepercayaan Digital di Indonesia

Dalam upaya membangun ekosistem digital yang aman, tepercaya, dan berkelanjutan, penyusunan kerangka kerja kepercayaan digital di Indonesia harus selaras dengan berbagai strategi nasional yang mendukung transformasi digital, termasuk Stranas KA. Stranas KA memberikan landasan bagi pengembangan dan implementasi AI yang bertanggung jawab, yang mencakup aspek keamanan, privasi, transparansi, serta regulasi yang harmonis. Berikut adalah keterkaitan utama antara Stranas KA dan kerangka kerja kepercayaan digital dalam menciptakan kepercayaan digital di Indonesia.

1. Keamanan Data dan Privasi
   Kerangka kerja kepercayaan digital berfokus pada pelindungan data pribadi dan keamanan siber sebagai fondasi kepercayaan digital. Stranas KA juga

menekankan pentingnya kedaulatan data nasional, standar keamanan, dan privasi dalam pengembangan AI.

2. Transparansi dan Akuntabilitas dalam AI
   Salah satu prinsip utama dalam kerangka kerja kepercayaan digital adalah transparansi algoritma dan akuntabilitas dalam pemrosesan data. Stranas KA mengusulkan pembentukan Dewan Etika Data untuk mengawasi pemanfaatan AI serta memastikan kepatuhan terhadap standar etika.

3. Keamanan Infrastruktur Digital
   Kerangka kerja kepercayaan digital mengharuskan infrastruktur digital yang aman dan tahan serangan. Stranas KA mencakup strategi keamanan siber AI untuk memastikan sistem yang digunakan dalam pemerintahan dan sektor bisnis tidak rentan terhadap ancaman siber.

4. Penguatan Regulasi dan Standarisasi
   Stranas KA menekankan pentingnya kebijakan yang harmonis dengan regulasi nasional, termasuk UU PDP dan regulasi AI yang lebih spesifik. Hal ini sejalan dengan kerangka kerja kepercayaan digital yang menuntut adanya standar kepatuhan dalam transaksi digital dan pengolahan data.

5. Kepercayaan Publik terhadap Teknologi AI
   Kerangka kerja kepercayaan digital bertujuan membangun ekosistem digital yang dipercaya oleh masyarakat dan pelaku industri. Stranas KA berkontribusi pada upaya ini dengan mengedepankan prinsip AI yang etis, tidak bias, dan bertanggung jawab, serta meningkatkan literasi digital masyarakat.

Secara keseluruhan, Stranas KA memberikan landasan penting dalam memperkuat kepercayaan digital di Indonesia dengan memastikan bahwa pemanfaatan kecerdasan artifisial dilakukan secara aman, etis, dan bertanggung jawab. Hal ini diwujudkan melalui penyusunan regulasi yang adaptif, peningkatan keamanan data untuk melindungi privasi pengguna, serta penerapan transparansi dalam pengembangan dan penggunaan AI. Selain itu, Stranas KA juga menekankan pentingnya pengembangan SDM yang memiliki keterampilan digital dan literasi AI yang memadai, sehingga mendukung ekosistem digital yang lebih aman dan bertanggungjawab. Seluruh upaya ini selaras dengan kerangka kerja kepercayaan digital, yang bertujuan untuk menciptakan lingkungan digital yang aman dan dapat dipercaya bagi masyarakat serta pelaku industri.

5

Potret Kepercayaan Digital Indonesia

> Without digital trust, transformation fails. It's not just about technology—it's about confidence.
>
> — Accenture Digital Trust Insight

Hasil analisis kerangka kerja yang dikembangkan oleh berbagai negara, seperti Singapura, Malaysia, Uni Eropa, Amerika Latin, dan Turki, serta komunitas global seperti WEF, PwC, dan ISACA, menunjukkan bahwa setiap negara dan komunitas memiliki pendekatan yang unik dalam menerapkan kepercayaan digital. Namun, terdapat benang merah yang menghubungkan seluruh pendekatan tersebut, yaitu bahwa kepercayaan digital tidak hanya berkaitan dengan kepatuhan terhadap regulasi, tetapi juga merupakan faktor fundamental dalam menciptakan ekosistem digital yang aman, stabil, dan berkelanjutan. Di Indonesia, transformasi digital telah menjadi visi nasional yang membutuhkan dukungan serta kolaborasi berbagai pihak. Oleh karena itu, kepercayaan digital menjadi aspek penting yang harus diupayakan demi terciptanya rasa aman dalam bertransaksi dan berinteraksi di dunia digital.

Transformasi digital juga telah masif terjadi dalam pembangunan ekonomi dan sosial di Indonesia. Hal ini tercantum dalam visi jangka panjang seperti Indonesia Emas 2045, Rencana Pembangunan Jangka Menengah Nasional (RPJMN), dan

Visi Indonesia Digital 2045. Agenda ini menekankan pentingnya ekonomi digital di semua sektor, pemerintahan berbasis data, serta pemanfaatan teknologi mutakhir untuk meningkatkan daya saing global. Namun, di tengah pesatnya adopsi teknologi, tantangan kompleks seperti kerentanan siber, kesenjangan regulasi, dan literasi digital yang belum merata mulai muncul. Penelitian ini bertujuan untuk menganalisis dinamika transformasi digital di Indonesia, mengidentifikasi risiko sistemik, serta memberikan rekomendasi strategis untuk memaksimalkan potensi ekonomi digital melalui transaksi digital.

Visi Indonesia Emas 2045 dan RPJMN menetapkan transformasi digital sebagai tulang punggung pembangunan ekonomi, dengan target kontribusi sektor digital mencapai 18% terhadap Pendapatan Domestik Bruto (PDB). Visi Indonesia Digital 2045 memperkuat hal ini melalui tiga pilar utama: infrastruktur digital yang merata, pemerintahan berbasis data (*e-government*/satu data), dan pemberdayaan usaha mikro, kecil, dan menengah (UMKM) melalui platform digital. Kebijakan ini mendorong adopsi teknologi seperti *Quick Response Code Indonesian Standard* (QRIS) untuk transaksi keuangan yang mandiri, *Artificial Intelligence* (AI) dalam layanan publik, dan *blockchain* untuk sertifikasi digital. Namun, pencapaian visi ini sangat bergantung pada kemampuan Indonesia untuk mengatasi ancaman siber dan kesenjangan regulasi yang semakin mengemuka seiring dengan pertumbuhan pasar digital.

Indonesia telah mencatat kemajuan signifikan dalam adopsi teknologi digital, yang menjadi pendorong utama transformasi ekonomi dan sosial di berbagai sektor. Salah satu indikatornya adalah pertumbuhan pesat industri *e-commerce* dan *fintech*, termasuk layanan pinjaman *online* (pinjol), yang mencapai rata-rata 25% per tahun. Pertumbuhan ini didorong oleh penetrasi internet yang mencakup hingga 78% populasi, menjadikan Indonesia sebagai salah satu pasar digital terbesar di Asia Tenggara [322].

Di bidang sistem pembayaran, QRIS telah diadopsi oleh lebih dari 32 juta *merchant*, memperkuat integrasi transaksi mikro dan makro di seluruh negeri. Sistem ini tidak hanya meningkatkan efisiensi transaksi, tetapi juga mendukung perluasan akses keuangan bagi masyarakat yang sebelumnya sulit mendapatkan layanan perbankan. Selain itu, aset kripto seperti Bitcoin, Ethereum, dan koin lokal mulai bermunculan dan menarik perhatian investor meskipun volatilitasnya tinggi. Di sisi pemerintahan, implementasi *e-government* berbasis *single data* menjadi langkah penting untuk menyederhanakan birokrasi dan meningkatkan akuntabilitas layanan publik. Penggunaan tanda tangan digital juga semakin meluas, mempercepat proses administrasi tanpa mengorbankan keamanan. Namun, di tengah kemajuan ini, sejumlah tantangan serius perlu diantisipasi agar transformasi digital dapat berjalan dengan aman dan andal. Maraknya kasus penipuan digital menjadi ancaman serius bagi masyarakat. Berdasarkan data Indeks Masyarakat Digital Tahun 2022 - 2023 [22] diketahui bahwa Indonesia memiliki indeks (skala 1-100), yaitu 37,8 pada tahun 2022 dan 43,18 pada tahun 2023. Selain itu, tingkat literasi digital yang rendah dibuktikan oleh hanya 32% masyarakat yang memahami konsep perlindungan data pribadi, dan 45% pengguna *fintech* tidak menyadari risiko penyalahgunaan data [323]. Kondisi ini semakin mengkhawatirkan dengan meningkatnya skema

penipuan *online* yang semakin canggih. Kecanggihan ini antara lain melibatkan unsur *social engineering* memanfaatkan kelemahan manusia melalui manipulasi psikologis, seperti *phishing*, *vishing*, dan *pretexting*.

Transformasi digital juga memberikan dampak ketergantungan pada pihak ketiga, seperti *vendor* teknologi dan penyedia layanan *cloud*, sehingga meningkatkan risiko *third party exposure*. Banyak insiden kebocoran data di Indonesia terjadi akibat lemahnya pengawasan dan kontrol keamanan pada mitra eksternal. Ancaman ini semakin relevan seiring dengan masifnya digitalisasi rantai pasok dan integrasi sistem lintas organisasi, sehingga celah keamanan pada pihak ketiga dapat dimanfaatkan untuk menembus sistem utama perusahaan atau institusi pemerintah [324].

Teknologi canggih seperti *Artificial Intelligence* (AI) tidak hanya membawa manfaat, tetapi juga membuka peluang bagi serangan siber berbasis AI. *Threat actor* kini menggunakan AI untuk mengotomasi serangan, menciptakan *malware* yang adaptif, serta melakukan *spear phishing* yang lebih meyakinkan. AI juga digunakan untuk melakukan *reconnaissance* dan analisis kelemahan secara cepat, sehingga meningkatkan efektivitas serangan terhadap target di Indonesia, termasuk sektor infrastruktur kritis dan keuangan [324].

Ancaman dari orang dalam (*insider threat*) menjadi perhatian khusus di era digital. *Insider threat* dapat berupa karyawan, kontraktor, atau mitra yang memiliki akses ke sistem dan data sensitif. Motifnya bisa berupa keuntungan finansial, sabotase, atau kelalaian. Di Indonesia, kasus-kasus *insider threat* sering kali tidak terdeteksi karena lemahnya sistem pemantauan dan kurangnya pelatihan keamanan bagi pegawai. Serangan ini semakin berbahaya karena *insider* memiliki pemahaman mendalam tentang sistem internal dan dapat menghindari deteksi tradisional.

Risiko-risiko ini menegaskan perlunya regulasi yang kuat serta edukasi masif untuk memastikan bahwa transformasi digital berjalan secara aman, andal, dan berkelanjutan menuju ekonomi digital yang positif. Dengan pendekatan yang tepat, Indonesia dapat memanfaatkan potensi ekonomi digital untuk mewujudkan visi jangka panjangnya sebagai negara maju pada tahun 2045.

Pesatnya adopsi teknologi digital tidak lepas dari risiko keamanan yang semakin kompleks. Salah satu ancaman utama adalah serangan siber (*cybersecurity threat*), yang dapat merugikan individu, bisnis, maupun pemerintah. Indonesia menempati peringkat kelima di Asia Tenggara dalam indeks keamanan siber (*Global Cybersecurity Index* 2023). Sepanjang 2023, terjadi 1,2 miliar serangan siber dengan kerugian ekonomi mencapai USD 3 miliar, termasuk kasus *data breach* besar seperti kebocoran data 34 juta pengguna *e-commerce*. Ancaman ini diperparah oleh minimnya kesadaran masyarakat, indeks literasi keamanan siber Indonesia hanya 3,49 dari skala 5. Kasus-kasus *data breach* di Indonesia semakin marak, dengan pelaku sering kali mengeksploitasi celah keamanan sistem untuk mencuri data pribadi atau melakukan penipuan *online*. Misalnya, banyak masyarakat yang menjadi korban penipuan melalui *platform digital*, termasuk pinjaman *online* ilegal yang menyalahgunakan data pengguna.

Sebuah studi kolaboratif yang dirilis oleh Microsoft Indonesia dan IDC Asia-Pasifik

pada tahun 2019 mengungkapkan bahwa tingkat kepercayaan konsumen Indonesia terhadap layanan digital masih berada pada tingkat yang cukup rendah. Dalam studi yang berjudul Understanding Consumer Trust in Digital Services in Asia Pacific tersebut, hanya 44% responden dari Indonesia yang menyatakan bahwa mereka mempercayai penyedia layanan digital dalam mengelola dan melindungi data pribadi mereka secara memadai [325].

Penelitian ini melibatkan 457 responden dari Indonesia dan merupakan bagian dari survei yang lebih luas di kawasan Asia Pasifik, dengan total partisipasi lebih dari 6.000 konsumen. Hasilnya menunjukkan bahwa konsumen Indonesia menilai lima elemen utama sebagai dasar dari kepercayaan terhadap layanan digital, yaitu keamanan, privasi, keandalan, etika, dan kepatuhan hukum. Di antara kelima elemen tersebut, tiga aspek yang paling menentukan dalam membangun kepercayaan adalah keamanan (87%), privasi (86%), dan etika (85%).

Sektor jasa keuangan, pendidikan, dan kesehatan muncul sebagai bidang yang paling diharapkan oleh masyarakat untuk menunjukkan tingkat kepercayaan digital yang tinggi. Menariknya, studi ini juga mencatat bahwa konsumen Indonesia cenderung tidak mudah tergoda oleh harga layanan yang lebih murah apabila penyedia layanan tersebut tidak dapat dipercaya. Hanya enam persen konsumen yang bersedia menggunakan layanan digital yang tidak tepercaya meskipun biayanya lebih rendah, sementara 63% menyatakan akan tetap menggunakan atau bahkan merekomendasikan layanan digital yang tepercaya meskipun memiliki harga yang lebih tinggi. Studi ini juga menunjukkan bahwa hilangnya kepercayaan terhadap layanan digital memiliki dampak nyata terhadap perilaku konsumen. Sekitar 46% responden mengaku pernah kehilangan kepercayaan terhadap layanan digital tertentu; dari jumlah tersebut, 56% memutuskan untuk beralih ke penyedia lain, 37% mengurangi penggunaan layanan, dan 33% menghentikan penggunaan layanan secara total.

Pimpinan Microsoft Indonesia saat itu, Haris Izmee, bersama Country Manager IDC Indonesia, Mevira Munindra, menekankan bahwa kepercayaan merupakan aset strategis yang harus ditempatkan di pusat perencanaan dan inovasi produk digital. Mereka menegaskan bahwa kolaborasi antara sektor swasta/industri dan pemerintah diperlukan untuk membangun ekosistem digital yang tepercaya melalui peningkatan aspek keamanan, perlindungan privasi, dan penerapan prinsip-prinsip etika dalam setiap proses operasional layanan digital.

Selain itu, regulasi terkait transaksi digital masih belum sepenuhnya memadai. Meskipun beberapa regulasi sudah ada, seperti UU Pelindungan Data Pribadi (PDP), Peraturan Bank Indonesia (BI), Otoritas Jasa Keuangan (OJK), UU ITE, PP PSTE, dan Perpres 82, implementasinya masih terbatas, terfragmentasi, dan sering kali tidak sesuai dengan dinamika teknologi yang berkembang pesat. Hal ini membuat banyak pelaku usaha dan masyarakat rentan terhadap praktik-praktik yang tidak etis atau bahkan ilegal. Contohnya, pengawasan pinjol melibatkan OJK, BI, dan Kemenkominfo/Kemkomdigi, namun, tumpang tindih kewenangan menyebabkan celah penegakan hukum. Sementara itu, transaksi aset kripto dan AI belum diatur secara komprehensif, menimbulkan ketidakpastian bisnis.

Salah satu faktor yang memperburuk situasi adalah rendahnya literasi digital masyarakat. Berdasarkan indeks literasi digital, sebagian besar masyarakat Indonesia masih memiliki pemahaman yang minim tentang cara menggunakan teknologi secara aman dan bertanggung jawab. Tingkat indeks literasi keamanan siber juga masih rendah, sehingga banyak individu yang mudah menjadi korban penipuan atau serangan siber. Selain itu, literasi terkait pelindungan data pribadi (PDP) dan aset digital masih sangat terbatas, membuat masyarakat kurang waspada terhadap potensi eksploitasi data. Indeks Literasi Digital Indonesia 2023 berada di angka 3,54 dari 5, dengan disparitas antara wilayah perkotaan dan pedesaan. Hanya 32% masyarakat memahami konsep pelindungan data pribadi, dan 45% pengguna *fintech* tidak menyadari risiko penyalahgunaan data. Rendahnya literasi ini menjadi penghambat utama pemanfaatan teknologi secara optimal serta meningkatkan kerentanan terhadap penipuan digital.

Untuk mengatasi hal ini, edukasi massal tentang literasi digital dan keamanan siber harus menjadi prioritas. Program-program seperti Gerakan Nasional Literasi Digital (GNLD) Siberkreasi, Kampanye Literasi Keamanan Siber (KLiKS) BSSN, dan Sandikamimania perlu diperluas untuk menjangkau lebih banyak kelompok masyarakat, termasuk pelajar, pekerja, dan UMKM.

Meskipun tantangan besar masih ada, peluang pertumbuhan ekonomi melalui transaksi digital di Indonesia sangat menjanjikan. Pada tahun 2024, transaksi digital di Indonesia diperkirakan mencapai USD 90 miliar, menjadikannya pasar digital terbesar di Asia Tenggara. Hal ini merupakan bukti nyata bahwa ekonomi digital dapat menjadi mesin pertumbuhan ekonomi nasional.

Pertumbuhan ini didorong oleh beberapa faktor, seperti meningkatnya jumlah pengguna internet, adopsi teknologi baru, serta dukungan pemerintah melalui kebijakan pro-digital. Misalnya, implementasi QRIS telah mempercepat transisi menuju ekonomi nontunai, sementara penggunaan AI dan IoT membuka peluang baru di berbagai sektor industri. Selain itu, inisiatif seperti *Satu Data Indonesia* dan *e-government* membantu meningkatkan efisiensi layanan publik, yang pada gilirannya mendukung pertumbuhan ekonomi. Namun, untuk memastikan bahwa peluang ini dapat dimaksimalkan, Indonesia perlu memperkuat fondasi ekosistem digitalnya. Regulasi yang lebih komprehensif, peningkatan literasi digital, serta investasi dalam infrastruktur keamanan siber harus menjadi prioritas utama.

Berdasarkan fakta-fakta tersebut, diperlukan kerangka kerja kepercayaan digital yang kuat untuk memastikan bahwa setiap entitas dalam transaksi digital, baik konsumen, penyedia layanan, regulator, maupun pihak ketiga, dapat beroperasi dengan aman, transparan, dan tepercaya. Dengan demikian, transformasi digital dapat benar-benar berkontribusi pada pertumbuhan ekonomi dan kesejahteraan nasional.

Bab ini menyajikan pemetaan tematik berdasarkan lima pertanyaan utama yang menjadi dasar penyusunan kerangka kerja kepercayaan digital di Indonesia. Pendekatan ini bertujuan untuk membangun ekosistem digital yang aman, andal, dan tepercaya, sekaligus mendorong partisipasi masyarakat dalam lingkungan digital yang lebih sehat. Selain memberikan perlindungan bagi seluruh pemangku ke-

pentingan, kerangka kerja ini juga memastikan bahwa transformasi digital selaras dengan nilai sosial, hukum, dan ekonomi nasional. Setiap aspek yang dikaji memberikan gambaran komprehensif mengenai urgensi, tujuan, pemangku kepentingan, tahapan implementasi, serta strategi yang digunakan dalam membangun ekosistem digital yang tepercaya. Berikut adalah pemetaan hasil identifikasi penerapan kepercayaan digital di Indonesia berdasarkan lima pertanyaan tematik, yang menjadi landasan dalam penyusunan kerangka kerja kepercayaan digital nasional.

5.1 Mengapa Kepercayaan Digital Penting (*Why*)

Kepercayaan digital menjadi elemen fundamental dalam mendukung transformasi digital nasional. Tanpa kepercayaan, masyarakat dan pelaku usaha akan ragu dalam menggunakan layanan digital, yang pada akhirnya dapat menghambat pertumbuhan ekonomi dan inovasi teknologi. Dengan meningkatnya ancaman siber serta penggunaan data secara masif, penting bagi Indonesia untuk membangun ekosistem digital yang aman, transparan, dan dapat diandalkan.

Seiring dengan pertumbuhan ekonomi digital di Indonesia, risiko keamanan dan privasi juga meningkat. Kasus penyalahgunaan data pribadi, penipuan *online*, hingga serangan siber semakin sering terjadi dan semakin kompleks. Dalam konteks ini, membangun kepercayaan digital tidak hanya menjadi kebutuhan teknis, tetapi juga strategis, terutama dalam menjaga kedaulatan data nasional di tengah dominasi platform digital global. Tanpa adanya kepercayaan digital yang berbasis regulasi dan teknologi lokal, data warga negara berisiko terus dimonetisasi dan dikendalikan oleh pihak asing, sehingga melemahkan kemandirian digital Indonesia. Lebih lanjut, kepercayaan digital juga merupakan prasyarat bagi keberhasilan adopsi kecerdasan artifisial (AI) secara masif. Tanpa fondasi kepercayaan, akan muncul *trust deficit* antara masyarakat dengan sistem berbasis AI yang berpotensi menghambat penerimaan dan pemanfaatannya secara luas.

Kerangka kerja kepercayaan digital diperlukan untuk menjamin bahwa setiap individu, bisnis, dan pemerintah dapat berpartisipasi dalam ekosistem digital secara aman dan percaya diri. Berikut adalah beberapa alasan utama mengapa kepercayaan digital memiliki peran strategis bagi Indonesia:

1. Mendukung Ekonomi Digital
   Indonesia memiliki potensi ekonomi digital yang besar, dengan proyeksi nilai ekonomi digital mencapai USD 360 miliar pada tahun 2030. Kepercayaan digital sangat penting untuk memastikan bahwa penyelenggara transaksi digital menyediakan sistem yang aman. Ketika konsumen merasa lebih percaya dalam bertransaksi, nilai ekonomi digital akan meningkat, membuka lebih banyak peluang investasi.

2. Melindungi Data dan Privasi Pengguna
   Dengan meningkatnya penggunaan teknologi digital, penyelenggara sistem elektronik tidak hanya perlu memastikan bahwa sistem yang digunakan aman

dan tepercaya, namun juga memastikan bahwa data pribadi dan aset digital tidak disalahgunakan oleh pihak yang tidak memiliki wewenang. Kepercayaan digital diperlukan untuk memastikan perlindungan aset digital dan data pribadi pengguna melalui regulasi yang berlaku di Indonesia, yaitu UU PDP dan UU ITE.

3. Menjamin Keamanan Nasional dan Siber
   Serangan siber terhadap infrastruktur vital, seperti perbankan, layanan publik, dan pertahanan, dapat mengancam keamanan nasional. Untuk mengatasinya, kepercayaan digital berperan penting dalam membangun sistem pertahanan siber yang tangguh. Hal ini dapat dicapai dengan menerapkan jaminan keamanan sejak level terkecil, seperti sistem transaksi digital dan sistem elektronik, melalui pendekatan *secure by design* yang mengutamakan keamanan dalam setiap tahap perancangan.

4. Mendorong Adopsi Teknologi dan Inklusi Digital
   Hadirnya kepercayaan digital memungkinkan masyarakat lebih percaya diri mengakses layanan digital dan beradaptasi dengan teknologi baru tanpa takut akan penyalahgunaan data, misalnya pada penggunaan teknologi identitas digital, transaksi elektronik, layanan keuangan digital, dan pemanfaatan kecerdasan artifisial untuk meningkatkan kinerja sistem elektronik.

5. Mendorong terwujudnya Visi Indonesia Digital 2045 dan Strategi Nasional Kecerdasan Artifisial 2020-2045
   Pemanfaatan teknologi digital baru, selain memberikan manfaat yang besar, tentunya memberikan ancaman dan risiko baru. Kepercayaan digital diperlukan untuk menjamin hak atas aset dan informasi digital dari setiap entitas.

6. Negara melalui sektor pemerintahan perlu hadir untuk mengatur dan memastikan ekosistem kepercayaan digital tumbuh secara harmonis
   Di Indonesia, kepercayaan digital belum menjadi topik utama secara nasional. Namun, beberapa komunitas dan industri global telah mulai memperkenalkan konsep ini dari perspektif masing-masing. Oleh karena itu, diperlukan kerangka kerja kepercayaan digital yang dapat mengakomodasi kebutuhan dan hak seluruh warga negara, memastikan keamanan dalam transaksi digital, serta mendukung pencapaian tujuan nasional.

Substansi pada aspek *Why* di atas menjelaskan urgensi kepercayaan digital dalam konteks ekonomi, keamanan, privasi, serta kedaulatan data. Agar kerangka kerja kepercayaan digital memiliki legitimasi yang kuat dan dapat dioperasionalkan, diperlukan landasan hukum yang jelas. Indonesia telah memiliki sejumlah regulasi yang secara langsung maupun tidak langsung mendukung aspek-aspek tersebut. Pemetaan pada Tabel 5.1 berikut menunjukkan keterkaitan antara alasan pentingnya kepercayaan digital dengan peraturan perundang-undangan yang relevan.

Tabel 5.1: Pemetaan Aspek *Why* dengan Regulasi Terkait di Indonesia

Aspek *Why*	**Regulasi/Peraturan Terkait**
Mendukung Ekonomi Digital	- UU No. 11 Tahun 2008 tentang ITE (jo. UU No. 19 Tahun 2016 jo. UU No. 1/2024) - PP No. 71 Tahun 2019 tentang Penyelenggaraan Sistem dan Transaksi Elektronik (PSTE)
Melindungi Data dan Privasi Pengguna	- UU No. 27 Tahun 2022 tentang Pelindungan Data Pribadi (UU PDP) - UU ITE
Menjamin Keamanan Nasional dan Siber	- Perpres No. 47 Tahun 2023 tentang Strategi Keamanan Siber Nasional dan Manajemen Krisis Siber - Peraturan BSSN No. 2 Tahun 2024 tentang Manajemen Krisis Siber - Peraturan BSSN No. 7 Tahun 2024 tentang Indonesia Common Criteria - Peraturan BSSN No. 11 Tahun 2024 tentang Algoritma Kriptografi Indonesia
Mendorong Adopsi Teknologi dan Inklusi Digital	- UU ITE - UU PDP - Perpres No. 95 Tahun 2018 tentang Sistem Pemerintahan Berbasis Elektronik (SPBE)
Mendukung Visi Indonesia Digital 2045 dan Strategi Nasional AI 2020–2045	- Strategi Nasional Kecerdasan Artifisial 2020–2045 - UU PDP
Peran Negara dalam Ekosistem Kepercayaan Digital	- UU No. 20 Tahun 2014 tentang Standardisasi dan Penilaian Kesesuaian - UU ITE - UU PDP - Perpres No. 47 Tahun 2023 - Peraturan BSSN (No. 2, 7, dan 11 Tahun 2024)

Berdasarkan pemetaan aspek *Why* terhadap regulasi yang terkait di Indonesia, dapat disimpulkan bahwa dasar kebijakan nasional dalam membangun kepercayaan digital didukung oleh kerangka hukum yang komprehensif dan saling melengkapi. Regulasi-regulasi tersebut tidak hanya berfokus pada perlindungan data dan keamanan siber, tetapi juga menekankan peran strategis negara dalam mendorong transformasi digital yang kolaboratif dan berdaya saing.

Undang-undang seperti UU ITE, UU PDP, serta berbagai peraturan turunan seperti PP PSTE dan peraturan BSSN menunjukkan konsistensi pemerintah dalam memastikan keamanan informasi, perlindungan privasi, dan keandalan infrastruktur digital nasional. Sementara itu, kebijakan jangka panjang seperti *Strategi Nasional Kecerdasan Artifisial 2020–2045* dan visi *Indonesia Digital 2045* mempertegas orientasi pemerintah menuju ekosistem digital yang berkelanjutan dan berdaulat. Dengan demikian, aspek *Why* dalam konteks kepercayaan digital Indonesia merepresentasikan komitmen negara untuk menyeimbangkan antara pertumbuhan ekonomi digital, keamanan nasional, perlindungan hak warga negara, dan inovasi teknologi sebagai pilar utama menuju transformasi digital yang aman dan tepercaya.

5.2 Tujuan Pengenalan Kepercayaan Digital (*What*)

Kepercayaan digital bukan hanya prasyarat bagi terselenggaranya transformasi digital yang berkelanjutan, melainkan juga elemen fundamental dalam memperkuat keamanan nasional, mendorong pertumbuhan ekonomi digital, dan menciptakan tata kelola ruang siber yang berintegritas. Dalam konteks kebijakan nasional, pemerintah Indonesia merancang dan memperkenalkan kerangka kepercayaan digital untuk menjawab tantangan keamanan, privasi, dan ketimpangan digital yang semakin kompleks. Tujuan pengenalan kepercayaan digital meliputi enam fokus utama berikut:

1. Menciptakan lingkungan digital yang aman dan tepercaya melalui tersedianya regulasi yang menjamin keamanan data, privasi, dan transaksi digital.
   Pemerintah dan lembaga terkait perlu menyediakan regulasi yang komprehensif untuk menjamin keamanan data, privasi, dan transaksi digital, terutama di era transformasi digital yang semakin pesat. Regulasi ini harus mencakup pelindungan terhadap data pribadi pengguna, mekanisme enkripsi yang kuat untuk menjaga kerahasiaan informasi, serta standar keamanan bagi sistem pembayaran dan transaksi digital agar terhindar dari ancaman kejahatan siber. Selain itu, regulasi yang diterapkan harus bersifat adaptif terhadap perkembangan teknologi dan mampu mengakomodasi berbagai inovasi tanpa mengorbankan aspek perlindungan data. Dengan adanya regulasi yang jelas dan tegas, masyarakat serta pelaku usaha dapat menjalankan aktivitas digital dengan lebih aman dan percaya diri, sehingga mendorong pertumbuhan ekonomi digital yang lebih stabil dan berkelanjutan.

2. Meningkatkan kesadaran dan literasi digital masyarakat untuk mencegah penyalahgunaan teknologi digital, seperti penipuan *online* dan serangan siber.
   Mencegah penyalahgunaan teknologi digital, seperti penipuan *online* dan serangan siber, merupakan langkah fundamental dalam membangun dan menjaga ekosistem digital yang aman dan tepercaya. Dalam era di mana teknologi merambah hampir seluruh aspek kehidupan, kepercayaan digital menjadi prasyarat utama bagi kelangsungan transformasi digital yang aman, andal dan berkelanjutan. Semakin tinggi ketergantungan terhadap sistem digital, semakin besar pula risiko eksploitasi dan kejahatan siber. Oleh karena itu, kepercayaan digital harus diperkuat melalui upaya preventif yang menyeluruh dan kolaboratif.
   Pemerintah, sektor swasta/industri, dan masyarakat memiliki peran penting dalam memperkuat dasar kepercayaan ini. Di antaranya melalui penerapan kebijakan perlindungan data yang ketat, penguatan infrastruktur keamanan siber, serta peningkatan literasi digital secara masif. Kepercayaan digital akan tumbuh ketika pengguna merasa aman dalam menggunakan layanan *online*, memahami hak dan kewajibannya, serta memiliki kemampuan untuk mengenali dan menghindari ancaman. Dalam konteks ini, edukasi tentang modus-modus penipuan dan cara mendeteksi potensi serangan menjadi langkah awal yang krusial. Selain itu, penegakan hukum terhadap pelaku

kejahatan siber juga perlu diperkuat untuk menciptakan efek jera dan menjamin bahwa ruang digital bukanlah wilayah tanpa hukum.
Lebih jauh, kepercayaan digital juga memainkan peran strategis dalam menjaga integritas demokrasi digital. Penyebaran disinformasi, ujaran kebencian, dan manipulasi algoritma di platform *online* dapat merusak tatanan demokrasi dan memicu konflik sosial, khususnya menjelang dan selama proses pemilu. Dalam konteks ini, kepercayaan masyarakat terhadap informasi digital harus dibangun melalui kolaborasi antara pemerintah, penyelenggara pemilu, dan platform digital dalam mengembangkan sistem deteksi konten berbahaya, memperkuat verifikasi informasi, serta menyediakan kanal pelaporan yang transparan dan responsif.
Kemampuan literasi digital yang kritis merupakan pilar utama dalam membentuk masyarakat yang resisten terhadap manipulasi informasi di ruang digital. Masyarakat yang memiliki kepercayaan digital yang kuat cenderung lebih cermat dalam menilai kebenaran suatu informasi dan tidak mudah terpengaruh oleh konten yang bersifat provokatif atau menyesatkan. Dalam konteks ini, kepercayaan digital berfungsi tidak hanya sebagai bentuk perlindungan individu dari ancaman teknologi, tetapi juga sebagai landasan etika dan sosial yang menopang kelangsungan demokrasi, memperkuat stabilitas sosial, serta menjaga persatuan nasional di tengah derasnya arus informasi digital.

3. Mempercepat transformasi digital di sektor publik dan swasta/industri

   - Mendorong digitalisasi layanan publik melalui Sistem Pemerintahan Berbasis Elektronik (SPBE).
     Pemerintah terus mendorong digitalisasi layanan publik melalui penerapan SPBE sebagai strategi untuk meningkatkan efisiensi, transparansi, dan kualitas pelayanan kepada masyarakat. Melalui pemanfaatan teknologi digital, berbagai layanan administrasi kini dapat diakses secara lebih cepat, mudah, dan terintegrasi, sehingga mampu menyederhanakan birokrasi yang selama ini dinilai kompleks serta meningkatkan efektivitas kerja aparatur negara. SPBE juga membuka peluang untuk mewujudkan interoperabilitas antarinstansi, yang memungkinkan pengelolaan data dan informasi secara lebih akurat dan efisien.
     Namun, seiring dengan meningkatnya ketergantungan pada sistem digital, ancaman siber terhadap SPBE menjadi tantangan yang tidak bisa diabaikan. Serangan seperti peretasan data, penyusupan *malware*, dan disrupsi layanan *online* dapat mengganggu operasional pemerintahan, merusak integritas data publik, dan menurunkan kepercayaan masyarakat terhadap sistem layanan digital pemerintah. Oleh karena itu, membangun dan memperkuat kepercayaan digital menjadi hal yang sangat krusial dalam ekosistem SPBE.
     Kepercayaan digital memainkan peran strategis dalam menciptakan rasa aman bagi masyarakat saat berinteraksi dengan layanan pemerintahan *online*. Hal ini mencakup jaminan terhadap pelindungan data pribadi, keandalan sistem, serta adanya mekanisme penanganan insiden siber yang efektif dan transparan. Ketika masyarakat merasa bahwa layanan

digital pemerintah aman dan tepercaya, maka partisipasi mereka dalam memanfaatkan SPBE akan meningkat. Pada akhirnya, digitalisasi layanan publik tidak hanya mempercepat transformasi birokrasi, tetapi juga memperkuat legitimasi dan kredibilitas pemerintah di era digital melalui penyelenggaraan layanan yang responsif, efisien, aman, dan akuntabel.

- Meningkatkan efisiensi dan transparansi dalam layanan publik berbasis digital. Pemanfaatan teknologi digital memungkinkan proses administrasi yang sebelumnya lambat dan manual menjadi lebih cepat, otomatis, dan mudah diakses. Otomatisasi prosedur mengurangi beban birokrasi yang berbelit serta meningkatkan akurasi pengelolaan data, sehingga mempercepat pengambilan keputusan yang tepat dan berbasis bukti.
  Selain meningkatkan kinerja internal pemerintahan, digitalisasi juga membuka ruang transparansi yang lebih luas. Melalui sistem digital yang terbuka, masyarakat dapat memantau secara *real-time* berbagai informasi terkait kebijakan, anggaran, layanan publik, serta proses pengaduan. Hal ini bukan hanya menekan potensi penyalahgunaan wewenang dan praktik korupsi, tetapi juga membangun pemerintahan yang akuntabel dan partisipatif.
  Dalam konteks ini, peran kepercayaan digital menjadi sangat penting. Kepercayaan digital menciptakan keyakinan masyarakat bahwa sistem layanan publik digital aman, dapat diandalkan, dan dikelola secara etis. Ketika pengguna merasa data pribadinya terlindungi dan interaksi digitalnya berlangsung dengan transparansi serta integritas, maka tingkat partisipasi dan adopsi layanan digital akan meningkat. Dengan demikian, kepercayaan digital tidak hanya memperkuat legitimasi pemerintah, tetapi juga menjadi fondasi utama dalam memastikan keberhasilan reformasi layanan publik berbasis teknologi.

4. Menerapkan konsep *Trust by Design* dalam penyelenggaraan sistem elektronik.
   Pendekatan *Trust by Design* merupakan strategi fundamental dalam membangun kepercayaan digital secara menyeluruh. Kepercayaan tidak terbentuk secara instan atau otomatis, melainkan harus ditanamkan secara sadar sejak tahap paling awal dalam perancangan sistem dan pengembangan layanan digital. Konsep ini menempatkan kepercayaan sebagai prinsip dasar dalam setiap proses desain, implementasi, dan pengelolaan teknologi informasi [326]. Inti dari pendekatan ini adalah integrasi menyeluruh terhadap aspek privasi dan keamanan, bukan sebagai tambahan di akhir proses, melainkan sebagai fondasi utama sejak perencanaan awal hingga pemeliharaan sistem. Dengan menempatkan kepercayaan sebagai bagian dari arsitektur desain, pengembang dapat secara proaktif mengidentifikasi dan memitigasi risiko sejak dini, sekaligus membangun sistem yang lebih resilien dan adaptif terhadap ancaman yang terus berkembang [327].
   Relevansi pendekatan ini semakin kuat dalam konteks percepatan transformasi digital, ketika layanan *online* telah menjadi tulang punggung aktivitas ekonomi, pemerintahan, dan interaksi sosial masyarakat. Kepercayaan digital menjadi faktor penentu keberhasilan adopsi teknologi, terutama ketika

pengguna dituntut untuk membagikan data pribadi mereka dalam berbagai layanan berbasis digital.
Dua komponen utama yang menjadi landasan dari *Trust by Design* adalah *Privacy by Design* dan *Security by Design*. Keduanya saling melengkapi dalam menjamin bahwa pelindungan data pribadi dan ketahanan sistem menjadi bagian yang tak terpisahkan dari setiap produk dan layanan digital yang dikembangkan. Bagian berikut akan membahas lebih lanjut mengenai kedua prinsip tersebut serta implementasinya dalam konteks Indonesia.

(a) *Privacy by Design*
Konsep *Privacy by Design* bertujuan untuk memastikan bahwa perlindungan privasi menjadi komponen inti dalam arsitektur sistem informasi dan proses bisnis. Pendekatan ini tidak menempatkan privasi sebagai tambahan di tahap akhir, melainkan sebagai bagian integral sejak tahap konseptualisasi hingga pascaimplementasi. Setiap langkah dalam siklus hidup pengembangan produk harus mempertimbangkan potensi dampak terhadap data pribadi pengguna [328].
Dalam konteks Indonesia, pendekatan ini menjadi semakin relevan seiring dengan penerapan UU PDP. Lembaga pemerintah dan pelaku usaha digital dituntut untuk menanamkan prinsip privasi tidak hanya demi kepatuhan terhadap regulasi, tetapi juga sebagai upaya membangun kepercayaan masyarakat terhadap layanan digital. Meningkatnya kesadaran publik terhadap hak-hak privasi menjadi pendorong penting bagi perusahaan teknologi untuk mengadopsi prinsip ini secara konsisten.

(b) *Security by Design*
Prinsip *Security by Design* mengharuskan pengembang sistem untuk mengintegrasikan mekanisme keamanan sejak tahap awal pengembangan produk. Tujuannya adalah untuk mengidentifikasi dan mengurangi risiko keamanan sebelum produk digunakan oleh publik. Pendekatan ini mencakup penilaian risiko siber secara berkala, penyusunan protokol mitigasi yang proaktif, serta penerapan pembaruan keamanan secara berkelanjutan [329, 330].
Di Indonesia, risiko kebocoran data, serangan *ransomware*, dan ancaman terhadap infrastruktur kritis terus meningkat. Menerapkan *Security by Design* secara sistematis dapat menjadi solusi preventif untuk menghadapi tantangan tersebut. Pengembangan aplikasi layanan publik, sistem pembayaran digital, dan platform *e-government* perlu memperhatikan prinsip ini agar sistem yang dihasilkan benar-benar tangguh dan andal dalam menghadapi potensi serangan siber.

Meskipun belum sepenuhnya mengadopsi kerangka kerja *digital trust by design* secara menyeluruh, beberapa perusahaan di Indonesia telah mengintegrasikan prinsip-prinsipnya dengan mematuhi regulasi yang berlaku. Contoh nyata terlihat pada Balai Besar Sertifikasi Elektronik (BSrE) di bawah BSSN, serta penyedia layanan seperti Privy dan Vida sebagai Penyelenggara Sertifikat Elektronik (PSrE). Ketiga entitas ini telah menerapkan teknologi kelas dunia untuk verifikasi identitas, autentikasi, dan tanda tangan elektronik yang

dirancang sejak awal dengan mengedepankan prinsip privasi dan keamanan. Standar internasional seperti ISO 27001 menjadi acuan utama, sementara audit berkala yang dilakukan memperkuat keandalan sistem dan meningkatkan tingkat kepercayaan dari pengguna dan mitra bisnis.
Perusahaan teknologi terkemuka seperti Tokopedia dan Gojek turut mengadopsi pendekatan *design thinking* yang menggabungkan keamanan dan kenyamanan pengguna. Tokopedia, misalnya, menerapkan desain antarmuka yang intuitif dan aman, mengurangi risiko kesalahan pengguna dan secara konsisten membangun kepercayaan melalui pembaruan sistem keamanan secara berkala. Inisiatif-inisiatif ini mencerminkan bagaimana prinsip *digital trust by design* telah diimplementasikan secara progresif dalam pengembangan layanan digital nasional.
Secara keseluruhan, implementasi *digital trust by design* di Indonesia telah menunjukkan kemajuan dengan menitikberatkan pada aspek-aspek berikut:

- Integrasi perlindungan privasi dan keamanan sejak tahap perancangan sistem.
- Transparansi kebijakan penggunaan data yang mudah diakses dan dipahami oleh pengguna.
- Pengendalian penuh oleh pengguna atas data pribadi mereka melalui mekanisme persetujuan.
- Pemanfaatan teknologi autentikasi dan enkripsi yang kuat serta sesuai standar internasional.

Keberhasilan *Trust by Design* bergantung pada komitmen untuk mengintegrasikan prinsip privasi dan keamanan sejak tahap desain awal. Praktik terbaik meliputi pelibatan tim keamanan dan kepatuhan dalam proses perancangan, penyusunan dokumentasi risiko, serta pelaksanaan evaluasi teknis secara berkala. Setiap iterasi produk harus disertai dengan pembaruan sistem perlindungan data dan audit keamanan yang relevan dengan ancaman terkini.
Penerapan prinsip *Trust by Design* membawa sejumlah manfaat penting. Risiko pelanggaran data dapat diminimalkan secara signifikan, baik dalam skala individu maupun institusi. Selain itu, kepatuhan terhadap regulasi, seperti UU PDP dan standar keamanan global, dapat dicapai dengan lebih efisien. Dalam jangka panjang, pendekatan ini memperkuat reputasi penyedia layanan digital dan meningkatkan daya saing nasional dalam ekosistem ekonomi digital global yang semakin kompetitif.

5. Memfasilitasi inovasi teknologi dengan regulasi yang adaptif
Memfasilitasi inovasi teknologi memerlukan regulasi yang adaptif agar perkembangan ekonomi digital dapat berjalan dengan lancar dan berkelanjutan. Oleh karena itu, diperlukan kerangka hukum yang fleksibel untuk menyesuaikan diri dengan dinamika teknologi yang terus berkembang, termasuk kecerdasan artifisial (AI), *blockchain*, dan *cloud computing*. Regulasi yang adaptif tidak hanya memberikan kepastian hukum bagi pelaku industri digital, tetapi juga membuka ruang bagi *startup* dan perusahaan teknologi untuk

bereksperimen serta mengembangkan solusi inovatif tanpa terbebani aturan yang kaku. Dengan pendekatan ini, pemerintah dapat menciptakan ekosistem digital yang kondusif, mendorong investasi, serta mempercepat adopsi teknologi dalam berbagai sektor, seperti keuangan, kesehatan, pendidikan, dan pemerintahan. Selain itu, regulasi yang pro-inovasi juga memungkinkan kolaborasi antara sektor publik dan swasta/industri untuk mengembangkan standar keamanan, transparansi, serta etika dalam penerapan teknologi baru. Dengan demikian, kebijakan terkait kepercayaan digital yang mendukung inovasi tidak hanya mempercepat transformasi digital, tetapi juga memastikan bahwa perkembangan teknologi tetap berlandaskan prinsip keadilan, perlindungan konsumen, dan keberlanjutan ekonomi.

6. Meningkatkan nilai ekonomi digital nasional
   Meningkatkan nilai ekonomi digital nasional memerlukan ekosistem yang aman dan tepercaya, di mana setiap entitas dapat bertransaksi secara digital tanpa kekhawatiran akan risiko keamanan dan privasi. Kepercayaan digital memainkan peran kunci dalam memastikan bahwa individu, bisnis, dan pemerintah merasa yakin dalam menggunakan teknologi digital untuk berbagai aktivitas ekonomi. Dengan adanya jaminan keamanan dalam transaksi digital, baik dari sisi perlindungan data, enkripsi, maupun regulasi yang mendukung, maka adopsi teknologi dalam sektor ekonomi akan semakin luas. Hal ini mendorong peningkatan permintaan terhadap produk dan jasa berbasis digital, yang pada akhirnya berdampak pada peningkatan volume transaksi serta investasi dalam sektor ekonomi digital. Seiring dengan semakin berkembangnya sistem pembayaran elektronik, *e-commerce*, dan layanan keuangan digital, kepercayaan digital akan menjadi faktor utama dalam mempercepat pertumbuhan ekonomi nasional serta menciptakan ekosistem bisnis yang lebih aman, andal dan berkelanjutan.

Dalam konteks Indonesia, berbagai tujuan yang dirumuskan dalam aspek *What* kepercayaan digital tidak dapat dipisahkan dari landasan hukum dan kebijakan nasional yang telah ditetapkan oleh pemerintah. Regulasi-regulasi ini berfungsi sebagai pilar normatif sekaligus instrumen operasional untuk memastikan bahwa keamanan, privasi, inovasi, serta keberlanjutan ekonomi digital dapat dicapai secara sistematis. Tabel 5.2 berikut memetakan keterkaitan antara fokus tujuan pengenalan kepercayaan digital dengan regulasi/peraturan yang relevan di Indonesia.

Tabel 5.2: Pemetaan Aspek *What* dengan Regulasi Terkait di Indonesia

Fokus Tujuan (*What*)	**Regulasi/Peraturan Terkait**
Keamanan data, privasi, dan transaksi digital	- UU No. 27 Tahun 2022 tentang Pelindungan Data Pribadi (UU PDP) - UU ITE (UU No. 11/2008 jo. UU No. 19/2016 jo. UU No. 1/2024) - Peraturan BSSN No. 7 Tahun 2024 (Indonesia Common Criteria) - Peraturan BSSN No. 11 Tahun 2024 (Algoritma Kriptografi Indonesia dan Penilaian Modul Kriptografi) - Regulasi BI/OJK terkait sistem pembayaran digital
Literasi digital dan pencegahan kejahatan siber	- Peraturan BSSN No. 2 Tahun 2024 tentang Manajemen Krisis Siber - UU ITE (penegakan hukum atas kejahatan siber)
Transformasi digital di sektor publik (SPBE)	- Perpres No. 95 Tahun 2018 tentang Sistem Pemerintahan Berbasis Elektronik (SPBE) - Perpres No. 47 Tahun 2023 tentang Strategi Keamanan Siber Nasional dan Manajemen Krisis Siber
Trust by Design (*Privacy by Design* dan *Security by Design*)	- UU PDP (2022) - Peraturan BSSN No. 11 Tahun 2024 (standar kriptografi nasional) - SNI ISO/IEC 27001 tentang Manajemen Keamanan Informasi
Regulasi adaptif untuk inovasi teknologi	- UU PDP dan regulasi turunannya - Kebijakan BI, OJK, dan Kemenkominfo terkait *fintech*, AI, *blockchain*, dan *cloud* - Peraturan BSSN No. 7/2024 dan No. 11/2024 (jaminan standar keamanan inovasi TI)
Peningkatan nilai ekonomi digital nasional	- Perpres No. 47 Tahun 2023 (Strategi Keamanan Siber Nasional) - UU PDP (jaminan keamanan transaksi digital) - Peraturan BSSN No. 2/2024, No. 7/2024, dan No. 11/2024

Kerangka regulasi di Indonesia menunjukkan adanya upaya komprehensif untuk membangun kepercayaan digital nasional. Pemetaan fokus tujuan dengan peraturan terkait memperlihatkan fokus utama pada keamanan data, privasi, dan transaksi digital, yang dijamin oleh pilar utama seperti UU PDP dan UU ITE, serta diperkuat oleh standar teknis BSSN dan peraturan spesifik sektor dari BI/OJK.

Pemerintah juga serius dalam mengintegrasikan aspek keamanan siber ke dalam ekosistem digital, terlihat dari upaya penegakan hukum ITE untuk pencegahan kejahatan siber, yang didukung oleh regulasi BSSN terkait literasi digital dan manajemen krisis. Regulasi ini tidak hanya menyentuh sektor privat, tetapi juga mendorong transformasi digital di sektor publik melalui Perpres SPBE, selaras dengan Strategi Keamanan Siber Nasional.

Prinsip dasar seperti *Trust by Design* (mencakup *Privacy* dan *Security by Design*) telah menjadi keharusan, diwujudkan melalui UU PDP dan standar kriptografi nasional yang ditetapkan BSSN. Pada akhirnya, semua kerangka hukum ini dirancang

untuk menciptakan regulasi adaptif yang mampu menjamin standar keamanan bagi inovasi teknologi (*fintech*, AI, *blockchain*), sekaligus bertujuan meningkatkan nilai ekonomi digital nasional dengan menyediakan lingkungan transaksi yang aman dan tepercaya bagi masyarakat dan pelaku usaha.

5.3 Siapa yang Bertanggung Jawab (*Who*)

Kepercayaan digital di Indonesia memiliki karakteristik tata kelola yang unik dan adaptif. Berbeda dengan pendekatan sentralistik yang mengandalkan entitas tunggal seperti *Digital Trust Committee*, Indonesia menerapkan model terdistribusi di mana fungsi strategis pengembangan kepercayaan digital diintegrasikan ke dalam tugas pokok dan fungsi berbagai kementerian serta lembaga terkait. Strategi ini memastikan bahwa aspek keamanan dan kepercayaan tidak berdiri sendiri, melainkan melekat pada setiap sektor layanan publik dan ekonomi.

Untuk mengorkestrasi fungsi-fungsi yang tersebar tersebut, Indonesia mengadopsi skema *pentahelix* yang menempatkan kolaborasi sebagai pilar utama. Dalam kerangka ini, pemerintah berperan sebagai regulator dan fasilitator, bersinergi dengan sektor swasta/industri yang menjadi motor inovasi, akademisi yang menyediakan landasan riset, masyarakat sipil yang menjalankan fungsi pengawasan, serta media yang berperan dalam edukasi publik. Sinergi lintas sektor ini bukan sekadar mekanisme koordinasi, melainkan fondasi vital untuk mengubah tanggung jawab keamanan siber dari beban sektoral menjadi komitmen kolektif, demi terwujudnya ekosistem digital nasional yang aman, kolaboratif, dan berkelanjutan.

1. Pemerintah dan Lembaga Negara
    - Kementerian Komunikasi dan Informatika (Kemenkominfo) atau Kementerian Komunikasi dan Digital (Kemkomdigi) memiliki peran utama dalam merumuskan dan mengimplementasikan regulasi serta kebijakan yang berkaitan dengan keamanan digital dan pelindungan data pribadi. Sebagai pengawas ekosistem digital, kementerian ini bertanggung jawab memastikan bahwa infrastruktur digital yang digunakan oleh masyarakat, pemerintah, dan sektor swasta/industri tetap aman dari ancaman siber, serta bahwa hak privasi setiap individu terlindungi sesuai dengan standar hukum yang berlaku. Dalam menjalankan tugasnya, Kementerian Komdigi mengembangkan berbagai regulasi terkait keamanan digital dan tata kelola data, sekaligus melakukan edukasi dan sosialisasi kepada masyarakat mengenai pentingnya literasi digital. Selain itu, kementerian ini juga bekerja sama dengan berbagai pemangku kepentingan, baik di tingkat nasional maupun internasional, untuk membangun sistem keamanan digital yang lebih kuat, mendukung inovasi teknologi, serta menanggulangi potensi ancaman siber yang semakin kompleks. Dengan pendekatan yang komprehensif, Kemenkominfo/Kemkomdigi berupaya menciptakan lingkungan digital yang aman, tepercaya, dan mendukung pertumbuhan ekonomi digital secara berkelanjutan.

- Badan Siber dan Sandi Negara (BSSN) berperan sebagai garda terdepan dalam menjaga keamanan siber nasional dengan mengawasi, mendeteksi, dan merespons berbagai ancaman yang berpotensi mengganggu stabilitas ruang siber di Indonesia. Sebagai lembaga yang bertanggung jawab atas ketahanan siber, BSSN mengembangkan kebijakan, standar, serta regulasi yang bertujuan untuk meningkatkan perlindungan terhadap infrastruktur siber nasional, baik di sektor pemerintahan, swasta, maupun industri strategis. Selain itu, BSSN juga berperan dalam menangani insiden siber dengan melakukan pemantauan aktif, investigasi, serta koordinasi dengan berbagai pihak, termasuk instansi pemerintah, penyedia layanan teknologi, dan lembaga internasional. Dalam menghadapi ancaman siber yang semakin kompleks, BSSN terus memperkuat kapabilitas keamanan siber melalui peningkatan sumber daya manusia, penggunaan teknologi canggih, serta kolaborasi dengan berbagai pemangku kepentingan guna menciptakan ekosistem siber yang aman, tangguh, dan tepercaya bagi seluruh masyarakat Indonesia.
- Otoritas Jasa Keuangan (OJK) dan Bank Indonesia (BI) memiliki peran penting dalam mengawasi transaksi keuangan digital, termasuk layanan keuangan berbasis teknologi (*fintech*) dan perbankan digital. Sebagai regulator, OJK bertanggung jawab memastikan bahwa penyedia layanan keuangan digital beroperasi sesuai dengan regulasi yang berlaku, melindungi konsumen dari potensi risiko, serta menjaga stabilitas sistem keuangan. Sementara itu, BI berfokus pada pengawasan sistem pembayaran digital, memastikan kelancaran transaksi, serta menetapkan kebijakan yang mendukung inovasi keuangan berbasis teknologi tanpa mengabaikan aspek keamanan dan perlindungan data. Melalui koordinasi yang erat, OJK dan BI berupaya menciptakan ekosistem keuangan digital yang aman dan andal sehingga dapat mendorong pertumbuhan ekonomi digital di Indonesia.
- Kementerian Dalam Negeri (Kemendagri) memiliki peran penting dalam pengelolaan identitas digital nasional, yang dijalankan melalui Direktorat Jenderal Kependudukan dan Pencatatan Sipil (Dukcapil). Salah satu inisiatif utama yang diemban adalah penyelenggaraan e-KTP digital, yang bertujuan untuk memperkuat sistem identitas penduduk berbasis teknologi. Dengan penerapan e-KTP digital, Kemendagri tidak hanya meningkatkan efisiensi administrasi kependudukan, tetapi juga memastikan keamanan dan validitas data pribadi setiap warga negara. Identitas digital yang dikelola secara terintegrasi ini berperan dalam mendukung berbagai layanan publik dan sektor swasta/industri, seperti perbankan, kesehatan, serta sistem pembayaran digital. Selain itu, Kemendagri terus berupaya memperluas akses dan pemanfaatan identitas digital guna mendorong transformasi digital nasional yang lebih aman, dan tepercaya.
- Kepolisian Republik Indonesia (POLRI) berperan sebagai penegak hukum dalam menindak berbagai pelanggaran yang berkaitan dengan penyalahgunaan informasi elektronik dan kejahatan siber. Dalam menja-

lankan tugasnya, POLRI memiliki wewenang untuk menyelidiki, mengidentifikasi, dan menindak pelaku kejahatan siber, seperti peretasan, pencurian data pribadi, penyebaran hoaks, penipuan *online*, serta berbagai bentuk kejahatan digital lainnya. Selain itu, POLRI juga berperan dalam meningkatkan kesadaran masyarakat terkait keamanan digital melalui sosialisasi dan edukasi mengenai ancaman siber serta cara pencegahannya. Dengan dukungan unit khusus seperti Direktorat Tindak Pidana Siber (Dittipidsiber) Bareskrim POLRI, aparat penegak hukum dapat lebih efektif dalam menangani kasus-kasus kejahatan siber yang semakin kompleks di era digital. Melalui langkah-langkah preventif dan represif yang dilakukan, POLRI berupaya menciptakan lingkungan digital yang lebih aman, sekaligus menjaga stabilitas dan ketertiban masyarakat di dunia maya.

- Penyelenggara Sistem Elektronik (PSE) di lingkup pemerintahan memiliki tanggung jawab strategis dalam mendukung transformasi digital sektor publik melalui penyediaan dan pengelolaan layanan digital yang andal, efisien, dan aman. Dalam implementasinya, PSE pemerintah mengoperasikan berbagai sistem elektronik yang menunjang layanan administrasi kependudukan, perizinan, keuangan, pendidikan, kesehatan, dan bidang-bidang pelayanan publik lainnya. Keberhasilan digitalisasi layanan publik sangat bergantung pada kualitas dan integritas sistem yang dikelola oleh PSE, baik dari aspek fungsionalitas maupun dari sisi keamanan dan perlindungan data.

  Sebagai pelaksana teknis dalam Sistem Pemerintahan Berbasis Elektronik (SPBE), PSE lingkup pemerintahan juga berada di garis depan dalam menjaga kepercayaan digital masyarakat. Kepercayaan digital dalam konteks ini mencakup persepsi masyarakat terhadap jaminan kerahasiaan, integritas, dan ketersediaan data serta layanan digital pemerintah. Ketika masyarakat merasa yakin bahwa informasi pribadinya aman dan bahwa layanan digital pemerintah transparan serta bebas dari manipulasi, maka partisipasi publik terhadap penggunaan layanan digital akan meningkat secara signifikan.

  Untuk mewujudkan ekosistem digital yang tepercaya, PSE lingkup pemerintahan harus menerapkan prinsip keamanan siber yang kuat, memperkuat interoperabilitas antarsistem, serta mematuhi kerangka regulasi yang berlaku, termasuk Peraturan BSSN tentang Infrastruktur Informasi Vital (IIV) dan pelindungan data pribadi. Di samping itu, peningkatan literasi digital aparatur dan penguatan mekanisme respon insiden juga menjadi bagian integral dalam membangun ketangguhan siber pemerintah.

2. Sektor swasta/industri dan Pelaku Usaha

   - Penyelenggara Sistem Elektronik (PSE), yang mencakup berbagai platform seperti *e-commerce*, *fintech*, dan media sosial, memiliki tanggung jawab besar dalam memastikan keamanan data pengguna serta kepatuhan terhadap regulasi digital yang berlaku. Dalam ekosistem digital yang

terus berkembang, pelindungan terhadap data pribadi menjadi aspek krusial untuk menjaga kepercayaan pengguna dan mencegah potensi penyalahgunaan informasi. Oleh karena itu, PSE wajib menerapkan langkah-langkah keamanan yang ketat, seperti enkripsi data, autentikasi berlapis, serta kebijakan privasi yang transparan. Selain itu, kepatuhan terhadap regulasi digital, termasuk UU PDP dan peraturan dari otoritas terkait, harus dijalankan secara konsisten guna memastikan operasional yang sesuai dengan standar hukum. Dengan menerapkan prinsip keamanan dan kepatuhan yang baik, PSE tidak hanya melindungi data pengguna, tetapi juga menciptakan ekosistem digital yang lebih aman, tepercaya, dan berkelanjutan.

- Asosiasi industri teknologi, seperti idEA (*Indonesian E-commerce Association*) dan AFTECH (Asosiasi *Fintech* Indonesia), memainkan peran penting dalam membangun standar kepercayaan digital di sektor industri digital dan keuangan. Melalui berbagai inisiatif, keduanya berkontribusi dalam penyusunan regulasi, pedoman keamanan, serta praktik terbaik yang memastikan ekosistem digital tetap aman, transparan, dan berorientasi pada perlindungan konsumen. idEA, sebagai wadah bagi industri *e-commerce*, mendorong standar keamanan transaksi *online*, perlindungan data pengguna, serta kebijakan yang mendukung perkembangan ekonomi digital. Sementara itu, AFTECH berperan dalam membangun sistem keuangan berbasis teknologi yang tepercaya dengan mengedepankan prinsip keamanan siber, inklusi keuangan, serta kepatuhan terhadap regulasi yang berlaku. Kolaborasi antara asosiasi ini dengan pemerintah, pelaku industri, dan masyarakat menjadi kunci dalam menciptakan lingkungan digital yang sehat dan berkelanjutan, sekaligus memperkuat kepercayaan publik terhadap layanan berbasis teknologi di Indonesia. Selain itu, terdapat pula asosiasi yang secara khusus bergerak di bidang keamanan siber, seperti ICSF (*Indonesia Cyber Security Forum*) dan CSIRT.ID (*Indonesia Computer Security Incident Response Team*). ICSF merupakan forum yang menghimpun berbagai pemangku kepentingan, termasuk pelaku industri, akademisi, dan pemerintah, untuk mendorong peningkatan kesadaran, kolaborasi, serta kapabilitas keamanan siber di tingkat nasional. Forum ini aktif dalam penyusunan rekomendasi kebijakan, pengembangan talenta keamanan siber, serta advokasi pentingnya tata kelola risiko digital di sektor publik dan swasta/industri.
  Sementara itu, CSIRT.ID, meskipun berawal dari inisiatif komunitas, kini telah berkembang menjadi bagian penting dari sistem tanggap insiden siber di Indonesia yang turut mendukung koordinasi dengan BSSN dan PSE. CSIRT.ID berperan dalam memperkuat ketahanan digital nasional melalui respons cepat terhadap insiden siber, pengumpulan intelijen ancaman, dan peningkatan kesiapsiagaan pelaku industri terhadap berbagai bentuk serangan siber.
  Kolaborasi antara asosiasi-asosiasi ini dengan pemerintah, pelaku industri, dan masyarakat menjadi kunci dalam menciptakan lingkungan digital yang sehat, adaptif, dan berkelanjutan. Mereka turut memper-

kuat fondasi kepercayaan digital di Indonesia melalui pengembangan ekosistem yang aman, berdaya saing, dan tangguh terhadap ancaman siber yang semakin kompleks di era transformasi digital.

3. Masyarakat dan Organisasi Masyarakat Sipil

   - Individu dan pengguna internet memiliki tanggung jawab besar dalam menjaga privasi dan keamanan digital pribadi agar terhindar dari ancaman seperti pencurian data, peretasan akun, serta penyalahgunaan informasi pribadi. Kesadaran akan pentingnya melindungi data pribadi harus dimulai dengan menerapkan kebiasaan digital yang aman, seperti menggunakan kata sandi yang kuat dan unik, mengaktifkan autentikasi dua faktor, serta berhati-hati dalam membagikan informasi di platform *online*. Selain itu, memahami kebijakan privasi aplikasi dan layanan yang digunakan juga menjadi langkah penting untuk mengontrol bagaimana data pribadi diproses dan disimpan. Dengan semakin berkembangnya teknologi dan meningkatnya risiko keamanan siber, setiap individu perlu terus meningkatkan literasi digital serta menerapkan langkah-langkah pencegahan agar tetap aman dalam beraktivitas di dunia digital.
   - Organisasi masyarakat sipil seperti SAFENet dan ICT Watch memiliki peran penting dalam memperjuangkan hak digital serta meningkatkan literasi digital di Indonesia. SAFENet, misalnya, aktif dalam advokasi kebebasan berekspresi, pelindungan data pribadi, serta hak-hak pengguna internet, terutama dalam menghadapi ancaman sensor dan represifitas digital. Sementara itu, ICT Watch berfokus pada edukasi dan kampanye literasi digital untuk mendorong penggunaan internet yang lebih aman, adil dan bertanggung jawab. Melalui berbagai inisiatif, seperti pelatihan, riset, serta kampanye kesadaran publik, kedua organisasi ini berupaya membangun ekosistem digital yang lebih sehat dengan menekankan pentingnya hak asasi manusia di ruang digital. Kehadiran mereka menjadi krusial dalam memastikan bahwa masyarakat tidak hanya memiliki akses terhadap teknologi, tetapi juga memahami hak-hak digitalnya serta mampu berpartisipasi secara aktif dan kritis dalam dunia digital yang terus berkembang.

4. Akademisi dan Lembaga Pendidikan
   Perguruan tinggi dan pusat riset memainkan peran yang sangat strategis dalam mendukung pembangunan ekosistem kepercayaan digital di Indonesia. Sebagai pusat keunggulan ilmu pengetahuan dan inovasi, institusi akademik tidak hanya menjadi sumber pengembangan teknologi digital, tetapi juga berkontribusi dalam penyusunan kebijakan publik berbasis bukti (*evidence-based policy*). Melalui kajian multidisipliner yang mencakup aspek teknis, sosial, hukum, dan etika, perguruan tinggi memberikan perspektif yang holistik terhadap isu-isu kepercayaan digital, seperti pelindungan data pribadi, keamanan siber, tata kelola internet, serta dampak sosial dari disinformasi dan algoritma.
   Selain itu, peran akademisi juga sangat penting dalam mendorong inovasi

teknologi yang aman dan bertanggung jawab, baik melalui riset fundamental maupun pengembangan teknologi terapan, seperti sistem identitas digital, enkripsi, keamanan perangkat IoT, dan kecerdasan artifisial yang etis. Pusat riset yang bekerja sama dengan sektor pemerintah dan industri dapat mempercepat lahirnya solusi lokal yang relevan dan adaptif terhadap tantangan global.

Dalam konteks literasi digital, perguruan tinggi juga bertindak sebagai motor penggerak transformasi budaya digital di masyarakat. Melalui program pendidikan, pelatihan, dan pengabdian kepada masyarakat, institusi pendidikan tinggi membekali mahasiswa dan masyarakat umum dengan keterampilan berpikir kritis, kemampuan mengenali ancaman digital, serta pemahaman atas hak dan tanggung jawab dalam ruang digital. Dengan demikian, pendidikan tinggi berperan penting dalam membentuk generasi pengguna digital yang tidak hanya cakap secara teknologis, tetapi juga sadar risiko, etis, dan berdaya dalam menjaga integritas ruang digital.

5. Media massa dan platform informasi turut serta dalam penyebaran informasi yang akurat mengenai hak digital, kebijakan pemerintah, serta berbagai isu terkait ancaman dan solusi keamanan siber. Peran mereka sangat penting dalam membentuk opini publik, memperkuat transparansi, serta menjembatani komunikasi antara pemangku kebijakan dan masyarakat luas. Dalam konteks kepercayaan digital, integritas media menjadi faktor kunci dalam memastikan bahwa informasi yang disampaikan bersifat faktual, berimbang, dan bebas dari manipulasi yang dapat merusak persepsi publik terhadap isu-isu strategis, seperti pelindungan data pribadi, penyalahgunaan teknologi, dan regulasi digital.

   Selain menyajikan pemberitaan harian, media juga berkontribusi dalam menyebarluaskan hasil-hasil riset terkait keamanan siber dan transformasi digital. Publikasi ini mencakup analisis tren serangan siber, efektivitas kebijakan keamanan, hingga evaluasi terhadap kesiapan institusi publik dan swasta/industri dalam menghadapi risiko digital. Melalui publikasi tersebut, media membantu memperkaya diskursus publik sekaligus mendorong akuntabilitas para pemangku kepentingan dalam merespons tantangan siber secara sistematis.

   Lebih dari sekadar penyampai informasi, media juga memiliki peran edukatif dalam meningkatkan literasi dan kesadaran masyarakat terhadap keamanan siber. Banyak media yang aktif memproduksi konten edukatif seperti artikel opini, infografik, program siaran, dan kampanye publik untuk mengedukasi pengguna internet mengenai cara-cara menghindari penipuan *online*, pentingnya manajemen kata sandi, serta cara melindungi data pribadi di dunia digital. Partisipasi aktif media dalam program literasi digital dan kampanye kesadaran keamanan siber turut memperkuat ekosistem digital yang lebih aman, tepercaya dan bertanggungjawab. Dengan peran yang multidimensional tersebut, media massa berkontribusi secara nyata dalam memperkuat kepercayaan digital di Indonesia, tidak hanya melalui penyampaian informasi yang jujur dan akurat, tetapi juga melalui peran aktif dalam pendidikan publik dan advokasi kebijakan berbasis bukti.

Tabel 5.3: Pemetaan Aspek *Who* dengan Regulasi Terkait di Indonesia

Aktor (*Who*)	**Regulasi/Peraturan Terkait**
Kementerian Komunikasi dan Informatika (Kemenkominfo/Kemkomdigi)	- UU No. 27 Tahun 2022 tentang Pelindungan Data Pribadi (UU PDP) - UU No. 11 Tahun 2008 jo. UU No. 19 Tahun 2016 jo. UU No. 1/2024 tentang ITE - Perpres No. 95 Tahun 2018 tentang SPBE
Badan Siber dan Sandi Negara (BSSN)	- Perpres No. 47 Tahun 2023 tentang Strategi Keamanan Siber Nasional dan Manajemen Krisis Siber - Peraturan BSSN No. 2 Tahun 2024 tentang Manajemen Krisis Siber - Peraturan BSSN No. 7 Tahun 2024 tentang Indonesia Common Criteria - Peraturan BSSN No. 11 Tahun 2024 tentang Algoritma Kriptografi Indonesia dan Sertifikasi Modul Kriptografi - Peraturan BSSN tentang Infrastruktur Informasi Vital (IIV)
Otoritas Jasa Keuangan (OJK) dan Bank Indonesia (BI)	- UU No. 21 Tahun 2011 tentang OJK - Peraturan OJK (POJK) terkait *fintech*, perlindungan konsumen, dan layanan keuangan digital - Peraturan Bank Indonesia terkait sistem pembayaran, QRIS, dan uang elektronik
Kementerian Dalam Negeri (Dukcapil)	- UU No. 24 Tahun 2013 tentang Administrasi Kependudukan - Perpres No. 95 Tahun 2018 (SPBE) terkait identitas digital
POLRI	- UU ITE (dasar hukum penegakan hukum kejahatan siber) - Peraturan Kapolri terkait tindak pidana siber (Dittipidsiber)
PSE Pemerintah	- Perpres No. 95 Tahun 2018 (SPBE) - UU PDP - Peraturan BSSN tentang IIV
PSE Swasta (*E-commerce*, *Fintech*, Media Sosial)	- UU PDP - UU ITE - PP No. 71 Tahun 2019 tentang PSTE - POJK dan Peraturan BI terkait sektor keuangan digital
Asosiasi Industri (idEA, AFTECH, ICSF, CSIRT.ID)	- Beroperasi dalam kerangka regulasi Kemenkominfo, OJK, BI, dan BSSN; mendukung penyusunan standar serta kebijakan keamanan digital
Masyarakat Sipil (SAFENet, ICT Watch)	- UU PDP - UU ITE (landasan advokasi hak digital dan kebebasan berekspresi)
Akademisi dan Perguruan Tinggi	- Perpres No. 95 Tahun 2018 tentang SPBE (kolaborasi riset dan inovasi) - Peraturan BSSN (kolaborasi riset bidang keamanan siber dan kriptografi)
Media Massa	- UU No. 40 Tahun 1999 tentang Pers - UU ITE (batasan distribusi informasi digital)

Pembangunan kepercayaan digital di Indonesia tidak dapat dilakukan secara parsial, melainkan menuntut orkestrasi peran seluruh aktor dalam kerangka hukum yang kokoh. Sinergi lintas sektor ini menjadi kunci dalam mewujudkan transformasi digital nasional yang aman, tepercaya, dan berkelanjutan. Dalam pelaksanaannya, setiap aktor beroperasi dalam koridor regulasi yang menetapkan arah serta batasan wewenang yang jelas. Kerangka regulasi tersebut berfungsi tidak hanya sebagai pedoman normatif, tetapi juga sebagai landasan legitimasi bagi pemerintah, industri, akademisi, masyarakat sipil, dan media dalam menjalankan fungsinya masing-masing. Keterkaitan antara aktor-aktor utama tersebut dengan instrumen hukum yang memayunginya dipetakan secara rinci dalam Tabel 5.3.

5.4 Waktu dan Tahapan Implementasi (*When*)

Transformasi digital nasional merupakan proses jangka panjang yang menuntut perencanaan yang matang, terstruktur, dan berkelanjutan. Dalam menghadapi kompleksitas tantangan dan peluang di era digital, Indonesia tidak dapat menerapkan pendekatan seragam yang bersifat instan. Oleh karena itu, diperlukan kerangka waktu yang realistis dan terukur guna memastikan bahwa setiap komponen, baik regulasi, infrastruktur, maupun sumber daya manusia, dapat berkembang secara selaras dan bertahap. Pembagian waktu dalam empat tahapan transformasi digital nasional dari 2025 hingga 2045 bukanlah keputusan yang bersifat arbitrer, melainkan merupakan strategi bertahap yang dirancang dengan mempertimbangkan kesiapan ekosistem digital Indonesia secara menyeluruh.

Setiap fase memiliki fokus, tujuan, dan indikator keberhasilan yang berbeda, disesuaikan dengan dinamika perkembangan regulasi, infrastruktur, kapasitas institusi, serta kesiapan masyarakat dan sektor industri serta selaras dengan Rencana Pembangunan Jangka Panjang Nasional sesuai UU Nomor 59 Tahun 2024. Dengan pendekatan ini, transformasi digital dapat dijalankan secara sistematis, adaptif, dan berkelanjutan demi mewujudkan visi Indonesia sebagai negara berdaya saing tinggi di era digital global.

1. 2025 - 2029: Penguatan Transformasi dan Landasan Regulasi
   Tahap awal transformasi digital Indonesia pada periode 2025–2029 diarahkan pada penguatan dasar ekosistem digital, salah satunya melalui transformasi tata kelola yang difokuskan pada perbaikan kelembagaan yang tepat fungsi, penyempurnaan fondasi penataan regulasi, pembentukan dan penguatan lembaga tunggal pengelola regulasi, serta penguatan keamanan manusia dan keamanan siber sebagai pilar-pilar keamanan nasional yang kuat, akuntabel berbasis digital. Penguatan ini merupakan prasyarat utama untuk menciptakan ruang digital yang aman, tertib, dan memiliki kepastian hukum. Implementasi Peraturan Presiden Nomor 82 Tahun 2023 tentang Percepatan Transformasi Digital serta Peraturan Presiden Nomor 47 Tahun 2023 tentang Strategi Keamanan Siber Nasional dan Manajemen Krisis Siber menjadi pijakan strategis yang mengatur arah dan koordinasi kebijakan lintas sektor

dalam proses digitalisasi nasional. Selaras dengan itu, penguatan instrumen hukum seperti UU PDP, UU ITE, serta berbagai peraturan pelaksananya ditujukan untuk melindungi hak-hak digital warga negara dan meningkatkan kepercayaan publik terhadap ekosistem digital nasional. Upaya ini diposisikan sebagai langkah dasar yang esensial sebelum melanjutkan ke tahap digitalisasi layanan publik secara menyeluruh. Dengan demikian, periode ini berfungsi sebagai fase konsolidasi kebijakan guna memastikan transformasi digital nasional berlangsung secara terstruktur, akuntabel, dan berkelanjutan.

2. 2030 - 2034: Akselerasi Transformasi dan Adopsi Layanan Digital
   Setelah landasan hukum terbentuk pada tahap awal, periode 2030–2034 berfokus pada penguatan transformasi digital melalui pemanfaatan teknologi digital yang semakin luas di berbagai aspek kehidupan, penguatan riset dan inovasi digital, serta percepatan pemanfaatan teknologi digital dalam pelayanan publik dan pengelolaan identitas warga negara. Fokus utama pada tahap ini adalah adopsi menyeluruh terhadap Sistem Pemerintahan Berbasis Elektronik (SPBE) dan Identitas Digital Nasional (Digital ID), yang berperan krusial dalam meningkatkan efisiensi birokrasi, integrasi data antarinstansi, serta kualitas layanan publik. Digital ID diterapkan sebagai standar utama untuk mengakses berbagai layanan digital, memungkinkan masyarakat mendapatkan layanan secara lebih mudah, aman, dan efisien, sekaligus memperkuat pelindungan data pribadi. Di sisi lain, penerapan SPBE secara penuh menjadi fondasi modernisasi tata kelola pemerintahan, mempercepat proses administratif, meningkatkan transparansi, dan memperluas jangkauan layanan. Integrasi antara SPBE dan Digital ID akan menciptakan ekosistem pemerintahan digital yang andal, tepercaya, dan adaptif terhadap kebutuhan masyarakat. Dengan demikian, tahap ini diharapkan dapat memperkuat kepercayaan publik terhadap pemerintah digital sekaligus mendorong partisipasi masyarakat dalam ruang digital yang aman dan akuntabel.

3. 2035 - 2039: Ekspansi Global dan Diplomasi Digital
   Tahap ketiga (2035–2039) merupakan periode akselerasi dan konsolidasi posisi Indonesia dalam peta ekonomi digital global. Pada fase ini, Indonesia menargetkan diri untuk menjadi pemimpin digital di Asia Tenggara dengan memperkuat daya saing melalui inovasi teknologi yang andal dan berkelanjutan. Fokus utama diarahkan pada pengembangan teknologi canggih, seperti kecerdasan artifisial (AI), *blockchain*, dan sistem keamanan digital generasi baru yang mampu meningkatkan kepercayaan publik terhadap layanan digital lintas sektor. Keberhasilan tahap ini sangat bergantung pada pelaksanaan dua fase sebelumnya yang membangun landasan regulatif, serta adopsi layanan digital secara masif. Dengan kerangka hukum yang sudah matang, Indonesia dapat memanfaatkan teknologi untuk menjamin keamanan data, melindungi privasi, dan mendorong efisiensi serta transparansi dalam berbagai aktivitas digital. Lebih dari sekadar penguatan internal, periode ini juga menjadi momentum penting bagi Indonesia untuk memperluas diplomasi digital, mengadopsi standar internasional, serta berkontribusi secara aktif dalam pembentukan tata kelola teknologi global. Dengan strategi yang terarah,

penguatan kapasitas inovasi, dan kolaborasi lintas sektor, Indonesia memiliki potensi besar untuk tampil sebagai pusat inovasi digital dan pemain utama dalam ekosistem digital kawasan Asia Tenggara.

4. 2040 - 2045: Perwujudan Indonesia Emas
   Pada tahap keempat (2040–2045), Indonesia mencapai puncak visinya sebagai Indonesia Emas, menandai keberhasilan transformasi menyeluruh menjadi negara maju. Fokus utama transformasi sosial diarahkan pada perwujudan manusia Indonesia yang tidak hanya sejahtera dan adaptif, tetapi juga berakhlak mulia serta berbudaya maju. Kualitas sumber daya manusia yang unggul dan berdaya saing global ini menjadi fondasi utama dalam membangun peradaban masyarakat yang tangguh dan bermartabat.
   Transformasi ekonomi pada periode ini didorong oleh pemanfaatan teknologi dan digitalisasi yang masif, mengantarkan Indonesia menjadi negara berpendapatan tinggi (*high-income country*). Optimalisasi bonus demografi diarahkan untuk mencetak talenta-talenta inovatif yang mampu menghasilkan karya berdaya saing global, memastikan Indonesia berperan sebagai pemain kunci dalam rantai nilai ekonomi dunia. Sinergi antara kapabilitas SDM dan ekosistem inovasi ini menjadi motor penggerak pertumbuhan ekonomi yang berkelanjutan.
   Keberlanjutan kemajuan tersebut ditopang oleh ekosistem kepercayaan digital yang kokoh, khususnya di sektor vital seperti ekonomi dan finansial. Integritas sistem digital yang terjamin keamanan dan transparansinya menjadi prasyarat mutlak bagi stabilitas transaksi nasional. Dengan demikian, perpaduan antara kemajuan peradaban, kekuatan ekonomi, dan kedaulatan digital akan mengukuhkan posisi Indonesia sebagai bangsa yang berdaulat, adil, dan makmur dalam tatanan global.

Secara keseluruhan, periodisasi ini mencerminkan pendekatan progresif: dimulai dari penataan fondasi regulasi (2025-2029), akselerasi adopsi layanan (2030-2034), ekspansi pengaruh global (2035-2039), hingga pencapaian puncak kemajuan nasional (2040-2045). Peta jalan ini memastikan bahwa ekosistem kepercayaan digital tumbuh selaras dengan kemajuan teknologi, demi mendukung visi Indonesia sebagai negara maju yang berdaulat secara digital.

Dalam konteks aspek *When*, lini masa pembangunan kepercayaan digital tersebut tidak dapat dipisahkan dari kerangka regulasi strategis yang memayunginya. Setiap fase waktu tidak hanya menandai perkembangan teknologi, tetapi juga merepresentasikan evolusi kebijakan, tata kelola, dan kesiapan infrastruktur hukum. Regulasi-regulasi ini berfungsi sebagai pilar untuk menjamin bahwa transformasi digital berlangsung secara terukur dan konsisten menuju visi Indonesia Emas 2045. Tabel 5.4 berikut menyajikan pemetaan antara tahapan waktu implementasi dengan instrumen kebijakan yang relevan.

Tabel 5.4: Pemetaan Aspek *When* dengan Regulasi Terkait di Indonesia

Tahapan Waktu (*When*)	**Regulasi/Peraturan Terkait**
2025–2029: Penguatan Transformasi dan Landasan Regulasi	- Perpres No. 82 Tahun 2023 tentang Percepatan Transformasi Digital - Perpres No. 47 Tahun 2023 tentang Strategi Keamanan Siber Nasional dan Manajemen Krisis Siber - UU No. 27 Tahun 2022 tentang Pelindungan Data Pribadi (UU PDP) - UU No. 11 Tahun 2008 jo. UU No. 19 Tahun 2016 jo. UU No. 1/2024 tentang Informasi dan Transaksi Elektronik (UU ITE) - Peraturan BSSN No. 2 Tahun 2024 tentang Manajemen Krisis Siber - Peraturan BSSN No. 7 Tahun 2024 tentang Indonesia Common Criteria - Peraturan BSSN No. 11 Tahun 2024 tentang Algoritma Kriptografi Indonesia dan Penilaian Kesesuaian Modul Kriptografi
2030–2034: Akselerasi Transformasi dan Adopsi Layanan Digital	- Perpres No. 95 Tahun 2018 tentang Sistem Pemerintahan Berbasis Elektronik (SPBE) - UU No. 24 Tahun 2013 tentang Administrasi Kependudukan sebagai dasar pengembangan Identitas Digital Nasional - UU No. 27 Tahun 2022 tentang Pelindungan Data Pribadi (UU PDP) untuk perlindungan data dalam layanan publik digital - Perpres No. 82 Tahun 2023 tentang Transformasi Digital Nasional sebagai dasar koordinasi lintas sektor - Kebijakan sektoral Kemenkominfo dan BSSN mengenai keamanan SPBE dan interoperabilitas data
2035–2039: Ekspansi Global dan Diplomasi Digital	- UU No. 59 Tahun 2024 tentang Rencana Pembangunan Jangka Panjang Nasional (RPJPN) 2025–2045 - Perpres No. 47 Tahun 2023 tentang Strategi Keamanan Siber Nasional sebagai dasar penguatan posisi Indonesia dalam diplomasi digital global - UU No. 27 Tahun 2022 tentang Pelindungan Data Pribadi (UU PDP) dan regulasi turunannya sebagai standar nasional perlindungan data - Adopsi standar internasional (ISO/IEC 27001, OECD, ENISA, dll.) untuk keamanan siber, kecerdasan artifisial, dan *blockchain*
2040–2045: Perwujudan Indonesia Emas Digital	- UU No. 59 Tahun 2024 tentang RPJPN 2025–2045 sebagai kerangka pembangunan nasional jangka panjang - Perpres No. 82 Tahun 2023 tentang Transformasi Digital dan Perpres No. 47 Tahun 2023 tentang Keamanan Siber Nasional sebagai pedoman integrasi teknologi dan ekonomi digital - Kebijakan penguatan SDM digital dan inovasi nasional oleh Kemenkominfo, BSSN, dan Bappenas - Strategi Nasional Kecerdasan Artifisial (AI) dan kebijakan inovasi digital berkelanjutan

5.5 Bagaimana Kepercayaan Digital Diterapkan (*How*)

Strategi untuk mewujudkan kepercayaan digital di Indonesia disusun berdasarkan peta jalan penerapannya serta hasil identifikasi empat pertanyaan tematik terkait. Strategi ini mencakup:

1. Regulasi dan Kebijakan Keamanan Digital

   - Implementasi UU PDP dan penguatan pelindungan data pribadi oleh PSE dan perusahaan penyedia teknologi.
     Implementasi UU PDP menjadi langkah krusial dalam memastikan keamanan dan privasi data masyarakat di era digital. Dengan semakin meningkatnya penggunaan layanan berbasis teknologi, PSE dan perusahaan teknologi memiliki tanggung jawab besar dalam memperkuat pelindungan data pribadi pengguna. Hal ini mencakup penerapan kebijakan yang transparan, sistem keamanan yang ketat, serta mekanisme pengelolaan data yang sesuai dengan regulasi. Selain itu, perusahaan teknologi juga harus memastikan kepatuhan terhadap prinsip-prinsip perlindungan data, seperti persetujuan pengguna, pembatasan akses, serta penerapan enkripsi untuk mencegah kebocoran atau penyalahgunaan informasi pribadi. Dengan adanya regulasi yang jelas dan pengawasan yang ketat, implementasi UU PDP diharapkan dapat meningkatkan kepercayaan masyarakat terhadap ekosistem digital serta mendorong inovasi yang bertanggung jawab dalam pengelolaan data di Indonesia.
   - Pengawasan ketat terhadap kepatuhan sektor digital melalui OJK, BI, Kemenkominfo/Kemkomdigi, BSSN, dan POLRI.
     Pengawasan ketat terhadap kepatuhan sektor digital dilakukan melalui koordinasi antara OJK, BI, Kemenkominfo/Kemkomdigi, BSSN, dan POLRI guna memastikan ekosistem digital yang aman, transparan, dan sesuai dengan regulasi yang berlaku. OJK berperan dalam mengawasi penyelenggara jasa keuangan digital, termasuk perbankan, *fintech*, dan asuransi, agar beroperasi sesuai dengan prinsip kehati-hatian serta perlindungan konsumen. Sementara itu, BI bertanggung jawab dalam mengatur dan mengawasi sistem pembayaran digital, termasuk transaksi elektronik dan dompet digital, guna menjaga stabilitas moneter serta kelancaran sistem pembayaran nasional.
     Kemenkominfo/Kemkomdigi memiliki peran krusial dalam memastikan keamanan siber, pelindungan data pribadi, serta pengelolaan infrastruktur telekomunikasi yang mendukung layanan digital secara nasional. Di sisi lain, BSSN berperan sebagai otoritas utama dalam perlindungan infrastruktur informasi vital dan penguatan ketahanan siber nasional. BSSN mengembangkan kebijakan teknis, standar keamanan, serta melakukan pemantauan dan koordinasi tanggap insiden siber pada sistem digital yang digunakan oleh instansi pemerintah maupun sektor strategis.

Keterlibatan BSSN memperkuat kerangka kepercayaan digital melalui pendekatan preventif dan responsif terhadap potensi ancaman siber yang kompleks.
Adapun POLRI, melalui Direktorat Tindak Pidana Siber (Dittipidsiber), menjalankan fungsi penegakan hukum terhadap pelanggaran di ruang digital, termasuk kejahatan siber seperti peretasan, pencurian data, penyebaran hoaks, penipuan *online*, dan bentuk penyalahgunaan teknologi lainnya. Kehadiran POLRI menjadi penting untuk memberikan efek jera terhadap pelaku kejahatan digital sekaligus menjamin kepastian hukum bagi masyarakat pengguna layanan digital.
Dengan sinergi antara kelima lembaga ini, pengawasan terhadap sektor digital dapat dilakukan secara lebih menyeluruh dan berlapis, menciptakan lingkungan digital yang aman, tepercaya, serta mendorong inovasi yang tetap berada dalam koridor hukum dan kepatuhan terhadap standar keamanan nasional.

- Penerapan peraturan perundangan oleh setiap penyelenggaran sistem transaksi elektronik untuk mewujudkan kepercayaan digital.
  Penerapan peraturan perundangan oleh setiap penyelenggara sistem transaksi elektronik menjadi langkah krusial dalam membangun ekosistem digital yang aman dan tepercaya. Standar ini mencakup berbagai aspek, seperti pelindungan data pribadi, keamanan transaksi, serta transparansi dalam pengelolaan informasi, sehingga dapat meminimalkan risiko penyalahgunaan dan ancaman siber. Dengan adanya kepatuhan terhadap regulasi dan kebijakan yang ditetapkan, baik oleh pemerintah maupun lembaga terkait, pengguna layanan digital dapat merasa lebih aman dalam melakukan transaksi elektronik. Selain itu, penerapan peraturan perundangan juga berkontribusi dalam meningkatkan kepercayaan masyarakat terhadap teknologi digital, mendorong inklusi keuangan, serta mempercepat adopsi layanan berbasis digital di berbagai sektor. Dengan demikian, kepatuhan terhadap standar yang berlaku tidak hanya melindungi konsumen, tetapi juga mendukung pertumbuhan ekonomi digital yang berkelanjutan dan berdaya saing tinggi.

2. Peningkatan Infrastruktur Keamanan Siber

   - Pembangunan Pusat Data Nasional (PDN) merupakan langkah strategis dalam upaya pengelolaan dan penyimpanan data negara secara terpusat, aman, dan efisien. PDN berfungsi sebagai infrastruktur utama untuk menyimpan data strategis yang mencakup informasi pemerintahan, kependudukan, keuangan, serta sektor-sektor penting lainnya. Dengan adanya PDN, integrasi dan interoperabilitas sistem antarinstansi dapat ditingkatkan, sehingga mendukung efisiensi layanan publik serta mempercepat transformasi digital di Indonesia. Selain itu, PDN juga dirancang dengan standar keamanan tinggi untuk melindungi data dari ancaman siber dan kebocoran informasi, sehingga memastikan kedaulatan serta perlindungan data nasional. Melalui pembangunan PDN, pemerintah dapat memperkuat tata kelola data yang lebih terstruktur, meningkatkan

transparansi, serta mendukung pengambilan kebijakan berbasis data yang akurat dan tepercaya.

- BSSN membangun National Cyber Security Operation Center (NSOC) sebagai upaya strategis dalam menangani ancaman siber secara *real-time*. NSOC berfungsi sebagai pusat kendali yang memantau, mendeteksi, dan merespons berbagai serangan siber yang berpotensi mengancam infrastruktur digital nasional, termasuk sektor pemerintahan, keuangan, dan layanan publik lainnya. Dengan teknologi canggih dan analisis berbasis kecerdasan artifisial, NSOC mampu mengidentifikasi pola ancaman siber serta memberikan respons cepat untuk meminimalkan dampaknya. Selain itu, pusat operasi ini juga berperan dalam koordinasi lintas sektor guna meningkatkan ketahanan siber nasional melalui kerja sama dengan instansi pemerintah, sektor swasta/industri, dan komunitas keamanan siber. Pengembangan NSOC tidak hanya meningkatkan kemampuan pertahanan digital Indonesia tetapi juga memperkuat kepercayaan masyarakat terhadap keamanan ekosistem digital yang semakin berkembang pesat.

3. Peningkatan Literasi Digital dan Kesadaran Masyarakat

- Kampanye edukasi tentang hoaks, keamanan siber, dan etika digital melalui program Gerakan Nasional Literasi Digital bertujuan untuk meningkatkan kesadaran serta pemahaman masyarakat dalam menghadapi tantangan di era digital. Melalui program ini, berbagai inisiatif dilakukan, seperti pelatihan, seminar, dan penyebaran informasi edukatif yang membantu masyarakat mengenali serta mencegah penyebaran berita hoaks yang dapat menyesatkan opini publik. Selain itu, aspek keamanan siber menjadi perhatian utama dengan memberikan pemahaman mengenai pelindungan data pribadi, cara mengamankan akun digital, serta langkah-langkah menghindari ancaman siber, seperti peretasan dan penipuan *online*. Tidak kalah penting, kampanye ini juga menanamkan nilai-nilai etika digital, seperti bertanggung jawab dalam bermedia sosial, menghargai privasi orang lain, serta membangun komunikasi yang positif di dunia maya. Dalam kerangka ini, lembaga pendidikan memainkan peran strategis melalui integrasi kurikulum berbasis literasi digital, penguatan mata kuliah keamanan informasi, serta pemberdayaan dosen dan tenaga kependidikan sebagai agen literasi. Perguruan tinggi dan sekolah menengah atas juga didorong untuk mengembangkan program *digital citizenship* yang membekali siswa dan mahasiswa dengan kompetensi digital yang etis dan kritis. Dengan kolaborasi antara pemerintah, komunitas, dan institusi pendidikan, diharapkan masyarakat semakin cerdas dalam memanfaatkan teknologi digital secara aman, bijak, dan bertanggung jawab.
- Kampanye edukasi tentang hoaks, keamanan siber, dan etika digital melalui program Gerakan Nasional Literasi Digital bertujuan untuk meningkatkan kesadaran serta pemahaman masyarakat dalam menghadapi tantangan di era digital. Melalui program ini, berbagai inisiatif

dilakukan, seperti pelatihan, seminar, dan penyebaran informasi edukatif yang membantu masyarakat mengenali serta mencegah penyebaran berita hoaks yang dapat menyesatkan opini publik. Selain itu, aspek keamanan siber menjadi perhatian utama dengan memberikan pemahaman mengenai pelindungan data pribadi, cara mengamankan akun digital, serta langkah-langkah menghindari ancaman siber seperti peretasan dan penipuan *online*. Tidak kalah penting, kampanye ini juga menanamkan nilai-nilai etika digital, seperti bertanggung jawab dalam bermedia sosial, menghargai privasi orang lain, serta membangun komunikasi yang positif di dunia maya. Sebagai contoh, Kemenkominfo bekerja sama dengan Gerakan Nasional Literasi Digital **Siberkreasi** telah menyelenggarakan lebih dari satu juta kegiatan literasi digital sejak diluncurkan, menjangkau jutaan peserta di seluruh Indonesia. Program-program seperti *Cek Fakta Sebelum Sebar*, kampanye anti-hoaks pemilu, dan edukasi pelindungan data pribadi menjadi bagian penting dari upaya edukasi publik. Di sisi lain, **Badan Siber dan Sandi Negara (BSSN)** juga secara aktif mengedukasi masyarakat tentang keamanan siber, baik melalui seminar, pelatihan teknis, maupun publikasi panduan pengamanan sistem elektronik yang ditujukan bagi instansi pemerintah, sektor strategis, dan masyarakat umum. BSSN juga merilis materi edukasi publik seperti buku saku keamanan informasi dan video edukatif yang dapat diakses secara *online* untuk mendorong kesadaran akan pentingnya perlindungan data dan ketahanan siber nasional. Sementara itu, **Politeknik Siber dan Sandi Negara (Poltek SSN)** sebagai institusi pendidikan tinggi kedinasan di bawah BSSN berperan dalam pengembangan sumber daya manusia di bidang keamanan siber dan kriptografi. Selain menyelenggarakan pendidikan vokasi, Poltek SSN juga aktif melakukan pengabdian masyarakat dan literasi digital melalui kegiatan seminar/konferensi internasional, pelatihan pelajar dan guru, serta kerja sama riset dan inovasi keamanan siber dengan berbagai perguruan tinggi. Kontribusi ini memperkuat ekosistem pengetahuan siber nasional sekaligus memperluas jangkauan literasi digital berbasis kompetensi teknis yang kuat.

- Penyediaan pelatihan keamanan siber bagi masyarakat dan pelaku usaha digital menjadi langkah krusial dalam menghadapi ancaman siber yang terus berkembang. Dengan meningkatnya ketergantungan pada teknologi digital, individu dan bisnis perlu memahami cara melindungi data pribadi, mengenali potensi serangan siber, serta menerapkan praktik keamanan yang tepat dalam aktivitas *online* mereka. Pelatihan ini dapat mencakup berbagai aspek, seperti pengelolaan kata sandi yang aman, deteksi *phishing*, penggunaan enkripsi data, serta strategi mitigasi risiko siber. Bagi pelaku usaha digital, pemahaman yang lebih mendalam mengenai kepatuhan terhadap regulasi keamanan data dan penerapan protokol keamanan jaringan sangat penting untuk menjaga kepercayaan pelanggan serta kelangsungan bisnis. Di sisi lain, institusi pendidikan vokasi dan politeknik memiliki peluang besar untuk menjadi pusat pelatihan keamanan siber berbasis kebutuhan industri, dengan mena-

warkan program sertifikasi, *bootcamp*, maupun kursus *online* terbuka (*massive open online courses*) yang menjangkau masyarakat luas. Selain itu, kolaborasi dengan industri dan pemerintah dalam mengembangkan laboratorium keamanan siber serta *cyber range* berbasis simulasi dapat meningkatkan kesiapan sumber daya manusia secara nyata. Dengan adanya program pelatihan yang terstruktur dan mudah diakses, diharapkan masyarakat dan sektor usaha semakin sadar akan pentingnya keamanan siber, sehingga dapat menciptakan ekosistem digital yang lebih aman, tepercaya, dan tangguh terhadap berbagai ancaman.

4. Mendorong Kerja Sama Internasional

   - Indonesia berperan aktif dalam berbagai forum keamanan siber global, termasuk ASEAN Digital Masterplan 2025, sebagai bagian dari upaya memperkuat ketahanan digital dan membangun kepercayaan dalam ekosistem digital. Melalui keterlibatan ini, Indonesia berkontribusi dalam berbagi praktik terbaik terkait perlindungan data, mitigasi ancaman siber, serta peningkatan kapasitas dalam menghadapi tantangan digital yang semakin kompleks. Partisipasi dalam forum ini juga memungkinkan Indonesia untuk memperkuat kolaborasi dengan negara-negara ASEAN dalam menciptakan standar keamanan siber yang harmonis, mendukung kebijakan tata kelola digital yang kolaboratif, serta mendorong inovasi berbasis teknologi yang aman dan tepercaya. Dengan demikian, keterlibatan aktif Indonesia dalam inisiatif regional dan global ini tidak hanya memperkuat infrastruktur keamanan sibernya sendiri, tetapi juga berkontribusi pada stabilitas dan kepercayaan digital di kawasan Asia Tenggara secara keseluruhan.
   - Kerja sama dengan perusahaan teknologi global memainkan peran penting dalam penegakan hukum digital serta penguatan standar keamanan data di era transformasi digital. Kolaborasi ini memungkinkan pertukaran informasi dan teknologi terkini yang dapat membantu pemerintah serta lembaga penegak hukum dalam mengidentifikasi, mencegah, dan menangani kejahatan siber secara lebih efektif. Selain itu, melalui sinergi dengan perusahaan teknologi global, standar keamanan data dapat ditingkatkan dengan menerapkan praktik terbaik internasional, seperti enkripsi tingkat lanjut, kebijakan perlindungan privasi yang ketat, serta mekanisme deteksi ancaman yang lebih canggih. Kerja sama ini juga mencakup upaya harmonisasi regulasi dan kepatuhan terhadap norma-norma global terkait pelindungan data pribadi, sehingga menciptakan lingkungan digital yang lebih aman dan tepercaya bagi masyarakat serta pelaku industri. Dengan demikian, kolaborasi antara pemerintah dan perusahaan teknologi global tidak hanya memperkuat ketahanan siber nasional, tetapi juga mendukung pertumbuhan ekosistem digital yang inovatif dan berkelanjutan.

5. Mendorong terwujudnya ekosistem kepercayaan digital

- Pendekatan *pentahelix*
  Mewujudkan kepercayaan digital memerlukan keterlibatan aktif dari seluruh unsur *pentahelix*: pemerintah, akademisi, industri, komunitas, dan media. Masing-masing memiliki peran strategis yang saling melengkapi dalam membentuk ekosistem digital yang aman, kolaboratif, dan berkelanjutan. Pemerintah bertanggung jawab dalam menyusun kebijakan, menetapkan regulasi, dan menyediakan infrastruktur pendukung yang memungkinkan ekosistem digital tumbuh secara sehat dan terjaga dari risiko-risiko sistemik. Selain itu, pemerintah juga berperan dalam menjamin kepastian hukum serta tata kelola ruang digital yang transparan dan akuntabel.
  Sementara itu, akademisi memberikan kontribusi penting melalui penelitian, kajian ilmiah, dan inovasi teknologi yang mendasari pengembangan solusi digital yang andal dan etis. Akademisi juga memiliki peran dalam meningkatkan kapasitas sumber daya manusia melalui pendidikan, pelatihan, serta kurikulum yang relevan dengan kebutuhan era digital dan keamanan informasi.
  Industri memiliki tanggung jawab untuk memastikan penerapan prinsip-prinsip keamanan, privasi, dan transparansi dalam setiap tahapan pengembangan produk dan layanan digital. Komitmen terhadap pelindungan data pribadi, kepatuhan terhadap standar keamanan informasi, serta praktik bisnis yang etis menjadi indikator penting dalam membangun kepercayaan publik terhadap sektor ini.
  Komunitas, yang mencakup organisasi masyarakat sipil, kelompok advokasi, serta masyarakat digital secara luas, berperan dalam meningkatkan kesadaran, edukasi, serta pengawasan terhadap penyelenggaraan layanan digital. Peran ini juga mencakup pembelaan terhadap hak-hak digital dan partisipasi aktif dalam proses pengambilan kebijakan yang bertanggungjawab.
  Media sebagai pilar kelima, memainkan peran krusial dalam membentuk opini publik dan menyebarluaskan informasi mengenai isu-isu digital. Melalui pemberitaan yang edukatif, kritis, dan faktual, media dapat mendorong pemahaman masyarakat mengenai pentingnya kepercayaan digital serta menekan penyebaran disinformasi. Media juga berfungsi sebagai saluran akuntabilitas publik terhadap praktik-praktik digital yang menyimpang dan sebagai jembatan komunikasi antara pemerintah, industri, dan masyarakat. Dengan sinergi yang erat di antara kelima unsur *pentahelix* tersebut, kepercayaan digital dapat dibangun secara berkelanjutan, memperkuat transformasi digital nasional, serta menciptakan ruang digital yang lebih aman, adil, dan berdaya saing.
- Kebijakan nasional tentang kepercayaan digital
  Penyusunan kebijakan nasional yang mengatur penerapan kepercayaan digital di Indonesia merupakan langkah strategis untuk membangun ekosistem digital yang aman, transparan, dan tepercaya. Kebijakan ini perlu mencakup berbagai aspek, antara lain pelindungan data pribadi, keamanan siber, standar identitas digital, serta regulasi terkait

pemanfaatan teknologi dalam transaksi digital. Dengan adanya regulasi yang jelas dan terintegrasi, pemerintah dapat memastikan bahwa seluruh pemangku kepentingan, baik dari sektor publik maupun swasta/industri, menerapkan prinsip kepercayaan digital secara konsisten. Selain itu, kebijakan ini juga harus mendorong peningkatan kesadaran dan literasi digital masyarakat agar memahami hak dan kewajiban mereka di ruang digital. Dengan demikian, kebijakan kepercayaan digital yang komprehensif tidak hanya melindungi pengguna dari risiko penyalahgunaan teknologi, tetapi juga memperkuat daya saing dan ketahanan ekonomi digital Indonesia di tingkat global.

- Etika dalam AI dan perlindungan data
  Semakin meluasnya penggunaan kecerdasan artifisial (AI) dalam layanan publik dan sektor strategis menuntut adanya pendekatan etis dan transparan untuk menjaga kepercayaan masyarakat. Untuk itu, diperlukan kerangka *governance* AI yang adaptif, yang tidak hanya memastikan akurasi teknis sistem AI, tetapi juga menjamin nondiskriminasi, keadilan, dan auditabilitas algoritma. Dengan membangun kepercayaan digital secara komprehensif melalui pelindungan data pribadi dan tata kelola AI yang etis, Indonesia akan mampu menciptakan ekosistem digital yang aman, bertanggungjawab, dan berdaya saing, sekaligus memperkuat legitimasi pemerintah dan sektor swasta/industri dalam memimpin transformasi digital nasional.

Aspek *How* berfokus pada strategi implementasi kepercayaan digital di Indonesia, yang mencakup regulasi, infrastruktur, literasi masyarakat, kerja sama internasional, hingga pengembangan ekosistem digital yang aman dan tepercaya. Substansi ini memiliki keterkaitan langsung dengan berbagai regulasi yang telah diterbitkan, baik pada level undang-undang, peraturan presiden, maupun peraturan teknis BSSN dan lembaga terkait. Pemetaan berikut menunjukkan keterkaitan antara komponen utama dalam aspek *How* dengan peraturan atau kebijakan yang relevan.

Pemetaan pada Tabel 5.5 menegaskan bahwa strategi penerapan kepercayaan digital di Indonesia tidak hanya bergantung pada inisiatif sektoral, tetapi juga pada sinkronisasi regulasi lintas bidang. Dengan dasar hukum yang kuat dan terintegrasi, kepercayaan digital dapat diwujudkan secara konsisten di seluruh ekosistem, mulai dari regulasi, infrastruktur, literasi masyarakat, hingga kerja sama internasional.

Tabel 5.5: Pemetaan Aspek *How* dengan Regulasi Terkait di Indonesia

Aspek *How*	**Regulasi/Peraturan Terkait**
Regulasi dan Kebijakan Keamanan Digital	- UU No. 27 Tahun 2022 tentang Pelindungan Data Pribadi (UU PDP) - UU No. 11 Tahun 2008 jo. UU No. 19 Tahun 2016 jo. UU No. 1/2024 tentang ITE - Perpres No. 47 Tahun 2023 tentang Strategi Keamanan Siber Nasional dan Manajemen Krisis Siber - Perpres No. 82 Tahun 2023 tentang Percepatan Transformasi Digital - Peraturan BSSN No. 2 Tahun 2024 tentang Manajemen Krisis Siber - Peraturan BSSN No. 7 Tahun 2024 tentang Indonesia Common Criteria - Peraturan BSSN No. 11 Tahun 2024 tentang Algoritma Kriptografi Indonesia dan Penilaian Kesesuaian Modul Kriptografi - Regulasi OJK dan BI terkait layanan keuangan digital dan sistem pembayaran
Peningkatan Infrastruktur Keamanan Siber	- Perpres No. 82 Tahun 2023 tentang Percepatan Transformasi Digital (Pusat Data Nasional) - Perpres No. 95 Tahun 2018 tentang Sistem Pemerintahan Berbasis Elektronik (SPBE) - Kebijakan teknis BSSN tentang National Cyber Security Operation Center (NSOC)
Peningkatan Literasi Digital dan Kesadaran Masyarakat	- Program Gerakan Nasional Literasi Digital (Siberkreasi) oleh Kemenkominfo - Pedoman teknis keamanan siber BSSN - Kurikulum literasi digital Kemendikbudristek, Kemenkominfo, dan BSSN - Program pengembangan SDM siber oleh Politeknik Siber dan Sandi Negara (Poltek SSN)
Kerja Sama Internasional	- ASEAN Digital Masterplan 2025 - Forum internasional terkait tata kelola siber (ITU, OECD, dan lainnya) - Kolaborasi pemerintah dengan perusahaan teknologi global
Ekosistem Kepercayaan Digital	- UU PDP dan UU ITE (perlindungan data dan transaksi elektronik) - Rencana tata kelola AI nasional (Kemenkominfo/Bappenas)

5.6 Inisiatif Kepercayaan Digital Indonesia

Indonesia telah mengambil berbagai inisiatif untuk membangun kepercayaan digital sebagai bagian dari transformasi digital nasional. Kepercayaan ini menjadi landasan penting agar masyarakat, pelaku usaha, dan pemerintah merasa aman dalam beraktivitas di ruang digital. Fokus utamanya mencakup peningkatan keamanan

siber, pelindungan data pribadi, serta pengembangan ekosistem digital yang andal. Dalam bidang keamanan siber, pemerintah memperkuat kebijakan dan infrastruktur untuk menghadapi ancaman yang semakin kompleks, termasuk penguatan koordinasi lintas lembaga dan peningkatan kapasitas sumber daya manusia. Di sisi lain, pengesahan Undang-Undang Nomor 27 Tahun 2022 tentang Pelindungan Data Pribadi menjadi langkah penting dalam memastikan pengelolaan data yang lebih transparan, aman, dan akuntabel.

Selain itu, pemerintah juga menekankan pentingnya pembangunan keamanan ekosistem digital yang merata. Upaya ini dilakukan melalui peningkatan literasi digital, perluasan akses terhadap teknologi, serta edukasi keamanan siber bagi masyarakat. Pendekatan ini diharapkan dapat menciptakan lingkungan digital yang mendorong partisipasi luas dan meningkatkan kepercayaan publik terhadap layanan digital. Dengan langkah-langkah tersebut, Indonesia berupaya mewujudkan transformasi digital yang tidak hanya inovatif, tetapi juga berkelanjutan dan berorientasi pada perlindungan kepentingan masyarakat. Berikut adalah beberapa inisiatif utama yang telah dilakukan Indonesia.

1. Kebijakan dan Regulasi

   - Undang-Undang Pelindungan Data Pribadi (UU PDP) [279]
     UU PDP disahkan pada tahun 2022 sebagai langkah penting dalam menjamin hak individu atas privasi data pribadi di Indonesia. Undang-undang ini bertujuan untuk melindungi setiap warga negara dari penyalahgunaan data pribadi dengan menetapkan aturan yang jelas mengenai bagaimana data harus dikelola, disimpan, dan digunakan.
     Selain melindungi hak individu, UU PDP juga mengatur kewajiban bagi organisasi, baik pemerintah maupun swasta, untuk mengelola data secara etis dan aman. Hal ini mencakup penerapan prinsip transparansi, keamanan informasi, serta tanggung jawab dalam pemrosesan data pribadi. Di samping itu, undang-undang ini menetapkan sanksi hukum yang tegas bagi pihak-pihak yang melanggar ketentuan privasi data, sehingga diharapkan mampu menekan praktik penyalahgunaan data yang marak terjadi di era digital.
     Secara keseluruhan, UU PDP menjadi landasan utama dalam membangun kepercayaan masyarakat terhadap penggunaan teknologi digital. Dengan adanya jaminan perlindungan hukum atas data pribadi, masyarakat dapat merasa lebih aman dan terlindungi dalam berinteraksi di ruang digital, sementara organisasi dituntut untuk lebih bertanggung jawab dalam menjaga keamanan dan kerahasiaan data pengguna.
   - Rancangan Undang-Undang Keamanan dan Ketahanan Siber [331]
     Rancangan Undang-Undang ini masih dalam tahap pembahasan dan ditujukan untuk membentuk kerangka hukum nasional yang komprehensif dalam pengelolaan keamanan dan ketahanan siber di Indonesia. Melalui pengaturan ini, pemerintah berupaya memastikan adanya koordinasi yang jelas antara berbagai lembaga negara dalam menjaga keamanan ruang siber nasional, sekaligus memperkuat sinergi lintas sektor.

RUU ini juga menegaskan peran dan tanggung jawab para pihak yang terlibat, termasuk penyelenggara sistem elektronik (PSE), sektor swasta, serta masyarakat, dalam menjaga keamanan dan keandalan ruang digital. Selain itu, rancangan ini memberikan dasar hukum yang kuat bagi proses penegakan hukum terhadap pelanggaran siber, baik melalui sanksi administratif maupun pidana, guna menciptakan efek jera dan menumbuhkan kepatuhan terhadap aturan.
Aspek perlindungan terhadap infrastruktur informasi kritis turut menjadi perhatian utama. Sektor-sektor strategis seperti keuangan, energi, layanan publik, dan telekomunikasi dipandang perlu mendapatkan perlindungan ekstra dari potensi ancaman dan serangan siber yang dapat mengganggu stabilitas nasional.
Dengan pengesahannya, RUU ini diharapkan dapat memperkuat sistem pertahanan siber nasional, meningkatkan kepastian hukum di ruang digital, serta mendorong terciptanya ekosistem digital yang aman, tepercaya, dan mendukung pertumbuhan ekonomi digital yang berkelanjutan bagi masyarakat dan pelaku usaha.

- UU No. 11 Tahun 2008 juncto No. 19 Tahun 2019 juncto No 1 Tahun 2024 tentang Informasi dan Transaksi Elektronik (ITE), PP No 71 tahun 2019 tentang Penyelenggara Sistem dan Transaksi Elektronik, Peraturan Menteri Komunikasi dan Informatika No. 5 Tahun 2020 juncto No. 10 Tahun 2021 tentang Penyelenggara Sistem Elektronik Lingkup Privat [278, 281, 292].
  Tujuan : Mengatur pemanfaatan informasi elektronik dan penyelenggaraan transaksi elektronik secara aman dan tepercaya, mencakup perlindungan pengguna dan penyedia layanan.
- Peraturan Presiden No. 95 Tahun 2018 tentang Sistem Pemerintahan Berbasis Elektronik (SPBE) [282]
  Peraturan Presiden ini bertujuan untuk mendorong penerapan sistem digital yang aman dan efisien di seluruh sektor pemerintahan. Melalui regulasi ini, pemerintah berupaya memperkuat penggunaan teknologi informasi guna meningkatkan kualitas layanan publik, transparansi, serta efektivitas tata kelola pemerintahan. Selain itu, Peraturan Presiden ini juga menekankan pentingnya memastikan interoperabilitas antarinstansi pemerintah dengan menerapkan standar keamanan yang jelas dan terpadu. Dengan demikian, setiap instansi dapat saling terhubung dan bertukar data secara aman, konsisten, serta mendukung terciptanya ekosistem pemerintahan digital yang terintegrasi dan berkelanjutan.

2. Infrastruktur Keamanan Siber
   Pemerintah Indonesia memperkuat pertahanan dan ketahanan siber nasional melalui pembentukan Badan Siber dan Sandi Negara (BSSN) pada tahun 2017, sebagaimana diatur dalam Peraturan Presiden Nomor 53 Tahun 2017 yang kemudian diperbarui dengan Peraturan Presiden Nomor 133 Tahun 2017. Lembaga ini memiliki mandat utama untuk mengoordinasikan berbagai upaya keamanan siber nasional, meliputi penanganan insiden siber, penguatan

tata kelola keamanan informasi di instansi pemerintah, serta peningkatan kesadaran keamanan siber di masyarakat dan sektor industri.
Dalam menjalankan fungsinya, BSSN berperan penting dalam menghadapi berbagai ancaman siber, seperti serangan *ransomware*, kebocoran data, maupun gangguan terhadap infrastruktur vital nasional. Selain itu, BSSN juga berkomitmen membangun budaya keamanan siber melalui program edukasi publik, pelatihan teknis, serta kolaborasi lintas sektor untuk memperkuat kesiapan nasional menghadapi insiden siber.
Salah satu inisiatif strategis BSSN adalah penyusunan Rencana Induk Keamanan Siber Nasional (RIKSN) yang berfungsi sebagai panduan kebijakan dan arah strategis pembangunan keamanan siber di Indonesia. Di samping itu, BSSN mengembangkan platform berbagi intelijen ancaman siber (*Cyber Threat Intelligence Sharing Platform*) yang memungkinkan pertukaran informasi secara cepat dan aman antara instansi pemerintah, sektor swasta, dan komunitas keamanan siber.
Sebagai bagian dari infrastruktur keamanan nasional, BSSN juga membangun Pusat Operasi Keamanan Siber Nasional (*National Security Operations Center* – NSOC). Pusat ini berfungsi untuk memantau aktivitas siber secara *real-time*, mendeteksi potensi ancaman, serta merespons insiden dengan cepat dan terkoordinasi. Melalui SOC Nasional, BSSN memperkuat sistem peringatan dini terhadap serangan siber dan memfasilitasi koordinasi teknis antarinstansi.
Dalam pelaksanaannya, BSSN menjalin kerja sama dengan berbagai pihak, termasuk sektor swasta, akademisi, serta lembaga internasional. Kolaborasi ini bertujuan untuk memperkuat kapasitas nasional di bidang keamanan siber, mendorong inovasi teknologi pertahanan siber, dan memastikan perlindungan yang berkelanjutan terhadap data serta infrastruktur digital nasional.

3. Edukasi dan Kesadaran Publik
   Upaya peningkatan literasi digital dan kesadaran masyarakat terhadap keamanan siber menjadi salah satu pilar penting dalam mewujudkan ekosistem digital yang aman dan bertanggung jawab. Pemerintah Indonesia, melalui berbagai lembaga terkait, telah meluncurkan sejumlah program strategis untuk membangun kesadaran publik dalam penggunaan teknologi dan media digital secara bijak.
   Salah satu inisiatif utama adalah Gerakan Nasional Literasi Digital (GNLD) Siberkreasi [332]. Program ini merupakan bagian dari Program Literasi Digital Nasional yang dikoordinasikan oleh Kementerian Komunikasi dan Informatika (Kemenkominfo). GNLD Siberkreasi bertujuan untuk meningkatkan pemahaman masyarakat tentang keamanan digital, privasi, serta etika dalam penggunaan internet. Program ini juga dirancang untuk menjangkau berbagai kelompok masyarakat, termasuk pelajar, pekerja, dan pelaku usaha mikro, kecil, dan menengah (UMKM).
   Berbagai aktivitas dilaksanakan dalam kerangka program ini, antara lain melalui penyelenggaraan *workshop*, seminar, serta kampanye daring yang berfokus pada peningkatan literasi digital. Selain itu, Siberkreasi juga aktif memproduksi konten edukatif yang memberikan panduan kepada masyarakat

tentang cara melindungi diri dari penipuan daring, serangan siber, serta praktik kejahatan digital lainnya.
Sejalan dengan upaya tersebut, pemerintah juga menjalankan Kampanye Anti-Hoaks [333] sebagai bentuk komitmen dalam menjaga ruang digital yang sehat dan tepercaya. Kampanye ini melibatkan berbagai lembaga seperti Kemenkominfo, BSSN, serta Polri. Tujuan utama dari inisiatif ini adalah untuk mengurangi penyebaran informasi palsu (hoaks) yang dapat merusak kepercayaan publik, sekaligus mengedukasi masyarakat mengenai pentingnya memverifikasi informasi sebelum menyebarkannya. Melalui kedua program tersebut, pemerintah berupaya menumbuhkan kesadaran kolektif masyarakat dalam menggunakan teknologi secara bertanggung jawab dan kritis. Literasi digital dan kemampuan memverifikasi informasi diharapkan menjadi modal utama dalam memperkuat ketahanan nasional di ranah siber.

4. Kolaborasi Publik-Privat
   Kolaborasi antara sektor publik dan swasta merupakan salah satu langkah strategis dalam memperkuat keamanan siber nasional. Upaya ini diwujudkan melalui pembentukan Forum Koordinasi Keamanan Siber yang melibatkan berbagai pemangku kepentingan, antara lain pemerintah, perusahaan teknologi, lembaga pendidikan, serta komunitas digital. Forum tersebut berfungsi sebagai wadah untuk berbagi informasi mengenai potensi ancaman siber dan mengembangkan solusi bersama guna meningkatkan ketahanan serta keamanan digital di tingkat nasional.
   Selain itu, pemerintah juga menjalin kemitraan dengan perusahaan teknologi global seperti Google, Microsoft, dan Alibaba Cloud. Kolaborasi ini bertujuan untuk memperkuat keamanan platform digital nasional serta mendorong penerapan standar keamanan informasi internasional, termasuk SNI ISO/IEC 27001. Melalui kerja sama ini, diharapkan terbangun ekosistem digital yang lebih aman, tangguh, dan adaptif terhadap dinamika ancaman siber yang terus berkembang.

5. Pengembangan Ekosistem Digital
   Pengembangan platform digital yang aman menjadi salah satu prioritas utama dalam transformasi digital pemerintah dan sektor publik di Indonesia. Berbagai inisiatif telah dilakukan untuk mewujudkan sistem layanan yang efisien, transparan, dan berorientasi pada keamanan data pengguna. Salah satu contohnya adalah aplikasi PeduliLindungi, yang dikembangkan sebagai alat pelacakan kontak selama pandemi COVID-19 dengan memperhatikan aspek privasi serta keamanan informasi pribadi masyarakat. Selain itu, terdapat platform MyPertamina yang berfungsi sebagai sarana digital untuk distribusi dan pembelian bahan bakar bersubsidi. Melalui sistem ini, proses penyaluran dapat dilakukan secara lebih aman, efisien, dan transparan, sekaligus meminimalkan potensi penyalahgunaan subsidi.
   Di sisi lain, pemanfaatan teknologi *blockchain* juga mulai dikembangkan dalam berbagai sektor sebagai upaya memperkuat transparansi dan keandalan data. Teknologi ini memungkinkan setiap transaksi atau aliran informasi tercatat secara terdistribusi dan sulit dimanipulasi, sehingga meningkatkan

kepercayaan dan integritas sistem digital. Contohnya, penerapan *blockchain* pada sistem logistik dapat membantu pelacakan rantai pasokan secara *real-time*, memastikan keaslian dokumen, serta mendukung efisiensi operasional di berbagai tingkat distribusi barang dan jasa.

6. Fokus pada Sektor Prioritas
   Regulasi dan pengawasan sektor keuangan digital berada di bawah kewenangan Otoritas Jasa Keuangan (OJK). Melalui Peraturan OJK Nomor 21 Tahun 2023 tentang Penyelenggaraan Teknologi Informasi oleh Lembaga Jasa Keuangan, OJK menetapkan standar keamanan dan tata kelola teknologi informasi bagi lembaga jasa keuangan, termasuk penyelenggara *financial technology* (*fintech*) dan layanan uang elektronik (*e-wallet*). Kebijakan ini bertujuan memperkuat aspek keamanan, keandalan, dan integritas sistem digital dalam ekosistem keuangan nasional.
   Selain itu, Bank Indonesia juga berperan penting melalui peluncuran *National Payment Gateway* (NPG), sebuah infrastruktur pembayaran nasional yang dirancang untuk memfasilitasi transaksi elektronik secara lebih aman, efisien, dan terintegrasi. Kehadiran NPG memperkuat sinergi antarpenyedia jasa pembayaran dan mendukung ekosistem pembayaran nontunai di Indonesia [334].
   Sementara itu, dalam bidang pemerintahan digital, berbagai inisiatif telah dikembangkan untuk meningkatkan efisiensi layanan publik dan memperluas akses masyarakat terhadap pelayanan pemerintah. Beberapa di antaranya mencakup pengembangan portal terpadu seperti Layanan.go.id dan sistem *Online Single Submission* (OSS) [335], yang berfungsi sebagai platform digital untuk mempermudah proses perizinan usaha dan akses layanan publik.
   Seiring dengan peningkatan kebutuhan keamanan data dan kepercayaan pengguna, beberapa layanan pemerintah mulai menerapkan sistem autentikasi dua faktor (*Two-Factor Authentication*/2FA) guna memastikan perlindungan lebih baik terhadap identitas dan data pengguna. Langkah ini menjadi bagian dari strategi nasional dalam memperkuat tata kelola keamanan siber di sektor pemerintahan.

7. Kerjasama Internasional
   Dalam menghadapi ancaman siber yang bersifat lintas batas, kerja sama internasional menjadi elemen penting dalam memperkuat keamanan digital suatu negara. Melalui kolaborasi regional maupun global, negara-negara dapat saling bertukar informasi, teknologi, dan praktik terbaik untuk meningkatkan ketahanan siber bersama.
   Salah satu bentuk kerja sama regional yang signifikan adalah ASEAN Cybersecurity Cooperation [336]. Inisiatif ini bertujuan untuk membangun koordinasi antarnegara anggota ASEAN dalam menghadapi ancaman siber lintas batas. Melalui program ini, negara-negara di kawasan Asia Tenggara berkomitmen untuk berbagi praktik terbaik, memperkuat kapasitas teknis, serta mengembangkan teknologi keamanan siber yang dapat digunakan bersama untuk menjaga stabilitas digital kawasan.
   Selain kerja sama di tingkat regional, Indonesia juga aktif menjalin kemitraan

dengan organisasi global. Salah satu contohnya adalah kolaborasi dengan International Telecommunication Union (ITU) dalam pengembangan standar keamanan digital yang selaras dengan praktik internasional. Di samping itu, Indonesia berpartisipasi dalam berbagai forum global seperti World Economic Forum (WEF), yang menjadi wadah diskusi penting mengenai isu kepercayaan digital, tata kelola siber, serta kebijakan keamanan global. Melalui berbagai bentuk kerja sama tersebut, Indonesia berupaya memperkuat posisinya dalam ekosistem keamanan siber internasional sekaligus memastikan bahwa kebijakan nasional tetap sejalan dengan perkembangan dan standar global di bidang keamanan digital.

6

Kerangka Kerja Kepercayaan Digital Indonesia

> Strong digital trust drives innovation by reducing fear and enabling collaboration across ecosystems.
>
> — MIT Technology Review

Kerangka kerja kepercayaan digital yang yang diusulkan bertujuan membantu Indonesia membangun tingkat kepercayaan digital yang tinggi demi menciptakan dunia digital yang aman. Pembahasan akan mencakup elemen-elemen kerangka kerja kepercayaan digital yang diusulkan secara komprehensif. Proses ini juga mempertimbangkan fleksibilitas implementasi dalam menghadapi dinamika digital yang cepat berubah, termasuk penetrasi AI, aliran data lintas batas, dan munculnya ancaman-ancaman baru terhadap privasi dan keamanan siber.

Sebagai langkah awal, dilakukan penentuan jenis kerangka kerja yang akan diadopsi. Dalam literatur, dikenal dua jenis utama: kerangka teoritis dan kerangka konseptual. Menurut Labaree [337], kerangka teoritis didefinisikan sebagai seperangkat teori terintegrasi yang memberikan dasar untuk menjelaskan atau memprediksi fenomena. Sebaliknya, Miles dan Huberman [338] mendefinisikan kerangka konseptual sebagai representasi visual atau tertulis yang menjelaskan faktor kunci, variabel utama, serta hubungan antar-elemen tersebut. Camp [339] mempertegas bahwa kerangka teoritis lebih fokus pada konsep abstrak, sedangkan kerangka konseptual menggambarkan struktur yang diderivasi langsung dari fenomena nyata. Berdasarkan karakteristik tersebut, usulan dalam penelitian ini dikategorikan sebagai kerangka konseptual.

Mengacu pada Jabareen [340], pengembangan kerangka konseptual ini dilakukan melalui pendekatan analisis kualitatif.

Keberhasilan kerangka kerja ini sangat bergantung pada kemampuannya dalam menjaga keseimbangan antara perlindungan dan inovasi, serta antara kepastian hukum dan ruang bagi pertumbuhan teknologi. Di satu sisi, perlindungan terhadap data, privasi, dan keamanan digital perlu dijamin melalui regulasi yang jelas dan berpihak pada kepentingan publik. Di sisi lain, inovasi harus tetap diberi ruang melalui kebijakan yang adaptif dan tidak menghambat kreativitas pelaku industri, peneliti, maupun pengembang teknologi.

Sebagai panduan strategis sekaligus operasional, dokumen ini disusun dengan mempertimbangkan kondisi sosial, ekonomi, dan teknologis di Indonesia. Relevansi konteks lokal menjadi landasan dalam perancangannya, sehingga kerangka ini dapat diadopsi secara luas oleh seluruh pemangku kepentingan dalam model *pentahelix* (pemerintah, industri, akademisi, komunitas, dan media) dengan pendekatan yang komprehensif dan kolaboratif. Dengan membangun dasar kepercayaan digital yang kokoh melalui tata kelola yang transparan, partisipatif, dan berorientasi pada kepentingan nasional, Indonesia dapat memperkuat kedaulatan digital, memperluas inklusi digital, dan menciptakan ekosistem teknologi yang tangguh. Langkah ini menjadi landasan strategis untuk meningkatkan daya saing bangsa dalam menghadapi dinamika ekonomi digital global yang semakin kompetitif dan kompleks.

6.1 Prinsip Umum dan Nilai Dasar Kepercayaan Digital Indonesia

Kerangka kerja kepercayaan digital di Indonesia perlu dibangun di atas seperangkat prinsip dan nilai dasar yang menjadi dasar etis, hukum, dan teknis dalam pengembangan serta penyelenggaraan sistem digital nasional. Prinsip-prinsip tersebut bukan hanya berfungsi sebagai pedoman normatif, melainkan juga sebagai kerangka operasional yang memandu arah kebijakan, desain arsitektur sistem, hingga evaluasi program dalam ekosistem digital. Dengan berpegang pada prinsip ini, Indonesia dapat memperkuat kepercayaan publik, menjamin hak-hak digital warga negara, sekaligus mendorong pertumbuhan ekonomi digital yang aman, adil, dan merata.

1. Keamanan dan Ketahanan Digital
   Sistem digital nasional harus dibangun dengan ketangguhan yang mampu menghadapi berbagai ancaman siber, baik yang bersifat teknis maupun sosial. Penerapan prinsip *secure by design* memastikan keamanan menjadi bagian integral sejak tahap perancangan. Selain itu, penguatan enkripsi, pemantauan ancaman secara proaktif, dan penerapan arsitektur *zero trust* menjadi elemen penting untuk menciptakan ekosistem digital yang adaptif terhadap dinamika risiko teknologi.

2. Privasi dan Pelindungan Data Pribadi
   Hak atas privasi digital adalah bagian dari hak asasi manusia yang tidak

dapat diabaikan. Oleh karena itu, setiap proses pengumpulan, penyimpanan, hingga pemanfaatan data pribadi harus dilakukan secara sah, terbatas pada tujuan tertentu, transparan, dan berbasis persetujuan eksplisit pengguna. Dengan cara ini, individu tetap memiliki kendali atas data pribadinya sekaligus terlindungi dari potensi penyalahgunaan.

3. Transparansi dan Akuntabilitas
   Kepercayaan publik hanya dapat tumbuh apabila penyelenggara layanan digital bersikap terbuka dan dapat dipertanggungjawabkan. Transparansi mencakup penyediaan informasi yang jelas mengenai kebijakan privasi, penggunaan algoritma, serta hak-hak pengguna. Sementara itu, akuntabilitas menuntut adanya mekanisme yang adil dan tegas ketika terjadi pelanggaran atau kegagalan sistem, termasuk kewajiban pemulihan dan pemberian ganti rugi.

4. Interoperabilitas dan Keterbukaan Sistem
   Transformasi digital nasional membutuhkan sistem yang mampu saling terhubung lintas sektor dan platform tanpa mengorbankan keamanan maupun efisiensi. Adopsi standar terbuka menjadi kunci untuk mempercepat integrasi layanan, mengurangi fragmentasi sistem, serta mendorong terciptanya ekosistem inovasi yang sehat, termasuk dukungan terhadap produk dan layanan lokal.

5. Keadilan dan Inklusi Digital
   Akses terhadap layanan digital harus dipandang sebagai hak kolektif yang merata bagi seluruh lapisan masyarakat. Prinsip ini menekankan pentingnya kebijakan afirmatif yang memastikan kelompok rentan, seperti penyandang disabilitas, masyarakat adat, maupun warga negara di wilayah 3TP (Tertinggal, Terpencil, Terluar, dan Perbatasan), tidak tertinggal dari arus transformasi digital. Inklusi digital tidak hanya soal akses, tetapi juga literasi dan kemampuan adaptasi masyarakat dalam memanfaatkan teknologi.

6. Etika dan Tanggung Jawab Sosial Teknologi
   Penggunaan teknologi digital harus diarahkan untuk kebaikan bersama, bukan hanya keuntungan ekonomi. Etika teknologi mencakup prinsip nondiskriminasi, keadilan dalam algoritma, serta kehati-hatian dalam adopsi teknologi baru seperti kecerdasan artifisial (AI). Selain itu, dampak sosial dan lingkungan harus diperhitungkan agar inovasi digital benar-benar memberi manfaat tanpa menimbulkan ketidakadilan baru.

7. Kedaulatan dan Kepemilikan Digital Nasional
   Indonesia perlu memastikan bahwa infrastruktur strategis, data penting, dan teknologi inti dikelola secara mandiri dengan berpijak pada kepentingan nasional. Kedaulatan digital bukan sekadar isu teknis, melainkan juga aspek geopolitik dan keamanan negara. Dengan menegaskan kepemilikan digital, Indonesia dapat menjaga kendali atas data warga negaranya serta memastikan pengambilan keputusan strategis di ruang digital tidak dikendalikan oleh pihak eksternal.

Dengan menjadikan prinsip-prinsip tersebut sebagai landasan, kerangka kerja kepercayaan digital Indonesia dapat berfungsi sebagai pedoman yang kokoh, baik secara normatif maupun praktis. Prinsip ini akan menuntun arah kebijakan publik, memastikan desain sistem digital yang berorientasi pada keamanan dan keadilan, serta menjadi tolok ukur dalam evaluasi berkelanjutan. Pada akhirnya, penerapan kerangka kerja ini akan membangun ekosistem digital nasional yang kompetitif sekaligus berakar pada kepentingan dan nilai-nilai bangsa.

6.2 Kerangka Kerja Kepercayaan Digital Indonesia

Kerangka kerja kepercayaan digital Indonesia dirancang sebagai acuan strategis dalam membangun ekosistem digital yang aman, kolaboratif, dan berkelanjutan. Untuk memahami bagaimana kerangka ini bekerja secara menyeluruh, perlu ditelaah terlebih dahulu definisi konseptual kepercayaan digital, tujuan utama yang ingin dicapai, mekanisme pengelolaan yang mendasarinya, serta faktor-faktor kunci yang memengaruhi efektivitas penerapannya.

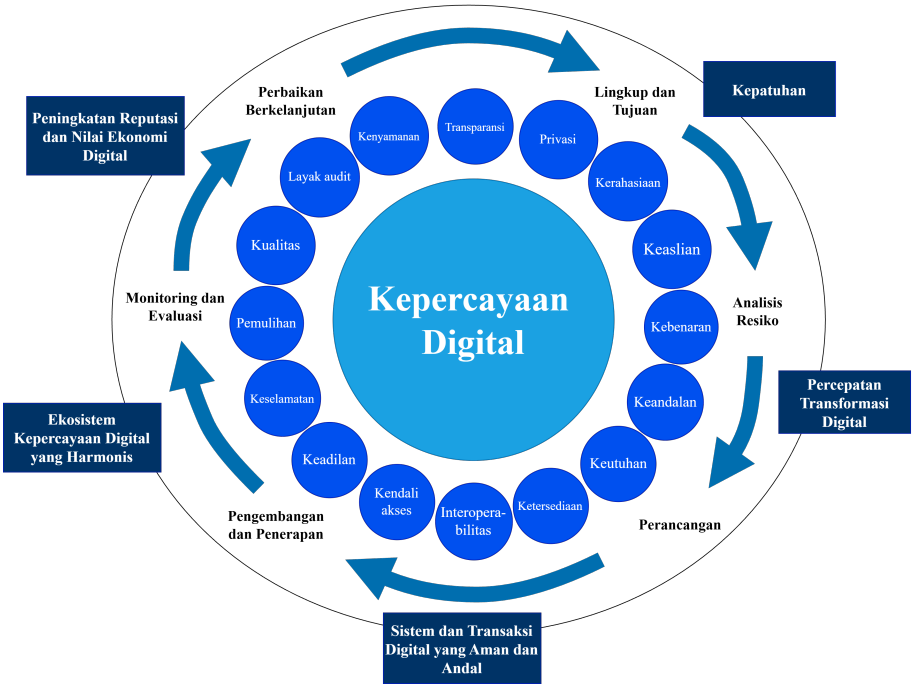
6.2.1 Rasional Desain Kerangka Kerja Kepercayaan Digital Indonesia

Kerangka kerja kepercayaan digital Indonesia disusun berdasarkan prinsip bahwa kepercayaan tidak dapat dibangun hanya dari satu aspek, melainkan hasil integrasi antara tujuan strategis, mekanisme manajemen, serta faktor teknis dan nonteknis yang saling melengkapi. Desain berlapis pada Gambar 6.1 mencerminkan logika hierarkis dari luar ke dalam, di mana setiap lapisan memiliki fungsi dan kontribusi spesifik.

Lapisan paling luar merepresentasikan tujuan strategis kepercayaan digital, yakni kepatuhan, percepatan transformasi digital, keandalan sistem dan transaksi, ekosistem digital yang harmonis, serta peningkatan nilai ekonomi digital. Tujuan ini berfungsi sebagai arah dan sasaran akhir dari seluruh upaya membangun kepercayaan digital.

Lapisan kedua menekankan aspek manajemen kepercayaan digital melalui siklus berkelanjutan mulai dari perencanaan, analisis risiko, perancangan, penerapan, hingga monitoring, evaluasi, dan perbaikan berkelanjutan. Mekanisme ini diposisikan pada lapisan kedua karena menjadi instrumen penggerak untuk mewujudkan tujuan strategis yang telah ditetapkan.

Lapisan ketiga berisi faktor-faktor kunci seperti transparansi, privasi, kerahasiaan, integritas, keandalan, interoperabilitas, kendali akses, keselamatan, pemulihan, kualitas, auditabilitas, hingga kenyamanan pengguna. Faktor-faktor ini dipilih karena mewakili dimensi fundamental yang secara langsung membentuk atau merusak kepercayaan dalam sistem digital. Dengan memenuhinya secara konsisten, ekosistem digital dapat menjaga legitimasi, keamanan, dan inklusivitas.



Gambar 6.1: Kerangka Kerja Kepercayaan Digital Indonesia

Lapisan terdalam adalah inti kepercayaan digital itu sendiri, yang merepresentasikan model kerangka kerja kepercayaan digital. Penempatan kepercayaan digital pada pusat desain menekankan bahwa semua tujuan, mekanisme manajemen, dan faktor pendukung dapat diimplementasikan dengan menerapkan model kerangka kerja kepercayaan digital (lihat Gambar 6.1). Struktur berlapis ini juga menunjukkan keterkaitan erat antarelemen. Tujuan strategis menjadi arah, manajemen kepercayaan menyediakan mekanisme, faktor kunci berperan sebagai landasan teknis dan operasional, sementara inti berupa model kepercayaan digital berisi panduan teknis untuk implementasi kepercayaan digital. Dengan demikian, kerangka kerja ini dirancang tidak hanya sebagai model konseptual, tetapi juga sebagai panduan praktis yang dapat diimplementasikan lintas sektor secara adaptif dan berkelanjutan.

6.2.2 Definisi Kepercayaan Digital

Kepercayaan digital dapat diartikan sebagai kepercayaan antara entitas yang terlibat dalam transaksi digital yang meliputi konsumen, penyedia barang/jasa, dan pihak ketiga. Peraturan Pemerintah (PP) Nomor 71 Tahun 2019 tentang Penyelenggaraan Sistem dan Transaksi Elektronik, menyebutkan bahwa transaksi digital atau transaksi elektronik diartikan sebagai perbuatan hukum yang dilakukan dengan menggunakan komputer, jaringan komputer, dan/atau media elektronik lainnya. Dengan adanya program transformasi digital Indonesia, perkembangan teknologi

dan ancaman siber, inisiasi serta peluang pemanfaatan teknologi di sisi ekonomi, maka negara melalui pemerintah perlu hadir untuk memastikan hak setiap entitas dalam transaksi digital terpenuhi demi kemajuan ekonomi nasional dan mewujudkan kesejahteraan rakyat Indonesia. Kerangka kerja kepercayaan digital yang diusulkan sesuai dengan Gambar 6.1. terdiri atas empat lapisan, yaitu lapisan paling luar adalah tujuan kepercayaan digital, lapisan kedua adalah manajemen kepercayaan digital, lapisan ketiga adalah faktor kunci kepercayaan digital dan lapisan terdalam adalah kepercayaan digital yang memuat model kerangka kerja kepercayaan digital.

6.2.3 Tujuan Kepercayaan Digital

Kepercayaan digital bertujuan untuk menciptakan ekosistem digital yang aman, transparan, dan tepercaya, sehingga dapat mendorong pertumbuhan ekonomi, percepatan transformasi digital, serta peningkatan reputasi dan keandalan sistem digital. Untuk mencapai tujuan ini, diperlukan kepatuhan terhadap regulasi, percepatan adopsi teknologi, keamanan sistem, serta kolaborasi antarpemangku kepentingan dalam ekosistem digital. Berikut adalah tujuan utama dari kepercayaan digital:

1. Kepatuhan
   Kepercayaan digital memastikan bahwa setiap entitas mematuhi kebijakan, regulasi, dan standar yang berlaku. Untuk itu, diperlukan aturan yang jelas sebagai acuan serta mekanisme pemantauan dan evaluasi guna meningkatkan efektivitas penerapannya.

2. Percepatan Transformasi Digital
   Kepercayaan digital meningkatkan keyakinan pengguna dalam bertransaksi dan memanfaatkan teknologi digital. Dengan rasa aman yang lebih tinggi, adopsi serta adaptasi terhadap teknologi baru dapat berjalan lebih cepat, sehingga mempercepat transformasi digital di berbagai sektor.

3. Sistem dan Transaksi Digital yang Aman dan Andal
   Kepercayaan digital mendorong penyelenggara layanan digital untuk membangun sistem yang aman, dapat diandalkan, dan tahan terhadap ancaman siber, sehingga pengguna dapat berinteraksi di dunia digital tanpa rasa khawatir.

4. Ekosistem Kepercayaan Digital yang Harmonis
   Kepercayaan digital terwujud melalui sinergi antara pemerintah, bisnis, dan masyarakat. Dengan regulasi yang jelas dan standar yang diterapkan secara konsisten, setiap entitas dapat menjalankan perannya secara optimal, menciptakan interaksi yang harmonis dalam ekosistem digital.

5. Peningkatan Reputasi dan Nilai Ekonomi Digital
   Kepercayaan digital memperkuat reputasi organisasi serta penyelenggara sistem digital. Dengan meningkatnya kepercayaan pengguna, transaksi digital akan terus bertumbuh, meningkatkan nilai ekonomi digital, serta membuka peluang investasi yang lebih luas.

6.2.4 Manajemen Kepercayaan Digital

Manajemen kepercayaan digital merupakan suatu pendekatan sistematis dalam membangun, mengelola, dan memastikan keberlanjutan kepercayaan di ekosistem digital. Proses ini mengacu pada siklus PDCA (*Plan-Do-Check-Act*), sebuah metode yang diterapkan secara berulang guna memastikan efektivitas strategi dan kebijakan kepercayaan digital dalam mencapai tujuan yang telah diuraikan sebelumnya.

1. Penentuan Lingkup dan Tujuan
   Tahap awal merupakan tahap perencanaan. Pada proses perencanaan perlu ditentukan tujuan organisasi dan lingkup kepercayaan digital. Pada tahap ini juga bisa dianalisis faktor internal dan eksternal yang dapat memengaruhi tercapainya tujuan organisasi. Organisasi dapat menentukan sendiri metode untuk menyusun tujuan dan analisis kondisi internal dan eksternal.

2. Analisis Risiko
   Tahap kedua melakukan analisis risiko yang merupakan langkah awal pada tahap pelaksanaan. Analisis risiko dilakukan untuk mengetahui dan memprioritaskan risiko khususnya risiko siber/digital yang dapat memengaruhi tercapainya tujuan. Jika risiko telah teridentifikasi dengan baik, maka akan mempermudah tahap perancangan kepercayaan digital. Organisasi dapat menentukan sendiri metode analisis risiko.

3. Perancangan
   Tahap pelaksanaan berikutnya adalah perancangan implementasi kepercayaan digital pada sistem dan transaksi digital. Untuk mempermudah tahap perancangan, organisasi dapat mengacu instrumen kepercayaan digital yang lebih lengkap akan dijelaskan di model kerangka kerja kepercayaan digital. Adapun *output* pada tahap perancangan adalah rancangan sistem elektronik dan isian intrumen pilar kepercayaan digital untuk setiap domain. Organisasi dapat menentukan sendiri metode pengembangan sistem elektronik.

4. Pengembangan dan Penerapan
   Tahap pelaksanaan berikutnya adalah tahap pengembangan dan penerapan. Organisasi dapat menentukan sendiri metode pengembangan sistem elektronik dan memastikan bahwa penerapan kepercayaan digital dapat dimonitor dan dievaluasi.

5. Monitoring dan Evaluasi
   Tahap monitoring dan evaluasi menjadi bagian dari tahap pengecekan. Pada tahap ini organisasi perlu melakukan monitoring untuk memastikan rencana penerapan kepercayaan digital berjalan dengan baik, memastikan semua entitas yang terlibat bertindak sesuai dengan peran masing-masing, terpenuhinya indikator kunci kepercayaan digital, dan tercapainya tujuan organisasi. Sedangkan evaluasi dilakukan untuk mengukur kepatuhan dan efektivitas penerapan kepercayaan digital. Organisasi dapat menentukan sendiri metode monitoring dan evaluasi yang akan dilakukan.

6. Perbaikan Berkelanjutan
   Perbaikan berkelanjutan merupakan tahap tindak lanjut. Setelah mengetahui hasil monitoring dan evaluasi, organisasi perlu menyusun strategi perbaikan untuk meningkatkan hasil monitoring dan evaluasi.

Dengan menerapkan siklus PDCA secara konsisten, kepercayaan digital dapat dikelola secara proaktif, memungkinkan penyesuaian terhadap perkembangan teknologi, perubahan regulasi, serta dinamika ancaman siber yang terus berkembang.

6.2.5 Faktor Kunci Kepercayaan Digital

Kepercayaan digital tidak terbentuk secara instan, melainkan merupakan hasil dari integrasi berbagai faktor penting yang menopang terciptanya ekosistem digital yang aman, transparan, dan dapat diandalkan. Faktor-faktor ini menjadi landasan utama dalam menumbuhkan keyakinan bagi seluruh entitas yang terlibat dalam ruang digital, baik individu, pelaku bisnis, maupun pemerintah.

Dengan memahami dan mengelola faktor-faktor tersebut secara holistik, transformasi digital dapat berjalan secara berkelanjutan, sekaligus meminimalkan risiko seperti ancaman keamanan siber, penyalahgunaan data, maupun ketimpangan akses. Adapun faktor-faktor kunci yang berkontribusi dalam membangun dan mempertahankan kepercayaan digital antara lain sebagai berikut:

1. Transparansi (*Transparancy*): Kemampuan untuk memahami proses dan keputusan dalam sistem digital, termasuk siapa yang mengakses, memodifikasi, dan mengelola data.
2. Privasi (*Privacy*): Perlindungan terhadap informasi pribadi agar tidak digunakan atau diakses tanpa persetujuan eksplisit dari pemilik data.
3. Kerahasiaan (*Confidentiality*): Menjamin bahwa informasi sensitif hanya dapat diakses oleh pihak yang berwenang, biasanya dengan penerapan enkripsi dan kontrol akses yang ketat.
4. Keaslian (*Authenticity*): Verifikasi identitas dari pengguna dan sistem melalui mekanisme autentikasi dan sertifikat digital guna memastikan interaksi yang sah.
5. Kebenaran (*Accuracy*): Keakuratan serta validitas data yang dikumpulkan, disimpan, dan diproses di dalam sistem digital.
6. Keandalan (*Reliability*): Konsistensi sistem dalam menjalankan fungsinya sesuai harapan tanpa terjadi gangguan yang signifikan.
7. Keutuhan (*Integrity*): Jaminan bahwa data tidak dimodifikasi secara tidak sah selama proses penyimpanan maupun transmisi.
8. Ketersediaan (*Availability*): Sistem dan data harus dapat diakses oleh pengguna yang berhak kapan pun dibutuhkan, termasuk dalam kondisi darurat.

9. Interoperabilitas (*Interoperability*): Kemampuan sistem untuk berbagi dan menggunakan informasi secara efisien antarplatform dan teknologi yang berbeda.
10. Kendali Akses (*Access Control*): Pengaturan hak akses terhadap sumber daya digital berdasarkan prinsip otorisasi dan prinsip *minimal privilege*.
11. Keadilan (*Fairness*): Perlakuan yang adil terhadap semua pengguna, serta keputusan algoritmik yang tidak bias.
12. Keselamatan (*Safety*): Perlindungan terhadap sistem dan data dari ancaman baik fisik maupun digital yang dapat menimbulkan kerusakan atau kerugian.
13. Pemulihan (*Recovery*): Kemampuan sistem untuk memulihkan kondisi operasional pascagangguan atau serangan dengan cepat dan efisien.
14. Kualitas (*Quality*): Tingkat pemenuhan terhadap kebutuhan dan ekspektasi pengguna, termasuk aspek efisiensi, keandalan, dan kemudahan penggunaan.
15. Layak Audit (*Audit Worthy*): Sistem dirancang agar dapat diaudit secara efektif guna menjamin kepatuhan terhadap kebijakan, standar, dan regulasi yang berlaku.
16. Kenyamanan (*Convenience*): Pengalaman pengguna yang intuitif dan ramah terhadap kebutuhan manusia, menempatkan nilai-nilai *human-centric* sebagai prioritas utama dalam perancangan sistem digital.

6.3 Model Kerangka Kerja Kepercayaan Digital

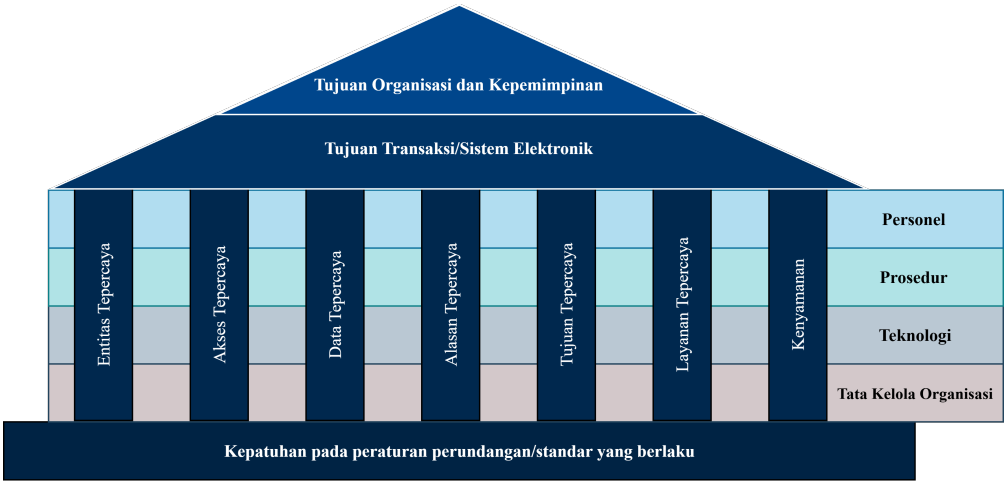
Pada manajemen kepercayaan digital, model kerangka kerja kepercayaan digital membantu dalam merancang implementasi kepercayaan digital pada sistem elektronik. Model kerangka kerja ini dirancang untuk menjadi panduan komprehensif bagi penyelenggara sistem dan transaksi elektronik dalam membangun, mengelola, dan menerapkan kepercayaan digital secara efektif. Model ini bertujuan untuk memastikan bahwa setiap transaksi digital berlangsung dengan aman, transparan, dan tepercaya, sehingga dapat meningkatkan keyakinan pengguna serta mendukung transformasi digital yang berkelanjutan.

Kerangka kerja ini terdiri atas beberapa elemen utama yang saling berkaitan. Landasan utama dari model ini adalah kepatuhan terhadap aturan, yang mencakup regulasi, kebijakan, serta standar yang berlaku sebagai dasar penerapan kepercayaan digital. Selanjutnya, terdapat pilar-pilar pembentuk kepercayaan digital, yang berfungsi sebagai faktor penentu dalam membangun ekosistem digital yang andal.

Di dalam model ini juga terdapat domain kepercayaan digital, yaitu area spesifik yang menjadi fokus utama dalam implementasi kepercayaan digital pada sistem elektronik dalam suatu organisasi, yang meliputi personel, prosedur, teknologi, dan tata kelola organisasi. Semua elemen tersebut disusun secara sistematis untuk

mencapai tujuan akhir, yaitu menciptakan ekosistem digital yang tidak hanya memberikan perlindungan bagi pengguna, tetapi juga mendorong pertumbuhan ekonomi digital melalui peningkatan kepercayaan terhadap teknologi.

Struktur lengkap dari model kerangka kerja ini dapat dilihat pada Gambar 6.2, yang mengilustrasikan hubungan antara setiap komponen dalam membangun sistem kepercayaan digital yang terintegrasi dan berkelanjutan.



Gambar 6.2: Model Kerangka Kerja Kepercayaan Digital Indonesia

6.3.1 Landasan Penerapan Kepercayaan Digital

Kepercayaan digital dibangun di atas fondasi utama, yaitu kepatuhan terhadap aturan, regulasi, dan standar yang berlaku. Kepatuhan ini memastikan bahwa setiap entitas dalam ekosistem digital, baik individu, bisnis, maupun pemerintah dapat beroperasi dalam lingkungan yang aman, transparan, dan dapat diandalkan. Oleh karena itu, ketersediaan regulasi yang jelas dan terimplementasi secara efektif menjadi faktor kunci dalam membangun serta mempertahankan kepercayaan digital.

Seiring dengan pesatnya perkembangan teknologi dan transformasi digital, negara telah mengambil langkah-langkah untuk mengatur pemanfaatan teknologi digital melalui berbagai kebijakan dan perundangan yang mencakup aspek keamanan siber, pelindungan data pribadi, transaksi elektronik, serta tata kelola teknologi informasi. Regulasi ini berfungsi sebagai kerangka hukum yang tidak hanya memberikan perlindungan bagi pengguna tetapi juga menciptakan kepastian hukum bagi penyedia layanan digital. Dengan adanya regulasi yang komprehensif dan penegakan hukum yang kuat, kepercayaan masyarakat terhadap layanan digital dapat meningkat, sehingga mendorong pertumbuhan ekonomi berbasis digital yang berkelanjutan. Saat ini, berbagai undang-undang dan peraturan telah diterapkan secara integratif untuk memberikan kepastian hukum, melindungi hak-hak pengguna, serta mengatur tata kelola pemanfaatan teknologi digital. Instrumen hukum utama yang menjadi

pilar kepercayaan digital nasional meliputi:

- Undang-Undang Informasi dan Transaksi Elektronik (UU ITE)
  Sebagai payung hukum utama (*lex generalis*) dalam aktivitas digital, UU ITE beserta perubahannya (terakhir UU No. 1 Tahun 2024) mengatur keabsahan informasi dan dokumen elektronik sebagai alat bukti hukum yang sah. Undang-undang ini tidak hanya mendefinisikan perbuatan yang dilarang di ruang siber (*cybercrime*), tetapi juga memberikan legitimasi terhadap tanda tangan elektronik, penyelenggaraan sistem elektronik, dan sertifikasi keandalan. Hal ini krusial untuk menjamin bahwa setiap transaksi digital memiliki kekuatan hukum yang mengikat dan dapat dipertanggungjawabkan.

- Undang-Undang Pelindungan Data Pribadi (UU PDP)
  UU No. 27 Tahun 2022 tentang PDP hadir sebagai instrumen spesifik (*lex specialis*) yang menjamin kedaulatan data warga negara. UU ini mengatur secara komprehensif mengenai hak-hak subjek data pribadi serta kewajiban dan tanggung jawab para Pengendali dan Prosesor Data. Dengan menetapkan standar kepatuhan yang ketat, termasuk prinsip pemrosesan data, mekanisme persetujuan (*consent*), serta sanksi atas pelanggaran, UU PDP menjadi landasan utama dalam membangun kepercayaan masyarakat terhadap bagaimana data mereka dikelola oleh entitas publik maupun privat.

- Peraturan Perundangan Sektoral dan Pendukung
  Selain kedua undang-undang utama tersebut, kepercayaan digital juga diperkuat oleh regulasi turunan dan sektoral yang relevan, antara lain:

  - Regulasi Keamanan Siber: Termasuk Peraturan Presiden No. 47 Tahun 2023 tentang Strategi Keamanan Siber Nasional dan berbagai peraturan BSSN yang mengatur standar keamanan sistem elektronik serta perlindungan Infrastruktur Informasi Vital (IIV).
  - Regulasi Sistem Pemerintahan Berbasis Elektronik (SPBE): Peraturan Presiden No. 95 Tahun 2018 yang mengatur tata kelola digital di sektor pemerintahan untuk menjamin layanan publik yang terpadu, efektif, dan aman.
  - Regulasi Sektor Keuangan: Peraturan dari Bank Indonesia (BI) dan Otoritas Jasa Keuangan (OJK) yang mengatur keamanan transaksi pembayaran digital, perbankan digital, serta inovasi keuangan teknologi (*fintech*) demi menjaga stabilitas dan kepercayaan konsumen di sektor ekonomi digital.

Pada tingkat organisasi, kepatuhan terhadap regulasi dan standar menjadi aspek krusial dalam membangun kepercayaan digital. Organisasi tidak hanya perlu merujuk pada peraturan yang ditetapkan oleh koordinator sektor, tetapi juga harus menyesuaikan dengan kebijakan teknis yang dikeluarkan oleh pemerintah serta standar internasional yang berlaku di industri terkait. Dalam implementasinya, setiap aturan yang diadopsi harus diintegrasikan ke dalam regulasi internal organisasi secara sah dan terdokumentasi dengan baik. Hal ini memastikan bahwa

kebijakan yang diterapkan selaras dengan kerangka hukum yang lebih luas, sehingga dapat meningkatkan transparansi, akuntabilitas, dan perlindungan terhadap semua pemangku kepentingan. Selain itu, dengan merujuk pada standar global yang diakui, organisasi dapat memperkuat daya saingnya, memperluas akses ke pasar internasional, serta memastikan bahwa sistem dan proses yang dijalankan tetap relevan dengan dinamika perkembangan teknologi dan regulasi yang terus berubah.

6.3.2 Pilar Penerapan Kepercayaan Digital

Pilar kepercayaan digital merupakan aspek utama dalam membangun ekosistem digital yang aman, transparan, dan tepercaya. Pilar ini mencerminkan komitmen kuat dari berbagai pemangku kepentingan dalam memastikan bahwa setiap transaksi digital berlangsung dengan integritas, keandalan, dan perlindungan yang memadai. Pilar kepercayaan digital tidak hanya mengatur kapabilitas yang harus dimiliki oleh setiap entitas, tetapi juga menetapkan jaminan serta standar yang harus dipenuhi dalam setiap proses transaksi digital.

Keberadaan pilar ini menjadi kunci dalam menghadapi tantangan utama dalam transformasi digital, seperti keamanan siber, privasi data, regulasi, serta literasi digital. Sejalan dengan faktor-faktor kunci yang telah dibahas sebelumnya, pilar kepercayaan digital berfungsi sebagai kerangka kerja yang memastikan bahwa semua aspek dalam ekosistem digital, baik dari sisi teknologi, regulasi, maupun perilaku pengguna, berjalan selaras dan mendukung tujuan Indonesia. Dengan mempertimbangkan berbagai tantangan serta peluang dalam lanskap digital Indonesia, berikut adalah pilar-pilar utama yang membentuk kepercayaan digital Indonesia.

1. Entitas Tepercaya
   Dalam ekosistem digital, keabsahan setiap entitas yang terlibat dalam transaksi harus dipastikan agar keamanan dan kepercayaan dalam sistem tetap terjaga. Untuk mencapai hal ini, proses autentikasi dan verifikasi menjadi langkah krusial dalam mengidentifikasi serta memastikan bahwa setiap pihak yang berinteraksi dalam transaksi digital adalah entitas yang sah. Autentikasi berfungsi untuk memastikan identitas pengguna melalui berbagai metode, seperti kata sandi, biometrik, atau autentikasi dua faktor, sementara verifikasi bertujuan untuk membuktikan keakuratan data yang diberikan. Dengan penerapan mekanisme ini, risiko kejahatan siber, seperti pencurian identitas, penipuan, dan akses tidak sah, dapat diminimalkan. Selain itu, regulasi dan standar keamanan yang ketat perlu diterapkan agar proses autentikasi dan verifikasi berjalan secara optimal, memberikan perlindungan bagi pengguna, serta memperkuat kepercayaan dalam transaksi digital.

2. Akses Tepercaya
   Dalam ekosistem transaksi digital, setiap entitas yang terlibat harus memiliki kendali akses yang sesuai dengan tingkat otorisasi yang diberikan terhadap aset digital atau sistem yang digunakan. Hal ini bertujuan untuk memastikan bahwa hanya pihak yang berwenang yang dapat mengakses, mengelola, atau

memodifikasi data dan sistem, sehingga keamanan informasi tetap terjaga. Penerapan mekanisme kontrol akses yang ketat, seperti autentikasi berbasis multifaktor dan enkripsi data, menjadi langkah krusial dalam mencegah akses tidak sah yang berpotensi menimbulkan risiko kebocoran atau penyalahgunaan informasi. Selain itu, sistem manajemen akses yang transparan dan terstruktur juga memungkinkan pemantauan serta audit berkala, sehingga setiap aktivitas dalam ekosistem digital dapat tercatat dengan jelas dan dapat dipertanggungjawabkan. Dengan demikian, kendali akses yang tepat tidak hanya melindungi aset digital dari ancaman siber, tetapi juga meningkatkan kepercayaan pengguna terhadap layanan digital yang digunakan.

3. Data Tepercaya
   Memastikan bahwa data atau informasi yang dipertukarkan memenuhi standar kebenaran, akurasi, keaslian, dan keutuhannya merupakan aspek krusial dalam ekosistem digital yang tepercaya. Informasi yang benar dan tidak menyesatkan sangat penting untuk mencegah penyebaran hoaks, manipulasi data, serta kesalahan dalam pengambilan keputusan, baik di sektor publik maupun swasta/industri. Akurasi data juga harus dijaga agar tidak terjadi distorsi yang dapat berdampak negatif pada kebijakan, transaksi, atau analisis yang bergantung pada informasi tersebut. Selain itu, keaslian data harus dapat diverifikasi untuk memastikan bahwa informasi yang digunakan berasal dari sumber yang valid dan tidak mengalami perubahan yang tidak sah selama proses transmisi. Keutuhan data juga perlu dijaga agar informasi tetap utuh dan tidak mengalami modifikasi yang dapat merugikan pengguna atau mengubah makna aslinya. Dengan demikian, sistem keamanan dan mekanisme validasi yang ketat harus diterapkan untuk mendukung pertukaran data yang andal, membangun kepercayaan digital, serta menciptakan lingkungan informasi yang lebih transparan dan tepercaya.

4. Alasan Tepercaya
   Dalam ekosistem digital yang semakin berkembang, penting untuk memastikan bahwa setiap proses dan tindakan yang dilakukan dalam transaksi digital mematuhi regulasi yang berlaku, mengikuti prinsip etika, serta mendapatkan kesepakatan dari semua entitas yang terlibat. Kepatuhan terhadap regulasi tidak hanya bertujuan untuk menjaga stabilitas dan keamanan transaksi, tetapi juga untuk melindungi hak serta kepentingan pengguna dalam ekosistem digital. Selain itu, aspek etika menjadi landasan utama dalam membangun kepercayaan di antara para pelaku transaksi, sehingga setiap keputusan yang diambil didasarkan pada transparansi, tanggung jawab, dan keadilan. Dengan adanya kesepakatan yang jelas antara semua pihak, risiko perselisihan atau penyalahgunaan dalam transaksi digital dapat diminimalkan, menciptakan lingkungan digital yang lebih aman, tepercaya, berkelanjutan, dan layak audit.

5. Tujuan Tepercaya
   Dalam ekosistem digital yang semakin berkembang, penting untuk memastikan bahwa data, informasi, dan aset digital yang terlibat dalam transaksi hanya digunakan sesuai dengan tujuan yang telah disepakati oleh setiap en-

titas yang terlibat. Hal ini mencakup perlindungan terhadap segala bentuk penyalahgunaan, seperti kebocoran data (*data breach*) dan tindakan penipuan yang dapat merugikan individu maupun institusi. Untuk itu, penerapan regulasi yang ketat serta mekanisme keamanan yang andal menjadi faktor utama dalam menjaga integritas dan kepercayaan dalam ekosistem digital. Selain itu, aspek privasi pada pelindungan data pribadi harus dijamin melalui enkripsi, sistem autentikasi yang kuat, serta kepatuhan terhadap standar keamanan yang berlaku, sehingga informasi sensitif tetap terjaga dan tidak disalahgunakan oleh pihak yang tidak berwenang.

6. Layanan Tepercaya
   Layanan melalui sistem elektronik harus dijamin keamanannya agar pengguna dapat bertransaksi dan berinteraksi tanpa khawatir terhadap ancaman siber, kebocoran data, atau penyalahgunaan informasi pribadi. Selain itu, keandalan sistem menjadi faktor penting untuk memastikan layanan dapat diakses kapan saja tanpa gangguan, dengan infrastruktur yang stabil dan responsif terhadap kebutuhan pengguna. Kualitas layanan juga harus dijaga melalui inovasi teknologi, peningkatan pengalaman pengguna, serta kepatuhan terhadap standar dan regulasi yang berlaku. Dengan kombinasi keamanan, keandalan, dan kualitas yang terjamin, sistem elektronik dapat meningkatkan kepercayaan masyarakat, mempercepat adopsi teknologi digital, serta mendukung ekosistem digital yang lebih aman dan efisien.

7. Kenyamanan
   Kemajuan teknologi memungkinkan entitas, baik individu, perusahaan, maupun lembaga, untuk melakukan transaksi digital dengan lebih mudah, cepat, dan efisien dalam memenuhi berbagai kebutuhan serta mencapai tujuan mereka. Dengan adanya berbagai platform dan sistem pembayaran digital yang semakin canggih, proses transaksi kini dapat dilakukan secara *real-time* tanpa terbatas oleh lokasi atau waktu. Untuk itu dibutuhkan sistem yang menjamin interoprabilitas dan kemampuan pemulihan paska bencana. Kemudahan ini tidak hanya mendukung kelancaran aktivitas ekonomi, tetapi juga mendorong pertumbuhan ekosistem digital yang lebih andal dan tepercaya, baik di sektor bisnis maupun layanan publik.

Tabel 6.1 menyajikan hubungan antara pilar utama kepercayaan digital dengan faktor-faktor kunci yang mendukung implementasinya. Pilar kepercayaan digital mencerminkan aspek fundamental yang harus dipenuhi untuk menciptakan ekosistem digital yang aman, transparan, dan tepercaya. Sementara itu, faktor kunci kepercayaan digital mencakup elemen-elemen strategis yang berperan dalam memastikan bahwa setiap pilar dapat diterapkan secara efektif dalam sistem transaksi elektronik. Dengan adanya pemetaan ini, pemangku kepentingan dapat memahami bagaimana setiap faktor mendukung pilar tertentu, serta mengidentifikasi langkah-langkah yang perlu diambil untuk meningkatkan kepercayaan dalam transaksi digital.

Tabel 6.1: Pemetaan Pilar dan Faktor Kunci Kepercayaan Digital

Pilar	**Penjelasan**	**Faktor Kunci**
Entitas Tepercaya	Entitas yang terlibat dalam transaksi digital dijamin kebenarannya melalui proses autentikasi dan verifikasi.	Keaslian
Akses Tepercaya	Entitas yang terlibat dalam transaksi digital memiliki kendali akses sesuai dengan otorisasinya terhadap aset digital/sistem.	Keaslian Kendali akses Transparansi Layak audit
Data Tepercaya	Memastikan data/informasi yang dipertukarkan adalah data yang benar/tidak menyesatkan, akurat, terjamin keaslian dan keutuhannya.	Kerahasiaan Kebenaran Keutuhan Ketersediaan
Alasan Tepercaya	Memastikan setiap proses, tindakan, akibat dari proses/tindakan yang dilakukan pada saat transaksi digital telah sesuai dengan regulasi yang berlaku, sesuai dengan etika, dan disepakati oleh semua entitas.	Layak audit Keadilan Transparansi
Tujuan Tepercaya	Memastikan bahwa data/informasi/aset digital yang ada dalam transaksi digital hanya digunakan untuk kepentingan yang telah disepakati antarsetiap entitas, dan memastikan tidak adanya penyalahgunaan (*data breach*, penipuan) serta menjamin kerahasiaan data pribadi.	Privasi Transparansi
Layanan Tepercaya	Layanan melalui sistem elektronik dijamin aman, andal, dan berkualitas.	Keselamatan Kualitas Keandalan
Kenyamanan	Entitas dapat dengan mudah melakukan transaksi digital untuk memenuhi kebutuhan dan tujuannya.	Kenyamanan Pemulihan Interoperabilitas

6.3.3 Domain Kepercayaan Digital

Dalam ekosistem digital yang dinamis, kepercayaan merupakan aset fundamental yang dibangun melalui sinergi antara kepatuhan regulasi dan penerapan prinsip keamanan, transparansi, serta akuntabilitas yang ketat. Domain Kepercayaan Digital hadir sebagai kerangka kerja komprehensif yang mengintegrasikan elemen-elemen krusial tersebut ke dalam dimensi yang terstruktur, mencakup aspek personel, operasional, teknologi, dan kebijakan. Pendekatan holistik ini memastikan bahwa setiap lapisan interaksi digital, mulai dari kompetensi sumber daya manusia hingga ketangguhan infrastruktur teknis, dikelola secara sistematis untuk memitigasi risiko dan melindungi kepentingan seluruh pemangku kepentingan, baik penyedia layanan, konsumen, maupun mitra pihak ketiga.

Implementasi domain-domain ini bukan sekadar pemenuhan kewajiban administratif, melainkan strategi vital untuk menciptakan lingkungan digital yang resilien dan berkelanjutan. Dengan menerjemahkan prinsip-prinsip kepercayaan ke dalam stan-

dar operasional yang nyata, organisasi dapat menjamin keandalan sistem sekaligus menjawab ekspektasi pengguna yang semakin kritis terhadap perlindungan data mereka. Pada akhirnya, penguasaan terhadap domain kepercayaan digital menjadi tolok ukur kredibilitas organisasi, memastikan bahwa inovasi teknologi berjalan beriringan dengan kepastian hukum dan etika, sehingga mampu mendorong adopsi layanan digital yang lebih luas dan tepercaya.

1. Personel
   Personel merupakan domain utama dalam penerapan kepercayaan digital karena berperan sebagai pelaku, baik sebagai pengguna, penyedia layanan, maupun pihak ketiga. Setiap personel memiliki tanggung jawab dan kompetensi tertentu yang berkontribusi terhadap terwujudnya kepercayaan digital. Dalam kerangka kerja kepercayaan digital, penyelenggara sistem perlu mengidentifikasi personel yang terlibat, menentukan peran dan tugasnya, serta memastikan kompetensi mereka sesuai dengan pilar-pilar kepercayaan digital yang diterapkan.

2. Proses/Prosedur
   Domain ini berfokus pada penetapan mekanisme kerja yang tepat untuk mendukung setiap pilar kepercayaan digital. Proses dan prosedur menentukan bagaimana prinsip-prinsip kepercayaan digital diterapkan secara konsisten di seluruh tahapan operasional. Hubungan antara prosedur dan teknologi bersifat timbal balik — pemilihan teknologi dipengaruhi oleh prosedur yang ditetapkan, dan sebaliknya. Secara umum, proses dan prosedur bersifat lebih teknis dibandingkan aturan atau regulasi.

3. Teknologi dan Infrastruktur
   Domain teknologi dan infrastruktur merupakan komponen kunci dalam mewujudkan kepercayaan digital. Tanpa dukungan keduanya, sistem dan transaksi elektronik tidak dapat berfungsi secara optimal maupun tepercaya. Setiap teknologi memiliki karakteristik, prosedur penerapan, tingkat kerentanan, dan kebutuhan infrastruktur yang berbeda, sehingga pemilihannya harus disesuaikan dengan kebutuhan operasional dan kebijakan organisasi. Oleh karena itu, penyelenggara sistem dan transaksi elektronik bertanggung jawab untuk memastikan bahwa seluruh pilar kepercayaan digital didukung oleh teknologi dan infrastruktur yang tepat, aman, andal, serta memenuhi standar yang berlaku.

4. Tata Kelola dan Organisasi
   Tata kelola dan organisasi merupakan faktor penentu keberhasilan penerapan kepercayaan digital. Tata kelola yang baik memastikan perencanaan, implementasi, dan evaluasi kebijakan berjalan secara efektif dengan dukungan sumber daya yang memadai, komitmen pimpinan, dan partisipasi seluruh pihak terkait. Penyelenggara sistem dan transaksi elektronik dapat mengacu pada peraturan nasional maupun standar internasional yang berlaku untuk menyusun tata kelola yang transparan, akuntabel, dan berkelanjutan.

Pada tahap perancangan penerapan kepercayaan digital dalam sistem dan transaksi elektronik, pilar dan domain kepercayaan digital dikombinasikan untuk membentuk instrumen penerapan yang komprehensif. Instrumen ini berfungsi tidak hanya sebagai panduan implementasi, tetapi juga sebagai alat pemantauan dan evaluasi untuk memastikan efektivitas serta kepatuhan terhadap prinsip kepercayaan digital. Melalui instrumen tersebut, pemangku kepentingan dapat menilai tingkat penerapan kepercayaan digital, mengidentifikasi area yang memerlukan perbaikan, serta mengoptimalkan kebijakan dan strategi guna menjaga keamanan, transparansi, dan keandalan sistem digital. Langkah ini menjadi dasar penting dalam membangun ekosistem digital nasional yang berkelanjutan dan tepercaya, sejalan dengan visi transformasi digital Indonesia.

6.3.4 Target, Tujuan, dan Kepemimpinan

Dalam manajemen penerapan kepercayaan digital, langkah pertama yang harus dilakukan adalah menentukan tujuan dan lingkup implementasi. Tujuan ini merupakan unsur penting dalam membangun ekosistem digital yang aman, transparan, dan tepercaya. Dalam model kerangka kerja kepercayaan digital, tujuan ditempatkan pada posisi paling atas karena merepresentasikan target dalam mencapai hasil akhir yang diharapkan dari penerapan prinsip kepercayaan digital dalam suatu organisasi atau penyelenggara sistem dan transaksi elektronik.

Bagi organisasi atau entitas yang mengelola sistem digital berskala besar dengan berbagai layanan atau platform, penentuan tujuan tidak hanya bersifat umum, tetapi juga dapat dikelompokkan berdasarkan sistem yang dikelola. Setiap sistem dapat memiliki tujuan spesifik yang berkontribusi terhadap pencapaian tujuan strategis organisasi secara keseluruhan. Misalnya, dalam sebuah perusahaan teknologi yang menyediakan layanan *e-commerce*, sistem pembayaran digital mungkin berfokus pada keamanan transaksi dan kepatuhan regulasi, sementara sistem layanan pelanggan lebih mengutamakan keandalan dan perlindungan data pengguna. Dengan pendekatan ini, organisasi dapat lebih efektif dalam mengelola risiko, meningkatkan efisiensi, serta memastikan penerapan kepercayaan digital yang selaras dengan kebutuhan dan visi bisnisnya. Namun, penetapan tujuan dan struktur teknis saja tidak cukup untuk menjamin keberhasilan penerapan kepercayaan digital. Salah satu elemen krusial yang sering kali kurang mendapat perhatian adalah kepemimpinan digital yang visioner dan etis, yang tidak hanya menetapkan arah kebijakan dan tata kelola, tetapi juga menjadi teladan dalam menjunjung nilai-nilai kepercayaan, keamanan, dan perlindungan privasi. *Kepemimpinan* yang dimaksud adalah kepemimpinan yang bertanggung jawab, visioner, dan kolaboratif dalam menetapkan arah kebijakan digital, membangun budaya organisasi yang mengutamakan kepercayaan, serta mendorong partisipasi publik dalam pengambilan keputusan teknologi.

Kepemimpinan yang proaktif memainkan peran sentral dalam membentuk budaya kepercayaan digital yang berkelanjutan. Pemimpin yang memahami pentingnya keamanan informasi, transparansi, serta pelindungan data pribadi akan mendorong

seluruh lini organisasi untuk bertindak secara bertanggung jawab dan konsisten. Peran mereka mencakup penetapan arah strategis, penyediaan sumber daya yang memadai, dan penguatan nilai-nilai integritas, akuntabilitas, serta penghormatan terhadap hak-hak digital sebagai bagian dari praktik organisasi sehari-hari.

Dengan kombinasi antara penetapan tujuan yang terstruktur dan kepemimpinan yang berkomitmen terhadap nilai-nilai kepercayaan digital, organisasi tidak hanya mampu mempertahankan kepercayaan publik, tetapi juga menumbuhkannya sebagai keunggulan kompetitif yang berkelanjutan di era transformasi digital yang kian cepat dan kompleks.

6.4 Ekosistem Kepercayaan Digital

Perkembangan pesat teknologi digital di Indonesia telah mendorong lahirnya ekosistem digital yang semakin kompleks dan saling terhubung. Dalam ekosistem ini, kepercayaan digital menjadi faktor kunci yang memastikan setiap entitas, baik individu, bisnis, maupun pemerintah, dapat bertransaksi dan berinteraksi secara aman, transparan, dan tepercaya. Kepercayaan digital tidak hanya bergantung pada keamanan teknologi yang digunakan, tetapi juga pada kepatuhan terhadap regulasi, literasi digital masyarakat, serta kolaborasi antarpemangku kepentingan.

Ekosistem kepercayaan digital merujuk pada hubungan timbal balik antara berbagai entitas dalam lingkungan digital yang bekerja sama untuk menciptakan sistem yang andal dalam setiap transaksi digital. Ekosistem ini tidak hanya melibatkan pengguna dan penyedia layanan digital, tetapi juga regulator, penyedia infrastruktur teknologi, serta pihak ketiga yang berperan dalam mendukung keamanan dan kelancaran transaksi.

Di Indonesia, ekosistem kepercayaan digital mencakup berbagai aspek, mulai dari regulasi dan kebijakan pemerintah, infrastruktur teknologi, sistem transaksi digital, hingga partisipasi aktif masyarakat dan sektor industri. Untuk membangun ekosistem yang kuat, diperlukan sinergi antara pemerintah, sektor swasta/industri, dan masyarakat dalam memastikan perlindungan data, penguatan sistem keamanan siber, serta peningkatan literasi digital. Sinergi ini memberikan keseimbangan kolektif dalam berbagi tanggung jawab bersama dan kental dengan budaya Indonesia yaitu prinsip gotong royong.

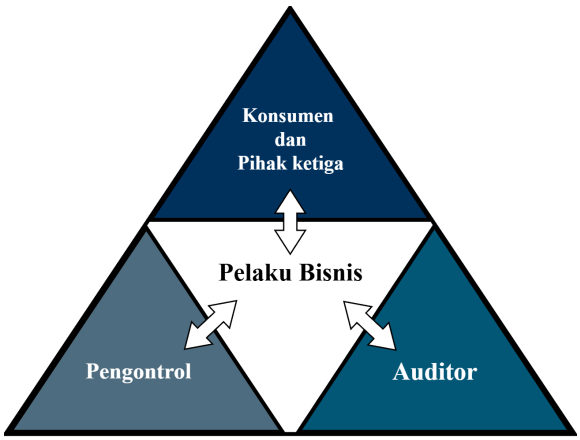
Dalam ekosistem ini, berbagai teknologi dan kebijakan diterapkan untuk memastikan perlindungan data, verifikasi identitas, serta integritas sistem. Teknologi seperti enkripsi, tanda tangan digital, autentikasi multifaktor, dan *blockchain* digunakan untuk meningkatkan keamanan serta mengurangi risiko penyalahgunaan data. Selain itu, regulasi dan standar keamanan yang ditetapkan oleh pemerintah dan lembaga terkait, seperti UU PDP, UU ITE, serta kebijakan dari BI dan OJK, berfungsi sebagai landasan dalam menjaga kepatuhan dan transparansi dalam ekosistem ini.

Kepercayaan dalam ekosistem digital juga dibangun melalui penerapan praktik terbaik, termasuk edukasi dan peningkatan literasi digital bagi masyarakat, pe-

ngawasan terhadap keamanan sistem, serta kolaborasi antara sektor publik dan swasta/industri dalam mengatasi ancaman siber. Dengan adanya keseimbangan antara inovasi teknologi, kebijakan yang adaptif, dan kesadaran pengguna, ekosistem kepercayaan digital dapat berkembang secara berkelanjutan, mendukung pertumbuhan ekonomi digital, serta memberikan perlindungan yang optimal bagi seluruh entitas yang terlibat.

6.4.1 Lini Ekosistem Kepercayaan Digital

Dalam ekosistem digital yang kompleks, perlu dibagi peran dan tanggung jawab masing-masing pihak agar pengelolaan risiko lebih terukur dan sistematis. Pengelolaan risiko ini menggunakan kerangka Lini Ekosistem Kepercayaan Digital.



Gambar 6.3: Lini Ekosistem Kepercayaan Digital

Kepercayaan digital (*digital trust*) merupakan hasil dari integrasi yang erat antara proses, personel, dan teknologi yang dikelola secara sistematis dan berlapis. Dalam membangun ekosistem kepercayaan digital yang kokoh, diperlukan struktur tata kelola risiko yang mampu mengatur peran dan tanggung jawab berbagai pemangku kepentingan secara jelas, sekaligus memungkinkan terciptanya umpan balik yang bersifat dinamis dan berkelanjutan. Konsep ini divisualisasikan dalam Gambar 6.3 melalui model Lini Ekosistem Kepercayaan Digital (*Digital Trust Ecosystem Lines*), yang memetakan empat lini utama dalam sistem tata kelola kepercayaan digital.

Sinergi yang efektif antara keempat lini menjadi dasar yang kokoh bagi terbentuknya ekosistem digital yang aman, transparan, dan andal. Setiap lini memiliki peran strategis dalam mendukung pengelolaan risiko serta memperkuat kepercayaan digital di seluruh tingkatan organisasi. Penjabaran berikut menguraikan fungsi dan kontribusi setiap lini dalam membangun kepercayaan digital yang berkelanjutan.

1. **Lini Pusat – Pelaku Bisnis (*Operational Management*)**
   Lini pusat merujuk pada unit atau entitas yang bertanggung jawab langsung

terhadap pelaksanaan proses bisnis harian dan pengelolaan risiko operasional yang terkait. Mereka berperan dalam merancang dan menerapkan kepercayaan digital pada sistem elektronik serta memastikan kegiatan berjalan efisien, efektif, dan sesuai dengan strategi organisasi, kebijakan internal, dan regulasi eksternal.

Dalam konteks kepercayaan digital, lini ini berfokus pada pengelolaan risiko dan penerapan strategi mitigasi risiko pada proses bisnis yang memanfaatkan sistem elektronik. Konsistensi dan integritas perilaku pelaku bisnis akan membentuk persepsi awal pemangku kepentingan terhadap keamanan dan reliabilitas layanan digital. Oleh karena itu, tanggung jawab lini pusat meliputi:

- Menentukan lingkup dan tujuan organisasi, proses bisnis, dan penerapan kepercayaan digital;
- Mengidentifikasi dan mengelola risiko serta menyusun strategi mitigasi sejak tahap perancangan hingga eksekusi layanan digital;
- Merancang, mengembangkan, dan menerapkan kerangka kerja kepercayaan digital pada layanan digital;
- Menerapkan kebijakan, standar, dan *standard operating procedures* (SOP) yang sejalan dengan prinsip kepercayaan digital;
- Menjaga keamanan informasi dan mencegah akses tidak sah terhadap sistem atau data pelanggan;
- Mempromosikan budaya etika digital serta kepatuhan melalui pelatihan berkelanjutan dan literasi keamanan siber.

Komitmen dan kapabilitas lini pusat berkontribusi besar dalam membentuk struktur kepercayaan digital yang kokoh dan berkelanjutan di organisasi.

2. **Lini Pertama - Konsumen dan Pihak Ketiga**
   Lini pertama merupakan pihak lain yang berinteraksi langsung dengan pelaku bisnis, baik sebagai pengguna maupun pendukung layanan. Dalam ekosistem kepercayaan digital, lini pertama dapat menjadi sumber ancaman yang perlu dikelola oleh lini pusat. Terdapat hak-hak lini pertama yang harus dipenuhi oleh lini pusat sesuai dengan Pilar dan Domain Kepercayaan Digital. Di samping itu, terdapat pula kewajiban yang harus dilakukan sesuai dengan standar dan kepatuhan yang ditetapkan oleh lini pusat. Berikut merupakan hal-hal yang menjadi hak dari lini pertama.

   - Tersedianya entitas tepercaya: jaminan bahwa pihak yang menyediakan layanan memiliki identitas, otorisasi, dan reputasi yang dapat diverifikasi;
   - Tersedianya akses tepercaya: tersedianya sistem autentikasi dan kontrol akses yang memastikan akses hanya diberikan kepada pihak yang berwenang;
   - Tersedianya data tepercaya: jaminan atas akurasi, integritas, dan pelindungan data pribadi serta data transaksi;

- Tersedianya alasan tepercaya: transparansi dalam tujuan pengumpulan, penggunaan, dan pengolahan data digital;
- Tersedianya tujuan tepercaya: kejelasan orientasi layanan digital yang konsisten dengan nilai dan kepentingan pengguna;
- Tersedianya layanan tepercaya: layanan yang dapat diandalkan, tersedia, dan bebas dari manipulasi atau penyalahgunaan;
- Tersedianya kenyamanan: pengalaman pengguna yang intuitif, tidak membebani, dan memberikan rasa aman dalam berinteraksi secara digital.

Selain itu juga terdapat kewajiban yang harus dipatuhi oleh lini pertama, yaitu sebagai berikut:

- Mengedukasi diri dan meningkatkan kesadaran keamanan siber dengan memahami risiko digital, mengenali ancaman umum, serta memahami hak-hak digital yang dimiliki;
- Menerapkan langkah-langkah *cyber hygiene* dengan menjaga kredensial pribadi, menghindari tautan mencurigakan, serta memperbarui perangkat lunak secara berkala;
- Memberikan masukan pada lini pusat untuk meningkatkan kualitas layanan dengan menyampaikan keluhan, saran, atau pelaporan insiden demi perbaikan layanan secara berkelanjutan.

3. **Lini Kedua – Fungsi Pengendalian (*Risk and Compliance*)**
Berposisi di sisi kiri bawah dalam model visual, lini kedua berperan sebagai fungsi pengendalian dan pengawasan yang memberikan dukungan serta keahlian kepada lini pusat. Lini kedua tidak terlibat langsung dalam operasional, tetapi menjalankan peran *check and balance* terhadap pengelolaan risiko dan kepatuhan pada aturan terkait penerapan kepercayaan digital.

   Fungsi utama lini kedua antara lain:

   - Menentukan dan mengimplementasikan kerangka kerja pengendalian risiko, indikator risiko kunci (*key risk indicators*), serta mekanisme pelaporan dan pemantauan efektivitas kontrol;
   - Melakukan kajian berkala terhadap *standard operating procedure* (SOP) dan kebijakan dari lini pusat yang berkaitan dengan kepercayaan digital untuk memastikan keselarasan dengan hukum dan regulasi yang terkait;
   - Melakukan verifikasi penilaian dampak privasi, mengevaluasi desain kontrol keamanan yang diusulkan unit bisnis, dan memberikan konsultasi kepada lini pusat jika diperlukan;
   - Memastikan lini pusat dapat melaksanakan respons insiden dan memastikan prosedur penanganan insiden terdokumentasi, cepat, serta transparan.

   Dalam mendukung kepercayaan digital, lini kedua juga memiliki tanggung jawab strategis berikut:

- Menyusun, meninjau, dan menyosialisasikan kebijakan keamanan informasi dan perlindungan data;
- Menyediakan panduan dan validasi implementasi terhadap standar internasional sesuai dengan peraturan yang berlaku;
- Menilai efektivitas pengendalian digital secara berkala dan memberikan laporan yang objektif.

Keberadaan lini kedua memperkuat struktur kepercayaan digital dengan memastikan organisasi bertindak konsisten, patuh, dan tanggap terhadap risiko digital yang dinamis, serta memastikan lini pusat mengimplementasikan rancangan kepercayaan digital yang telah ditetapkan sebelumnya.

4. **Lini Ketiga – Audit Independen**
   Terletak di sisi kanan bawah, lini ketiga dijalankan oleh auditor internal maupun eksternal yang memiliki fungsi evaluatif dan bersifat independen. Mereka tidak terlibat dalam aktivitas operasional atau kontrol sehari-hari, sehingga dapat memberikan *assurance* yang objektif terhadap efektivitas tiga lini sebelumnya.

   Peran kunci lini ketiga meliputi:

   - Melakukan audit berkala, tematik, dan berbasis risiko untuk mengevaluasi tata kelola, keamanan informasi, dan perlindungan data;
   - Menyelenggarakan audit forensik dalam merespons insiden serius seperti kebocoran data atau kompromi sistem kritikal;
   - Mengevaluasi kematangan budaya risiko organisasi serta kecukupan kontrol dan tata kelola digital;
   - Menyampaikan rekomendasi perbaikan, memantau tindak lanjutnya, dan melaporkan hasil audit kepada lini pusat;
   - Meningkatkan transparansi publik melalui pernyataan kepatuhan (misalkan ISO/IEC 27001) dan publikasi temuan material.

   Dengan memberikan evaluasi yang objektif dan menyeluruh, lini ketiga memastikan bahwa sistem kepercayaan digital tidak hanya berjalan sesuai rencana tetapi juga terus berkembang menuju keunggulan. Keberadaan lini ini memberi keyakinan tambahan kepada pemangku kepentingan bahwa pengelolaan risiko digital dan perlindungan data dilakukan secara profesional, transparan, dan berintegritas tinggi.

Secara keseluruhan, integrasi yang sinergis antara keseluruhan lini ekosistem kepercayaan digital, baik pelaku bisnis, konsumen dan pihak ketiga, fungsi pengendalian, serta audit independen, menciptakan arsitektur tata kelola risiko digital yang tangguh. Sinergi ini tidak hanya menjamin efektivitas pengelolaan risiko dan kepatuhan, tetapi juga menciptakan ekosistem kepercayaan digital yang adaptif terhadap dinamika ancaman siber dan perubahan regulasi. Namun, keberhasilan integrasi ini sangat bergantung pada kualitas kepemimpinan yang ditunjukkan oleh manajemen puncak.

6.4.2 Interaksi Ekosistem Kepercayaan Digital

Dalam ekosistem kepercayaan digital di Indonesia, berbagai bentuk hubungan dan interaksi direpresentasikan melalui konsep seperti G2G (*Government to Government*), G2B (*Government to Business*), G2C (*Government to Citizen*), B2B (*Business to Business*), dan B2C (*Business to Consumer*) merepresentasikan berbagai bentuk hubungan dan interaksi yang terjadi dalam ruang digital. Singkatan "G" merujuk pada Pemerintah, "B" pada Bisnis atau pelaku usaha, dan "C" pada Konsumen atau masyarakat umum.

G2G mengacu pada interaksi antarlembaga pemerintah dalam penyelenggaraan layanan publik secara digital, misalnya integrasi sistem antara Kementerian Dalam Negeri dan Badan Pertanahan Nasional untuk mempermudah proses administrasi kependudukan. G2B melibatkan keterhubungan antara pemerintah dan sektor bisnis, seperti platform pengadaan barang dan jasa pemerintah secara elektronik (*e-procurement*) yang meningkatkan transparansi dan efisiensi. G2C mencakup layanan digital yang langsung menyasar masyarakat, seperti aplikasi kesehatan, pendidikan, atau program bantuan sosial berbasis data kependudukan.

Sementara itu, B2B menggambarkan interaksi antarperusahaan dalam rantai pasok digital, termasuk pertukaran data logistik, pembayaran digital, dan integrasi sistem antarmitra bisnis. Sedangkan B2C merupakan model yang paling familiar di masyarakat, seperti transaksi *e-commerce*, layanan *fintech*, hingga *media streaming* yang menuntut perlindungan data dan keamanan siber yang ketat.

Keberhasilan transformasi digital di Indonesia sangat bergantung pada tingkat kepercayaan dalam kelima jenis interaksi tersebut. Tanpa adanya rasa percaya dari sisi keamanan data, privasi, maupun kualitas layanan, inisiatif digital, baik dari pemerintah maupun swasta/industri, akan sulit mendapatkan penerimaan luas dari masyarakat. Oleh karena itu, prinsip transparansi, akuntabilitas, dan perlindungan data harus menjadi fondasi utama dalam penyelenggaraan setiap layanan digital. Penguatan regulasi seperti UU PDP, kesadaran digital masyarakat, serta komitmen pelaku usaha dan instansi pemerintah dalam menjaga etika digital akan semakin mendukung terciptanya ekosistem digital yang aman dan tepercaya di Indonesia.

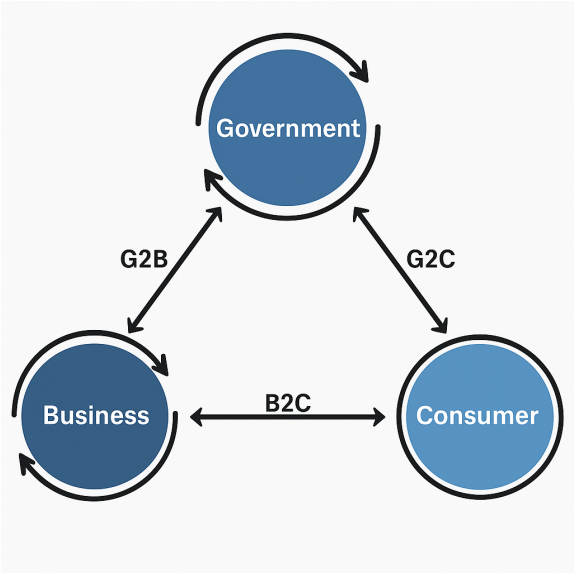
6.4.3 Kepercayaan Digital dalam Ekosistem G2G, G2B, G2C, B2B, dan B2C

Keberhasilan transformasi digital menuntut adanya kepercayaan digital yang kuat, sebagai landasan bagi interaksi yang aman, transparan, dan berkelanjutan antara pemerintah dan semua pihak yang terlibat. Gambar 6.4 menyajikan representasi visual dari ekosistem kepercayaan digital yang terintegrasi, mencerminkan pola interaksi utama antara aktor-aktor kunci: pemerintah (G), bisnis (B), dan konsumen (C). Diagram ini menekankan adanya keterhubungan yang saling menguatkan antara entitas pemerintah dan dunia usaha, yang divisualisasikan melalui sirkulasi (*loop*) timbal balik. *Loop* ini mencerminkan proses dinamis antara regulasi dan implementasi, pengawasan dan inovasi, serta kepatuhan dan adaptasi yang terus

berlangsung dalam ekosistem digital nasional.

Setiap bentuk interaksi dalam ruang digital harus dirancang dan dijalankan dengan memperhatikan secara menyeluruh berbagai faktor kunci yang membentuk kepercayaan digital. Hal ini penting guna memastikan bahwa tujuan penerapan kepercayaan digital, yakni menciptakan ekosistem digital yang aman, adil, transparan, dan andal, dapat tercapai secara konsisten dan berkelanjutan.

Keandalan infrastruktur, jaminan terhadap privasi dan kerahasiaan data, serta kemampuan sistem untuk tetap tersedia dan utuh dalam menghadapi gangguan, menjadi elemen yang tidak dapat dinegosiasikan. Selain itu, interoperabilitas, pengendalian akses, serta mekanisme autentikasi yang kuat, memperkuat kredibilitas sistem dan mencegah terjadinya penyalahgunaan. Tidak kalah penting adalah penerapan prinsip keadilan, auditabilitas, dan desain yang berorientasi pada pengguna, agar sistem digital tidak hanya berfungsi dengan baik secara teknis, tetapi juga menjunjung tinggi nilai-nilai inklusivitas dan akuntabilitas. Dengan memastikan bahwa seluruh faktor ini terintegrasi dalam setiap proses dan kebijakan yang diterapkan, kepercayaan digital tidak hanya menjadi jargon normatif, tetapi benar-benar mewujud sebagai kerangka kerja nyata yang mendasari keberlangsungan interaksi digital yang aman dan berkelanjutan.



Gambar 6.4: Pola Interaksi Ekosistem Kepercayaan Digital Indonesia

1. *Government to Government* (G2G): Fondasi Internal Kepercayaan Antar-Institusi

Pola G2G mencerminkan keterhubungan antarlembaga pemerintah dalam berbagi data, menyelenggarakan layanan, dan mengoordinasikan kebijakan melalui

infrastruktur digital yang terintegrasi. Contoh nyata dari penerapan G2G adalah integrasi data kependudukan dari Ditjen Dukcapil dengan layanan BPJS, perpajakan, atau layanan pendidikan yang memungkinkan validasi data yang cepat dan andal tanpa redundansi administratif. Kolaborasi ini menuntut jaminan interoperabilitas, keamanan data, dan pengendalian akses yang ketat antarlembaga.

2. *Government to Citizen* (G2C): Wujud Kepercayaan Publik terhadap Layanan Digital Pemerintah

G2C menggambarkan hubungan digital langsung antara pemerintah dan masyarakat melalui penyediaan layanan publik berbasis digital. Layanan seperti e-KTP, aplikasi layanan kesehatan, sistem pengaduan *online*, maupun platform bantuan sosial digital merupakan bagian dari pola ini. Kepercayaan di sini dibangun di atas keandalan infrastruktur, jaminan privasi, dan desain yang berorientasi pengguna (*user-centric*). Tanpa itu, masyarakat akan ragu mengadopsi layanan digital meskipun mudah diakses.

3. *Government to Business* (G2B): Kolaborasi Digital antara Regulator dan Pelaku Usaha

Pola G2B mengacu pada hubungan antara pemerintah sebagai regulator dengan sektor bisnis sebagai penyedia layanan atau produk di ruang digital. Dalam konteks ini, kepercayaan digital dibangun melalui kerangka tata kelola yang menjamin kepastian hukum, kejelasan regulasi, serta kemudahan akses terhadap layanan administratif berbasis digital, seperti izin usaha berbasis risiko melalui sistem perizinan *online single submission* (OSS), kebijakan perlindungan data, dan standar keamanan siber yang berlaku bagi entitas bisnis. Kepercayaan digital dalam konteks G2B memungkinkan terciptanya iklim usaha yang sehat, adil, dan inovatif, sekaligus mempercepat integrasi sektor swasta/industri ke dalam agenda transformasi digital nasional.

4. *Business to Business* (B2B): Kepercayaan sebagai Prasyarat Kolaborasi Komersial

Interaksi B2B mencakup hubungan digital antara dua atau lebih entitas bisnis dalam menyediakan barang, jasa, atau teknologi. Kepercayaan digital dalam B2B menjadi prasyarat untuk kolaborasi rantai pasok yang efisien dan aman. Aspek seperti mekanisme autentikasi yang kuat dan auditabilitas transaksi menjadi krusial untuk mencegah risiko operasional dan reputasi, sekaligus menjadi katalis inovasi kolaboratif antarbisnis terutama dalam ekosistem digital lintas sektor dan lintas negara.

5. *Business to Consumer* (B2C): Kepercayaan sebagai Fondasi Loyalitas Konsumen

Pola B2C menggambarkan interaksi antara pelaku bisnis dan konsumen akhir dalam penyediaan produk atau layanan digital. Dalam ekosistem ini, kepercayaan digital menjadi penentu utama terhadap keputusan konsumen dalam memilih, menggunakan, atau merekomendasikan layanan digital tertentu. Ketika kepercayaan ini terjaga secara konsisten, loyalitas konsumen terhadap merek digital akan semakin kuat, bahkan menjadi advokat alami dalam ekosistem digital melalui testimoni, ulasan, dan rekomendasi.

6. Ekosistem Kepercayaan Digital sebagai Sistem yang Terhubung

Seluruh pola interaksi, G2G, G2B, G2C, B2B, dan B2C, merupakan elemen yang saling bergantung dalam satu ekosistem digital yang utuh. Kualitas layanan G2C, misalnya, sangat ditentukan oleh efektivitas G2G dan G2B, sedangkan kekuatan hubungan B2B dan B2C tidak dapat dilepaskan dari regulasi dan infrastruktur yang dikembangkan oleh pemerintah.

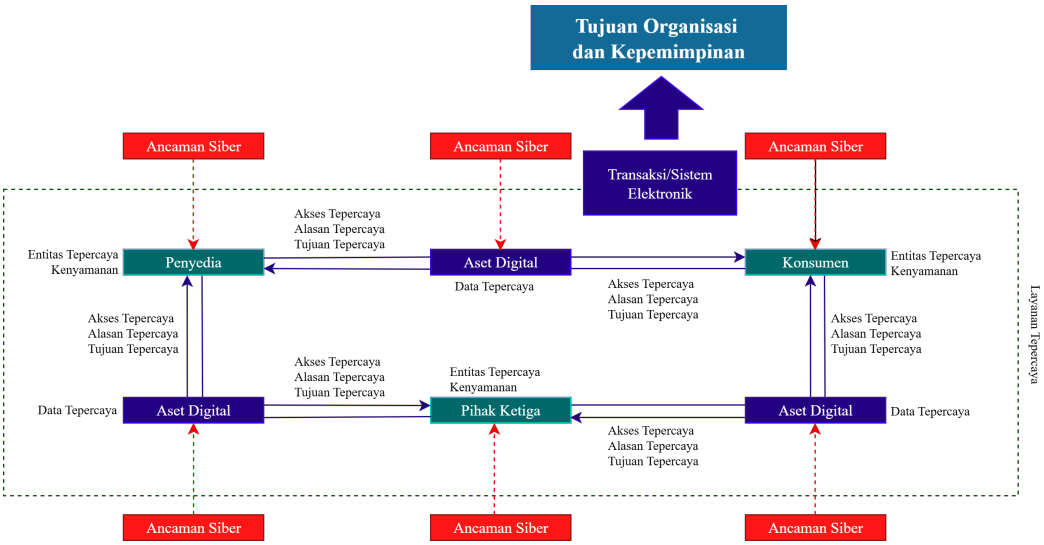
Dengan kata lain, kepercayaan digital tidak hanya dibangun pada satu titik interaksi, melainkan pada keseluruhan jejaring relasi digital yang terkoordinasi, transparan, dan responsif. Untuk itu, pendekatan sistemik yang mengintegrasikan tata kelola teknologi, proses bisnis, dan nilai sosial menjadi kunci dalam membangun ekosistem kepercayaan digital yang kolaboratif, berkelanjutan, dan resiliensi terhadap ancaman masa depan.

6.5 Penerapan Kepercayaan Digital pada Sistem dan Transaksi Elektronik (STE)

Kepercayaan digital merupakan aspek krusial dalam memastikan keamanan, transparansi, dan integritas dalam sistem serta transaksi elektronik. Seiring dengan meningkatnya digitalisasi di berbagai sektor, sistem transaksi elektronik semakin kompleks dan melibatkan berbagai entitas, seperti konsumen, penyedia layanan, dan pihak ketiga. Untuk menjaga kepercayaan dalam ekosistem ini, diperlukan mekanisme yang dapat menjamin keabsahan, keamanan, dan kepatuhan terhadap regulasi yang berlaku.

Penerapan kepercayaan digital dalam sistem dan transaksi elektronik mencakup berbagai aspek, mulai dari perlindungan data, manajemen risiko, hingga kepatuhan terhadap standar keamanan. Setiap tahap dalam siklus hidup transaksi, mulai dari pembuatan, transmisi, penyimpanan, hingga pemusnahan data, harus dirancang dengan mempertimbangkan ancaman siber yang dapat muncul dari berbagai sisi. Oleh karena itu, pendekatan berbasis analisis risiko dan pemenuhan pilar keper-

cayaan digital menjadi langkah penting dalam membangun ekosistem transaksi elektronik yang andal dan tepercaya.



Gambar 6.5: Penerapan Kepercayaan Digital pada Sistem dan Transaksi Elektronik

Gambar 6.5 menunjukkan contoh penerapan kepercayaan digital dalam sistem transaksi elektronik. Setiap sistem atau transaksi elektronik dirancang dengan tujuan tertentu yang berkontribusi terhadap pencapaian sasaran organisasi. Dalam ekosistem ini, terdapat tiga entitas utama yang terlibat, yaitu konsumen, penyedia layanan, dan pihak ketiga, yang masing-masing memiliki peran dan tanggung jawab dalam menjaga keamanan serta keandalan transaksi.

Agar kepercayaan digital dapat terbangun secara berkelanjutan, diperlukan komitmen kolektif dari seluruh entitas tersebut dalam menerapkan prinsip-prinsip utama kepercayaan digital, seperti integritas, transparansi, privasi, dan keandalan sistem. Namun demikian, keberhasilan implementasi kepercayaan digital tidak hanya ditentukan oleh kesiapan teknologi atau kebijakan, tetapi juga oleh peran strategis kepemimpinan dalam organisasi.

Kepemimpinan yang kuat dan visioner berperan penting dalam menetapkan arah, memastikan tata kelola yang akuntabel, mendorong budaya keamanan digital, serta membangun sinergi antarpemangku kepentingan. Tanpa dukungan dan komitmen dari tingkat pimpinan, berbagai inisiatif kepercayaan digital cenderung bersifat parsial, tidak konsisten, dan sulit diintegrasikan ke dalam proses bisnis inti organisasi.

Namun, penerapan sistem transaksi elektronik tidak terlepas dari berbagai ancaman siber yang dapat muncul dari berbagai sisi, baik dari faktor entitas pengguna, teknologi yang digunakan (baik perangkat keras maupun perangkat lunak), maupun dari siklus hidup informasi atau aset digital, mulai dari tahap penciptaan, transmisi, penyimpanan, hingga pemusnahan. Oleh karena itu, diperlukan analisis risiko

untuk mengidentifikasi, mengevaluasi, dan menentukan prioritas dalam mengelola risiko yang mungkin terjadi.

Hasil analisis risiko ini menjadi dasar dalam pemenuhan pilar-pilar kepercayaan digital yang harus dipenuhi oleh setiap entitas dan dalam setiap proses transaksi. Untuk mendukung proses ini, diperlukan instrumen kepercayaan digital yang berfungsi sebagai alat bantu dalam mendokumentasikan hasil identifikasi risiko serta menentukan kebutuhan keamanan di setiap domain kepercayaan digital. Semakin besar dan kompleks suatu sistem, semakin tinggi pula tingkat risiko yang dihadapi, sehingga perancangan kepercayaan digital harus disiapkan dengan lebih matang dan sistematis. Kata-kata yang ditandai dengan warna kuning dalam Gambar 6.5 menunjukkan pilar kepercayaan digital yang perlu dipenuhi oleh setiap entitas dan dalam setiap tahap proses transaksi elektronik.

7

Rekomendasi Strategis Kepercayaan Digital Indonesia

> Trust is earned when actions meet words.
>
> — Chris Butler

Kepercayaan digital menjadi elemen kunci dalam mewujudkan transformasi digital. Tanpa adanya rasa percaya yang kuat dari masyarakat, upaya pengembangan ekosistem digital berisiko kehilangan legitimasi sosial dan dukungan partisipatif. Kepercayaan ini melingkupi keyakinan terhadap pelindungan data pribadi, keamanan layanan digital, serta tata kelola teknologi yang akuntabel dan transparan. Dalam konteks Indonesia, urgensi membangun kepercayaan digital semakin tinggi seiring dengan meningkatnya adopsi layanan berbasis teknologi, maraknya insiden siber, serta tumbuhnya kesadaran publik terhadap pentingnya perlindungan hak-hak digital.

Kerangka kerja kepercayaan digital Indonesia perlu dirancang sebagai peta jalan strategis yang mampu mengintegrasikan nilai, kebijakan, dan praktik kepercayaan digital ke dalam tata kelola nasional. Tujuannya tidak hanya menciptakan ekosistem digital yang tangguh dan andal, tetapi juga mendorong kolaborasi lintas sektor, pemerintah, swasta/industri, akademisi, masyarakat sipil, dan media, dalam menjunjung tinggi etika digital dan prinsip hak asasi manusia di ruang siber. Kerangka kerja ini disusun berdasarkan analisis komparatif terhadap praktik-praktik global, ketentuan regulatif nasional, serta realitas sosial-ekonomi dan tantangan teknologi yang dihadapi Indonesia.

Berikut ini disajikan sejumlah rekomendasi strategis yang dirumuskan berdasarkan pemetaan isu, pembelajaran dari praktik terbaik internasional, serta evaluasi terhadap kebutuhan dan prioritas nasional. Rekomendasi ini diharapkan menjadi landasan yang kokoh bagi pengembangan dan penerapan kerangka kerja kepercayaan digital Indonesia ke depan.

7.1 Rekomendasi Strategis

Pembangunan ekosistem kepercayaan digital yang tangguh dan berkelanjutan menuntut arah kebijakan yang strategis, menyeluruh, dan adaptif terhadap dinamika teknologi global. Seiring meningkatnya ketergantungan pada layanan digital di sektor publik maupun swasta, urgensi untuk merumuskan langkah konkret yang menjamin keandalan, keamanan, dan akuntabilitas sistem digital nasional menjadi kian mendesak.

Rekomendasi strategis berikut disusun untuk memperkokoh fondasi kepercayaan digital nasional melalui penegasan prinsip dasar di tingkat kebijakan, harmonisasi regulasi, serta penguatan kelembagaan dan infrastruktur teknologi. Di sisi implementasi, penerapan standar keamanan dan audit teknologi yang berfokus pada sektor prioritas nasional, serta integrasi prinsip *trust by design*, menjadi pilar vital dalam transformasi sistem digital Indonesia. Lebih jauh lagi, aspek pendidikan dan literasi digital, pemanfaatan kecerdasan artifisial (AI) untuk memperkuat keamanan siber, serta dorongan terhadap kolaborasi multipemangku kepentingan (*multi-stakeholder*) dan diplomasi digital, merupakan elemen kunci dalam membangun kepercayaan yang mampu meningkatkan daya saing nasional di kancah global.

7.1.1 Penegasan Prinsip Nasional Kepercayaan Digital

Kepercayaan digital harus dimulai dari rumusan prinsip-prinsip nasional yang menjadi fondasi dalam setiap kebijakan dan penyelenggaraan layanan digital, baik oleh sektor publik maupun swasta/industri. Prinsip-prinsip ini perlu didefinisikan secara eksplisit sebagai kerangka normatif yang mendasari transformasi digital di Indonesia.

Prinsip-prinsip kepercayaan digital pada dasarnya mencerminkan komitmen terhadap perlindungan hak digital warga negara, keamanan sistem elektronik, serta tata kelola teknologi yang transparan dan akuntabel. Dalam konteks transformasi digital yang semakin kompleks, prinsip-prinsip tersebut tidak hanya terbatas pada aspek teknis, tetapi juga mencakup dimensi etika, sosial, dan kedaulatan. Keamanan dan ketahanan digital menuntut sistem yang tangguh dan adaptif terhadap risiko, sementara privasi dan perlindungan data pribadi menegaskan pentingnya penghormatan terhadap hak asasi digital. Di sisi lain, transparansi dan akuntabilitas dalam pengelolaan teknologi perlu dijalankan bersamaan dengan keterbukaan sistem dan interoperabilitas untuk mendorong efisiensi dan inovasi. Kepercayaan digital juga harus memastikan akses yang merata dan adil bagi seluruh lapisan masyarakat,

serta menjunjung tinggi tanggung jawab sosial dalam penggunaan teknologi, khususnya kecerdasan artifisial. Dalam kerangka kedaulatan digital, penguasaan atas infrastruktur strategis dan data nasional menjadi krusial agar arah pengembangan teknologi tetap berpihak pada kepentingan nasional. Dengan demikian, kepercayaan digital menjadi landasan yang menyatukan dimensi perlindungan individu, tata kelola yang baik, dan kepentingan strategis negara di era digital.

Rumusan prinsip ini tidak cukup hanya menjadi deklarasi moral, tetapi harus dituangkan dalam bentuk kebijakan nasional atau regulasi lintas sektor yang mengikat. Dokumen resmi tersebut akan berperan sebagai acuan operasional bersama bagi seluruh pemangku kepentingan, pemerintah, swasta/industri, akademisi, dan masyarakat sipil, dalam membangun ekosistem digital yang tepercaya, adil, dan bertanggung jawab.

7.1.2 Harmonisasi dan Integrasi Regulasi

Fragmentasi regulasi menjadi salah satu tantangan krusial dalam mewujudkan tata kelola kepercayaan digital di Indonesia. Perbedaan interpretasi, tumpang tindih kewenangan, dan ketidaksinkronan antarperaturan, seperti UU PDP, UU ITE, Perpres SPBE, dan berbagai regulasi sektoral lainnya, kerap menghambat pelaksanaan perlindungan data dan keamanan siber secara efektif.

Untuk mengurai kompleksitas tersebut, diperlukan kerangka hukum yang terintegrasi, harmonis, dan responsif terhadap dinamika teknologi. Pemerintah perlu membentuk gugus tugas lintas kementerian dan lembaga yang berfungsi sebagai simpul koordinasi regulasi. Gugus tugas ini harus memiliki mandat yang kuat untuk merancang kebijakan bersama, menyusun standar interoperabilitas sistem digital nasional, serta memastikan keterpaduan antara kebijakan nasional dan praktik di lapangan.

Selain aspek hukum, harmonisasi juga harus memperhatikan realitas teknis dan operasional antarsektor, sehingga memungkinkan integrasi sistem digital antara layanan publik dan swasta/industri berjalan secara efisien, aman, dan tepercaya. Kerangka regulasi yang sinkron akan menjadi dasar yang kokoh bagi pengembangan ekosistem kepercayaan digital nasional. Selain memberikan kepastian hukum bagi para pelaku industri digital, integrasi regulasi ini juga akan memperkuat kepercayaan masyarakat terhadap penggunaan teknologi, mendorong inovasi yang bertanggung jawab.

7.1.3 Penguatan Kelembagaan dan Infrastruktur

Penguatan kelembagaan merupakan pilar strategis dalam mendukung tata kelola kepercayaan digital nasional. Dalam ekosistem digital yang kian kompleks dan terhubung lintas sektor, kejelasan peran serta demarkasi kewenangan antarlembaga menjadi sangat penting untuk memastikan koordinasi berjalan secara efektif dan respons terhadap tantangan siber dapat dilakukan secara terpadu.

Badan Siber dan Sandi Negara (BSSN) perlu diperkuat posisinya sebagai otoritas teknis utama yang memegang komando keamanan siber nasional serta pengawas implementasi prinsip keamanan dalam kepercayaan digital. Mandat BSSN mencakup perumusan kebijakan teknis keamanan informasi, manajemen krisis insiden siber nasional, dan orkestrasi pengamanan Infrastruktur Informasi Vital (IIV) lintas sektor. Dalam kerangka kerja ini, BSSN mutlak didukung oleh kewenangan regulasi yang kuat, kapasitas teknis mumpuni, dan mekanisme respons yang adaptif terhadap evolusi ancaman.

Secara paralel, Kementerian Komunikasi dan Digital (Kenkomdigi) berperan sebagai regulator utama dalam tata kelola ekosistem digital, literasi publik, dan kedaulatan data. Tanggung jawab strategis ini meliputi pengawasan kepatuhan Penyelenggara Sistem Elektronik (PSE), penetapan standar layanan digital yang inklusif, serta penyediaan infrastruktur informasi publik. Kementerian ini juga memegang peran sentral dalam memastikan inovasi digital berjalan selaras dengan prinsip transparansi, akuntabilitas publik, dan perlindungan hak digital warga negara.

Guna mencegah tumpang tindih fungsi (*overlapping*) dan meningkatkan efektivitas kebijakan, penyusunan peta jalan kelembagaan serta peta kewenangan yang presisi mutlak diperlukan. Koordinasi lintas sektor harus dilembagakan melalui kerangka regulasi yang tegas maupun forum kolaborasi teknis, sehingga setiap institusi dapat menjalankan fungsinya secara optimal, saling melengkapi, dan menghilangkan mentalitas silo sektoral.

Selain dimensi kelembagaan, ketersediaan infrastruktur digital yang andal merupakan prasyarat fundamental dalam membangun kepercayaan publik terhadap layanan digital. Pemerintah perlu mengakselerasi pembangunan dan pemerataan akses internet berkualitas tinggi, khususnya di wilayah 3TP (Tertinggal, Terpencil, Terluar, dan Perbatasan), untuk menjamin hak setiap warga negara dalam berpartisipasi secara setara dalam transformasi digital.

Pengembangan infrastruktur tidak hanya terbatas pada konektivitas jaringan, tetapi juga mencakup penguatan kedaulatan komputasi. Hal ini meliputi optimalisasi sistem komputasi awan pemerintah (*Government Cloud*) serta pembangunan Pusat Data Nasional (PDN) yang mandiri, berstandar global, dan memiliki resiliensi tinggi terhadap serangan siber. Infrastruktur ini berfungsi sebagai tulang punggung layanan publik nasional—mulai dari *e-government* hingga identitas digital—yang menuntut jaminan keamanan tanpa kompromi sebagai dasar kepercayaan pengguna.

Lebih jauh, pembentukan *Digital Trust Testing Center* perlu segera direalisasikan sebagai sarana strategis untuk pengujian, verifikasi, dan sertifikasi keamanan sistem digital. Fasilitas ini dirancang untuk melayani instansi pemerintah, sektor industri, hingga UMKM, guna memastikan bahwa setiap sistem yang diluncurkan ke publik telah memenuhi standar keamanan dan privasi yang ketat. Keberadaan fasilitas ini akan memperkuat mekanisme pertahanan preventif sekaligus memberikan jaminan mutu (*quality assurance*) terhadap ekosistem digital di Indonesia.

Melalui harmonisasi kelembagaan yang solid dan percepatan pembangunan infrastruktur yang berorientasi pada keamanan, Indonesia dapat meletakkan fondasi

kokoh bagi kerangka kerja kepercayaan digital yang tidak hanya aman dan andal, tetapi juga adaptif terhadap dinamika teknologi global.

7.1.4 Penerapan Standar Keamanan dan Audit Teknologi

Adopsi standar teknis yang diakui secara internasional merupakan langkah fundamental dalam membangun dasar kepercayaan terhadap layanan digital. Standar seperti SNI ISO/IEC 27001 untuk manajemen keamanan informasi, SNI ISO/IEC 27701 untuk perlindungan privasi, serta ISO/IEC 42001 untuk tata kelola kecerdasan artifisial, perlu ditetapkan sebagai persyaratan minimum bagi seluruh penyedia layanan digital, baik di sektor publik maupun swasta/industri. Penerapan standar-standar ini tidak hanya menjamin interoperabilitas, tetapi juga menyediakan kerangka kerja yang andal untuk memastikan integritas, keamanan, dan transparansi sistem digital yang digunakan masyarakat luas.

Untuk memastikan standar tersebut terimplementasi secara konsisten dan terukur, diperlukan pedoman operasional yang komprehensif. Panduan ini harus mencakup mekanisme teknis penerapan standar, pengembangan skema audit sistem elektronik berbasis risiko, serta penetapan indikator kinerja utama (KPI) untuk evaluasi kepatuhan secara berkala. Pelaksanaan audit teknologi yang independen menjadi instrumen vital dalam menjaga akuntabilitas penyelenggara sistem, sekaligus berfungsi sebagai landasan bagi peningkatan berkelanjutan (*continuous improvement*) kualitas dan kepercayaan publik terhadap ekosistem digital nasional.

7.1.5 Implementasi pada Sektor Prioritas Nasional

Beberapa sektor strategis, seperti pemerintahan, keuangan, pendidikan, dan kesehatan, memiliki peran vital dalam ekosistem nasional. Oleh karena itu, penerapan kerangka kepercayaan digital di sektor-sektor ini memerlukan perhatian khusus dan pendekatan yang terukur.

Pada sektor pemerintahan, pemerintah sebagai penyedia layanan publik digital memegang tanggung jawab utama dalam membangun kepercayaan masyarakat. Prioritas utama adalah penguatan interoperabilitas antarsistem pemerintahan melalui implementasi penuh inisiatif *Satu Data Indonesia*. Langkah ini bertujuan memastikan pertukaran data yang konsisten, aman, dan efisien antarinstansi, serta meminimalkan redundansi dan potensi kesalahan data.

Selain interoperabilitas, keandalan aplikasi layanan publik seperti e-KTP digital, BPJS Online, dan platform penyaluran bantuan sosial harus ditingkatkan dengan jaminan privasi yang ketat. Hal ini juga berlaku pada sistem administrasi pemerintahan, seperti *Online Single Submission* (OSS). Sistem ini perlu menerapkan autentikasi berlapis dan mekanisme kontrol akses yang ketat guna menjamin integritas transaksi antarpemerintah (G2G) maupun antara pemerintah dan masyarakat (G2C). Integrasi data lintas instansi yang mulus menjadi kunci untuk meminimalkan risiko kebocoran akibat fragmentasi sistem, sekaligus mempercepat proses layanan

publik.

Untuk mengatasi meningkatnya kompleksitas ancaman siber terhadap sistem elektronik pemerintah, pendekatan *Zero Trust Architecture* (ZTA) perlu diadopsi secara menyeluruh. Setiap akses terhadap sistem harus diverifikasi secara ketat, menggunakan autentikasi bertingkat dan kontrol berbasis konteks. Pendekatan ini tidak hanya meningkatkan keamanan teknis, tetapi juga membentuk budaya kehati-hatian dalam pengelolaan sistem digital pemerintahan. Dengan penguatan interoperabilitas, peningkatan keamanan layanan, serta adopsi arsitektur keamanan modern seperti ZTA, sektor pemerintahan dapat menjadi pelopor dalam penerapan prinsip-prinsip kepercayaan digital di Indonesia, sekaligus memperkuat legitimasi digital negara di mata warganya.

Pada sektor keuangan dan *fintech*, penguatan kepercayaan digital perlu dimulai dari penegakan regulasi yang lebih ketat terhadap layanan ilegal, seperti *fintech* tak berizin dan praktik pinjaman *online* yang merugikan konsumen. Upaya ini wajib diiringi dengan penerapan standar teknologi keamanan yang komprehensif, mencakup autentikasi dua faktor (2FA), enkripsi *end-to-end*, serta mekanisme pelaporan insiden yang transparan. Penggunaan QRIS sebagai sarana pembayaran juga perlu terus dikembangkan dengan memastikan sistem keamanannya terintegrasi sesuai dengan standar nasional.

Di sisi lain, Otoritas Jasa Keuangan (OJK) memegang peran sentral untuk mempercepat penyusunan dan implementasi standar keamanan minimum bagi penyelenggara *fintech* dan dompet digital (*e-wallet*). Standarisasi ini krusial untuk melindungi konsumen dari risiko penipuan digital (*fraud*) dan penyalahgunaan data finansial, yang merupakan landasan utama kepercayaan dalam ekosistem ekonomi digital.

Sektor pendidikan memerlukan transformasi digital yang diimbangi dengan pembangunan kepercayaan terhadap ekosistem pembelajaran. Fokus utama harus diarahkan pada pelatihan literasi digital yang berkelanjutan bagi guru, siswa, dan tenaga kependidikan. Materi pelatihan perlu mencakup etika digital, pengelolaan identitas *online*, serta mitigasi dasar terhadap ancaman siber, sehingga teknologi dapat digunakan secara produktif dan bertanggung jawab.

Di sisi infrastruktur, pengembangan platform pembelajaran *online* dan sistem administrasi akademik wajib memprioritaskan keamanan dan pelindungan data pribadi pengguna. Setiap sistem digital yang digunakan dalam pendidikan, baik untuk keperluan pembelajaran maupun administrasi, wajib menjamin kerahasiaan dan integritas data siswa serta tenaga pendidik. Dengan membangun ekosistem pendidikan digital yang aman dan tepercaya, proses belajar-mengajar dapat berlangsung lebih adaptif terhadap teknologi, dan konsisten dengan prinsip-prinsip kepercayaan siber nasional.

Sektor kesehatan merupakan sektor yang sangat sensitif karena mengelola data pribadi yang bersifat kritis. Di tengah maraknya digitalisasi melalui Sistem Informasi Manajemen Rumah Sakit (SIMRS) dan *telemedicine*, perlindungan data pasien menjadi prioritas mutlak. Sistem digital harus menjamin kerahasiaan (*confidentiality*), integritas, dan ketersediaan data medis dalam seluruh siklus hidup data.

Pendekatan *privacy by design* perlu diterapkan sejak tahap perancangan sistem untuk memastikan bahwa perlindungan data menjadi bagian integral dari layanan kesehatan digital, bukan sekadar fitur tambahan.

Upaya integrasi sistem kesehatan nasional perlu diarahkan pada pembangunan arsitektur digital yang interoperabel, namun tetap menjaga prinsip keamanan dan privasi sebagai prioritas utama. Salah satu inisiatif penting yang perlu didorong adalah pengembangan sistem rekam medis elektronik yang terstandar dan terintegrasi lintas fasilitas layanan kesehatan. Untuk mendukung keabsahan dan keandalan informasi medis tersebut, penggunaan tanda tangan digital dan mekanisme verifikasi data wajib diimplementasikan secara menyeluruh. Pendekatan ini tidak hanya meningkatkan efisiensi administrasi layanan kesehatan, tetapi juga memperkuat kepercayaan pasien bahwa hak-hak privasi mereka terlindungi dengan baik dalam ekosistem kesehatan digital.

7.1.6 Prinsip *Trust by Design* dalam Sistem Digital Nasional

Pengembangan sistem digital nasional harus berlandaskan pada prinsip *trust by design*, sebuah pendekatan yang memastikan elemen kepercayaan dibangun secara inheren sejak tahap awal perencanaan. Penerapan prinsip ini menuntut agar aspek kepercayaan tidak sekadar menjadi fitur tambahan teknis di akhir proses, melainkan menjadi landasan utama dalam seluruh siklus hidup sistem, mulai dari perancangan, implementasi, hingga pemeliharaan.

Secara praktis, kerangka *trust by design* ditopang oleh tiga pilar utama. Pertama, adopsi *privacy by design* yang mengintegrasikan perlindungan data pribadi ke dalam arsitektur sistem secara mendasar. Kedua, integrasi aspek keamanan dan kepatuhan (*compliance*) secara proaktif di setiap fase pengembangan untuk memastikan bahwa standar hukum dan etika terpenuhi. Ketiga, penerapan kontrol akses yang ketat melalui autentikasi multifaktor dan enkripsi mutakhir sebagai syarat mutlak untuk mencegah pelanggaran privasi serta akses yang tidak sah.

Implementasi prinsip ini perlu diperluas ke berbagai sektor strategis, termasuk layanan publik, keuangan, transportasi, pendidikan, dan kesehatan. Di sektor keuangan dan pemerintahan, misalnya, penggunaan tanda tangan digital dan sertifikat elektronik harus menjadi standar transaksi untuk menjamin akuntabilitas. Selain itu, teknologi *blockchain* dapat dimanfaatkan untuk memperkuat integritas data dengan menciptakan jejak audit (*audit trail*) yang transparan dan tidak dapat dimanipulasi.

Sebagai *enabler* utama ekosistem ini, pembangunan platform identitas digital nasional yang aman dan terverifikasi menjadi krusial. Platform ini harus menjadi manifestasi konkret dari prinsip *security* dan *privacy by design*, yang mampu menjamin kedaulatan individu atas data pribadinya sekaligus memitigasi risiko pencurian identitas. Dengan mengintegrasikan seluruh elemen tersebut, Indonesia dapat membangun infrastruktur digital yang tidak hanya tangguh secara teknis, tetapi juga memiliki legitimasi sosial dan kepercayaan publik yang kokoh.

Konsep *trust by design* telah dikenalkan melalui kerangka kerja dan model kepercayaan digital dalam buku ini. Lebih detail dapat dilihat pada bab sebelumnya.

7.1.7 Pendidikan dan Literasi Kepercayaan Digital

Literasi digital yang matang merupakan fondasi utama dalam membangun kepercayaan digital nasional. Upaya peningkatan kesadaran ini harus bersifat inklusif dan berkelanjutan, menjangkau seluruh lapisan masyarakat, terutama kelompok rentan yang paling berisiko. Pemahaman mendasar tidak hanya terbatas pada aspek teknis, tetapi juga mencakup hak digital, etika penggunaan teknologi, serta kewaspadaan terhadap ancaman seperti rekayasa sosial. Penanaman nilai-nilai ini sejak dini menjadi krusial untuk membentuk ekosistem digital yang berintegritas.

Integrasi isu kepercayaan digital ke dalam kurikulum pendidikan formal, mulai dari tingkat dasar hingga perguruan tinggi, harus dilakukan secara sistematis. Di luar jalur formal, pendekatan pelatihan yang terarah bagi pelaku Usaha Mikro, Kecil, dan Menengah (UMKM), tenaga pendidik, serta komunitas lokal diperlukan untuk menjangkau segmen yang sering kali luput dari intervensi kebijakan. Pendidikan di sektor ini bertujuan untuk mengubah pola pikir dari sekadar pengguna teknologi menjadi partisipan digital yang sadar akan keamanan.

Pada skala nasional, inisiatif seperti Gerakan Nasional Literasi Digital (GNLD) perlu diperluas jangkauannya, tidak hanya secara geografis ke wilayah Tertinggal, Terdepan, Terluar, dan Perbatasan (3TP), tetapi juga dalam kedalaman substansi. Materi edukasi harus dirancang secara kontekstual dan relevan, mencakup strategi mitigasi disinformasi dan perlindungan privasi. Untuk tingkat yang lebih lanjut, khususnya bagi instansi pemerintah dan sektor industri, metode pembelajaran berbasis simulasi serangan siber (*cyber drill*) menjadi pendekatan yang efektif untuk meningkatkan kesiapsiagaan dan respons insiden secara nyata.

Selain kesadaran (*awareness*), masyarakat dan dunia usaha perlu dibekali dengan keterampilan ketahanan digital (*digital resilience*), yaitu kemampuan untuk menavigasi, bertahan, dan pulih dari risiko siber. Keterampilan esensial ini meliputi praktik kebersihan siber (*cyber hygiene*) seperti penerapan autentikasi dua faktor (2FA), deteksi dini *phishing*, serta pemahaman terhadap teknik manipulasi psikologis. Melalui kolaborasi lintas sektor yang melibatkan orang tua, pendidik, dan organisasi masyarakat sipil, literasi digital tidak hanya meningkatkan kapasitas individu, tetapi juga memperkuat imunitas kolektif bangsa dalam menjaga ekosistem kepercayaan digital.

7.1.8 Peluang Kecerdasan Artifisial (AI) dalam Keamanan *Online*

Untuk menjamin keberlanjutan keamanan *online*, para pemangku kepentingan dituntut untuk senantiasa berada satu langkah di depan pelaku kejahatan siber. Di tengah akselerasi teknologi, kecerdasan artifisial (AI) menghadirkan dualisme

dalam lanskap keamanan digital: sebagai peluang strategis sekaligus tantangan baru. AI tidak hanya menawarkan kapabilitas deteksi dan respons ancaman yang lebih cepat dan presisi, tetapi juga kemampuan prediktif untuk mengantisipasi pola serangan yang kompleks dan terus berevolusi.

Pemanfaatan AI dalam pertahanan siber mencakup spektrum yang luas, mulai dari analisis anomali perilaku, deteksi intrusi berbasis pembelajaran mesin, hingga orkestrasi respons insiden secara otomatis. Namun, ekuilibrium keamanan ini terganggu ketika aktor jahat turut mengeksploitasi AI untuk meningkatkan kecanggihan serangan. Fenomena seperti *deepfake*, *spear-phishing* yang sangat personal, hingga penemuan celah kerentanan secara otomatis (*automated exploit generation*) menjadi bukti nyata bahwa AI telah mengubah medan pertempuran siber.

Oleh karena itu, adopsi AI secara strategis adalah suatu keharusan. Para pemangku kepentingan—pemerintah, sektor industri, dan komunitas teknologi—wajib mengintegrasikan AI ke dalam arsitektur keamanan mereka dengan tetap berpegang pada prinsip etika, akuntabilitas, dan perlindungan privasi. Implementasi ini harus didukung oleh konsep *explainable AI* untuk memastikan keputusan sistem keamanan dapat dipahami, serta pengawasan ketat oleh dewan etik, khususnya pada sektor kritikal seperti layanan kesehatan, keuangan, dan administrasi pemerintahan.

Dalam tataran makro, peran pembuat kebijakan menjadi sangat krusial untuk menciptakan tata kelola yang tepat. Diperlukan kerangka regulasi yang menyeimbangkan dorongan inovasi dengan mitigasi risiko penyalahgunaan. Kerangka ini idealnya mencakup standar transparansi algoritma yang aman, audit terhadap model AI berisiko tinggi, serta investasi pada peningkatan kapasitas nasional untuk pengembangan AI yang tepercaya. Dengan pendekatan yang proaktif dan kolaboratif ini, AI dapat bertransformasi menjadi aset vital dalam memperkuat pertahanan digital nasional, menciptakan ekosistem *online* yang adaptif, tangguh, dan berkelanjutan.

7.1.9 Kolaborasi *Multi-Stakeholder* dan Diplomasi Digital

Keberhasilan pembangunan kepercayaan digital tidak dapat bertumpu semata pada inisiatif pemerintah, melainkan menuntut orkestrasi peran aktif seluruh pemangku kepentingan, mulai dari sektor industri, akademisi, komunitas teknologi, hingga masyarakat sipil. Sinergi lintas sektor ini harus difasilitasi secara sistematis guna memastikan harmoni antara kebijakan regulatif, laju inovasi, dan kebutuhan publik yang dinamis.

Untuk melembagakan partisipasi tersebut, diperlukan penguatan mekanisme konsultatif melalui forum kebijakan digital, konsultasi publik daring, dan panel etika teknologi. Sebagai langkah konkret, pembentukan Komite Nasional Kepercayaan Digital dapat menjadi wadah koordinatif strategis yang menjembatani dinamika ekosistem dengan regulasi. Di level operasional, forum dialog tripartit antara regulator, penyedia layanan, dan pengguna juga harus diintensifkan. Hal ini krusial tidak hanya untuk respons cepat terhadap insiden siber, tetapi juga untuk meningkatkan akuntabilitas pelaku usaha dalam menjamin perlindungan data dan hak pengguna.

Dalam kancah global, Indonesia perlu mempertegas posisi tawar melalui diplomasi digital yang proaktif. Partisipasi dalam perumusan norma internasional menjadi imperatif untuk memastikan prinsip keadilan dan kedaulatan digital nasional terakomodasi, khususnya pada isu strategis seperti interoperabilitas data lintas batas (*Cross-Border Data Flow*), tata kelola kecerdasan artifisial (AI), serta pengawasan dominasi platform global. Namun, diplomasi yang kuat harus didukung oleh kemandirian domestik. Oleh karena itu, pengembangan teknologi lokal dan kemandirian infrastruktur pusat data nasional menjadi prasyarat mutlak untuk menjaga kedaulatan sekaligus meningkatkan daya saing Indonesia dalam konstelasi digital global.

Mengingat ekosistem digital rentan terhadap ancaman yang bersifat asimetris dan transnasional, kolaborasi tidak boleh terhenti pada batas yurisdiksi. Kerja sama antara pelaku industri global dan aparat penegak hukum menjadi keharusan untuk memfasilitasi pertukaran informasi intelijen dan respons kolektif terhadap serangan siber. Di tingkat regional, platform seperti ASEAN harus dioptimalkan sebagai ruang berbagi praktik terbaik (*best practices*) dalam memerangi kejahatan lintas negara, termasuk isu mendesak seperti eksploitasi seksual anak secara daring. Melalui jejaring kerja sama bilateral dan multilateral yang kokoh, Indonesia dapat memperluas kapabilitas keamanan nasional sekaligus berkontribusi menciptakan ruang siber global yang aman, tepercaya, dan inklusif.

7.2 Penutup

Rangkaian rekomendasi yang disusun dalam dokumen ini tidak hanya dimaksudkan sebagai arahan normatif, melainkan juga sebagai pedoman strategis yang relevan dengan kebutuhan aktual Indonesia dalam membangun ekosistem digital yang tepercaya. Oleh karena itu, penyusunan kerangka kerja kepercayaan digital harus dilakukan secara holistik, dengan mempertimbangkan kekhasan sosial, ekonomi, hukum, dan budaya Indonesia, mencakup tataran prinsip hingga tahapan implementasi.

Kepercayaan digital bukan sekadar isu teknis, melainkan menyangkut aspek mendasar kehidupan berbangsa dan bernegara, termasuk perlindungan hak asasi manusia, tata kelola demokrasi digital, serta daya saing ekonomi nasional. Pengembangan kerangka kerja ini harus mampu mengharmonisasikan nilai-nilai lokal dan prinsip-prinsip universal dalam keseimbangan yang tepat.

Dinamika tantangan global, mulai dari disinformasi, risiko penyalahgunaan kecerdasan artifisial (AI), kebocoran data, hingga intervensi asing di ruang siber, menuntut respons kebijakan yang adaptif, terukur, dan berkelanjutan. Di sisi lain, potensi besar ekonomi digital hanya dapat direalisasikan apabila masyarakat memiliki rasa aman dan keyakinan penuh terhadap integritas sistem digital yang mereka gunakan.

Keberhasilan implementasi kerangka kepercayaan digital Indonesia sangat bergantung pada sinergi kolaboratif antarsektor: pemerintah sebagai regulator dan fasilitator, sektor industri sebagai penyedia layanan dan inovator, akademisi sebagai

pengembang riset, serta masyarakat sipil sebagai pengawas sekaligus penerima manfaat. Budaya gotong royong yang berlandaskan Pancasila dan Bhinneka Tunggal Ika menjadi modal sosial utama bangsa Indonesia untuk memastikan partisipasi aktif dan rasa kepemilikan bersama terhadap agenda transformasi digital nasional.

Dengan meneguhkan komitmen pada prinsip keamanan, transparansi, akuntabilitas, dan keadilan, Indonesia berpotensi besar menjadi pelopor di kawasan dalam membangun ekosistem digital yang berdaulat. Kerangka kerja kepercayaan digital ini diharapkan menjadi pijakan strategis dalam menata masa depan digital Indonesia yang aman, inklusif, dan bermartabat.

Daftar Referensi

[1] Indonesia Investments. Economic Update Indonesia. Diakses 1 Juli 2025. [Online]. Available: https://www.indonesia-investments.com/id/news/news-columns/economic-update-indonesia-indonesian-economy-expands-by-4.87-in-q1-2025/item9816

[2] Badan Pusat Statistik. Pertumbuhan PDB Tahun 2010 Mencapai 6,1 Persen - Badan Pusat Statistik Indonesia. Diakses 1 Juli 2025. [Online]. Available: https://www.bps.go.id/id/pressrelease/2011/02/07/891/pertumbuhan-pdb-tahun-2010-mencapai-6-1-persen.html

[3] ——. Pertumbuhan PDB 2013 Mencapai 5,78 Persen - Badan Pusat Statistik Indonesia. Diakses 1 Juli 2025. [Online]. Available: https://www.bps.go.id/id/pressrelease/2014/02/05/222/pertumbuhan-pdb-2013-mencapai-5-78-persen.html

[4] ——. Pertumbuhan Ekonomi Indonesia Tahun 2014 tumbuh 5,02 Persen, melambat sejak lima tahun terakhir - Badan Pusat Statistik Indonesia. Diakses 1 Juli 2025. [Online]. Available: https://www.bps.go.id/id/pressrelease/2015/02/05/1114/pertumbuhan-ekonomi-indonesia-tahun-2014-tumbuh-5-02-persen--melambat-sejak-lima-tahun-terakhir.html

[5] Ekonomi Indonesia Triwulan IV 2015 tumbuh 5,04 persen tertinggi selama tahun 2015 - Badan Pusat Statistik Indonesia. Diakses 1 Juli 2025. [Online]. Available: https://www.bps.go.id/id/pressrelease/2016/02/05/1267/ekonomi-indonesia-triwulan-iv-2015-tumbuh-5-04-persen-tertinggi-selama-tahun-2015.html

[6] International Monetary Fund. (2025) World Economic Outlook (April 2025) - Real GDP growth. International Monetary Fund. Diakses 1 Juli 2025. [Online]. Available: https://www.imf.org/external/datamapper/NGDP_RPCH@WEO/IDN?zoom=IDN&highlight=IDN

[7] World Bank. (2023) GDP (current US$) - Indonesia | Data. The World Bank. Diakses 1 Juli 2025. [Online]. Available: https://data.worldbank.org/indicator/NY.GDP.MKTP.CD?end=2023&locations=ID&start=2010

[8] Republik Indonesia, "Undang-Undang Republik Indonesia Nomor 59 Tahun 2024 tentang Rencana Pembangunan Jangka Panjang Nasional Tahun 2025-2045," 2024.

[9] Beranda - RPJPN 2025-2045. Diakses 1 Juli 2025. [Online]. Available: https://indonesia2045.go.id/

[10] Mustofa, Ardian Alif and Rasendriyo, Bhanu and Hanan, Haedar Said and Azzahra, Kinanti Fatimah, "The Role of Digital Transformation in Shaping Economic Growth: A Literature Review," in *Proceeding of the International Conference on Economics, Accounting, and Taxation*, vol. 1, no. 1, 2024, pp. 117–127. [Online]. Available: https://prosiding.areai.or.id/index.php/ICEAT

[11] World Bank. Digital Transformation Overview: Development news, research, data | World Bank. Diakses 25 September 2025. [Online]. Available: https://www.worldbank.org/en/topic/digital/overview

[12] Oliver Wyman. (2024) Decoding The Potential Of AI-Driven Growth In Indonesia. Diakses 24 September 2025. [Online]. Available: https://www.oliverwyman.com/our-expertise/insights/2024/oct/unlocking-potential-of-ai-driven-growth-in-indonesia.html

[13] Agarwal, A. and others, "Does Artificial Intelligence Influence the Operational Performance of Companies?" *ResearchGate*, 2022. [Online]. Available: https://www.researchgate.net/publication/358218744

[14] Byungjun Park and Taeyong Kim and Jeong Jong-pil, "AI-Smart Factory: Design and verification of Korean SME AI smart factory using level diagnosis system," *Procedia Computer Science*, vol. 224, pp. 169–179, 2023. [Online]. Available: https://www.sciencedirect.com/science/article/pii/S1877050923010724

[15] OECD. (2024) Indonesia: Stronger productivity, digitalisation and green transition are key to the country's future prosperity. Diakses 24 September 2025. [Online]. Available: https://www.oecd.org/en/about/news/press-releases/2024/11/indonesia-stronger-productivity-digitalisation-and-green-transition-are-key-to-the-country-s-future-prosperity.html

[16] Kevin Russell, Chris Bradley, Khoon Tee Tan, Jeongmin Seong, Phillia Wibowo, Indiana Jusi, Olivia White, Ashwin Balasubramanian, Antonius Santoso, and Guillaume de Gantès, "Propelling Indonesia's Productivity," McKinsey Global Institute, Tech. Rep., 2025. [Online]. Available: https://www.mckinsey.com/mgi/our-research/the-enterprising-archipelago-propelling-indonesias-productivity

[17] Hikmat, A. A. and others, "Artificial Intelligence (AI) in Telkom Indonesia's Digital Transformation," *Electronic Journal of Education, Social Economic and Technology*, vol. 6, no. 1, 2025. [Online]. Available: https://ejeset.saintispub.com/ejeset/article/download/404/279

[18] Maghfirah, P., "The Impact of Artificial Intelligence on Operational Cost Reduction in SMEs," *International Journal of Business, Management and Economic Research*, 2024. [Online]. Available: https://www.ijbmer.org/uploads2024/BMER_7_584.pdf

[19] M. M. Wihardja, "The Heterogeneous Impacts of Digital Transformation Investment – Indonesia," ERIA, Tech. Rep., 2024. [Online]. Available: https://www.eria.org/uploads/The-Heterogeneous-Impacts-of-Digital-Transformation-Investment-Indonesia.pdf

[20] Indonesia Investment Authority. (2022) Indonesia Digital Transformation: A Strategic Investment. Diakses 24 September 2025. [Online]. Available: https://www.ina.go.id/ina-in-the-news/indonesia-digital-transformation-a-strategic-investment

[21] IBM ASEAN Newsroom. (2025) Indonesia Businesses Primed for AI, But Face Gaps in Security, Infrastructure, Ethics and Talent. Diakses 24 September 2025. [Online]. Available: https://asean.newsroom.ibm.com/2025-06-04-IBM-Study-Indonesia-Businesses-Primed-for-AI-But-Face-Gaps-in-Security-Infrastructure-Ethics-and-Talent

[22] Badan Penelitian dan Pengembangan Sumber Daya Manusia Kementerian Komunikasi dan Informatika Republik Indonesia, "Indeks Masyarakat Digital indonesia," Kemenkominfo, Tech. Rep., 2023. [Online]. Available: https://data.komdigi.go.id/opendata/dataset/indeks-masyarakat-digital-indonesia-imdi

[23] We Are Social and Kepios. (2025) Digital 2025: Laporan Komprehensif tentang Dunia Digital di Indonesia. Diakses 25 Juli 2025. [Online]. Available: https://wearesocial.com/id/blog/2025/02/digital-2025/

[24] World Bank. (2021) Beyond Unicorns: Harnessing Digital Technologies for Inclusion in Indonesia — Infographic "Digital Economy in Indonesia". Diakses 24 September 2025. [Online]. Available: https://www.worldbank.org/en/news/infographic/2021/10/28/digital-economy-in-indonesia

[25] Kementerian Keuangan Republik Indonesia. (2025) Mewujudkan Asta Cita Melalui APBN 2025. Diakses 25 Juli 2025. [Online]. Available: https://opini.kemenkeu.go.id/article/read/mewujudkan-asta-cita-melalui-apbn-2025

[26] F. M. for Economic Affairs and Energy, "Digital strategy 2025," Germany, Tech. Rep., 2016. [Online]. Available: https://www.de.digital/DIGITAL/Redaktion/EN/Publikation/digital-strategy-2025.pdf?___blob=publicationFile&v=9

[27] T. F. Goverment, "Artificial intelligence strategy of the german federal government," Germany, Tech. Rep., 2020.

[28] T. F. M. of Justice and C. Protection, "Federal climate action act," Germany, Tech. Rep., 2024.

[29] E. Union, “France 2025 digital decade country report,” European Union, Tech. Rep., 2023. [Online]. Available: https://digital-strategy.ec.europa.eu/en/factpages/france-2025-digital-decade-country-report

[30] Ambassade De France Au Royaume-Uni. (2023) AI for Humanity. Diakses 6 Oktober 2025. [Online]. Available: https://uk.ambafrance.org/France-s-AI-strategy

[31] European Parliament. (2024) France’s climate action strategy. Diakses 6 Oktober 2025. [Online]. Available: https://www.europarl.europa.eu/RegData/etudes/BRIE/2024/767181/EPRS_BRI(2024)767181_EN.pdf

[32] M. of Planning and E. Development, “The national agenda for sustainable development,” Egypt, Tech. Rep., 2023. [Online]. Available: https://mped.gov.eg/Files/Egypt_Vision_2030_EnglishDigitalUse.pdf

[33] N. C. for Artificial Inteligence, “Egypt national artificial intelligence strategy,” Egypt, Tech. Rep., 2023. [Online]. Available: https://mped.gov.eg/Files/Egypt_Vision_2030_EnglishDigitalUse.pdf

[34] I. Authority, “Ict authority strategic plan 2024 - 2027,” Republic of Kenya, Tech. Rep., 2023. [Online]. Available: https://cms.icta.go.ke/sites/default/files/2024-09/SP_2024_-_2027_0912.pdf

[35] C. Ministry of Information and the Digital Economy, “Kenya artificial intelligence strategy 2025 - 2030,” Republic of Kenya, Tech. Rep., 2025. [Online]. Available: https://ict.go.ke/sites/default/files/2025-03/Kenya%20AI%20Strategy%202025%20-%202030.pdf

[36] M. of Energy, “Kenya national energy efficiency and conservaton strategy,” Republic of Kenya, Tech. Rep., 2020. [Online]. Available: https://unepccc.org/wp-content/uploads/2020/09/kenya-national-energy-efficiency-and-conservation-strategy-2020-1.pdf

[37] M. of Digital Transition and A. Reform, “Digital morocco 2030,” Kingdom of Moroco, Tech. Rep., 2025. [Online]. Available: https://www.mmsp.gov.ma/sites/default/files/2024-09/PlaquetteInstitutionnel_18092024_Ang.pdf

[38] A. Union, “The digital transformation strategy for africa 2020-2030,” African Union, Tech. Rep., 2020. [Online]. Available: https://au.int/sites/default/files/documents/38507-doc-DTS_for_Africa_2020-2030_English.pdf

[39] CNBC Indonesia. (2023) 9 Bidang Ekonomi Digital Ini Akan Diatur Bersama Negara ASEAN. Diakses 25 Juli 2025. [Online]. Available: https://www.cnbcindonesia.com/tech/20230904180115-37-469093/9-bidang-ekonomi-digital-ini-akan-diatur-bersama-negara-asean

[40] Sekretariat Kabinet Republik Indonesia. (2023) DEFA Andalan ASEAN Wujudkan Epicentrum of Growth. Diakses 25 Juli 2025. [Online]. Available: https://setkab.go.id/defa-andalan-asean-wujudkan-epicentrum-of-growth/

[41] CIPS Indonesia. (2024) Ekonomi Digital ASEAN Siap Lepas Landas dengan Digital Economy Framework Agreement (DEFA). Diakses 25 Juli 2025. [Online]. Available: https://www.cips-indonesia.org/post/ekonomi-digital-asean-siap-lepas-landas-dengan-digital-economy-framework-agreement-defa?lang=id

[42] The ASEAN Secretariat. (2024) The ASEAN Digital Economy Framework Agreement. Diakses 7 Juli 2025. [Online]. Available: https://theaseanmagazine.asean.org/article/the-asean-digital-economy-framework-agreement/

[43] A. of Southeast Asian Nations Secretariat, "The ASEAN ICT Masterplan 2020," ASEAN, Tech. Rep. 70, 2020. [Online]. Available: https://asean.org/wp-content/uploads/2024/11/ASEAN-ICT-Masterplan-2020.pdf

[44] Association of Southeast Asian Nations Secretariat, "ASEAN Digital Masterplan 2025," ASEAN, Tech. Rep., 2025.

[45] B. Tseen, F. Lee, J. P. Sims, U. Desarrollo, B. Tseen, F. Lee, L. D. Dinh, J. P. Sims, and S. A. Bettani, "ASEAN Digital Economy Framework Agreement (DEFA): Implications for Digital Trade and Regional Economic Integration," *Journal of Strategic and Global Studies*, vol. 8, no. 1, 2025.

[46] World Economic Forum. (2024) How ASEAN is building trust in its digital economy. Diakses 26 Juni 2025. [Online]. Available: https://www.weforum.org/stories/2024/01/asean-building-trust-digital-economy/

[47] Connolly, Barry, *Digital Trust: Social Media Strategies to Increase Trust and Engage Customers.* Bloomsbury Business, 2020.

[48] Paliszkiewicz, Joanna and Chen, Kuanchin, *Trust, Organizations and the Digital Economy.* Routledge, 2021.

[49] Xu, Hao, "Cross-border Data Flows: Regulations in international digital trade and China's solution," *Finance & Economics*, vol. 1, no. 7, 2024.

[50] Republik Indonesia, "Peraturan Presiden Nomor 47 Tahun 2023 tentang Strategi Keamanan Siber Nasional dan Manajemen Krisis Siber," 2023.

[51] ISACA. (2022) Understanding the Full Digital Trust Ecosystem. Diakses 20 Oktober 2025. [Online]. Available: https://www.isaca.org/resources/news-and-trends/isaca-now-blog/2022/understanding-the-full-digital-trust-ecosystem

[52] J. Boehm, L. Grennan, A. Singla, and K. Smaje. (2022) Why digital trust truly matters. Diakses 18 Juli 2025. [Online]. Available: https://www.mckinsey.com/capabilities/quantumblack/our-insights/why-digital-trust-truly-matters#/

[53] OECD. (2023) OECD Privacy Principles and Data Protection Framework. Diakses 20 Oktober 2025. [Online]. Available: https://www.oecd.org/en/topics/privacy-principles.html

[54] World Economic Forum, "How Businesses Can Make Data Practices More Responsible," WEF, Tech. Rep., 2020. [Online]. Available: https://www.weforum.org/agenda/2020/01/responsible-data-privacy-security-mastercard

[55] Julija Saveljeva and Tatjana Volkova, "A Survey on Digital Trust: Towards a Validated Definition," *Digital*, vol. 5, no. 2, p. 14, 2025.

[56] Centre for Strategic and International Studies, "Data Governance Principles for the Global Digital Economy," CSIS, Tech. Rep., 2021. [Online]. Available: https://www.csis.org/analysis/data-governance-principles-global-digital-economy

[57] M. Deutsch, "Trust and suspicion," *Journal of Conflict Resolution*, vol. 2, no. 4, 1958.

[58] D. H. McKnight and L. L. Cummings and N. L. Chervany, "Initial trust formation in new organizational relationships," *Academy of Management Review*, vol. 23, no. 3, pp. 473–490, 1998.

[59] E. Kim and S. Tadisina, "A model of customers' trust in E-businesses: Micro level inter-party trust formation," *The Journal of Computer Information Systems*, vol. 48, no. 1, pp. 88–104, 2007.

[60] B. Yang, "Theoretical model establishment and empirical study of customer trust in e-commerce," PhD thesis, Central South University, 2009.

[61] D. E. Zand, "Trust and managerial problem solving," *Administrative Science Quarterly*, vol. 17, no. 2, pp. 229–239, 1972.

[62] C. Moorman and R. Deshpande and G. Zaltman, "Factors affecting trust in marketing research relationships," *Journal of Marketing*, vol. 57, no. 1, pp. 81–101, 1993.

[63] M. Fishbein and I. Ajzen, "Belief, attitude, intention, and behavior: An introduction to theory and research," *Philosophy and Rhetoric*, vol. 10, no. 2, pp. 177–188, 1977.

[64] J. D. Lewis and A. Weigert, "Trust as a social reality," *Social Forces*, vol. 63, no. 4, pp. 967–985, 1985.

[65] Ferrin, D. and Gillespie, N, *Trust Differences Across National-Societal Cultures: Much to Do, or Much A do about Nothing?* Cambridge, 2010.

[66] World Bank, *Results, Performance Budgeting and Trust in Government.* Washington, DC: World Bank, 2010.

[67] Piotr Pietrzak and Josu Takala, "Digital Trust - a systematic literature review," *Forum Scientiae Oeconomia*, vol. 9, no. 3, 2021.

[68] Mubarak, M. F. and Petraite, M., "Industry 4.0 technologies, digital trust and technological orientation: What matters in open innovation," *Technological Forecasting and Social Change*, vol. 161, p. 120332, 2020.

[69] D. E. Kozhevnikov and A. S. Korolev, "Digital trust as a basis for the digital transformation of the enterprise and economy," in *Eleventh International Conference Management of Large-scale System Development*, 2018, pp. 1–3.

[70] Buechner, J. and Tavani, H., "Trust and multi-agent systems: Applying the "diffuse, default model" of trust to experiments involving artificial agents," *Ethics and Information Technology*, vol. 13, no. 1, pp. 39–51, 2011.

[71] Buechner, J., "A revision of the Buechner–Tavani model of digital trust and a philosophical problem it raises for social robotics," *Information*, vol. 11, no. 1, p. 48, 2020.

[72] Wu, X., "Digital trust and reconstruction of trust in digital society," *Study and Practice*, vol. 10, pp. 87–96, 2020.

[73] Marcial, D. and Launer, M., "Towards the measurement of digital trust in the workplace: A proposed framework," *International Journal of Scientific Engineering and Science*, vol. 3, pp. 1–7, 2019.

[74] Hermawan, D., "The importance of digital trust in E-commerce: Between brand image and customer loyalty," *International Journal of Applied Research in Management and Economics*, vol. 2, no. 3, pp. 18–30, 2020.

[75] Mukherjee, S. and Chittipaka, D. V. and Baral, M. M., *Developing a model to highlight the relation of digital trust with privacy and security for the blockchain technology.* IGI Global, 2021, pp. 110–125.

[76] Kelley, K. Brian, "The Digital Trust Imperative: Defining, Establishing and Measuring Digital Trust," *ISACA Journal*, vol. 1, 2023, available at: https://www.isaca.org/-/media/files/isacadp/project/isaca/articles/journal/2023/volume-1/defining-establishing-and-measuring-digital-trust_joa_eng_0123.pdf.

[77] World Economic Forum. (2022) Earning Digital Trust: Decision-Making for Trustworthy Technologies. Diakses 26 Juni 2025. [Online]. Available: https://www.weforum.org/reports/earning-digital-trust-decision-making-for-trustworthy-technologies

[78] PricewaterhouseCoopers, "Building Digital Trust: The Role of Audit and Assurance in the Digital World," PwC Singapore, Tech. Rep., 2013. [Online]. Available: https://www.pwc.com/sg/en/publications/assets/build_digital_trust_201312.pdf

[79] Information Systems Audit and Control Association, "Digital Trust," ISACA, Tech. Rep., 2023. [Online]. Available: https://higherlogicdownload.s3.amazonaws.com/ISACA/583ac694-051a-4186-ae65-6e0950c52114/UploadedImages/2023/ISACA_Digital_Trust_Oct_2023.pdf

[80] World Economic Forum. (2022) Digital Trust — About. Diakses 18 Juli 2025. [Online]. Available: https://www.weforum.org/stories/2022/12/losing-digital-trust-will-harm-technological-innovation/

[81] McKinsey & Company, "Why Digital Trust Truly Matters," McKinsey Digital, Tech. Rep., 2022. [Online]. Available: https://www.mckinsey.com/capabilities/quantumblack/our-insights/why-digital-trust-truly-matters

[82] DigiCert, "2022 state of digital trust survey," DigiCert, Tech. Rep., 2022. [Online]. Available: https://www.digicert.com/campaigns/digital-trust-survey

[83] A. Singh and V. Malhotra, "The Cyber Trust Landscape Report 2022," Cyber Security Works, Tech. Rep., 2022. [Online]. Available: https://mkai.org/the-cyber-trust-landscape-report-2022/

[84] Business Insider Intelligence, "The 2020 Digital Trust Report," Business Insider Intelligence, Tech. Rep., 2020. [Online]. Available: https://www.businessinsider.com/intelligence/digital-trust-enterprise-report-preview

[85] D. A. Williamson. (2022) User Trust in Social Platforms is Falling, According to Our New Study. Diakses 18 Juli 2025.

[86] Corritore, Cynthia L. and Kracher, Beverly and Wiedenbeck, Susan, "Online trust: Concepts, evolving themes, a model," *International Journal of Human-Computer Studies*, vol. 58, no. 6, pp. 737–758, 2003.

[87] Kożuch, Barbara, *The Dimensions of Trust in the Digital Era.* US: Routledge, 2021, pp. 15–26.

[88] Shankar, Venkatesh and Urban, Glen L. and Sultan, Fareena, "Online trust: A stakeholder perspective, concepts, implications, and future directions," *The Journal of Strategic Information Systems*, vol. 11, no. 3, pp. 325–344, 2002.

[89] Accenture. (2014) The Four Keys to Digital Trust. Diakses 25 Juli 2025. [Online]. Available: https://www.slideshare.net/OptimediaSpain/accenture-four-keys-digital-trust

[90] H. Lynch, R. Bartley, J. Metcalf, M. Petroni, A. Ahuja, and S. L. David, "Building Digital Trust: The Role of Data Ethics in the Digital Age," Accenture, Tech. Rep., 2016. [Online]. Available: https:https://www.dhi.ac.uk/san/waysofbeing/data/governance-crone-tiell-2016.pdf

[91] (2025) Digital Trust Ecosystems. Sustainability Directory. Diakses 30 Juli 2025. [Online]. Available: https://fashion.sustainability-directory.com/term/digital-trust-ecosystems/

[92] SGTech, "Digital Trust: Unlocking the Next Wave of Growth in the Digital Economy," SGTech, Tech. Rep., 2022. [Online]. Available: https://globalfutureseries.com/digitrust/wp/wp-content/uploads/2022/10/Digital_Trust_White_Paper_Unlocking_the_Next_Wave_of_Growth_in_the_Digital_Economy_FINAL_lowres.pdf

[93] Information Systems Audit and Control Association, "Digital Trust Ecosystem Framework™ (DTEF) – Overview," ISACA, Technical Report, 2023. [Online]. Available: https://www.isaca.org/-/media/files/isacadp/project/isaca/dtef/dtef_overview.pdf

[94] World Economic Forum, "Unlocking the Potential of Digital Trust," World Economic Forum, Geneva, Insight Report, 2024. [Online]. Available: https://www.weforum.org/publications/unlocking-the-potential-of-digital-trust/

[95] P. Goepel and R. Wester, "IDC Future of Trust: Framework and Definitions," International Data Corporation (IDC), 2023. [Online]. Available: https://www.idc.com/

[96] Paliszkiewicz, Joanna and Chen, Kai, *Building Digital Trust in Business.* US: Routledge, 2023, pp. 3–11.

[97] Ani Nenkova and Kathleen McKeown, "Survey of Text Summarization Techniques," in *Mining Text Data*, C. C. Aggarwal and C. Zhai, Eds. Springer, 2012, pp. 43–76.

[98] Inderjeet Mani, *Automatic Summarization*, ser. Natural Language Processing. John Benjamins Publishing, 2001, vol. 3.

[99] Yukihiro Nakamura and Shin-yo Muto and Yoshio Maeda and Makoto Mizukawa and Manabu Motegi and Youichi Takashima, "Proposal of Framework Based on 4W1H and Properties of Robots and Objects for Development of Physical Service System," *Journal of Robotics and Mechatronics*, vol. 26, no. 6, pp. 758–771, 2014.

[100] Bajaj, Garvita and Agarwal, Rachit and Singh, Pushpendra and Georgantas, Nikolaos and Issarny, Valérie, "4W1H in IoT Semantics," *IEEE Access*, vol. 6, pp. 65 488–65 506, 2018.

[101] Knop, Krzysztof and Mielczarek, Krzysztof, "Using 5W-1H and 4M Methods to Analyse and Solve the Problem with the Visual Inspection Process - case study," in *MATEC Conferences*, vol. 183, 2018, p. 03006. [Online]. Available: https://doi.org/10.1051/matecconf/201818303006

[102] Liao, S. Matthew and Haykel, Iskandar and Cheung, Katherine and Matalon, Taylor, "Navigating the Complexities of AI and Digital Governance: The 5W1H Framework," *SSRN Electronic Journal*, 2025, available at SSRN: https://ssrn.com/abstract=5327613.

[103] Rene Abraham and Johannes Schneider and Jan vom Brocke, "Data governance: A conceptual framework, structured review, and research agenda," *International Journal of Information Management*, vol. 49, pp. 424–438, 2019. [Online]. Available: https://www.sciencedirect.com/science/article/pii/S0268401219300787

[104] Lewicka, Dagmara, "Interpersonal Trust At Work and Organisational and Professional Commitment Interdependency Model," *Journal of Positive Management*, vol. 6, no. 3, p. 83, 2016.

[105] J. Paliszkiewicz, K. Chen, and M. Mendel, *Trust in Social and Business Relations*, 1st ed. New York: Routledge, 2024.

[106] Paliszkiewicz, Joanna and Gołuchowski, Jerzy and Koohang, Alex, "Leadership, trust, and knowledge management in relation to organizational performance: Developing an instrument," *Online Journal of Applied Knowledge Management*, vol. 3, no. 2, pp. 19–35, 2015.

[107] Srinivasan, S, "Role of trust in e-business success," *Information Management & Computer Security*, vol. 12, no. 1, pp. 66–72, 2004.

[108] World Economic Forum. (2023) Digital Trust: The Key to Unlocking Digital Transformation. Diakses 18 Februari 2025. [Online]. Available: https://www.weforum.org/reports/digital-trust-the-key-to-unlocking-digital-transformation/

[109] Verizon. (2024) 2024 Data Breach Investigations Report. Diakses 18 Juli 2025. [Online]. Available: https://www.verizon.com/business/resources/reports/dbir/

[110] Personal Data Protection Commission Singapore. (2023) Personal Data Protection Act 2012. Diakses 18 Juli 2025. [Online]. Available: https://www.pdpc.gov.sg/Overview-of-PDPA/The-Legislation/Personal-Data-Protection-Act

[111] Department of Personal Data Protection Malaysia, "Personal Data Protection Act 2010 (Act 709)," 2024. [Online]. Available: https://www.pdp.gov.my/ppdpv1/en/akta/pdp-act-2010-en/

[112] European Commission, "General Data Protection Regulation (GDPR)," 2023. [Online]. Available: https://ec.europa.eu/info/law/law-topic/data-protection/data-protection-eu_en

[113] Autoridade Nacional de Proteção de Dados (ANPD), "Lei Geral de Proteção de Dados (LGPD)," 2023. [Online]. Available: https://www.gov.br/anpd/pt-br/assuntos/legislacao/lgpd

[114] Republic of Türkiye Ministry of Transport and Infrastructure, "National Cybersecurity Strategy and Action Plan 2020-2023," Republic of Türkiye Ministry of Transport and Infrastructure, Tech. Rep., 2020. [Online]. Available: https://hgm.uab.gov.tr/uploads/pages/siber-guvenlik/national-cyber-security-strategy-2020-2023.pdf

[115] Kementerian Komunikasi dan Informatika Republik Indonesia, "Undang-undang nomor 27 tahun 2022 tentang perlindungan data pribadi," 2022. [Online]. Available: https://www.kominfo.go.id/content/detail/46550/uu-nomor-27-tahun-2022-tentang-perlindungan-data-pribadi/0/peraturan

[116] C. S. A. of Singapore, "Singapore Cybersecurity Strategy 2021," CSA, Tech. Rep., 2021. [Online]. Available: https://www.csa.gov.sg/resources/publications/the-singapore-cybersecurity-strategy-2021

[117] Smart Nation Singapore. (2025) Smart Nation 2.0: A Thriving Digital Future for All. Diakses 25 Juli 2025. [Online]. Available: https://www.smartnation.gov.sg/about/our-vision/sn2

[118] W. E. Forum. (2023) Digital Trust: The Key to Unlocking Digital Transformation. Diakses 18 Juli 2025. [Online]. Available: https://www.weforum.org/reports/digital-trust-the-key-to-unlocking-digital-transformation/

[119] C. S. A. of Singapore. (2023) Cybersecurity Awareness Survey 2023. Diakses 18 Januari 2025. [Online]. Available: https://www.csa.gov.sg/news-events/press-releases/csa-releases-key-findings-from-singapore-cybersecurity-health-report-2023

[120] I. Security. (2023) Cost of a Data Breach Report 2023. Diakses 28 Desember 2024. [Online]. Available: https://www.ibm.com/reports/data-breach

[121] E. D. B. Singapore, "Annual Report 2023," Economic Development Board Singapore, Tech. Rep., 2024. [Online]. Available: https://www.edb.gov.sg/en/about-edb/media-releases-publications.html

[122] Cyber Security Agency of Singapore, "CSA Collaborates with Microsoft and Google to Strengthen National Cyber Defence and Cybersecurity," (CSA), Tech. Rep., 2024. [Online]. Available: https://www.csa.gov.sg/news-events/press-releases/csa-collaborates-with-microsoft-and-google-to-strengthen-national-cyber-defence-and-cybersecurity

[123] ——, "Cybersecurity Act," 2018. [Online]. Available: https://www.csa.gov.sg/legislation/cybersecurity-act/

[124] ——, "CSA's Cyber Essentials and Cyber Trust Marks Expanded to Include Cloud Security, Artificial Intelligence, and Operational Technology," 2023. [Online]. Available: https://www.csa.gov.sg/news-events/press-releases/csa-s-cyber-essentials-and-cyber-trust-marks-expanded-to-include-cloud-security--artificial-intelligence-and-operational-technology/

[125] Government Technology Agency of Singapore, "Formation of the Smart Nation and Digital Government Group in the Prime Minister's Office," 2017. [Online]. Available: https://www.tech.gov.sg/media/formation-of-the-smart-nation-and-digital-government-group-in-the-prime-minister-office

[126] ——. (2023) Our Enhanced Smart Nation Vision: Paving the Way for a New Digital Era. Diakses 29 September 2025. [Online]. Available: https://www.tech.gov.sg/media/technews/our-enhanced-smart-nation-vision-paving-the-way-for-a-new-digital-era/

[127] Cyber Security Agency of Singapore, "Singapore's Cybersecurity Strategy," CSA, Tech. Rep., 2016. [Online]. Available: https://www.csa.gov.sg/resources/publications/singapore-s-cybersecurity-strategy-2016

[128] ——, *The Singapore Cybersecurity Strategy.* Cyber Security Agency of Singapore, 2021.

[129] The Republic of Singapore, "The Statutes of The Republic of Singapore Personal Data Protection Act," 2012. [Online]. Available: https://sso.agc.gov.sg/Act/PDPA2012?ViewType=Pdf&_=20210111164941

[130] S. Stalla-Bourdillon, A. Knight, and C. Millard, "Data protection by design: Building the foundations of trustworthy data sharing," *Data & Policy*, vol. 2, p. e4, 2020. [Online]. Available: https://www.cambridge.org/core/journals/data-and-policy/article/data-protection-by-design-building-the-foundations-of-trustworthy-data-sharing/4A4579B8FD774F7CDF8A1867A839B5FB

[131] Infocomm Media Development Authority and Personal Data Protection Commission, "Trusted Data Sharing Framework," (IMDA)&(PDPC), Tech. Rep., 2019. [Online]. Available: https://www.imda.gov.sg/programme-listing/Data-Innovation/Trusted-Data-Sharing-Framework

[132] International Data Spaces Association, "IDSA Rulebook," (IDSA), Tech. Rep., 2021. [Online]. Available: https://docs.internationaldataspaces.org/ids-knowledgebase/idsa-rulebook/

[133] GovTech Singapore. (2023) SingPass: Digital Identity. Diakses 29 September 2025. [Online]. Available: https://developer.singpass.gov.sg/

[134] ——. (2023) MyInfo: How It Works. Diakses 29 September 2025. [Online]. Available: https://v2.developer.tech.gov.sg/products/categories/digital-identity/myinfo/how-it-works

[135] Smart Nation and Digital Government Group (SNDGG). (2016) Simplified 2-Step Verification Setup Process for SingPass Users. Diakses 29 September 2025. [Online]. Available: https://www.tech.gov.sg/media/simplified-2-step-verification-setup-process-for-singpass-users/

[136] Personal Data Protection Commission, "Model AI Governance Framework," Singapore, Tech. Rep., 2020. [Online]. Available: https://www.pdpc.gov.sg/-/media/files/pdpc/pdf-files/resource-for-organisation/ai/sgmodelaigovframework2.pdf

[137] Infocomm Media Development Authority and Personal Data Protection Commission. (2022) Singapore launches world's first AI testing framework and toolkit to promote transparency, invites companies to pilot and contribute to international standards development. Diakses 29 September 2025. [Online]. Available: https://www.imda.gov.sg/resources/press-releases-factsheets-and-speeches/press-releases/2022/sg-launches-worlds-first-ai-testing-framework-and-toolkit-to-promote-transparency

[138] Smart Nation Singapore. (2023) SingPass - National Digital Identity Initiative. Diakses 29 September 2025. [Online]. Available: https://www.smartnation.gov.sg/initiatives/singpass/

[139] Monetary Authority of Singapore. (2023) SGFinDex: Digital infrastructure to enable more effective financial planning by Singaporeans. Diakses 29 September 2025. [Online]. Available: https://www.mas.gov.sg/development/fintech/sgfindex

[140] Cyber Security Agency of Singapore. (2020) CSA Launches Second National Cybersecurity Awareness Campaign. Diakses 29 September 2025. [Online]. Available: https://www.csa.gov.sg/news-events/press-releases/csa-launches-second-national-cybersecurity-awareness-campaign

[141] GovTech Singapore. (2022) Serving Citizens Better Through Data-Driven Decision-Making: Smart Nation Sensor Platform. Diakses 29 September 2025. [Online]. Available: https://www.developer.tech.gov.sg/our-digital-journey/singapore-digital-government-journey/ai-and-data-driven-government/serving-citizens-better-through-data-driven-decision-making.html

[142] Infocomm Media Development Authority (IMDA). (2023) IoT Standards in Support of Singapore's Smart Nation Initiative. Diakses 29 September 2025. [Online]. Available: https://www.imda.gov.sg/regulations-and-licensing-listing/ict-standards-and-quality-of-service/it-standards-and-frameworks/internet-of-things

[143] The Business Times. (2020) Trafigura pilots US$20m trade on Singapore blockchain platform developed by DBS. Diakses 29 September 2025. [Online]. Available: https://www.businesstimes.com.sg/international/trafigura-pilots-us20m-trade-singapore-blockchain-platform-developed-dbs-imda

[144] Infocomm Media Development Authority (IMDA). (2020) Singapore Invests$12 Million in First National Effort to Expand Blockchain Technology Research. Diakses 29 September 2025. [Online]. Available: https://www.imda.gov.sg/resources/press-releases-factsheets-and-speeches/press-releases/2020/singapore-invests-$12-million-in-first-national-effort-to-expand-blockchain-technology-research

[145] Singapore Blockchain Innovation Programme. (2023) FAQ – SBIP Support and Activities. Diakses 29 September 2025. [Online]. Available: https://sbip.sg/faq/

[146] International Finance Corporation (IFC), Monetary Authority of Singapore (MAS), and World Economic Forum (WEF). (2023) IFC, the Monetary Authority of Singapore, and the World Economic Forum Partner to Advance Digital Inclusion in Emerging and Developing Markets. Diakses 30 September 2025. [Online]. Available: https://www.ifc.org/en/pressroom/2023/ifc-the-monetary-authority-of-singapore-and-the-world-economic-forum-partner-to-advance-digital-inclusion-in-emerging-and-developing-markets

[147] Cyber Security Agency of Singapore (CSA), "Singapore and ASEAN Member States Deepen Commitment to Enhance Collective Cybersecurity in the Region," CSA, Tech. Rep., 2024. [Online]. Available: https://www.csa.gov.sg/news-events/press-releases/singapore-and-asean-member-states-deepen-commitment-to-enhance-collective-cybersecurity-in-the-region

[148] DS Group, "Singapore's Personal Data Protection Act (PDPA)," 2021. [Online]. Available: https://www.dsavocats.com/mailing/Singapore%E2%80%93Personal-Data-Protection-Amendment.pdf

[149] P. Lanois. (2014) The Personal Data Protection Framework in Singapore . Diakses 18 Februari 2025. [Online]. Available: https://iapp.org/news/a/the-personal-data-protection-framework-in-singapore

[150] PIKOM (The National Tech Association of Malaysia, "Digital TRUST Model for Digital Prosperity," PIKOM, Technical Report, 2024. [Online]. Available: https://www.pikom.org.my/DigitalTrustModel/Digital_TRUST_Model.pdf

[151] Ministry of Digital Malaysia, "Framework, Infrastructure and Education Main Pillars to Create Digital Trust," Malaysia, Tech. Rep., 2025. [Online]. Available: https://www.digital.gov.my/api/file/file/15072025_PRESS%20RELEASE_FRAMEWORK%2C%20INFRASTRUCTURE%20AND%20EDUCATION%20MAIN%20PILLARS%20TO%20CREATE%20DIGITAL%20TRUS.pdf

[152] A. M. Yusof, M. N. Ismail, Z. Noh, and N. A. Rahim, "Modeling a Digital Trust Framework to Address Cybersecurity Issues in Malaysia's Digital Economy," *Transactions on Science and Technology*, vol. 15, no. 4, pp. 147–156, 2024. [Online]. Available: https://tuengr.com/V15/15A4B.pdf

[153] PricewaterhouseCoopers, "2022 Global Digital Trust Insights: Malaysia Report," PwC, Tech. Rep., 2022. [Online]. Available: https://www.pwc.com/my/en/assets/publications/2022/pwc-2022-global-digital-trust-insights-malaysia-report.pdf

[154] Economic Planning Unit, "Malaysia digital economy blueprint," Prime Minister of Malaysia, Tech. Rep., 2021.

[155] National Security Council, "Malaysia Cyber Security Strategy 2020-2024," Prime Minister of Malaysia, Tech. Rep., 2020.

[156] Mayer Brown LLP, "From Legislative Reform to Practical Guidance: Key Amendments to Malaysia's PDPA and the Launch of Cross-Border Transfer Guidelines," *Mayer Brown Insights*, 2025. [Online]. Available: https://www.mayerbrown.com/en/insights/publications/2025/07/from-legislative-reform-to-practical-guidance-key-amendments-to-malaysias-pdpa-and-the-launch-of-cross-border-transfer-guidelines

[157] K. Harinderan. (2024) PDP & Futurise Develop Personal Data Protection Standards. Diakses 1 Oktober 2025. [Online]. Available: https://www.businesstoday.com.my/2024/01/16/pdp-futurise-develop-personal-data-protection-standards

[158] Ministry of Digital. (2025) Malaysia Cyber Security Academy to Begin Operations in 2025. Diakses 1 Oktober 2025. [Online]. Available: https://www.digital.gov.my/en-GB/siaran/Malaysia-Cyber-Security-Academy-to-Begin-Operations-In-2025

[159] ——. (2024) Rakyat Digital: Meningkatkan Literasi Digital Untuk Daya Saing Negara. Diakses 1 Oktober 2025. [Online]. Available: https://www.digital.gov.my/en-GB/siaran/Rakyat-Digital%3AMeningkatkan-Literasi-Digital-Untuk-Daya-Saing-Negara

[160] M. Mail. (2024) Enhancing Trust in Cross-Border Data Transfer through PDPA Amendment. Diakses 1 Oktober 2025. [Online]. Available: https://www.malaymail.com/news/what-you-think/2024/04/26/enhancing-trust-in-cross-border-data-transfer-through-personal-data-protection-act-amendment-personal-data-protection-department/130937

[161] Personal Data Protection Department Malaysia, "Press Release: PDP Commissioner and Futurise Collaboration on Data Protection Standards," PDP Commissioner, Tech. Rep., 2024. [Online]. Available: https://www.pdp.gov.my/ppdpv1/wp-content/uploads/2024/12/PRESS-RELEASE-PDP-COMMISIONER-AND-FUTURISE-18-November.pdf

[162] Parliament of Malaysia, "Laws of Malaysia Act 709 Personal Data Protection Act," 2010.

[163] M. S. Hashim, "Malaysia's National Cyber Security Policy: The country's cyber defence initiatives," in *2011 Second Worldwide Cybersecurity Summit (WCS)*, 2011, pp. 1–7.

[164] Parliament of Malaysia, "Laws of Malaysia Act 854 Cyber Security Act," 2024. [Online]. Available: http://www.agc.gov.my/agcportal/uploads/files/Publications/LOM/EN/Act15.pdf

[165] Government of Malaysia, "National Cyber Security Policy," 2021. [Online]. Available: https://www.readkong.com/page/national-cyber-security-policy-2021-july-2021-ministry-9352134

[166] Rahim, Siti Sabrina Imji and Huda, Mohd Ikbal Mohd and Sa'ad, Shahrizal and Moorthy, Ravichandran, "Cyber Security Crisis/Threat: Analysis of Malaysia National Security Council (NSC) Involvement Through the Perceptions of Government, Private and People Based on the 3P Model," *Journal of Social Sciences and Humanities*, vol. 21, no. 2, pp. 191–201, 2024.

[167] A. Mamat, "MyDIGITAL: Progress, Challenges, and Opportunities," *Medium*, 2021. [Online]. Available: https://medium.com/@azraee.mamat/mydigital-progress-challenges-and-opportunities-3787af7cd4f6

[168] N. A. Rahman, F. Ismail, and N. Ahmad, "The Readiness of Malaysia Digital Economy: A Study on Policy and Implementation," *International Journal of Economics and Finance*, vol. 14, no. 2, pp. 45–58, 2022.

[169] Cieh, Edwin Lee Yong, *Limitations of the Personal Data Protection Act 2010 and Personal Data Protection in Selected Sectors.* Berlin, Heidelberg: Springer Berlin Heidelberg, 2013, pp. 65–98.

[170] Dhanya Laxmi Sivanantham & Alfred Tan Hsiong Vei, "Malaysian Personal Data Protection Act 2010: Does it Apply to Government Agencies?" Azmi & Associates, Tech. Rep., 2019. [Online]. Available: https://amcham.com.my/malaysian-personal-data-protection-act-2010-does-it-apply-to-government-agencies/

[171] World Bank Group & Ministry of Finance, "Malaysia Economic Monitor: Navigating Change," World Bank Malaysia, Tech. Rep., 2018. [Online]. Available: https://openknowledge.worldbank.org/bitstream/handle/10986/30383/129777.pdf

[172] A. Kusumastuti and A. Nuryani, "Digital Literacy Levels in ASEAN (Comparative Study on ASEAN Countries)," in *13th International Interdisciplinary Studies Seminar*, 2020.

[173] Ensar Seker. (2024) Unraveling the Complexities of EU Legislation. Diakses 2 Oktober 2025. [Online]. Available: https://ensarseker1.medium.com/unraveling-the-complexities-of-eu-legislation-part-1-cybersecurity-7a323d5bebed

[174] Kai Zenner. (2023) A datashet on EU legislation for the digital world. Diakses 2 Oktober 2025. [Online]. Available: https://www.linkedin.com/posts/kzenner_a-dataset-on-eu-legislation-for-the-digital-activity-7087742110149263360-VYwO/#

[175] European Union, "General Data Protection Regulation (GDPR)," 2016. [Online]. Available: https://gdpr-info.eu/

[176] ——, "Regulation (EU) No 910/2014 on electronic identification and trust services for electronic transactions in the internal market (eIDAS)," 2014. [Online]. Available: https://eur-lex.europa.eu/eli/reg/2014/910/oj

[177] ——, "EU Cybersecurity Act (Regulation (EU) 2019/881)," 2019. [Online]. Available: https://eur-lex.europa.eu/eli/reg/2019/881/oj

[178] B. Chakravorti, A. Bhalla, and R. S. Chaturvedi. (2021) How Digital Trust Varies Around the World. Diakses 18 Februari 2025. [Online]. Available: https://hbr.org/2021/02/how-digital-trust-varies-around-the-world

[179] European Union, "Regulation (EU) 2016/679 General Data Protection Regulation (GDPR)," 2016. [Online]. Available: https://eur-lex.europa.eu/eli/reg/2016/679/oj

[180] Chaffer, Tomer Jordi and Goldston, Justin, "On the Existential Basis of Self-Sovereign Identity and Soulbound Tokens: An Examination of the "Self" in the Age of Web3," *Journal of Strategic Innovation and Sustainability*, vol. 17, no. 3, pp. 1–9, 2022.

[181] European Union, "Regulation (EU) 2024/1183 of the European Parliament and of the Council of 11 April 2024 amending Regulation (EU) No 910/2014 as regards establishing a framework for a European Digital Identity (eIDAS 2.0)," 2024. [Online]. Available: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=OJ:L_202401183

[182] ——, "Regulation (EU) 2019/881: EU Cybersecurity Act," 2019. [Online]. Available: https://eur-lex.europa.eu/eli/reg/2019/881/oj

[183] European Parliament and of the Council, "Horizontal Cybersecurity Requirements for Products with Digital Elements and Amending Regulation (EU) 2019/1020 (Cyber Resilience Act)," 2024, adopted 2024. [Online]. Available: https://www.craact.eu/full-text-and-pdf-download/

[184] European Union Agency for Cybersecurity (ENISA). (2025) ENISA – European Union Agency for Cybersecurity. Diakses 25 Juli 2025. [Online]. Available: https://www.enisa.europa.eu/

[185] European Union, "Directive (EU) 2016/1148 concerning measures for a high common level of security of network and information systems across the Union (NIS Directive)," 2016. [Online]. Available: https://eur-lex.europa.eu/eli/dir/2016/1148/oj

[186] ——, "Directive (EU) 2022/2555 on measures for a high common level of cybersecurity across the Union (NIS 2 Directive)," 2022. [Online]. Available: https://eur-lex.europa.eu/eli/dir/2022/2555/oj

[187] ——, "Regulation (EU) 2019/881 on ENISA and on information and communications technology cybersecurity certification (Cybersecurity Act)," 2019. [Online]. Available: https://eur-lex.europa.eu/eli/reg/2019/881/oj

[188] ——, "Regulation (EU) 2018/1807 on a framework for the free flow of non-personal data in the European Union," 2018. [Online]. Available: https://eur-lex.europa.eu/eli/reg/2018/1807/oj

[189] ——, "Directive (EU) 2019/1024 on open data and the re-use of public sector information (Open Data Directive)," 2019. [Online]. Available: https://eur-lex.europa.eu/eli/dir/2019/1024/oj

[190] ——, "Regulation (EU) 2022/868 on European data governance (Data Governance Act)," 2022. [Online]. Available: https://eur-lex.europa.eu/eli/reg/2022/868/oj

[191] ——, "Proposal for a Regulation on harmonised rules on fair access to and use of data (Data Act)," 2022. [Online]. Available: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52022PC0068

[192] ——, "Regulation (EU) 2022/1925 on contestable and fair markets in the digital sector (Digital Markets Act)," 2022. [Online]. Available: https://eur-lex.europa.eu/eli/reg/2022/1925/oj

[193] ——, "Regulation (EU) 2022/2065 on a Single Market for Digital Services (Digital Services Act)," 2022. [Online]. Available: https://eur-lex.europa.eu/eli/reg/2022/2065/oj

[194] ——, "Regulation (EU) 2024/1689 laying down harmonised rules on Artificial Intelligence (AI Act)," 2024. [Online]. Available: https://eur-lex.europa.eu/eli/reg/2024/1689/oj

[195] ——, "Proposal for a Regulation on horizontal cybersecurity requirements for products with digital elements (Cyber Resilience Act)," 2023. [Online]. Available: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52022PC0454

[196] European Commission, "A trusted and secure European e-ID (EUDI)," 2021. [Online]. Available: https://digital-strategy.ec.europa.eu/en/library/trusted-and-secure-european-e-id-regulation

[197] ——. (2023) EU Digital Identity Wallet Large Scale Pilots. Diakses 2 Oktober 2025. [Online]. Available: https://digital-strategy.ec.europa.eu/en/policies/eudi-wallet-implementation

[198] European Commission & High Representative for Foreign Affairs and Security Policy. (2025) EU Cybersecurity Strategy. Diakses 7 Juli 2025. [Online]. Available: https://digital-strategy.ec.europa.eu/en/policies/cybersecurity-strategy

[199] European Union, "Regulation (EU) 2022/2065: Digital Services Act," 2022. [Online]. Available: https://eur-lex.europa.eu/eli/reg/2022/2065/oj

[200] ——, "Regulation (EU) 2022/1925: Digital Markets Act," 2022. [Online]. Available: https://eur-lex.europa.eu/eli/reg/2022/1925/oj

[201] European Commission, "Directive (EU) 2022/2555: NIS2 Directive," 2022. [Online]. Available: https://eur-lex.europa.eu/eli/dir/2022/2555/oj

[202] ——, "Proposal for a Regulation laying down harmonised rules on Artificial Intelligence (AI Act)," 2021. [Online]. Available: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:52021PC0206

[203] ——, "European Blockchain Partnership and European Blockchain Services Infrastructure (EBSI)," 2022. [Online]. Available: https://digital-strategy.ec.europa.eu/en/policies/ebsi

[204] ——, "Code of Practice on Disinformation," 2022. [Online]. Available: https://digital-strategy.ec.europa.eu/en/policies/code-practice-disinformation

[205] ——, "Horizon Europe: EU Research and Innovation Programme 2021–2027," 2021. [Online]. Available: https://research-and-innovation.ec.europa.eu/funding/funding-opportunities/funding-programmes-and-open-calls/horizon-europe_en

[206] Information Commissioner's Office (ICO). (2024) Data Sharing Myth–busted. Diakses 25 Juli 2025. [Online]. Available: https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/data-sharing/data-sharing-myths-busted/

[207] Information Commissioner's Office. (2025) A Guide to the Data Protection Exemptions. Diakses 25 Juli 2025. [Online]. Available: https://ico.org.uk/fororganisations/uk-gdpr-guidance-and-resources/exemptions/a-guide-to-the-data-protectionexemptions/

[208] Organisation for Economic Co-operation and Development (OECD), "Shaping the Digital Transformation in Latin America," OECD Publishing, Paris, Tech. Rep., 2019. [Online]. Available: https://www.oecd.org/content/dam/oecd/en/publications/reports/2019/10/shaping-the-digital-transformation-in-latin-america_376dba7c/8bb3c9f1-en.pdf

[209] Belli, Luca and Zingales, Nicolo, "Cooperation and innovation to build meaningful data protection in Latin America," *Information & Communications Technology Law*, 2024. [Online]. Available: https://www.tandfonline.com/doi/full/10.1080/13600869.2024.2351670

[210] Porrúa, Miguel and Roseth, Benjamin, "The Link between Trust and Digital Transformation," in *Trust: The Key to Social Cohesion and Growth in Latin America and the Caribbean.* Inter-American Development Bank, 2022. [Online]. Available: https://ideas.repec.org/h/idb/idbchp/11771-c6.html

[211] Rubio, Mauricio and Tulcanaza-Prieto, Ana, "Digital Payments Trust in Latin America and the Caribbean," *Economies*, vol. 13, no. 5, p. 140, 2025. [Online]. Available: https://www.mdpi.com/2227-7099/13/5/140

[212] Chiang, Caroline and Ghosh, Sourojit and others, "Understanding Interface Design and Mobile Money Perceptions in Latin America," *arXiv preprint*, 2018. [Online]. Available: https://arxiv.org/abs/1803.05032

[213] Goyeneche, Marcela and Roseth, Benjamin and others, "Pandemics, Privacy, and Adoption of Technology: Perceptions of the Use of Digital Tools and Data Sharing During the COVID-19 Crisis in Latin America and the Caribbean," Inter-American Development Bank, Tech. Rep., 2022. [Online]. Available: https://publications.iadb.org/en/pandemics-privacy-and-adoption-technology-perceptions-use-digital-tools-and-data-sharing-during

[214] OECD, "Digital Government Review of Latin America and the Caribbean," Organisation for Economic Co-operation and Development, Tech. Rep., 2023. [Online]. Available: https://www.oecd.org/en/publications/2023/09/digital-government-review-of-latin-america-and-the-caribbean_75a4be05.html

[215] Derechos Digitales, "Cybersecurity in Latin America: National Strategies in 2024," Derechos Digitales, Tech. Rep., 2024. [Online]. Available: https://www.derechosdigitales.org/wp-content/uploads/DD_CYRILLA_ENG_2024pdf.pdf

[216] CEPAL, "Cybersecurity and the Role of the Board of Directors in Latin America and the Caribbean," United Nations Economic Commission for Latin America and the Caribbean, Tech. Rep., 2022. [Online]. Available: https://www.cepal.org/en/publications/45988-cybersecurity-and-role-board-directors-latin-america-and-caribbean

[217] Chew, Han Ei and Tan, Jeanne and Soon, Carol, "Digital Trust and Why It Matters," NUS Centre for Trusted Internet and Community, Singapore, CTIC Working Paper 05, 2023. [Online]. Available: https://ctic.nus.edu.sg/resources/CTIC-WP-05(2023).pdf

[218] OECD and IDB, *Broadband Policies for Latin America and the Caribbean.* Paris: OECD Publishing, 2016.

[219] OECD, CAF, and ECLAC, *Latin American Economic Outlook 2019: Development in Transition.* Paris: OECD Publishing, 2019.

[220] ——, *Latin American Economic Outlook 2018: Rethinking Institutions for Development.* Paris: OECD Publishing, 2018.

[221] Electronic Frontier Foundation. (2023) Who Defends Your Data in Latin America & Spain? A Comparative View of Telecom Companies' Commitments to User Rights. Diakses 1 Oktober 2025. [Online]. Available: https://www.eff.org/wp/who-defends-your-data-latin-america-spain-comparative-view-telecom-companies-commitments-user

[222] Derechos Digitales, "Cybersecurity in Latin America: National Strategies in 2024," Derechos Digitales, Tech. Rep., 2024. [Online]. Available: https://www.derechosdigitales.org/wp-content/uploads/DD_CYRILLA_ENG_2024pdf.pdf

[223] AFCEA International. (2023) South America Adopts Zero-Trust Principles. Diakses 1 Oktober 2025. [Online]. Available: https://www.afcea.org/signal-media/cyber-edge/south-america-adopts-zero-trust-principles

[224] TrustArc. (2025) Latin america's privacy pivot: How to build a regionally tailored compliance strategy in 2025. Diakses 1 Oktober 2025. [Online]. Available: https://trustarc.com/resource/latin-americas-privacy-compliance-strategy-2025/

[225] Castro, John and others, "Transparency Unleashed: Privacy Risks in the Age of E-Government," *Informatics*, vol. 12, no. 2, p. 39, 2024. [Online]. Available: https://www.mdpi.com/2227-9709/12/2/39

[226] CAF – Development Bank of Latin America. (2022) Digitization as a key to ensure transparency and reduce corruption. Diakses 1 Oktober 2025. [Online]. Available: https://www.caf.com/en/currently/news/digitization-as-a-key-to-ensure-transparency-and-reduce-corruption/

[227] República Federativa do Brasil, "Lei Geral de Proteção de Dados Pessoais (LGPD), Law No. 13.709/2018," 2018. [Online]. Available: https://www.gov.br/anpd/pt-br/assuntos/lei-geral-de-protecao-de-dados-lgpd

[228] República Argentina, "Ley de Protección de los Datos Personales No. 25.326," 2000. [Online]. Available: https://www.argentina.gob.ar/normativa/nacional/ley-25326-64790

[229] Estados Unidos Mexicanos, "Ley Federal de Protección de Datos Personales en Posesión de los Particulares," 2010. [Online]. Available: https://www.diputados.gob.mx/LeyesBiblio/pdf/LFPDPPP.pdf

[230] Ministerio de Tecnologías de la Información y las Comunicaciones, "Estrategia Nacional de Seguridad Digital 2023–2027," Colombia, Tech. Rep., 2023. [Online]. Available: https://www.mintic.gov.co/portal/inicio/715/w3-article-403023.html

[231] Gobierno de Chile, "Estrategia Nacional de Ciberseguridad de Chile," Chile, Tech. Rep., 2017. [Online]. Available: https://www.csirt.gob.cl

[232] República Oriental del Uruguay, "Ley No. 18.600: Documentos Electrónicos y Firma Digital," 2009. [Online]. Available: https://www.impo.com.uy/bases/leyes/18600-2009

[233] Cámaras de Comercio de Colombia. (2024) Registro Único Empresarial y Social (RUES). Diakses 1 Oktober 2025. [Online]. Available: https://www.rues.org.co

[234] Banco Central do Brasil. (2023) Digital Brazilian Real (DREX). Diakses 1 Oktober 2025. [Online]. Available: https://www.bcb.gov.br/en/financialstability/drex_en

[235] Organization of American States. (2023) OAS Cybersecurity Program (CICTE). Diakses 1 Oktober 2025. [Online]. Available: https://www.oas.org/en/sms/cicte/cybersecurity.asp

[236] Mercosur, "Decision No. 15/21: Agreement on Electronic Commerce," 2021. [Online]. Available: https://www.mercosur.int

[237] Ministerio de Ciência, Tecnologia e Inovações, Brasil. (2018) Programa Internet para Todos. Diakses 2 Oktober 2025. [Online]. Available: https://www.gov.br/mcti/pt-br

[238] Gobierno de México. (2017) Red Compartida Project. Diakses 3 Oktober 2025. [Online]. Available: https://digitalregulation.org/red-compartida-mexico/

[239] PanamaFuture. Revolutionize Real Estate Investment. Diakses 9 Oktober 2025. [Online]. Available: https://panamafuture.com/

[240] Yashika Thakur. How Panama is Becoming a Hub for Real Estate Tokenization in Latin America. Diakses 9 Oktober 2025. [Online]. Available: https://www.antiersolutions.com/blogs/how-panama-is-becoming-a-hub-for-real-estate-tokenization-in-latin-america/

[241] Government of Brazil. (2023) Debates on AI Ethics and Regulation in Brazil. Diakses 1 Oktober 2025. [Online]. Available: https://www.gov.br/mcti/pt-br

[242] Ministerio de Ciencia, Tecnología e Innovación, Argentina. (2022) Plataforma de Inteligencia Artificial en Argentina. Diakses 1 Oktober 2025. [Online]. Available: https://www.argentina.gob.ar/ciencia

[243] Latin American and Caribbean Economic System (SELA). (2021) No internet access for 244 million people in Latin America and the Caribbean. Diakses 18 Juli 2025. [Online]. Available: https://www.sela.org/en/no-internet-access-for-244-million-people-in-latin-america-and-the-caribbean/

[244] GSMA. (2024) Connectivity gaps in Latin America. Diakses 18 Juli 2025. [Online]. Available: https://www.gsma.com/about-us/regions/latin-america/gsma_resources/connectivity-gaps-in-latin-america/

[245] United Nations Development Programme. (2024) Missed Connections: The Incomplete Digital Revolution in Latin America and the Caribbean. Diakses 18 Juli 2025. [Online]. Available: https://www.undp.org/latin-america/blog/missed-connections-incomplete-digital-revolution-latin-america-and-caribbean-0

[246] GSMA Intelligence, "Mobile Investment Gaps: Caribbean Islands," GSMA, Tech. Rep., 2023. [Online]. Available: https://www.gsmaintelligence.com/research/mobile-investment-gaps-caribbean-islands

[247] Telefónica. (2023) Digital inclusion in Latin America: A road to equity and progress. Diakses 18 Juli 2025. [Online]. Available: https://www.telefonica.com/en/communication-room/blog/digital-inclusion-latin-america-road-equity-progress/

[248] ——, "Public Policies to Bridge the Digital Divide," Telefónica, Tech. Rep., 2023. [Online]. Available: https://www.telefonica.com/en/wp-content/uploads/sites/5/2024/03/public-policies-digital-gap-position-paper-2024.pdf

[249] Organisation for Economic Co-operation and Development, "Closing Broadband Connectivity Divides for All," OECD, Tech. Rep., 2025. [Online]. Available: https://www.oecd.org/content/dam/oecd/en/publications/reports/2025/05/closing-broadband-connectivity-divides-for-all_17ee89fa/d5ea99b2-en.pdf

[250] World Economic Forum. (2021) Latin America and the Caribbean's Digital Access Problem. [Online]. Available: https://www.weforum.org/stories/2021/07/latin-america-caribbean-digital-access/

[251] Presidency of Strategy and Budget of the Republic of Türkiye, "Twelfth Development Plan (2024–2028)," 2023. [Online]. Available: https://www.sbb.gov.tr/wp-content/uploads/2025/03/Twelfth-Development-Plan_2024-2028.pdf

[252] Organisation for Economic Co-operation and Development, "Digital Government Review of Türkiye," OECD, Tech. Rep., 2023. [Online]. Available: https://www.oecd.org/content/dam/oecd/en/publications/reports/2023/05/digital-government-review-of-turkiye_69ffd9d4/3958d102-en.pdf

[253] TRT World Research Centre, "Advancing the Frontier: Turkish Governmental Policies in Technology Development," TRT World, Tech. Rep., 2024. [Online]. Available: https://researchcentre.trtworld.com/wp-content/uploads/2024/09/Advancing-the-Frontier.pdf

[254] Digital Transformation Office, "National Artificial Intelligence Strategy (2021–2025)," Republic of Türkiye, Tech. Rep., 2021. [Online]. Available: https://wp.oecd.ai/app/uploads/2021/12/Turkey_National_Artificial_Intelligence_Strategy_2021-2025.pdf

[255] Şahin, M., "Digital Transformation of Public Services as State Transformation," *Alternatives: Global, Local, Political*, vol. 48, no. 3, 2022. [Online]. Available: https://repository.bilkent.edu.tr/bitstreams/5f4bc3a7-892c-4839-b0a1-6547e9ad9347/download

[256] Sayıştay Başkanlığı, "Dijital Dönüşüm Ofisi Başkanlığı Raporu," Sayıştay Başkanlığı, Tech. Rep., 2021. [Online]. Available: https://www.sayistay.gov.tr/reports/download/wEYDddqYyX-dijital-donusum-ofisi-baskanligi

[257] M. A. L. Firm. (2023) The Turkish Data Protection Law in 2023: Developments in Practice Over Its Seven Years. Diakses 2 Oktober 2025. [Online]. Available: https://www.morogluarseven.com/news-and-publications/the-turkish-data-protection-law-in-2023-developments-in-practice-over-its-seven-years-updated-edition

[258] Mondaq. (2025) Two-Minute Recap of Recent Developments in Turkish Data Protection Law. Diakses 2 Oktober 2025. [Online]. Available: https://www.mondaq.com/turkey/data-protection/1623308/two-minute-recap-of-recent-developments-in-turkish-data-protection-law-april-2025

[259] UNDP Türkiye, "Data Governance Framework - Recommendation Report for Türkiye," United Nations, Tech. Rep., 2024. [Online]. Available: https://www.undp.org/sites/g/files/zskgke326/files/2024-04/data_governance_framework_recommendation_report_for_turkiye_2024-final-13_march.pdf

[260] T.C. Cumhurbaşkanlığı Dijital Dönüşüm Ofisi. (2018) Dijital Dönüşüm Ofisi. Diakses 22 September 2025. [Online]. Available: https://cbddo.gov.tr/dijital-tr/

[261] O. for Economic Co-operation and Development, "OECD Digital Government Studies: Türkiye," OECD, Tech. Rep., 2023. [Online]. Available: https://cbddo.gov.tr/SharedFolderServer/Genel/OECD_Dijital_Devlet_Incelemesi_Turkiye_Raporu.pdf

[262] Presidency of the Republic of Türkiye, "Presidential Decree No. 1 : Organisation of the Presidency of the Republic of Türkiye," 2018. [Online]. Available: https://www.cbiko.gov.tr/en/institutional/presidential-decree-no-1-organisation-of-the-presidency

[263] Rüzgar, Merve Tuba, "Digital Transformation Policies in Türkiye," *Dergipark*, 2023. [Online]. Available: https://dergipark.org.tr/en/download/article-file/3716096

[264] Moroğlu Arseven Law Firm. (2024) Data Governance Framework Recommendation Report for Türkiye Has Been Released. Diakses 3 Oktober 2025. [Online]. Available: https://www.morogluarseven.com/news-and-publications/data-governance-framework-recommendation-report-for-turkiye-has-been-released/

[265] Presidency of Strategy and Budget, "Twelfth Development Plan 2024-2028," Republic of Türkiye, Tech. Rep., 2023. [Online]. Available: https://www.sbb.gov.tr/wp-content/uploads/2025/03/Twelfth-Development-Plan_2024-2028.pdf

[266] UNDP Digital, "Building People-Centric and Responsible Data Governance in Türkiye," United Nations, Tech. Rep., 2023. [Online]. Available: https://www.undp.org/digital/blog/building-people-centric-and-responsible-data-governance-turkiye

[267] K. V. K. Kanunu, "Personal Data Protection Law (Law No. 6698)," 2016. [Online]. Available: https://www.kvkk.gov.tr/Icerik/6649/Personal-Data-Protection-Law

[268] ——, "The Board Decision No. 2019/10 of 24.01.2019 — Procedures and Principles of Personal Data Breach Notification," 2019. [Online]. Available: https://www.kvkk.gov.tr/Icerik/6647/The-Board-Decision-No-2019-10-of-24-01-2019-about-Procedures-and-Principles-of-Personal-Data-Breach-Notification-

[269] ——, "By-Law on Data Controllers' Registry (VERBİS)," 2017. [Online]. Available: https://www.kvkk.gov.tr/Icerik/6635/By-Law-On-Data-Controllers-Registry

[270] ——, "Guidance on Data Security Obligations." [Online]. Available: https://www.kvkk.gov.tr/Icerik/6601/Obligations-Concerning-Data-Security-

[271] C. coordinated under Savunma Sanayii Başkanlığı, "Türkiye Siber Güvenlik Kümelenmesi (Turkish Cybersecurity Cluster)." [Online]. Available: https://siberkume.org.tr/

[272] u. B. Ulusal Siber Olaylara Müdahale Merkezi (TR-CERT/USOM). TR-CERT (USOM) — About Us. Diakses 3 Oktober 2025. [Online]. Available: https://www.usom.gov.tr/en/about-us

[273] Reuters. (2022) Turkey blocks access to Deutsche Welle, Voice of America for not getting licenses. Diakses 18 Juli 2025. [Online]. Available: https://www.reuters.com/business/media-telecom/turkey-blocks-access-deutsche-welle-voice-america-not-getting-licenses-official-2022-06-30/

[274] ISACA. Piecemeal Approach Insufficient to Create Digital Trust. Diakses 25 September 2025. [Online]. Available: https://www.isaca.org/resources/news-and-trends/isaca-now-blog/2022/piecemeal-approach-insufficient-to-create-digital-trust

[275] ——. Attaining Peace of Mind Under the Digital Trust Umbrella. Diakses 22 September 2025. [Online]. Available: https://www.isaca.org/resources/news-and-trends/newsletters/atisaca/2024/volume-11/attaining-peace-of-mind-under-the-digital-trust-umbrella

[276] Hive Five. (2023) Apa Tujuan Transformasi Digital di Indonesia? Diakses 17 Juni 2025. [Online]. Available: https://hivefive.co.id/apa-tujuan-transformasi-digital-di-indonesia

[277] Republik Indonesia, "Undang-Undang Nomor 17 Tahun 2007 tentang Rencana Pembangunan Jangka Panjang Nasional (RPJP) Nasional) Tahun 2005–2025," 2007.

[278] ——, "Undang-Undang Nomor 11 Tahun 2008 junto Nomor 19 Tahun 2016 junto Nomor 1 Tahun 2024 tentang Informasi dan Transaksi Elektronik (ITE)," 2024.

[279] ——, "Undang-Undang Nomor 27 Tahun 2022 tentang Pelindungan Data Pribadi," 2022.

[280] ——, "Undang-Undang Republik Indonesia Nomor 8 Tahun 1999 tentang Pelindungan Konsumen," 1999.

[281] ——, "Peraturan Pemerintah Nomor 71 Tahun 2019 tentang Penyelenggaraan Sistem dan Transaksi Elektronik," 2019.

[282] ——, "Peraturan Presiden Nomor 95 Tahun 2018 tentang Sistem Pemerintahan Berbasis Elektronik," 2018.

[283] Kompas.id. (2024) Kesulitan Integrasikan 27.000 Aplikasi, Pemerintah Fokus Sembilan Layanan Publik. Diakses 17 Juni 2025. [Online]. Available: https://www.kompas.id/baca/english/2024/03/25/en-kesulitan-integrasikan-27000-aplikasi-pemerintah-fokus-sembilan-layanan-publik

[284] Republik Indonesia, "Peraturan Presiden Republik Indonesia Nomor 82 Tahun 2022 tentang Pelindungan Infrastruktur Informasi Vital," 2022.

[285] ——, “Peraturan Presiden Nomor 132 Tahun 2022 tentang Arsitektur Sistem Pemerintahan Berbasis Elektronik Nasional,” 2022.

[286] ——, “Peraturan Presiden Nomor 82 Tahun 2023 tentang Percepatan Transformasi Digital dan Keterpaduan Layanan Digital Nasional,” 2023.

[287] INA Digital. (2024) INAPas – Identitas Digital Nasional Terpadu. Diakses 25 Juli 2025. [Online]. Available: https://inapas.go.id/

[288] Bank Indonesia. (2025) Sistem Pembayaran & Pengelolaan Uang Rupiah. Diakses 25 Juli 2025. [Online]. Available: https://www.bi.go.id/id/fungsi-utama/sistem-pembayaran/default.aspx

[289] I. Digital. (2025) Selamat Datang | INAgov. Diakses 25 Juli 2025. [Online]. Available: https://inagov.go.id/

[290] INA Digital. (2025) INAku – Satu Portal Layanan dan Informasi Pemerintah untuk Masyarakat Indonesia. Diakses 25 Juli 2025. [Online]. Available: https://inaku.go.id/

[291] Republik Indonesia, “Peraturan Presiden Nomor 17 Tahun 2023 tentang Percepatan Transformasi Digital di Bidang Pengadaan Barang/Jasa Pemerintah,” 2023.

[292] Kementerian Komunikasi dan Informatika, “Peraturan Menteri Komunikasi dan Informatika Nomor 5 Tahun 2020 junto Nomor 10 Tahun 2021 tentang Penyelenggara Sistem Elektronik Lingkup Privat,” 2021.

[293] Kementerian Komunikasi dan Digital, “Peraturan Menteri Komunikasi dan Digital Nomor 6 Tahun 2025 tentang Standar Teknis dan Prosedur Pembangunan dan Pengembangan Aplikasi Sistem Pemerintahan Berbasis Elektronik,” 2025.

[294] Kementerian Komunikasi dan Informatika, “Visi Indonesia Digital 2045,” Kemenkominfo, Tech. Rep., 2024. [Online]. Available: https://digital2045.id/bukuvid2045/

[295] Kementerian Komunikasi dan Digital. (2024) Siaran Pers No.07/HM/KOMINFO/01/2024. Diakses 25 September 2025. [Online]. Available: https://www.komdigi.go.id/berita/siaran-pers/detail/siaran-pers-no-07-hm-kominfo-01-2024-tentang-tingkatkan-literasi-digital-kominfo-latih-lebih-dari-24-juta-orang

[296] R. M. Q. Kiki Verico, “Indonesia’s Infrastructure and Inclusive Economic Growth,” Economic Research Institute for ASEAN and East Asia (ERIA), Tech. Rep., 2022.

[297] I. I. for Management Development, “World Digital Competitiveness Ranking,” IMD, Tech. Rep., 2024. [Online]. Available: https://www.imd.org/centers/wcc/world-competitiveness-center/rankings/world-digital-competitiveness-ranking/

[298] Khoirul Anam. (2023) Paling Rendah di ASEAN, Tingkat Literasi Digital RI Cuma 62%. Diakses 25 September 2025. [Online]. Available: https://www.cnbcindonesia.com/tech/20230214171553-37-413790/paling-rendah-di-asean-tingkat-literasi-digital-ri-cuma-62

[299] Yuniar A. (2023) BSSN: Kolaborasi adalah kunci ketahanan siber nasional. Diakses 25 September 2025. [Online]. Available: https://govinsider.asia/indo-en/article/bssn-kolaborasi-adalah-kunci-ketahanan-siber-nasional

[300] Bank Indonesia, "Peraturan Bank Indonesia Nomor 9/15/PBI/2007 tentang Penerapan Manajemen Risiko dalam Penggunaan Teknologi Informasi oleh Bank Umum," 2007.

[301] ——, "Peraturan Bank Indonesia Nomor 2 Tahun 2024 tentang Keamanan Sistem Informasi dan Ketahanan Siber bagi Penyelenggara Sistem Pembayaran, Pelaku Pasar Uang dan Valuta Asing, serta Pihak Lain," 2024.

[302] Kementerian Koordinator Bidang Perekonomian Republik Indonesia, "Buku Putih Strategi Nasional Pengembangan Ekonomi Digital Indonesia 2030," Kemenmenko Perekonomian, Tech. Rep., 2020.

[303] Otoritas Jasa Keuangan, "Peraturan Otoritas Jasa Keuangan Nomor 11 Tahun 2022 tentang Penyelenggaraan Teknologi Informasi oleh Bank Umum," 2022.

[304] ——, "Peraturan Otoritas Jasa Keuangan Nomor 21 Tahun 2023 tentang Layanan Digital oleh Bank Umum," 2023.

[305] ——, "Peraturan Otoritas Jasa Keuangan Nomor 40 Tahun 2024 tentang Layanan Pendanaan Bersama Berbasis Teknologi Informasi," 2024.

[306] Badan Siber dan Sandi Negara , "Peraturan Badan Siber dan Sandi Negara Nomor 8 Tahun 2020 tentang Sistem Pengamanan dalam Penyelenggaraan Sistem Elektronik," 2020.

[307] ——, "Peraturan Badan Siber dan Sandi Negara Nomor 4 Tahun 2021 tentang Pedoman Manajemen Keamanan Informasi Sistem Pemerintahan Berbasis Elektronik (SPBE)," 2021.

[308] ——, "Peraturan Badan Siber dan Sandi Negara Nomor 7 Tahun 2023 tentang Identifikasi Infrastruktur Informasi Vital (IIV)," 2023.

[309] ——, "Peraturan Badan Siber dan Sandi Negara Nomor 8 Tahun 2023 tentang Kerangka Kerja Pelindungan Infrastruktur Informasi Vital," 2023.

[310] ——, "Peraturan Badan Siber dan Sandi Negara Nomor 9 Tahun 2023 tentang Peningkatan Kapasitas Sumber Daya Manusia di Bidang Keamanan Siber dan Sandi," 2023.

[311] Badan Siber dan Sandi Negara, "Peraturan Badan Siber dan Sandi Negara Nomor 1 Tahun 2024 tentang Pengelolaan Insiden Siber," 2024.

[312] Badan Siber dan Sandi Negara , “Peraturan Badan Siber dan Sandi Negara Nomor 2 Tahun 2024 tentang Manajemen Krisis Siber,” 2024.

[313] ——, “Peraturan Badan Siber dan Sandi Negara Nomor 5 Tahun 2024 tentang Rencana Aksi Nasional Keamanan Siber,” 2024.

[314] Badan Siber dan Sandi Negara, “Peraturan Badan Siber dan Sandi Negara Nomor 7 Tahun 2024 tentang Penyelenggaraan Penilaian Kesesuaian Kriteria Umum Untuk Evaluasi Keamanan Teknologi Informasi Indonesia (Indonesia Common Criteria for Information Technology Security Evaluation),” 2024.

[315] ——, “Peraturan Badan Siber dan Sandi Negara Nomor 11 Tahun 2024 tentang Penyelenggaraan Algoritma Kriptografi Indonesia dan Penilaian Kesesuaian Keamanan Modul Kriptografi,” 2024.

[316] B. P. dan Penerapan Teknologi, “Strategi Nasional Kecerdasan Artifisial Indonesia,” BPPT, Tech. Rep., 2020. [Online]. Available: https://korika.id/wp-content/uploads/2024/07/stranas-ka-2045.pdf

[317] Kementerian Kesehatan RI. (2024) AI Mulai Wujudkan Efisiensi Pelayanan Kesehatan Indonesia. Diakses 17 Juni 2025. [Online]. Available: https://kemkes.go.id/id/rilis-kesehatan/ai-mulai-wujudkan-efisiensi-pelayanan-kesehatan-indonesia

[318] Universitas Muhammadiyah Sidoarjo. (2024) Pemanfaatan AI dalam Pengelolaan Data Rekam Medis. Diakses 17 Juni 2025. [Online]. Available: https://mik.umsida.ac.id/pemanfaatan-ai-dalam-pengelolaan-data-rekam-medis/

[319] Kementerian PANRB. (2023) Menilik Pemanfaatan Artificial Intelligence dalam Transformasi Digital Pelayanan Publik. Diakses 17 Juni 2025. [Online]. Available: https://menpan.go.id/site/berita-terkini/menilik-pemanfaatan-artificial-intelligence-dalam-transformasi-digital-pelayanan-publik

[320] Direktorat Jenderal Pendidikan Tinggi, Riset, dan Teknologi. (2022) Kembangkan Talenta di Bidang Artificial Intelligence, Ditjen Diktiristek Jalin Kerja Sama dengan NVIDIA. Diakses 17 Juni 2025. [Online]. Available: https://dikti.kemdikbud.go.id/kabar-dikti/kabar/kembangkan-talenta-di-bidang-artificial-intelligence-ditjen-diktiristek-jalin-kerja-sama-dengan-nvidia/

[321] Otorita Ibu Kota Nusantara. (2025) SERGEK Berhasil Menyelesaikan Uji Coba AI Smart Traffic dan Mobility di Nusantara. Diakses 18 Februari 2025. [Online]. Available: https://ikn.go.id/sergek-berhasil-menyelesaikan-uji-coba-ai-smart-traffic-dan-mobility-di-nusantara

[322] Google and Temasek and Bain & Company, “e-Economy SEA,” Google and Temasek and Bain & Company, Tech. Rep., 2024. [Online]. Available: https://economysea.withgoogle.com/report/

[323] N. Zahra, “Meningkatkan Inklusi dalam Indeks Literasi Digital Nasional: Dari Pengukuran hingga Pemberdayaan - Ringkasan Kebijakan CIPS,” CIPS, Tech. Rep. 19, 2023.

[324] SOCRadar, “Indonesia Threat Landscape Report,” SOCRadar, Tech. Rep., 2024. [Online]. Available: https://media.cert.europa.eu/static/MEMO/2021/TLP-WHITE-CERT-EU-Threat_Landscape_Report-Volume1.pdf

[325] Microsoft News Center Indonesia. (2019) Microsoft-IDC: Tingkat Kepercayaan Konsumen di Indonesia terhadap Layanan Digital Hanya Mencapai 44%. Diakses 7 Juli 2025. [Online]. Available: https://news.microsoft.com/id-id/2019/06/26/microsoft-studi-idc-tingkat-kepercayaan-konsumen-di-indonesia-terhadap-layanan-digital-hanya-mencapai-44/

[326] OECD, *OECD Digital Economy Outlook 2022*. Paris: OECD Publishing, 2022. [Online]. Available: https://doi.org/10.1787/1b2b0ee2-en

[327] European Union Agency for Cybersecurity, “Security by Design — Principles and Guidance for Secure Software Development,” ENISA, Tech. Rep., 2023. [Online]. Available: https://www.enisa.europa.eu/publications/security-by-design

[328] A. Cavoukian, “Privacy by Design: The 7 Foundational Principles,” Information and Privacy Commissioner of Ontario, Canada, Tech. Rep., 2009. [Online]. Available: https://privacy.ucsc.edu/resources/privacy-by-design---foundational-principles.pdf

[329] TechTarget Contributor. (2025) Security by Design. Diakses 1 Juli 2025. [Online]. Available: https://www.techtarget.com/whatis/definition/security-by-design

[330] Cybersecurity and Infrastructure Security Agency. (2023) Secure by Design. Diakses 30 Juli 2025. [Online]. Available: https://www.cisa.gov/securebydesign

[331] GovInsider. (2025) Pemerintah bahas RUU Keamanan Siber untuk dukung inovasi digital. GovInsider Asia. Diakses 2 Februari 2025. [Online]. Available: https://govinsider.asia/indo-en/article/pemerintah-bahas-ruu-keamanan-siber-untuk-dukung-inovasi-digital

[332] Tempo.co. (2022) Kemenkominfo Bersama GNLD Siberkreasi Meluncurkan 58 Buku Kolaborasi Seri Literasi Digital. Tempo. Diakses 2 Februari 2025. [Online]. Available: https://www.tempo.co/info-tempo/kemenkominfo-bersama-gnld-siberkreasi-meluncurkan-58-buku-kolaborasi-seri-literasi-digital-308237

[333] Kementerian Komunikasi dan Informatika. (2020) Kominfo Segera Luncurkan Masyarakat Anti Hoaks. Komite Kepercayaan Digital (KOMDIGI). Diakses 2 Februari 2025. [Online]. Available: https://www.komdigi.go.id/berita/pengumuman/detail/kominfo-segera-luncurkan-masyarakat-anti-hoax

[334] Tempo.co. (2019) Transfer Antarbank Semakin Murah dengan National Payment Gateway. Tempo. Diakses 2 Februari 2025. [Online]. Available: https://www.tempo.co/ekonomi/transfer-antar-bank-semakin-murah-dengan-national-payment-gateway-1258712

[335] Kementerian Investasi/BKPM. (2025) Online Single Submission (OSS). Pemerintah Republik Indonesia. Diakses 2 Februari 2025. [Online]. Available: https://oss.go.id/

[336] Association of Southeast Asian Nation Secretariat, "ASEAN Cybersecurity Cooperation Strategy 2021–2025," ASEAN Secretariat, Tech. Rep., 2021. [Online]. Available: https://asean.org/wp-content/uploads/2022/02/01-ASEAN-Cybersecurity-Cooperation-Paper-2021-2025_final-23-0122.pdf

[337] R. Labaree. (2013) Theoretical Framework – Organizing Your Social Sciences Research Paper. Diakses 18 Februari 2025. [Online]. Available: https://libguides.usc.edu/writingguide/theoreticalframework

[338] M. B. Miles and A. M. Huberman, *Qualitative Data Analysis: An Expanded Sourcebook*. SAGE Publications, 1994.

[339] W. G. Camp, "Formulating and evaluating theoretical frameworks for career and technical education research," *Journal of Vocational Education Research*, vol. 26, no. 1, pp. 4–25, 2001.

[340] Y. Jabareen, "Building a conceptual framework: philosophy, definitions, and procedure," *International Journal of Qualitative Methods*, vol. 8, no. 4, pp. 49–62, 2009. [Online]. Available: http://ejournals.library.ualberta.ca/index.php/IJQM/article/viewArticle/6118

ISBN 978-634-04-4762-0 (PDF)

9 786340 447620

Diterbitkan oleh:
Politeknik Siber dan Sandi Negara Press
Jl. Raya H. Usa Putat Nutug, Kec. Ciseeng,
Kabupaten Bogor, Jawa Barat 16120
perpustakaan@poltekssn.ac.id