

Framework Peringkat Keamanan Siber & Kepatuhan Data Pribadi untuk Dunia Perbankan Indonesia

**Menuju Sistem Nasional
“OJK CyberTrust & Data Privacy Ranking Framework”**

Onno W. Purbo
onno@indo.net.id
onno@itts.ac.id
Twitter onnowpurbo

**Institut Teknologi Tangerang Selatan (ITTS)
OnnoCenter
2025**

Lisensi & Catatan Karya

Karya ini dilisensikan di bawah lisensi **Creative Commons Attribution-ShareAlike 4.0 International (CC BY-SA 4.0)**.

Artinya, **siapa pun bebas untuk menggunakan, menyalin, membagikan, dan mengadaptasi** materi ini, **dengan syarat**:

- **Memberikan atribusi yang sesuai** (menyebut sumber asli),
- **Menyertakan lisensi yang sama** jika dimodifikasi atau dikembangkan lebih lanjut.

Lihat detail lisensi di sini <https://creativecommons.org/licenses/by-nd/4.0/legalcode.id>

Disclaimer

Dokumen ini disusun semata-mata untuk tujuan edukasi dan penguatan ekosistem **keamanan siber serta kepatuhan data pribadi** di sektor keuangan Indonesia. **Penulis bukan ahli keuangan atau regulator perbankan**, melainkan seorang **engineer dan praktisi teknologi** yang berfokus pada bidang *cybersecurity*, *data governance*, dan sistem digital berbasis *open source*. Seluruh pandangan, kerangka, dan rekomendasi di dalamnya merupakan hasil kajian teknis dan refleksi rekayasa sistem, bukan panduan hukum maupun kebijakan resmi. Penulis memohon maaf apabila terdapat kekeliruan istilah atau interpretasi dalam konteks keuangan, dan berharap karya ini dapat menjadi **pemicu dialog lintas disiplin** antara regulator, bank, dan komunitas teknologi untuk membangun **kepercayaan digital nasional yang kuat, transparan, dan berkelanjutan**.

Daftar Isi

Lisensi & Catatan Karya	2
Disclaimer	2
Daftar Isi	3
Kata Pengantar	14
Executive Summary	15
Bagian I — Visi dan Latar Belakang	16
Bab 1: Visi Nasional Keamanan Siber Perbankan Indonesia.....	16
Data sebagai “mata uang baru” sektor keuangan.....	16
Kepercayaan digital sebagai aset sistemik.....	18
Sinergi Digital Trust Economy dan stabilitas sistem keuangan.....	21
Bab 2: Mengapa OJK Perlu Framework Cyber & Privacy Rating.....	23
Risiko sistemik dari serangan siber.....	23
Pelajaran dari dunia internasional.....	24
Pelajaran dari Kebocoran data Pribadi di dunia.....	25
Pengawasan Berbasis Data & Risk Intelligence: dari reaktif ke prediktif.....	28
Ringkas.....	30
Bab 3: Pilar Transformasi: Dari Pengawasan Manual ke Data-Driven Supervision.....	31
Tren Global RegTech & SupTech: dari kepatuhan ke keunggulan.....	31
Integrasi Keamanan, Kepatuhan, dan Tata Kelola Data.....	34
Bagian II — Landasan Regulasi dan Standar	37
Bab 4: Dasar Hukum Nasional.....	37
UU No. 27 Tahun 2022 tentang Pelindungan Data Pribadi.....	37
POJK No. 38/POJK.03/2016 tentang Manajemen Risiko TI.....	39
Peraturan BSSN No. 8/2020 tentang Strategi Keamanan Siber Nasional.....	41
Bab 5: Keterkaitan dengan Standar Internasional.....	44
ISO/IEC 27001, NIST Cybersecurity Framework.....	44
Basel III, IFRS, dan prinsip tata kelola GCG.....	46
Bab 6: Kewenangan OJK dalam Pengawasan Siber & Data Privacy.....	49
Penilaian risiko digital sebagai bagian dari stabilitas sistem keuangan.....	49
Integrasi hasil rating ke dalam profil resiko bank.....	51
Bagian III — Konsep dan Pikiran Besar Framework	54
Bab 7: Paradigma Baru: Data = Uang, Keamanan = Kepercayaan.....	54
Dari financial rating ke digital trust rating.....	54
Mengapa pasar peduli?.....	54
Analogi antara Moody’s/S&P dan CyberRank.....	57
Bab 8: Definisi dan Tujuan Cyber & Privacy Rating Framework.....	60
Penilaian objektif kesiapan siber dan kepatuhan PDP.....	60
Dukungan terhadap transparency & accountability perbankan.....	63
Bab 9: Dimensi Penilaian Utama.....	66
Ketahanan siber (cyber resilience).....	66
Kepatuhan UU PDP dan pelaporan insiden.....	69

Manajemen risiko vendor dan rantai pasok.....	72
Keamanan data nasabah dan transaksi digital.....	75
Bagian IV — Framework & Arsitektur Penilaian.....	79
Bab 10: Struktur IISRI CyberRank Framework.....	79
Penjelasan IISRI CyberRank: Kriteria Ranking dari AAA hingga D.....	79
Komponen hukum, teknis, dan tata kelola.....	82
Indikator risiko siber & privasi (berbasis 33 pasal UU PDP + ISO 27001 + NIST CSF). 85	
Bab 11: Model Skor dan Interpretasi Rating (AAA–D).....	89
Tabel penilaian dan deskripsi tingkat risiko.....	89
Batas minimal rating per kategori bank (BUKU 2 – 4).....	93
Bab 12: Proses Audit dan Sertifikasi Tahunan.....	95
Pengumpulan data otomatis (data leak, domain risk, vendor exposure).....	95
Audit forensik, self-assessment, dan validasi oleh OJK.....	99
Bab 13: Integrasi dengan GCG & Profil Risiko Digital Bank.....	103
Penilaian Digital Maturity Index.....	103
Hubungan dengan OJK CyberTrust Scorecard.....	106
Bagian V — Strategi Implementasi Nasional.....	109
Bab 14: Tahapan Implementasi Framework di OJK.....	109
Fase 1: Pilot Test (bank Buku 4 dan BUMN).....	109
Fase 2: Integrasi dengan Sistem Pengawasan OJK Digital.....	113
Fase 3: Implementasi Nasional dan Public Disclosure.....	116
Bab 15: Sinkronisasi dengan BSSN dan Kemenkominfo.....	119
Pertukaran data ancaman siber nasional.....	119
Harmonisasi standar penilaian PDP.....	122
Bab 16: Keterlibatan Ekosistem: Bank — Fintech — Vendor Teknologi.....	125
Program kemitraan dan kolaborasi open audit.....	125
Bagian VI — Analisis Risiko dan Dampak Ekonomi.....	128
Bab 17: Kerugian Finansial dan Reputasional dari Breach.....	128
Dampak langsung: forensik, denda, hilangnya nasabah.....	128
Dampak tidak langsung: penurunan nilai saham & kepercayaan publik.....	131
Bab 18: Efek Sistemik terhadap Stabilitas Keuangan Nasional.....	134
Simulasi skenario “crisis of confidence”.....	134
Peran OJK dalam pencegahan efek berantai.....	137
Bagian VII — Roadmap Peningkatan & Mitigasi.....	140
Bab 19: Roadmap Peningkatan Tahunan bagi Bank.....	140
Target kenaikan rating per tahun (> 1 level).....	140
Program “PDP Compliance Improvement Plan”.....	143
Bab 20: Taktik Empowerment untuk Bank Berperingkat Rendah.....	147
Capacity building CISO dan DPO.....	147
Hibah teknologi & pendampingan oleh BSSN/OJK.....	151
Program “Cyber Resilience Bootcamp”.....	155
Bab 21: Mitigasi & Pemberdayaan Ekosistem Keamanan Digital.....	158
Skema insentif OJK untuk bank dengan rating tinggi.....	158

Kolaborasi industri untuk shared cyber intelligence.....	161
Bagian VIII — Pemantauan dan Evaluasi Berkelanjutan.....	164
Bab 22: Dashboard OJK CyberTrust Monitoring.....	164
Visualisasi real-time status rating seluruh bank.....	164
Bab 23: Audit Ulang Tahunan dan Sertifikasi Kepatuhan.....	168
Mekanisme penurunan atau kenaikan rating.....	168
Bab 24: Pelaporan Publik dan Transparansi Data.....	171
CyberTrust Report Card tahunan (OJK–BSSN–Bank Indonesia).....	171
Tantangan dan catatan penting.....	172
Langkah konkret yang diharapkan untuk Bab 24.....	172
Bagian IX — Manfaat dan Dampak Nasional.....	173
Bab 25: Bagi OJK & Regulator.....	173
Efisiensi pengawasan dan data-driven regulation.....	173
Standar global yang memandu regulator.....	173
Bab 26: Bagi Bank & Industri Keuangan.....	176
Kepercayaan nasabah dan akses insentif GCG.....	176
Bab 27: Bagi Publik dan Investor.....	179
Transparansi keamanan digital nasional.....	179
Lampiran 1: Template CyberRank Assessment Checklist.....	182
Lampiran 2: Contoh Audit Summary Bank A – Buku 4.....	187
Lampiran 3: Panduan Teknis Integrasi API CyberRank ↔ OJK Portal.....	191
Glosarium Istilah Teknis dan Regulasi.....	197
Referensi Hukum dan Standar Internasional.....	202
Tentang Penulis.....	207

Kata Pengantar

Dalam dunia keuangan modern, **kepercayaan digital (digital trust)** telah menjadi fondasi baru stabilitas sistem keuangan. Keamanan data dan privasi nasabah kini memiliki dampak langsung terhadap kepercayaan publik, nilai saham, bahkan likuiditas perbankan. Ketika satu insiden siber dapat mengguncang kepercayaan pasar dalam hitungan jam, jelas bahwa keamanan digital bukan lagi urusan teknis, melainkan **isu strategis bagi regulator dan direksi**.

Transformasi digital perbankan yang masif — melalui *cloud computing*, *open API*, dan kolaborasi lintas fintech — telah memperluas rantai risiko. Satu kelemahan konfigurasi atau vendor yang tidak patuh dapat menciptakan efek domino yang mengancam reputasi dan kestabilan sistem keuangan nasional. Karena itu, **penguatan kepercayaan digital harus menjadi bagian dari tata kelola (GCG) dan pengawasan prudensial** yang terukur dan berbasis data.

Kerangka *OJK CyberTrust & Data Privacy Ranking Framework* hadir sebagai terobosan untuk menggeser paradigma dari *compliance-based supervision* menuju *trust-based supervision*. Framework ini menilai kesiapan siber dan kepatuhan privasi lembaga keuangan secara objektif dan kuantitatif, serupa dengan *credit rating* yang selama ini menjadi acuan risiko finansial. Hasil peringkat bukan sekadar indikator teknis, tetapi cermin integritas digital dan tata kelola institusi.

Bagi regulator, sistem ini memungkinkan **pengawasan yang lebih efisien, prediktif, dan transparan**. Bagi direksi, ia menjadi dasar strategis untuk meningkatkan kepercayaan investor, efisiensi biaya modal, dan loyalitas nasabah. Dalam era di mana data menjadi aset utama, menjaga keamanan dan privasi berarti menjaga reputasi, nilai, dan keberlangsungan institusi.

Ke depan, kolaborasi lintas otoritas — OJK, BSSN, Bank Indonesia, dan Kemenkominfo — menjadi kunci dalam membangun ekosistem *digital trust* nasional. Hanya dengan koordinasi yang kuat dan standar yang seragam, kita dapat memastikan bahwa inovasi keuangan berjalan seiring dengan perlindungan publik. Melalui *CyberTrust & Data Privacy Ranking Framework*, Indonesia menegaskan bahwa **masa depan sistem keuangan ditentukan oleh kepercayaan digital — bukan hanya oleh modal, tetapi oleh kredibilitas dan keamanan**.

Jakarta, Oktober 2025
Onno W. Purbo

Executive Summary

Buku ini memperkenalkan **OJK CyberTrust & Data Privacy Ranking Framework**, kerangka nasional yang menilai ketahanan siber dan kepatuhan perlindungan data pribadi di industri keuangan Indonesia. Framework ini menempatkan **kepercayaan digital sebagai aset sistemik** yang menentukan stabilitas, reputasi, dan efisiensi biaya modal lembaga keuangan. Dengan pendekatan *data-driven supervision*, penilaian dilakukan secara objektif melalui skor *cyber resilience*, kepatuhan UU PDP, dan manajemen risiko vendor, menggunakan metodologi mirip *credit rating* (AAA–D). Tujuannya bukan sekadar *compliance*, tetapi menciptakan **ekosistem keuangan yang sehat, transparan, dan tangguh**. Selain mekanisme peringkat, dokumen ini menyajikan **strategi mitigasi dan pemberdayaan (empowerment)** bagi lembaga dengan skor rendah: mulai dari roadmap peningkatan tahunan, pelatihan keamanan data, *early-warning system*, hingga *mentorship program* antarbank. Pendekatan ini memastikan bahwa transformasi keamanan digital tidak bersifat menghukum, melainkan mendorong seluruh ekosistem menuju **resilience kolektif**, di mana setiap bank, fintech, dan vendor teknologi menjadi bagian dari rantai kepercayaan nasional yang kuat dan berkelanjutan.

Bagian I — Visi dan Latar Belakang

Bab 1: Visi Nasional Keamanan Siber Perbankan Indonesia

Data sebagai “mata uang baru” sektor keuangan

Data kini berfungsi seperti “mata uang” di industri keuangan. Bukan lagi sekadar catatan transaksi, data telah menjadi *aset strategis* yang menggerakkan keputusan, produk, dan keuntungan. Pergeseran ini terjadi karena data mampu “mencetak nilai” berulang kali: dari prediksi risiko, deteksi *fraud*, sampai *hyper-personalization* layanan nasabah. Bahkan, sejak 2017 banyak analis menyebut data sebagai sumber daya paling bernilai di ekonomi digital—menggeser “minyak”—karena ia memberi daya pasar dan posisi tawar bagi pelaku yang mampu mengumpulkannya, memprosesnya, dan menggunakannya secara unggul. ([The Economist](#))

Di tingkat praktik, bank yang memperlakukan data sebagai *aset produktif* cenderung unggul dalam akurasi penawaran produk, kecepatan layanan, dan efisiensi biaya. Kajian industri menunjukkan bahwa *personalization* berbasis data secara konsisten mendorong kenaikan pendapatan sekitar **5–15%** (dengan variasi 5–25% tergantung sektor dan eksekusi), sementara organisasi yang menata analitiknya dengan rapi dapat meluncurkan kampanye **2–4 kali** lebih cepat. Angka-angka ini menegaskan satu hal: **data menggerakkan pertumbuhan nyata bila dikelola dengan kapabilitas yang tepat.** ([McKinsey & Company](#))

Namun, seperti mata uang, **data membawa risiko sistemik.** Kebocoran, penyalahgunaan, dan keputusan berbasis data yang bias dapat menggerus kepercayaan publik dan pemicu biaya hukum, operasional, hingga pengetatan regulasi. Di sinilah kata kunci *digital trust* menjadi **aset sistemik**: jika kepercayaan runtuh, aktivitas ekonomi ikut terganggu. Karena itu, *governance* data, kualitas data (*data quality*), dan keamanan siber bukan “tambahan”—melainkan **inti** model bisnis perbankan modern. Temuan dan panduan dari komunitas perbankan Eropa menegaskan pentingnya *data analytics* dan *centres of excellence* untuk mengekstrak *insight* bernilai tinggi secara berkelanjutan—namun selalu dengan disiplin kualitas dan *compliance*. ([Abe EBA](#))

Konteks global juga bergerak cepat: **digitalisasi dan tokenisasi** mengubah infrastruktur keuangan—dari pembayaran lintas batas hingga pasar sekuritas. Otoritas moneter internasional menempatkan *tokenized platforms* dan *unified ledgers* sebagai kandidat tulang punggung sistem keuangan generasi berikutnya. Intinya sederhana: **masa depan uang akan lebih “berbasis data”**, lebih terprogram, dan menuntut tata kelola yang makin kuat—baik untuk stabilitas, transparansi, maupun efisiensi. Bagi industri yang menjadikan data sebagai *mata uang*, arah ini mempertegas kebutuhan standar keamanan, interoperabilitas, dan pengawasan berbasis data. ([Bank for International Settlements](#))

Apa artinya bagi Indonesia—khususnya OJK dan perbankan? Jika data adalah *mata uang*, maka regulasi, pengawasan, dan *rating* keamanan-privasi adalah **mekanisme “nilai tukar”**: bank yang mengelola data dengan aman, patuh, dan bernilai tambah akan memperoleh biaya modal kepercayaan yang lebih rendah—dari nasabah, investor, hingga regulator. Kerangka seperti **OJK CyberTrust & Data Privacy Ranking Framework**

memposisikan keamanan siber, kepatuhan PDP, *vendor risk*, dan kualitas data sebagai dimensi inti; bukan hanya demi mengurangi denda atau *incident cost*, tetapi untuk **memperkuat daya saing dan ketahanan industri**. Dengan bahasa sederhana: **di era ini, menjaga data sama pentingnya (bahkan lebih) daripada menjaga brankas**—sebab kebocoran data bukan sekadar kerugian finansial, tetapi **keruntuhan kepercayaan** yang mahal dan sulit dibeli kembali. ([Abe EBA](#))

Kesimpulan praktisnya jelas. Perlakukan data seperti uang: **dicatat rapi, diaudit, diamankan, dipakai secara etis, dan “diinvestasikan” ke kapabilitas analitik serta AI**. Lakukan *clean-room analytics*, penguatan *data quality*, *zero-trust security*, dan *privacy-by-design*. Karena ketika *data = mata uang*, pemenangnya adalah mereka yang **paling handal mengubah data menjadi nilai**—tanpa pernah menggadaikan kepercayaan. Dan itulah fondasi yang ingin dikuatkan oleh **OJK CyberTrust & Data Privacy Ranking Framework** ke depan. ([McKinsey & Company](#))

Kepercayaan digital sebagai aset sistemik

Kepercayaan digital adalah “modal” yang membuat transaksi modern bergerak lancar. Tanpa kepercayaan, nasabah tidak mau berbagi data, memakai *mobile banking*, atau mencoba produk baru. Akibatnya, pertumbuhan melambat, biaya naik, dan risiko membesar. OECD menegaskan: **keamanan digital adalah dimensi ekonomi dan sosial**—bukan sekadar isu teknis—karena langsung mempengaruhi kepercayaan dan ketahanan ekonomi yang semakin bergantung pada layanan digital. ([OECD](#))

Di sektor keuangan global, regulator melihat **kepercayaan digital sebagai aset sistemik**. Mengapa? Karena gangguan kepercayaan dapat menular cepat melalui jaringan pembayaran, pasar uang, dan lembaga keuangan lain. IMF mencatat: **insiden siber di sektor keuangan hampir seperlima dari total insiden dan kerugian ekstrem yang dilaporkan meningkat**—kasus terbesar mencapai **±US\$2,5 miliar**, naik lebih dari empat kali sejak 2017. Kerugian tidak langsung—biaya pemulihan, reputasi, *upgrade*—sering lebih besar dari kerugian langsung. Artinya, serangan siber bukan cuma masalah *IT*, melainkan **risiko stabilitas**. ([IMF](#))

Tiga alasan mengapa “trust” berskala sistemik

- **Interkoneksi tinggi.** Bank, *fintech*, gerbang pembayaran, *cloud*, dan vendor *core banking* saling terhubung. Satu insiden pada pemain kunci dapat memicu *spillover*. Bank sentral dan pengawas (mis. BIS, OCC, The Fed) menempatkan *cyber resilience* sebagai prioritas pengawasan dan menerbitkan panduan peningkatan ketahanan lintas lembaga. ([Bank for International Settlements](#))
- **Ekspektasi nasabah berubah.** Survei global menunjukkan **trust bergeser dari “sekadar patuh” menjadi “daya saing inti”**. Brand dan bank yang *pro-privacy* dan transparan unggul meraih akuisisi dan retensi. *Digital trust* bukan bonus, melainkan **pembeda pertumbuhan**. ([usercentrics.com](#))
- **Digitalisasi pembayaran meluas.** Adopsi pembayaran digital meningkat cepat (contoh: **62%** populasi di ekonomi berkembang melakukan atau menerima pembayaran digital pada 2024, dan **96%** di negara OECD). Ketergantungan tinggi berarti **guncangan kepercayaan** dapat berdampak ekonomi luas. ([OECD](#))

Apa wujud “aset sistemik” dalam praktik?

Pikirkan kepercayaan digital seperti “**cadangan kepercayaan**”: modal tak kasat mata yang memperlancar likuiditas layanan digital.

- **Di neraca publik (intangible).** Tidak muncul sebagai kas, tetapi **mempengaruhi biaya modal reputasi**: bank yang dipercaya cenderung memperoleh **biaya akuisisi nasabah lebih rendah**, *churn* lebih kecil, dan *cross-sell* lebih tinggi. (Temuan PwC untuk perbankan/keuangan menyorot celah *cyber resilience* yang langsung berdampak pada *business outcomes*). ([PwC](#))
- **Di arsitektur pengawasan.** Laporan IMF menempatkan *cyber risk* dalam **Global Financial Stability Report**, setara isu makro lain. Ini sinyal bahwa **trust** kini berkait langsung dengan **stabilitas sistem keuangan**. ([IMF](#))

- **Di kebijakan industri.** BIS menyorot sistem keuangan generasi baru yang makin “*data-rich*” dan “*tokenized*”—mendorong standar *resilience*, interoperabilitas, dan tata kelola yang menjaga **trust pada skala sistem**. ([Bank for International Settlements](#))

Apa implikasinya untuk bank?

Sederhana: perlakukan trust seperti aset yang dikelola aktif. Bukan asumsi.

- **Dari *compliance-only* ke *trust-by-design*.** Rancang proses, produk, dan *journey* nasabah yang *privacy-preserving* sejak awal (*privacy-by-design*), bukan ditempel di akhir. WEF menekankan *agency* individu sebagai inti *digital trust*: izin jelas, pilihan nyata, dan transparansi. ([World Economic Forum](#))
- **Dari kontrol titik ke ketahanan sistem.** Bangun *zero-trust architecture*, *rapid detection & response*, dan *table-top exercise* lintas fungsi. Gunakan metrik *mean time to detect/contain* sebagai **KPI bisnis**, bukan hanya KPI TI. (OCC/The Fed: penguatan berbagi intelijen dan koordinasi peringatan dini). ([OCC.gov](#))
- **Dari *vendor checklists* ke *chain-of-trust*.** Audit pemasok kritikal (*cloud*, *core*, *KYC/AML*), uji skenario kegagalan vendor, dan tetapkan *exit plan*. *Chain-of-trust* mencegah satu titik lemah merusak sistem. (BIS/IMF menilai keterhubungan NBFi-bank sebagai titik rawan transmisi stres). ([Financial Times](#))

“Trust premium” vs “trust discount”

- **Trust premium.** Bank dengan *cyber hygiene* kuat, *incident reporting* cepat, dan tata kelola data yang jelas biasanya menikmati **adopsi digital lebih tinggi** dan biaya akuisisi lebih rendah. Ini *compounding*. (PwC; tren *digital trust* sebagai pengungkit pertumbuhan). ([PwC](#))
- **Trust discount.** Kebocoran besar menciptakan **diskon kepercayaan**: biaya hukum, *remediation*, migrasi nasabah, dan pengetatan pengawasan. IMF menunjukkan **ekor risiko** (*tail risk*) makin berat—meski kejadian ekstrem jarang, dampaknya besar dan menular. ([IMF](#))

Apa arti semua ini bagi Indonesia dan OJK?

Kerangka “OJK CyberTrust & Data Privacy Ranking Framework” bisa memosisikan *digital trust* sebagai **aset sistemik** melalui tiga pengungkit:

1. **Skor *resilience* yang bermakna ekonomi.** Kaitkan *rating* dengan insentif: akses program efisiensi GCG, *regulatory fast-track* untuk inovasi yang aman, atau pengurangan *supervisory friction* bagi bank berperingkat tinggi. (Selaras arah pengawasan internasional untuk menginternalisasi risiko siber pada tata kelola). ([OCC.gov](#))
2. **Transparansi terukur.** Publikasikan *dashboard* agregat (tanpa membuka kerentanan spesifik) agar pasar melihat kemajuan industri. Transparansi yang tepat meningkatkan *market discipline* tanpa mengundang *security risk*. (Praktik pelaporan ketahanan sistem kian lazim di laporan tahunan bank sentral/otoritas). ([Bank for International Settlements](#))

3. **Interoperabilitas standar.** Selaraskan penilaian dengan ISO/IEC 27001, NIST CSF, dan *incident taxonomy* global; rangkai dengan *RegTech/SupTech* untuk *real-time supervision*. Hasilnya: **pengawasan berbasis data** dengan *signal-to-noise* lebih tinggi. (IMF dan OECD mendorong pendekatan manajemen risiko digital lintas ekonomi). ([IMF](#))

Ringkasan

- **Kepercayaan digital = aset sistemik.** Dampaknya langsung ke stabilitas dan pertumbuhan. ([IMF](#))
- **Tolok ukurnya nyata.** *Resilience metrics*, kecepatan deteksi/penanggulangan, dan *chain-of-trust* vendor. ([OCC.gov](#))
- **Pasar menghargai trust.** Ada *trust premium* bagi bank yang unggul, dan *trust discount* bagi yang lalai. ([PwC](#))
- **Arah global sejalan.** IMF, BIS, OCC/The Fed, OECD, WEF menempatkan *digital trust* di jantung *policy* dan pengawasan. ([IMF](#))

Sinergi *Digital Trust Economy* dan stabilitas sistem keuangan

Dalam ekonomi digital modern, kepercayaan bukan lagi hanya faktor moral—tetapi **fondasi ekonomi baru**. Istilah *digital trust economy* menggambarkan ekosistem keuangan yang bergantung pada rasa aman, transparansi, dan kepastian digital di antara pelaku pasar. Tanpa kepercayaan, transaksi digital berhenti, nasabah mundur, dan sistem keuangan kehilangan stabilitasnya. Itulah mengapa lembaga seperti IMF, OECD, dan Bank for International Settlements (BIS) kini menganggap *digital trust* sebagai **komponen sistemik** dari stabilitas ekonomi global.

Dalam konteks keuangan, sinergi antara *digital trust economy* dan stabilitas sistem keuangan bersifat dua arah. Kepercayaan digital memperkuat stabilitas, sementara stabilitas memberi ruang bagi tumbuhnya kepercayaan digital. Ketika nasabah yakin bahwa data mereka aman, transaksi akan meningkat, risiko penarikan dana massal berkurang, dan sistem pembayaran bekerja lebih efisien. Di sisi lain, ketika bank dan regulator mampu menjaga kestabilan sistem keuangan, masyarakat semakin percaya pada layanan digital yang mereka gunakan. Dua unsur ini—kepercayaan dan stabilitas—bagaikan dua sisi mata uang yang tidak dapat dipisahkan.

Di tingkat global, pola ini terlihat jelas. Laporan IMF tahun 2024 menunjukkan peningkatan signifikan dalam *cyber incidents* di sektor keuangan, di mana kerugian ekstrem per insiden bisa mencapai lebih dari **US\$2,5 miliar**. Namun, negara dengan tingkat *digital trust* yang tinggi seperti Singapura, Jepang, dan Uni Eropa mampu menahan efek berantai (*contagion effect*) karena memiliki tata kelola keamanan siber dan perlindungan data yang kuat. OECD menegaskan bahwa *digital trust* yang terjaga mampu mengurangi ketidakpastian pasar dan memperkuat keyakinan investor terhadap stabilitas ekonomi digital.

Sinergi ini juga berdampak langsung pada perilaku pasar. Bank yang transparan dalam melaporkan insiden siber dan cepat memulihkannya memperoleh kembali kepercayaan publik lebih cepat—efeknya, harga saham stabil dan dana pihak ketiga tidak lari. Sebaliknya, bank yang tertutup dan lamban merespons krisis kepercayaan sering mengalami *trust discount* di pasar: biaya operasional naik, reputasi turun, dan pengawasan regulator makin ketat. Dengan kata lain, kepercayaan digital menciptakan “*trust premium*”, sementara kegagalannya memunculkan “*trust penalty*”.

Bagi Indonesia, membangun sinergi *digital trust economy* dan stabilitas sistem keuangan berarti memperkuat tiga hal penting. Pertama, **standarisasi pelaporan insiden siber** seperti model *FIRE framework* dari Financial Stability Board (FSB), agar pengawasan bisa cepat dan akurat. Kedua, **penerapan prinsip *privacy-by-design* dan *zero-trust architecture*** di seluruh lembaga keuangan untuk melindungi data nasabah sejak tahap desain sistem. Ketiga, **integrasi pengawasan berbasis data (*suptech*)** oleh OJK agar deteksi risiko bisa dilakukan secara real-time. Ketika ketiga hal ini berjalan, kepercayaan publik akan meningkat—dan dengan itu, kestabilan keuangan nasional akan semakin kokoh.

Pada akhirnya, ekonomi berbasis kepercayaan digital bukanlah idealisme teknologi, melainkan kebutuhan strategis. Dunia keuangan yang kuat tidak hanya dibangun di atas modal dan regulasi, tetapi di atas **kepercayaan yang terukur, aman, dan berkelanjutan**. Sinergi antara *digital trust* dan stabilitas sistem keuangan adalah fondasi baru bagi ekonomi

Indonesia di era digital global—tempat di mana **keamanan data adalah modal, dan kepercayaan adalah likuiditas baru.**

Bab 2: Mengapa OJK Perlu Framework Cyber & Privacy Rating

Risiko sistemik dari serangan siber

Bayangkan jika dalam satu malam, jaringan *core banking* nasional berhenti bekerja. ATM tidak berfungsi. Transaksi digital gagal. Data nasabah tidak bisa diakses. Bukan karena bencana alam, melainkan **serangan siber terkoordinasi**. Inilah risiko baru dunia keuangan modern — risiko yang tidak lagi hanya mengancam satu bank, tetapi **bisa mengguncang seluruh sistem keuangan nasional**.

Dalam ekonomi digital yang saling terhubung, satu serangan bisa menyebar secepat *click*. Sistem pembayaran, *internet banking*, dan jaringan *cloud* kini membentuk ekosistem yang kompleks dan saling bergantung. Karena itu, setiap kelemahan kecil di satu titik — misalnya pada vendor teknologi atau sistem *third-party API* — bisa menciptakan **efek domino** yang mengguncang banyak lembaga sekaligus.

Mengapa serangan siber bisa menjadi risiko *sistemik*

1. **Keterhubungan digital antar bank semakin tinggi.** Menurut laporan Bank for International Settlements (BIS), lebih dari 70% transaksi lintas-lembaga keuangan di Asia kini bergantung pada *shared digital infrastructure* — mulai dari *SWIFT network* hingga *cloud provider* bersama. Jika satu penyedia terganggu, dampaknya langsung terasa ke seluruh jaringan. → Contohnya, serangan ransomware *NotPetya* tahun 2017 melumpuhkan sistem keuangan di Ukraina dan menyebar ke lebih dari 60 negara, termasuk bank besar di Eropa.
2. **Kecepatan propagasi serangan.** Serangan hari ini tidak lagi manual. Dengan *automation* dan *AI-generated malware*, peretas dapat memperluas dampak dalam hitungan menit. Dalam laporan IMF 2024, disebutkan bahwa **satu dari lima serangan siber global kini menargetkan sektor keuangan**, dan kerugian ekstrem (*tail risk*) bisa mencapai **lebih dari US\$2,5 miliar per insiden**.
3. **Efek kepercayaan dan stabilitas pasar.** Serangan pada bank besar bisa memicu *crisis of confidence*. Masyarakat panik, dana ditarik secara massal (*digital bank run*), nilai saham turun, dan pasar uang membeku. Ini pernah terjadi di Bangladesh Bank (2016), di mana serangan siber mengalihkan dana sebesar **US\$81 juta** dan memicu pengetatan sistem internasional *SWIFT*.
4. **Gangguan pada fungsi kritis sistem keuangan.** Lembaga seperti BIS dan Financial Stability Board (FSB) menegaskan bahwa gangguan pada “*Critical Financial Market Infrastructures*” — seperti sistem kliring, RTGS, atau *payment gateways* — dapat menyebabkan **kegagalan sistemik yang menyerupai krisis finansial**. Dengan kata lain, serangan siber bisa menimbulkan dampak yang setara dengan *bank run* atau krisis likuiditas.

Dampak yang terasa langsung di sektor keuangan

- **Kerugian finansial langsung:** denda, biaya pemulihan, forensik digital, serta kompensasi nasabah. Equifax (AS, 2017) membayar lebih dari **US\$1,38 miliar** akibat kebocoran 148 juta data pribadi.
- **Dampak reputasi dan kepercayaan:** kehilangan nasabah dan turunnya nilai saham. Setelah insiden Capital One (2019), nilai pasar perusahaan turun 6% dalam seminggu.
- **Biaya sistemik nasional:** peningkatan premi asuransi siber, revisi regulasi, serta kebutuhan peningkatan *cyber defense budget* lintas industri.

Pelajaran dari dunia internasional

Negara-negara maju kini menganggap keamanan siber sebagai bagian dari **stabilitas keuangan nasional**, bukan sekadar isu teknologi.

- **Uni Eropa** membangun *Digital Operational Resilience Act (DORA)* untuk memastikan semua bank, asuransi, dan *fintech* memiliki ketahanan digital yang sama kuatnya.
- **Amerika Serikat** melalui *Office of the Comptroller of the Currency (OCC)* dan *The Fed* mewajibkan uji coba *cyber resilience* lintas bank besar setiap tahun.
- **Singapura dan Korea Selatan** mengembangkan *financial sector computer emergency response team (FinCERT)* untuk koordinasi cepat saat terjadi insiden.

Semua kebijakan itu punya satu tujuan: **mencegah gangguan digital berubah menjadi krisis sistemik**.

Tantangan dan urgensi untuk Indonesia

Indonesia kini berada di titik kritis yang sama. Dengan lebih dari **300 juta transaksi digital per hari** di ekosistem perbankan dan *fintech*, ketergantungan pada infrastruktur digital sudah sangat tinggi. Namun, **belum semua bank memiliki kapasitas deteksi dan respon cepat**. Banyak serangan berhasil karena kesalahan konfigurasi, lemahnya kontrol vendor, atau kurangnya *cyber intelligence sharing* antar lembaga.

Karena itu, penting bagi OJK, BSSN, dan Bank Indonesia untuk **membangun mekanisme pengawasan terpadu berbasis data dan rating keamanan siber**. Framework seperti *OJK CyberTrust & Data Privacy Ranking* dapat membantu memetakan bank mana yang sudah siap menghadapi serangan, dan mana yang masih rentan.

Arah strategis ke depan

1. **Menyatukan pengawasan risiko siber dengan profil risiko bank.** Sama seperti *credit rating*, setiap bank perlu punya *cyber rating* nasional.
2. **Mendorong transparansi dan pelaporan cepat insiden.** Serangan yang diketahui cepat bisa ditangani sebelum menjadi bencana sistemik.

3. **Membangun ekosistem intelijen bersama.** *Threat intelligence sharing* antar bank, *fintech*, dan regulator menjadi fondasi dari ketahanan digital nasional.

Penutup

Serangan siber bukan lagi sekadar ancaman teknologi — ia adalah **ancaman sistemik terhadap keuangan nasional**. Kegagalan satu institusi bisa memicu efek berantai bagi banyak pihak. Oleh karena itu, langkah membangun *CyberTrust & Data Privacy Rating Framework* bukan hanya tentang *compliance*, tetapi tentang **menjaga jantung sistem keuangan Indonesia agar tetap berdetak di era digital**.

Pelajaran dari Kebocoran data Pribadi di dunia

Berikut adalah beberapa kasus kebocoran data pribadi besar di dunia yang memiliki dampak signifikan terhadap ekonomi finansial bank suatu negara. Saya fokus pada kasus-kasus di mana kebocoran tersebut menyebabkan kerugian ekonomi langsung, seperti penipuan massal, gangguan sistem pembayaran, penurunan kepercayaan konsumen, denda regulasi, atau biaya pemulihan yang membebani sektor perbankan nasional. Kasus-kasus ini dipilih berdasarkan skala (jumlah korban), dampak finansial, dan pengaruh terhadap ekonomi negara terkait. Saya menyusunnya dalam tabel untuk kemudahan pembacaan, dengan urutan berdasarkan skala korban (menurun).

No	Kasus dan Tanggal	Deskripsi Singkat	Dampak pada Ekonomi Finansial Bank Negara
1	Equifax (AS, 2017)	Kebocoran data pribadi sekitar 148 juta orang, termasuk nama, SSN, tanggal lahir, dan nomor kartu kredit, akibat kerentanan di sistem Apache Struts.	Menyebabkan kerugian \$1,38 miliar dalam penyelesaian hukum dan peningkatan biaya keamanan siber di sektor kredit AS. Dampaknya mengganggu sistem kredit nasional, meningkatkan risiko pencurian identitas, dan mendorong perubahan undang-undang untuk pembekuan kredit gratis, yang membebani bank-bank AS dengan biaya tambahan untuk pencegahan penipuan.

2	Heartland Payment Systems (AS, 2008-2009)	Kebocoran 130 juta data kartu kredit dan debit melalui injeksi SQL dan malware.	Menimbulkan kerugian \$170-200 juta bagi perusahaan, termasuk denda dan gugatan, yang memaksa penerbitan ulang kartu massal di AS. Ini mengganggu sistem pembayaran nasional dan meningkatkan biaya operasional bank-bank AS untuk keamanan transaksi.
3	Capital One (AS/Kanada, 2019)	Kebocoran data 106 juta pelanggan, termasuk SSN, nomor rekening bank, dan riwayat kredit, akibat konfigurasi firewall AWS yang salah.	Denda \$80 juta dan penyelesaian \$190 juta, plus biaya pemulihan yang membebani bank tersebut. Dampaknya meningkatkan pengawasan regulasi terhadap infrastruktur cloud di AS dan Kanada, menyebabkan biaya tambahan bagi sektor perbankan nasional untuk mitigasi risiko serupa.
4	JPMorgan Chase (AS, 2014)	Kebocoran data 83 juta akun, termasuk nama, alamat, dan email, melalui kerentanan zero-day di server tanpa autentikasi dua faktor.	Meskipun tidak ada pencurian dana langsung, ini memicu evaluasi ulang kerangka keamanan siber di sektor keuangan AS, dengan biaya tahunan JPMorgan untuk keamanan mencapai \$250 juta. Dampaknya menurunkan kepercayaan konsumen dan meningkatkan biaya regulasi bagi bank-bank nasional.
5	Experian (Afrika Selatan, 2020)	Kebocoran data 24 juta individu dan 800.000 bisnis, termasuk nama, ID, dan detail kontak, melalui rekayasa sosial.	Mengganggu sistem pelaporan kredit nasional di Afrika Selatan, meningkatkan risiko penipuan dan kerugian ekonomi dari pencurian identitas. Ini memaksa bank-bank lokal meningkatkan biaya keamanan dan pemantauan kredit.
6	Korea Credit Bureau (Korea Selatan, 2012-2013)	Kebocoran data 20 juta pengguna (40% populasi Korea Selatan) oleh insider, termasuk SSN,	Denda \$48 juta dan kompensasi bagi korban, yang mengganggu sektor kredit dan perbankan nasional. Dampaknya menurunkan kepercayaan konsumen dan meningkatkan biaya operasional bank-bank Korea Selatan untuk enkripsi data.

nomor kartu kredit,
dan alamat.

- | | | | |
|---|---|---|---|
| 7 | Desjardins Group
(Kanada, 2016-2019) | Kebocoran data 9,7 juta individu dan 173.000 bisnis, termasuk nama, SIN, dan riwayat transaksi, oleh insider. | Melibatkan pengawas privasi federal, meningkatkan biaya pemantauan dan kontrol akses di sektor keuangan Kanada. Ini menimbulkan risiko penipuan jangka panjang yang membebani ekonomi nasional melalui hilangnya kepercayaan pada lembaga keuangan. |
| 8 | Banco BCR
(Kosta Rika, 2019-2020) | Kebocoran 11 juta data kartu kredit melalui ransomware, yang dipublikasikan di dark web. | Mengganggu operasi bank negara milik pemerintah Kosta Rika, meningkatkan risiko penipuan massal dan kerugian ekonomi dari gangguan sistem keuangan nasional. |

Kasus-kasus ini menunjukkan bahwa kebocoran data sering kali disebabkan oleh kerentanan teknis, insider threat, atau rekayasa sosial, dan dampaknya meluas ke ekonomi nasional melalui biaya hukum, penurunan produktivitas bank, dan peningkatan penipuan. Di negara-negara seperti AS, Kanada, dan Korea Selatan, ini mendorong reformasi regulasi yang mempengaruhi seluruh sektor perbankan. Jika Anda membutuhkan detail lebih lanjut tentang kasus tertentu, beri tahu saya!

Pengawasan Berbasis Data & *Risk Intelligence*: dari reaktif ke prediktif

Di ekonomi yang serba digital, pengawasan keuangan tidak bisa lagi mengandalkan laporan manual yang datang terlambat. **Kita butuh pengawasan berbasis data (*data-driven supervision*) dan *risk intelligence* yang real-time**—agar regulator dan bank melihat risiko sebelum menjadi krisis. Tren global mengarah ke sana: regulator mendorong **format pelaporan insiden yang seragam lintas negara (FSB *FIRE*)**, **ketahanan operasional digital (UE *DORA*)**, dan **pemanfaatan *SupTech*** untuk analitik pengawasan. Intinya, pengawasan masa kini adalah pengolahan data, bukan sekadar pengumpulan dokumen. ([Financial Stability Board](#))

Mengapa sekarang? (realitas global)

- **Risiko menebal di “ekor”.** IMF menyoroti pola *tail risk*: sebagian besar insiden kecil, tetapi **kejadian ekstrem bisa menimbulkan kerugian > US\$2,5 miliar** per insiden dan menular ke lembaga lain. Ini menuntut deteksi cepat berbasis sinyal data, bukan laporan pasca-kejadian. ([Financial Times](#))
- **Standar baru sudah berlaku.** UE menerapkan **Digital Operational Resilience Act (DORA)** per **17 Jan 2025**: wajib *incident reporting*, *resilience testing*, dan pengelolaan risiko *third-party* secara ketat—sekaligus mendorong *near-real-time oversight*. ([eiopa.europa.eu](#))
- **Pelaporan insiden diseragamkan.** FSB merilis **FIRE** (Format for Incident Reporting Exchange) agar informasi insiden operasional/siber dapat **dibagi cepat dan konsisten** lintas otoritas dan yurisdiksi. ([Financial Stability Board](#))
- **Pengawasan makin digital.** *SupTech* (supervisory technology) dipakai untuk menelan data multi-sumber (regulatory filings, *threat intel*, log teknis), lalu **memicu peringatan dini** dan *risk scoring* otomatis. BIS bahkan menguji *platform* analitik terintegrasi lewat *Project Ellipse*. ([Bank for International Settlements](#))

Apa yang dimaksud *risk intelligence* untuk bank & regulator?

Risk intelligence adalah **kapasitas membaca risiko dari data**—menggabungkan sinyal teknis (*telemetry* TI, insiden vendor, *phishing*), sinyal bisnis (perubahan perilaku nasabah), dan sinyal pasar (berita, *dark-web leak*). Hasilnya adalah **peta risiko yang hidup**: siapa rapuh, di mana celah, dan apa prioritas tindakan—dengan **ukurannya** jelas (metrik).

Contoh metrik praktis yang mudah dihitung dan di-*dashboard*-kan:

- **MTTD/MTTR** (*mean time to detect / respond*).
- **Rate kebocoran data** (rekaman/1 juta akun/bulan).
- **Rasio insiden vendor** (jumlah insiden terkait *third-party* ÷ total insiden).
- **Uji ketahanan berkala** (jumlah temu-celah *TLPT*/tahun yang sudah ditutup).
- **Konsentrasi vendor kritis** (HHI sederhana untuk *cloud/core*).
- **Kepatuhan pelaporan insiden** (SLA pelaporan vs standar *FIRE*).

Metrik-metrik ini menyambungkan keamanan TI ke **bahasa bisnis**: kecepatan pemulihan, biaya potensi kerugian, dan dampak ke nasabah.

Bagaimana arsitektur pengawasan berbasis data bekerja?

- **Koleksi data otomatis.** Tarik *feed* terstruktur: *FIRE incident schema*, log keamanan, status SLA vendor, dan *threat intel*. Di Eropa, *DORA* memaksa kedalaman data *vendor risk* sampai *fourth-party*. (eiopa.europa.eu)
- **Normalisasi & taksonomi.** Gunakan **taksonomi insiden bersama (FSB FIRE)** untuk menghindari “apel vs jeruk” antar-bank dan memudahkan *benchmarking*. ([Financial Stability Board](https://www.fsb.eu))
- **Analitik SupTech.** Jalankan *risk scoring* harian: *outlier detection* pada metrik MTTD/MTTR, konsentrasi vendor, dan jejak kebocoran; gabungkan dengan sinyal pasar. (BIS *Ellipse* mengeksplorasi *insights-based supervision* lewat *reg-data* + analitik). ([Bank for International Settlements](https://www.bankforinternationalsettlements.com))
- **Peringatan dini & eskalasi.** Jika skor melewati ambang, sistem memicu **alert** ke pengawas tematik (TI/operasional) dan bank terkait—mendorong *remediation* terukur dan *follow-up* terjadwal.
- **Umpan balik ke kebijakan.** *Trend analytics* memberi dasar penyesuaian ketentuan *resilience testing*, ambang pelaporan, dan *playbook* krisis.

Pelajaran dari praktik internasional (yang bisa langsung ditiru)

- **UE (DORA):** jadikan *incident reporting*, *resilience testing*, dan *third-party risk* sebagai **pilar wajib**. Banyak lembaga menambah *near-real-time monitoring* dan *threat-led penetration testing (TLPT)* sebagai standar. ([TechRadar](https://www.techradar.com))
- **FSB (FIRE):** pakai format pelaporan yang sama untuk **mengurangi beban pelaporan multi-otoritas** dan mempercepat koordinasi lintas negara. ([Financial Stability Board](https://www.fsb.eu))
- **APAC (MAS & komunitas SupTech):** dorong **pemakaian AI/analitik** di pengawasan (*AIDA / GenAI* untuk *triage* dan ringkas insiden) serta *capacity building* pengawas. ([Mas Singapore](https://www.mas.gov.sg))

Terjemahan untuk Indonesia: apa yang perlu OJK & industri lakukan?

1. **Standarkan data & jamkan pelaporan.** Adopsi **FSB FIRE** sebagai **skema pelaporan nasional** (bank, *fintech*, dan vendor kritikal), dengan SLA jelas (*T+24h* untuk indikasi awal, *T+72h* untuk detail). Ini membuat *signal* nasional bersih dan bisa diolah otomatis. ([Financial Stability Board](https://www.fsb.eu))
2. **Bangun SupTech analitik OJK.** Mulai dari *risk cockpit* sederhana: **MTTD/MTTR**, *vendor concentration*, *data-loss rate*, *TLPT closure rate*. Targetkan **peringatan dini** dan **watchlist** bank/vendor berisiko—mirip *early warning system* makro, namun untuk siber/operasional. (Sejalan eksperimen BIS *Project Ellipse*). ([Bank for International Settlements](https://www.bankforinternationalsettlements.com))
3. **Kaitkan nilai bisnis.** Hubungkan *risk score* ke **profil risiko bank** dan **insentif pengawasan** (mis. frekuensi *thematic review*, *fast-track* untuk inovasi aman). Ini menyalurkan investasi keamanan ke **hasil yang terukur**—menurunkan *risk premium* industri.
4. **Terapkan “uji beban” digital.** Selenggarakan **TLPT industri** setahun sekali pada fungsi kritikal (RTGS/kliring, *core banking*, *internet banking*). Publikasikan hasil

agregat agar ada **disiplin pasar** tanpa membuka kerentanan spesifik. (Selaras semangat *DORA*). (eiopa.europa.eu)

5. **Perluas cakupan vendor.** Wajib **peta *fourth-party*** untuk layanan *cloud/core*. Pantau konsentrasi dengan indeks sederhana (HHI) dan tetapkan *exit plan*—agar kegagalan satu penyedia tidak berujung risiko sistemik. (Fokus sentral *DORA* & praktik pengawasan modern). ([TechRadar](https://www.techradar.com))

Ringkas

- **Pengawasan berbasis data** bukan pilihan; ini **syarat stabilitas** di era digital.
- **Standar global sudah siap:** *DORA* untuk ketahanan operasional; **FSB *FIRE*** untuk pelaporan insiden; **BIS *SupTech*** untuk analitik pengawasan. Tinggal **diintegrasikan** ke konteks Indonesia. (eiopa.europa.eu)
- Ke depannya, **OJK CyberTrust & Data Privacy Ranking** sebaiknya ditenagai *risk intelligence*—dengan metrik yang bisa diaudit, *alerting* yang cepat, dan *playbook* yang memaksa **aksi korektif sebelum krisis**.

Bab 3: Pilar Transformasi: Dari Pengawasan Manual ke *Data-Driven Supervision*

Tren Global *RegTech* & *SupTech*: dari kepatuhan ke keunggulan

Dunia keuangan bergerak cepat. Regulasi makin kompleks. Risiko digital makin besar. Jawabannya: **teknologi untuk regulasi dan pengawasan**. Inilah **RegTech** (teknologi untuk kepatuhan) dan **SupTech** (teknologi untuk pengawasan). Keduanya sekarang jadi arus utama di bank dan otoritas. BIS mencatat adopsi *regtech/suptech* tumbuh pesat dan meluas ke banyak fungsi inti. ([Bank for International Settlements](#))

Apa yang berubah secara global?

- **Bahasa bersama untuk insiden.** *Financial Stability Board* memfinalkan format **FIRE — Format for Incident Reporting Exchange**. Tujuannya sederhana: satu format global untuk laporan insiden operasional/siber, agar pelaporan ke banyak otoritas lebih mudah dan cepat. Dampaknya besar untuk *interoperability* dan *early warning*. ([Financial Stability Board](#))
- **Ketahanan digital dijadikan wajib.** Uni Eropa menerapkan **DORA — Digital Operational Resilience Act** per **17 Januari 2025**. Bank, asuransi, dan pelaku pasar harus siap gangguan TIK: dari *incident reporting*, *resilience testing*, sampai pengawasan *critical ICT third-party*. Ini mendorong *near-real-time oversight*. ([eiopa.europa.eu](#))
- **Data-sharing untuk AML/CFT.** MAS (Singapura) meluncurkan **COSMIC**: platform berbagi informasi lintas bank untuk melawan pencucian uang/pendanaan terorisme. Enam bank besar sudah ikut. Ini contoh *RegTech* kolaboratif yang langsung memperkuat pengawasan. ([Ministry of Finance](#))
- **Sandbox makin “berotot”.** FCA (Inggris) mengembangkan *regulatory/digital sandbox* dan inisiatif “**supercharged sandbox**” untuk uji coba AI bersama mitra teknologi. Tujuannya mempercepat inovasi yang aman dan mengurangi biaya eksperimen. ([FCA](#))
- **Gelombang riset dan kebijakan.** Unit FSI–BIS menempatkan *suptech* sebagai topik prioritas bersama AI, *stablecoins*, dan risiko iklim — tanda bahwa teknologi pengawasan kini bagian dari agenda tata kelola global. ([Bank for International Settlements](#))

Apa itu *RegTech* dan *SupTech*—dengan bahasa sederhana?

- **RegTech:** alat bantu bank agar **patuh** lebih cepat dan murah. Contoh: *KYC/AML automation*, *transaction monitoring* berbasis AI, *model risk management* yang terdokumentasi otomatis.
- **SupTech:** alat bantu regulator agar **mengawasi** lebih tajam dan real-time. Contoh: *dashboards* risiko, analitik anomali, konsolidasi laporan insiden pakai skema **FIRE**, dan *analytics* yang menyatukan data bank, vendor, serta intelijen ancaman. ([Financial Stability Board](#))

Mengapa tren ini penting untuk sektor perbankan?

- **Biaya kepatuhan turun.** Otomasi *reporting* dan *monitoring* mengurangi jam kerja manual dan *error*.
- **Kecepatan respons naik.** Deteksi anomali lebih dini → *fraud* tertahan, dampak insiden menyusut.
- **Transparansi meningkat.** Format laporan yang seragam (mis. **FIRE**) memudahkan komunikasi dengan pengawas lintas negara. ([Financial Stability Board](#))
- **Iklim inovasi aman.** *Sandbox* memungkinkan uji produk baru tanpa membahayakan nasabah. Inggris menunjukkan konsistensi dukungan melalui *digital sandbox* dan program AI. ([FCA](#))

Pola implementasi yang terlihat efektif

- **Standarisasi dulu, teknologi kemudian.** Uni Eropa menetapkan target ketahanan lewat **DORA**, baru mendorong alat *suptech/regtech* untuk memenuhi kewajiban itu. Hasilnya: tujuan jelas, metrik jelas. ([eiopa.europa.eu](#))
- **Kolaborasi data yang terkendali.** **COSMIC** menunjukkan *data sharing* bisa dilakukan dengan *governance* ketat, sasaran spesifik (AML/CFT), dan peserta yang jelas. ([Ministry of Finance](#))
- **Ruang eksperimen yang nyata.** *Sandbox* FCA menunjukkan akses *dataset* + pendampingan regulator mendorong produk lolos ke pasar dan mendapat pendanaan lanjut. ([FCA](#))
- **Pengawasan berbasis analitik.** BIS mendorong *suptech* yang menggabungkan data multi-sumber untuk *early warning* dan *risk scoring* harian. Ini membuat pengawasan **proaktif**, bukan reaktif. ([Bank for International Settlements](#))

Apa artinya untuk Indonesia dan OJK?

- **Adopsi format global.** Pakai **FIRE** sebagai skema pelaporan insiden nasional (bank, *fintech*, dan vendor kritikal). Ini mempercepat koordinasi dan kurangi beban pelaporan ganda. ([Financial Stability Board](#))
- **Targetkan ketahanan operasional.** Ambil pelajaran **DORA**: tetapkan kewajiban *resilience testing*, *ICT third-party risk management*, dan *incident reporting* dengan SLA tegas. ([eiopa.europa.eu](#))
- **Bangun *suptech* OJK yang modular.** Mulai dari *dashboards* MTTD/MTTR, kepatuhan **FIRE**, konsentrasi *cloud/core* kritikal, dan *threat intel* terintegrasi; lalu dikembangkan bertahap. (Sejalan arah BIS/FSI). ([Bank for International Settlements](#))
- **Sediakan *regulatory sandbox* bertema prioritas.** Misal: *AML analytics*, *secure open finance*, dan *cyber fraud prevention*. Rujuk praktik FCA agar eksperimen aman dan berdaya guna. ([FCA](#))
- **Dorong *shared utilities*.** Teladani **COSMIC** untuk case AML/CFT: *utility* berbagi sinyal risiko nasabah berisiko tinggi, dengan *consent* dan *governance* kuat. ([Ministry of Finance](#))

Ringkasan

- **RegTech** memotong biaya, **SupTech** menaikkan ketajaman pengawasan. Keduanya membentuk **infrastruktur kepercayaan** di era digital. ([Bank for International Settlements](#))
- **Standar global sudah ada: FIRE** untuk pelaporan insiden dan **DORA** untuk ketahanan digital. Tinggal dibawa ke konteks Indonesia. ([Financial Stability Board](#))
- **Arah aksi:** standarkan data, sediakan *sandbox*, bangun *suptech* modular, dan kembangkan *shared utilities* seperti **COSMIC** untuk area prioritas. ([Ministry of Finance](#))

Integrasi Keamanan, Kepatuhan, dan Tata Kelola Data

Di era perbankan digital, tiga hal ini **tidak bisa lagi dipisah: keamanan informasi, kepatuhan, dan tata kelola data**. Jika dipisah, biaya membengkak, respons lambat, dan risiko bocor ke mana-mana. Jika **diintegrasikan**, bank dapat **patuh lebih cepat, aman lebih kuat, dan mengambil keputusan berbasis data** dengan percaya diri.

Tren global mengarah ke penyatuan fungsi. **Uni Eropa** melalui **DORA** mewajibkan ketahanan operasional digital menyeluruh—termasuk **pengawasan critical ICT third-party** dan pelaporan insiden seragam lintas lembaga. Intinya: *security, compliance, dan third-party governance* harus **jalan bareng** di *day-to-day operations*. Mulai **17 Januari 2025**, aturan ini berlaku penuh. (esma.europa.eu)

Di tingkat standar teknis, **NIST CSF 2.0 (Feb 2024)** menambahkan penekanan kuat pada **fungsi Govern (Governance)**—menautkan manajemen risiko siber ke **tujuan bisnis, peran, dan akuntabilitas**. Artinya, *security* bukan lagi proyek TI; ia bagian dari tata kelola perusahaan dan pengambilan keputusan. ([NIST Technical Series Publications](#))

Di area privasi, **ISO/IEC 27701** (kerangka *privacy information management*) dipakai berdampingan dengan **ISO/IEC 27001** agar **kontrol keamanan** dan **kewajiban privasi nyambung**—dari *data inventory* sampai *consent* dan *data subject rights*. Versi **27701:2025** baru saja dirilis, menegaskan kembali pentingnya akuntabilitas privasi yang **terukur**. ([ISO](#))

Regulator Asia menuntut hal serupa. **MAS Singapore TRM** mengikat **technology risk governance, incident response, dan risiko pihak ketiga** dalam satu rangka. Saat terjadi gangguan serius, MAS dapat **memberi sanksi operasional dan modal**—contohnya kasus **DBS** yang dipaksa meningkatkan ketahanan dan menanggung *capital add-on* untuk risiko operasional. **Pesan besarnya**: tata kelola + kepatuhan + keamanan = **kesiapan bisnis**. ([Ministry of Finance](#))

Kenapa integrasi ini penting untuk bank?

- **Cepat patuh, cepat pulih.** Satu *control set* untuk **PDP/privasi, keamanan siber, dan risiko operasional** mengurangi duplikasi kerja dan mempercepat *remediation*. (DORA: *one framework* untuk ketahanan digital + pihak ketiga). (esma.europa.eu)
- **Akuntabilitas jelas.** Dengan *Govern* (NIST CSF 2.0), **peran & KPI** tertaut ke bisnis: dari **MTTD/MTTR** sampai **SLA pelaporan insiden**. Tidak ada lagi “ini urusan TI saja”. ([NIST Technical Series Publications](#))
- **Privasi menyatu dengan keamanan.** **ISO 27001 + 27701** menjembatani *access control* dengan **kewajiban PDP** (mis. dasar hukum pemrosesan, *consent, retention*). Hasilnya: **data bisa dipakai dengan aman dan patuh**. ([ISMS.online](#))
- **Risiko vendor terkendali.** Basel Committee mengeluarkan **prinsip manajemen third-party risk** dan **operational resilience**. Tujuannya: tahu ketergantungan, batasi konsentrasi, siapkan *exit plan*. ([Bank for International Settlements](#))

Cara praktis mengintegrasikan tiga domain (versi “langsung jalan”)

1. **Satu *policy stack*, tiga lensa.** Tulis kebijakan terpadu yang mengikat **keamanan (ISO 27001/NIST CSF)**, **privasi (ISO 27701/PDP)**, dan **operational resilience (DORA/Basel)**. Hindari *policy* terpisah yang saling tumpang-tindih. ([NIST Technical Series Publications](#))
2. ***Data governance by design*.** Bangun **data catalog** dan **data lineage**; tandai **PII** dan **critical data elements**. Hubungkan ke **kontrol akses**, **retention otomatis**, dan **consent ledger**. Praktik ini memudahkan audit PDP dan *breach response*. (ISO 27701 menuntut akuntabilitas PII). ([ISO](#))
3. ***Unified control mapping*.** Map kontrol **NIST CSF 2.0** ke **ISO 27001 Annex** dan **ISO 27701**. Satu kontrol, banyak bukti (*single evidence*). Kurangi *audit fatigue* dan percepat *regulatory response*. ([NIST Technical Series Publications](#))
4. ***Third-party governance* ketat.** Terapkan **pre-contract risk assessment**, **hak audit**, **pemantauan SLA**, dan **rencana keluar** untuk *cloud/core*. Ini sejalan DORA (pengawasan *critical ICT third-party*) dan Basel TPRM. ([esma.europa.eu](#))
5. ***SupTech-ready reporting*.** Siapkan **skema data pelaporan insiden** yang konsisten, *machine-readable*, dan *near real-time* agar mudah diproses pengawas. (DORA dan praktik MAS menunjukkan pelaporan cepat berujung pada **pemulihan lebih cepat dan disiplin pasar**). ([esma.europa.eu](#))

Contoh *metrics* yang menyatukan tiga dunia

- **MTTD/MTTR** (keamanan → ketahanan operasi).
- **Data loss rate & consent breach rate** (privasi → kepatuhan).
- **Kepatuhan SLA pelaporan** (kepatuhan → *suptech*).
- **Vendor concentration index** dan **hasil uji ketahanan (TLPT/DORA)** (tata kelola pihak ketiga → stabilitas). ([esma.europa.eu](#))

Relevansi untuk Indonesia & OJK CyberTrust

- **Tarik garis merah:** jadikan **rating keamanan & privasi** sebagai **komponen profil risiko bank**—selaras dengan **Basel operational resilience** dan praktik DORA. ([Bank for International Settlements](#))
- **Sinkronkan standar:** adopsi **NIST CSF 2.0 (fungsi Govern)** dan **ISO 27001/27701** sebagai **rujukan kontrol** di industri. Bank cukup *map* satu kali untuk beberapa kewajiban. ([NIST Technical Series Publications](#))
- **Dorong *third-party oversight*:** tetapkan *playbook* nasional untuk vendor kritikal (audit, exit, concentration cap). Ini penting di lanskap *cloud/core* yang terkonsentrasi. ([esma.europa.eu](#))

Ringkasan

- **Integrasi = efisiensi + ketahanan + kepercayaan.** Pisah-pisah fungsi itu mahal dan lambat.
- **Acuan global sudah jelas:** **DORA** (ketahanan & vendor), **NIST CSF 2.0** (fungsi Govern), **ISO 27001/27701** (keamanan + privasi), **Basel TPRM/operational**

resilience (tata kelola). Tinggal **ditarik ke praktik harian bank Indonesia**.
(esma.europa.eu)

Bagian II — Landasan Regulasi dan Standar

Bab 4: Dasar Hukum Nasional

UU No. 27 Tahun 2022 tentang Pelindungan Data Pribadi

UU PDP adalah “pagar utama” bagi data nasabah di Indonesia. Tujuannya jelas: **melindungi hak privasi**, memastikan **pemrosesan data yang tertib**, dan **menjaga kepercayaan** publik ke industri jasa keuangan. Sejak masa transisi berakhir **17 Oktober 2024**, semua pengendali dan prosesor data wajib **patuh penuh**. Bank dan pelaku *BFSI* tidak punya ruang abu-abu lagi. ([DLA Piper Data Protection](#))

Kenapa penting untuk bank? Karena data nasabah adalah “bahan bakar” bisnis. Salah kelola bukan hanya berujung denda. Yang paling mahal hilang adalah **kepercayaan**. UU PDP meletakkan standar minimum agar *customer trust* tetap tinggi dan stabil. (Secara konsep, UU ini banyak mengacu pada *GDPR* Eropa, jadi standar mainnya tinggi). ([Semantic Scholar](#))

5 hal kunci UU PDP untuk sektor perbankan

1. **Dasar hukum & hak nasabah (data subject rights).** Nasabah berhak tahu, mengakses, mengoreksi, membatasi, menolak, hingga meminta **penghapusan data**. Bank wajib punya mekanisme layanan hak-hak tersebut dan **mencatat aktivitas pemrosesan data** (*records of processing activities/ROPA*). ([Semantic Scholar](#))
2. **Waktu emas 3×24 jam bila ada insiden.** Jika terjadi **kegagalan pelindungan data** (*data breach*), bank **wajib memberi notifikasi tertulis paling lambat 3×24 jam** kepada **subjek data** dan **lembaga PDP** (selama lembaga belum berdiri, diarahkan ke kementerian yang berwenang). Untuk kasus yang berdampak luas, **wajib umumkan ke publik**. **Konten notifikasi** minimal: jenis data terdampak, kapan & bagaimana terjadi, serta langkah pemulihan. Ini *game-changer* untuk disiplin respons insiden di industri. ([ABNR - Counsellors at Law](#))
3. **Menunjuk Data Protection Officer (DPO).** Bank wajib menunjuk **pejabat/petugas pelindungan data** jika memproses data untuk **pelayanan publik**, melakukan **pemantauan sistematis skala besar**, atau memproses **data spesifik/berkaitan tindak pidana**. Putusan MK 2025 menegaskan tafsir yang **memperluas kewajiban** (pemenuhan **salah satu** kondisi sudah cukup). Praktiknya, hampir semua bank akan **masuk kriteria** ini. ([Mahkamah Konstitusi RI](#))
4. **Sanksi tegas & beban kepatuhan.** Ada **sanksi administratif** bertingkat, hingga **denda maksimal 2% dari pendapatan tahunan** perusahaan, selain **pidana** untuk pelanggaran serius (mis. mengungkapkan/menjual data tanpa hak). Artinya, biaya gagal patuh bisa “menggerus” laba, belum termasuk **ganti rugi** ke nasabah. ([denslawfirm.com](#))
5. **Selaras standar global.** Banyak prinsip UU PDP “satu frekuensi” dengan *GDPR* (hak akses, *erasure*, *lawful basis*, akuntabilitas). Ini memudahkan **kolaborasi lintas negara** dan **arus data** yang aman, sekaligus menaikkan *bar* tata kelola data perbankan Indonesia ke **kelas dunia**. ([Semantic Scholar](#))

Dampaknya bagi manajemen risiko bank

- **Risiko operasional turun** bila kontrol jalan: *data minimization, access control, enkripsi, monitoring, backup, incident response*.
- **Risiko reputasi** terkelola karena bank **proaktif**: ada *playbook 3×24 jam, root cause analysis*, dan perbaikan berkelanjutan.
- **Risiko regulasi** lebih terkendali: ada DPO, *ROPA, privacy impact assessment*, dan bukti kepatuhan yang rapi untuk OJK/otoritas.
- **Risiko litigasi** ditekan: *early notification* + remedi yang jelas = menurunkan peluang gugatan kolektif.

Intinya: kepatuhan PDP bukan *cost center* semata—ini **strategic risk hedge**.

Checklist praktis (versi singkat) untuk bank

- **Governance**. Tetapkan **DPO** dan *privacy steering committee*; pastikan mandat, wewenang, *reporting line* jelas. ([PwC](#))
- **Inventaris data & ROPA**. Peta aliran data end-to-end, siapa *controller/processor*, dasar pemrosesan, lokasi penyimpanan (*on-prem/cloud*). ([DLA Piper Data Protection](#))
- **Hak nasabah**. Buat **portal/self-service** untuk akses, koreksi, *withdraw consent, erasure*—target layanan ≤ **3×24 jam** sesuai ketentuan waktu layanan di UU PDP untuk beberapa hak. ([Hukum Online](#))
- **Incident readiness**. Susun **SOP notifikasi 3×24 jam**: *who/what/when/how* + *playbook* komunikasi publik untuk skenario berdampak sistemik. ([ABNR - Counsellors at Law](#))
- **Bukti kepatuhan**. Simpan *audit trail, training log, vendor due diligence, DPIA*, dan *testing* berkala (mis. *table-top exercise*).
- **Sanksi & controls**. Map pasal ke kontrol internal; *stress test* potensi denda **2% revenue** agar manajemen paham **risk exposure**. ([denslawfirm.com](#))

Apa artinya untuk “OJK CyberTrust & Data Privacy Ranking Framework”?

- **Metode skoring** dapat mengangkat **indikator taat UU PDP** sebagai *leading indicator* kepercayaan digital: ada DPO, ROPA, SLA hak nasabah, *breach drill 3×24 jam*, dan *closure* temuan. ([ABNR - Counsellors at Law](#))
- **Harmonisasi global**. Karena UU PDP seirama dengan *GDPR*, bank lokal yang patuh akan **lebih dipercaya** investor dan mitra internasional. ([Semantic Scholar](#))

Ringkasan

- **UU PDP = standar wajib** untuk melindungi data nasabah dan menjaga **digital trust**.
- **Deadline patuh sudah lewat**: per 17 Okt 2024, **semua** pelaku harus *compliant*. ([DLA Piper Data Protection](#))
- **Kunci eksekusi**: DPO aktif, *ROPA* rapi, layanan hak nasabah cepat, **notifikasi 3×24 jam**, dan kontrol teknis-organisasional yang hidup. ([ABNR - Counsellors at Law](#))

- **Risiko gagal patuh mahal:** denda **hingga 2% pendapatan tahunan**, potensi pidana, dan—yang paling mahal—hilangnya **kepercayaan**. (denslawfirm.com)

POJK No. 38/POJK.03/2016 tentang Manajemen Risiko TI

Teknologi informasi (TI) sekarang adalah “urat nadi” bank. Layanan, transaksi, dan data nasabah semua bergantung pada TI. Karena itu, **risiko TI = risiko bisnis**. POJK 38/2016 hadir sebagai *rulebook* agar bank **mengenali, mengukur, memantau, dan mengendalikan** risiko TI secara sistematis. Aturannya resmi, berlaku nasional, dan jadi acuan audit OJK. ([OJK](https://www.ojk.go.id))

Inti aturannya apa saja?

1. **Tata kelola & tone at the top.** Dewan Komisaris dan Direksi wajib menetapkan arah, kebijakan, dan akuntabilitas risiko TI. Tanggung jawab tidak bisa didelegasikan penuh ke unit TI. **Keamanan dan keandalan sistem adalah mandat manajemen puncak.** ([OJK](https://www.ojk.go.id))
2. **Kebijakan, standar, dan prosedur TI.** Bank harus punya dokumen yang jelas: klasifikasi informasi, *access control*, *change management*, *capacity planning*, *backup–restore*, *patching*, dan *vendor management*. Panduan rinci teknis–operasionalnya dijabarkan dalam **SEOJK 21/SEOJK.03/2017** (pelaksanaan POJK 38). ([OJK](https://www.ojk.go.id))
3. **Manajemen siklus hidup sistem.** Dari perencanaan, pengembangan, *testing*, hingga operasional dan *retirement*. Termasuk pengamanan aplikasi inti (*core banking*), jaringan, pusat data, dan *disaster recovery*. **Kontrol harus dibuktikan, bukan sekadar ada di atas kertas.** ([OJK](https://www.ojk.go.id))
4. **Incident response & business continuity.** Bank wajib punya *playbook* respons insiden dan rencana keberlangsungan bisnis (*BCP/DRP*), dengan *drill* berkala. Targetnya: **waktu pulih cepat** dan **dampak ke nasabah minimal**. ([OJK](https://www.ojk.go.id))
5. **Pengawasan pihak ketiga (*third-party risk*).** Jika memakai *cloud*, *switching*, *managed service*, atau *SaaS*, maka kontrak, SLA, lokasi data, kontrol keamanan, dan hak audit **harus jelas**. Risiko dari vendor adalah risiko bank. ([OJK](https://www.ojk.go.id))

Hubungan POJK 38/2016 dengan regulasi TI terbaru

Pada **2022**, OJK menerbitkan **POJK 11/POJK.03/2022 tentang Penyelenggaraan TI oleh Bank Umum**. Regulasi ini memperkuat *governance*, arsitektur, dan *lifecycle* TI yang sehat—selaras dan melengkapi disiplin manajemen risiko di POJK 38/2016. Bagi bank, artinya *bar* kepatuhan TI **semakin tinggi** dan **lebih terintegrasi**. ([OJK](https://www.ojk.go.id))

Konteks global: standar dan praktik baik

- Arah POJK 38/2016 sejalan dengan praktik global seperti *IT risk management* yang mewajibkan ***governance* kuat, kontrol teknis, dan *resilience***. Di banyak yurisdiksi, regulator mendorong penguatan TI pasca lonjakan serangan siber dan *outsourcing*

ke *cloud*. Indonesia mengikuti arus ini dengan kerangka yang makin ketat (lihat penguatan 2022). ([OJK](#))

Apa dampak praktisnya ke bank?

- **Lebih tahan gangguan.** Sistem inti dan kanal digital punya *redundancy* dan *failover*.
- **Lebih siap insiden.** Ada *early warning*, *war room*, dan *table-top exercise*.
- **Lebih tertib vendor.** *Due diligence*, penilaian keamanan, dan hak audit menjadi standar.
- **Lebih akuntabel.** Direksi–Komisaris memantau metrik risiko TI secara rutin. Semua ini memotong **risiko operasional**, **risiko hukum**, dan **risiko reputasi**.

Quick wins yang bisa dieksekusi

- Tetapkan **risk appetite** TI dan *dashboard* ke Direksi (bulanan/kuartalan). ([OJK](#))
- Perbarui kebijakan TI sesuai SEOJK 21/2017; *gap analysis* → *action plan*. ([OJK](#))
- Uji BCP/DRP minimal tahunan: *backup restore test*, *switch-over DC–DRC*. ([OJK](#))
- Audit vendor kritikal: keamanan, lokasi data, SLA, *exit plan*. ([OJK](#))
- Latih tim respons insiden: *phishing drill*, *ransomware tabletop*, dan *post-mortem* terukur. ([OJK](#))

Ringkasnya

- POJK 38/2016 adalah dasar “*risk-by-design*” untuk TI perbankan—mewajibkan *governance*, kontrol, dan *resilience* yang nyata. ([OJK](#))
- SEOJK 21/2017 memberi panduan teknis agar kebijakan berubah jadi praktik harian. ([OJK](#))
- POJK 11/2022 memperkuat penyelenggaraan TI secara menyeluruh, menaikkan standar industri. ([OJK](#))

Peraturan BSSN No. 8/2020 tentang Strategi Keamanan Siber Nasional

Keamanan siber kini menyatu dengan **stabilitas keuangan**. Gangguan ke *core banking*, *payment switch*, atau *channel* digital bisa merambat ke likuiditas, layanan nasabah, reputasi, bahkan kepercayaan publik. **BSSN No. 8/2020** mendorong semua *penyelenggara sistem elektronik*—termasuk sektor keuangan—untuk menerapkan *sistem pengamanan informasi* yang terukur dan terdokumentasi (kerangka *SMPI*), baik di lingkup publik maupun privat. Ini menjadi “fondasi nasional” yang melengkapi aturan spesifik perbankan dari OJK.

([Peraturan.go.id](https://peraturan.go.id))

Intinya untuk bank: keamanan siber bukan proyek IT saja. Ia adalah **fungsi manajemen risiko perusahaan**. Dan ia wajib punya bukti: kebijakan, proses, kontrol, *monitoring*, dan pelaporan yang konsisten.

Apa yang diatur BSSN 8/2020 (yang relevan bagi perbankan)?

- **Kewajiban *risk-based security*.** Pengamanan harus berbasis klasifikasi aset dan risiko. Aset paling kritikal—*core banking*, *payment*, *KMS/HSM*, *API*—harus prioritas. ([Peraturan.go.id](https://peraturan.go.id))
- **Penerapan *Sistem Manajemen Pengamanan Informasi (SMPI)*.** Ada siklus *plan–do–check–act*, audit berkala, dan *continuous improvement*. Bukti kontrol harus terdokumentasi. ([Scribd](https://scribd.com))
- **Cakupan publik dan privat.** Bank sebagai *penyelenggara sistem elektronik* wajib memastikan pengamanan juga melekat pada pihak ketiga: *cloud*, *switch*, *fintech partner*, dan *outsourcer*. ([Peraturan.go.id](https://peraturan.go.id))

Terjemahan praktis untuk bank: petakan aset kritikal, ukur risikonya, terapkan kontrol, uji pemulihan, dan laporkan kemajuan secara periodik. Jangan hanya *checklist*—buktikan efektivitasnya.

Sinkron dengan aturan OJK

BSSN 8/2020 menjadi *payung nasional*. Di sisi sektor, **POJK 38/2016** dan **SEOJK 21/2017** sudah mewajibkan **manajemen risiko TI** untuk bank: tata kelola, pengamanan, *BCP/DRP*, pengelolaan pihak ketiga, dan *incident response*. Keduanya selaras: BSSN menetapkan kerangka nasional, OJK menurunkan kontrol sektoral dan pengawasan *safety & soundness*. ([Peraturan BPK](https://peraturan.bpk.go.id))

Maknanya: bukti kepatuhan bank harus “klik” di dua sisi—dokumen dan praktik lapangan—sehingga **rating siber & privasi** (mis. *CyberTrust/Data Privacy Ranking*) dapat diintegrasikan ke **profil risiko** bank.

Posisi Indonesia vs praktik global

- **Uni Eropa.** Sektor finansial menerapkan *Digital Operational Resilience Act (DORA)* dan *NIS2* untuk ketahanan operasional TIK, uji ketangguhan (*threat-led testing*), pelaporan insiden cepat, dan pengawasan *critical third-party ICT*. Ini menegaskan *end-to-end resilience* dari bank sampai rantai pasok teknologi. ([Finance](https://finance))

- **Standar internasional sektor keuangan.** *Guidance on Cyber Resilience for FMI*s (CPMI–IOSCO/BIS) menuntut identifikasi aset, ketergantungan eksternal, *response & recovery* yang teruji, serta koordinasi ekosistem. Prinsip ini relevan untuk RTGS, *clearing*, dan *securities depository*. ([Bank for International Settlements](#))
- **Regulator lain bergerak.** Laporan *Federal Reserve* 2024 menempatkan siber sebagai risiko sistemik dan memasukkan *cyber* ke pengawasan rutin; RBI India menegaskan *operational resilience* dan kontrol *outsourcing* TI lintas industri keuangan; ECB baru-baru ini melakukan **cyber stress test** dan menemukan *shortcomings* kesiapan pemulihan bank Eropa. ([Federal Reserve](#))

Kesimpulan global: tren dunia adalah **ketahanan operasional digital** (*digital operational resilience*), bukan sekadar pencegahan insiden. Fokusnya: *recover fast, recover safely*, termasuk saat vendor gagal.

Apa yang perlu dilakukan bank (versi cepat dan praktis)?

- **Satukan keamanan–kepatuhan–tata kelola data.** Bentuk *data governance council* yang menyatukan CISO, DPO, *risk*, dan bisnis. **Tujuan:** satu peta risiko untuk teknologi dan data nasabah.
- **Buktikan kontrol yang hidup.** Jangan hanya SOP. Lakukan *tabletop exercise*, *red team*, dan uji *failover* lintas *data center* minimal tahunan.
- **Kelola vendor secara ketat.** Terapkan *pre-contract due diligence*, kewajiban *right to audit*, *incident SLAs*, dan *exit plan* untuk *cloud* atau *critical SaaS*. Ini juga roh DORA/NIS2. ([Finance](#))
- **Percepat deteksi & pelaporan insiden.** Waktu respons adalah mata uang kepercayaan. Adopsi *playbook* pelaporan yang konsisten dengan BSSN dan OJK. ([Peraturan.go.id](#))
- **Siapkan *metrics* untuk pengawasan.** Gunakan KPI seperti *mean time to recover (MTTR)*, tingkat *patch compliance*, persentase *critical control coverage*, dan *vendor risk score*. Ini memudahkan integrasi ke *risk appetite* dan **rating**.

Kenapa ini krusial untuk CyberTrust & Data Privacy Ranking?

- BSSN 8/2020 memberi kerangka minimal nasional.
- OJK memberi kewajiban sektoral dan pengawasan.
- Standar global memberi tolok ukur ketahanan.

Jika tiga lapis ini dipadukan, **rating siber & privasi** menjadi objektif dan dapat dibandingkan antar bank. Bank dengan kontrol kuat, *recovery* cepat, dan pengelolaan vendor yang rapi akan **naik rating**. Dampaknya nyata: **kepercayaan nasabah** meningkat, **biaya modal** berpotensi turun, dan **risiko sistemik** menurun.

Titik tekan yang perlu di-bold dalam komunikasi internal

- **BSSN 8/2020 = fondasi keamanan nasional** untuk semua penyelenggara sistem elektronik, termasuk bank. ([Peraturan.go.id](#))
- **POJK 38/2016 & SEOJK 21/2017 = kewajiban sektoral** manajemen risiko TI perbankan. ([Peraturan BPK](#))

- **DORA/NIS2, BIS–CPMI/IOSCO, Fed/ECB/RBI = referensi global** menuju *digital operational resilience*. ([Finance](#))

Pesan kunci: patuh saja tidak cukup. Bank harus **tangguh**, bisa **pulih cepat**, dan bisa **membuktikannya** dengan data.

Bab 5: Keterkaitan dengan Standar Internasional

ISO/IEC 27001, NIST Cybersecurity Framework

Di dunia perbankan, keamanan bukan sekadar *IT issue*. Ia adalah **bisnis inti**. Dua rujukan global yang paling sering dipakai adalah **ISO/IEC 27001** dan **NIST CSF**. ISO/IEC 27001 menata **sistem manajemen keamanan informasi** atau *Information Security Management System (ISMS)*—cara kerja menyeluruh untuk mengelola risiko, kebijakan, peran, dan *controls*. Sementara NIST CSF memberi **kerangka praktik teknis–operasional** yang konkret untuk mencegah, mendeteksi, dan merespons serangan siber. Keduanya saling menguatkan: **ISO = governance & management system**, **NIST CSF = technical-operational playbook**.

ISO/IEC 27001 — pondasi tata kelola keamanan

Inti ISO/IEC 27001: membangun ISMS yang **terukur** dan **berkelanjutan** (*continuous improvement*). Organisasi menetapkan ruang lingkup, menilai risiko, memilih *controls*, menjalankan, memantau, lalu meningkatkan. Sertifikasi pihak ketiga membuat disiplin ini **terverifikasi** dan dapat diaudit. Bagi bank, ini berarti **kepastian proses**: dari kebijakan *access control* hingga *incident management*—semua terdokumentasi dan diuji.

Apa dampaknya ke dunia bank/finance?

- **Konsistensi**: proses yang rapi lintas cabang, vendor, dan *cloud*.
- **Akuntabilitas**: peran jelas—*board*, manajemen risiko, CISO, *first line*.
- **Audit-ready**: memudahkan pembuktian kepatuhan ke regulator dan investor.

NIST CSF — kompas operasi siber harian

NIST CSF 2.0 menyederhanakan praktik siber ke **enam fungsi**: **Govern, Identify, Protect, Detect, Respond, Recover**. Dengan bahasa yang mudah dipraktekkan, bank dapat memetakan kemampuan, menutup *gap*, dan mengukur kemajuan secara rutin. Versi 2.0 menegaskan **fungsi “Govern”** di level tata kelola—menjadikan siber sebagai **risiko bisnis**, bukan urusan *IT* semata.

Apa dampaknya ke dunia bank/finance?

- **Pemetaan cepat**: dari *endpoint* hingga *core banking*, dari *API* hingga *SOC*.
- **Prioritas jelas**: kontrol yang paling penting untuk mencegah gangguan layanan.
- **Latihan insiden**: *playbook* respons dan pemulihan agar operasional tetap jalan.

ISO vs NIST? Bukan “pilih salah satu”, tapi pakai bersama

- **ISO/IEC 27001** menjawab “*bagaimana kita mengatur dan membuktikan*” melalui ISMS dan siklus *Plan–Do–Check–Act*.

- **NIST CSF** menjawab “*apa yang harus kita lakukan di lapangan*” lewat fungsi, kategori, dan *outcomes* yang operasional.

Banyak organisasi **menggabungkan**: ISO untuk **kerangka manajemen** dan audit sertifikasi; NIST CSF untuk **panduan teknis–operasional harian** serta *gap analysis* berkala. (NIST menegaskan struktur fungsi CSF 2.0 yang praktis; ISO menegaskan nilai ISMS dan sertifikasi yang diakui global).

Cara praktis menerapkannya di bank (ringkas dan menantang)

1. **Tetapkan “single source of truth”** Pakai **ISO/IEC 27001** sebagai *backbone* ISMS: kebijakan, risiko, peran, dan *metrics*. **Target**: *board* menandatangani *risk appetite* siber yang terukur.
2. **Bangun control library operasional** Turunkan kebijakan ISO ke kontrol operasional memakai **NIST CSF 2.0** (Govern–Identify–Protect–Detect–Respond–Recover). **Target**: peta kontrol per sistem—*core banking, mobile, internet banking, ATM, API*.
3. **Ukur kematangan, tutup gap** Lakukan *self-assessment* NIST CSF per kuartal. Kaitkan temuan ke **risiko bisnis** di ISMS. **Target**: *time-to-detect* turun, *time-to-recover* turun, dan *loss expectancy* terkendali.
4. **Latihan insiden dan tabletop** Simulasikan serangan *ransomware, account takeover, dan third-party breach*. Pastikan fungsi **Respond/Recover** berjalan. **Target**: *RPO/RTO* tercapai, layanan prioritas selalu pulih duluan.
5. **Audit & sertifikasi** Kejar **sertifikasi ISO/IEC 27001** untuk *trust* eksternal. Gunakan hasil *assessment* NIST sebagai bukti perbaikan berkelanjutan saat audit. **Target**: bukti *continuous improvement* yang kuat.

Pesan kunci untuk eksekutif bank

- **Bold move**: **ISO/IEC 27001** memberi **legitimasi dan disiplin** manajemen; **NIST CSF** memberi **kecepatan dan kejelasan eksekusi**.
- **Manfaat finansial nyata**: lebih sedikit insiden, waktu henti lebih singkat, biaya pemulihan turun, kepercayaan nasabah naik.
- **Kesiapan regulator**: struktur CSF 2.0 memudahkan dialog risiko dengan dewan dan pengawas; sertifikasi ISO membantu kredibilitas di mata pasar dan investor.

Ringkasnya

- **ISO/IEC 27001 = tulang punggung governance** (ISMS, kebijakan, audit, sertifikasi).
- **NIST CSF 2.0 = panduan lapangan** (Govern–Identify–Protect–Detect–Respond–Recover).
- **Digabungkan**, keduanya membentuk **bahasa bersama** antara *board*, regulator, *risk*, dan *engineer*—mendorong *digital trust* yang langsung berdampak pada ketahanan operasional bank.

Basel III, IFRS, dan prinsip tata kelola GCG

Kepercayaan lahir dari tiga hal: **modal yang kuat (Basel III)**, **laporan yang jujur & transparan (IFRS)**, dan **tata kelola yang sehat (GCG)**. Jika tiga pilar ini konsisten, bank dipercaya. Jika satu rapuh, krisis bisa menjalar.

- **Basel III** menuntut bank punya bantalan modal yang cukup, likuiditas yang memadai, dan disiplin *leverage*. Tujuannya sederhana: saat pasar goyang, bank tetap berdiri. ([IFRS Foundation](#))
- **IFRS** memastikan pengakuan rugi kredit lebih dini (*expected credit loss* di IFRS 9) dan pengungkapan risiko likuiditas/credit risk yang jelas (IFRS 7). Hasilnya: laporan lebih *forward-looking*, bukan reaktif. ([IFRS Foundation](#))
- **GCG** (prinsip OECD/G20) menekankan akuntabilitas, transparansi, dan perlindungan pemangku kepentingan. Di bank, ini berarti *board* yang melek risiko digital dan pengawasan yang tegas. ([OECD](#))

Basel III — “sabuk pengaman” stabilitas

Basel III lahir dari krisis 2008. Regulasi ini memperketat kualitas modal, menambah *buffers*, dan mengenalkan dua metrik likuiditas:

- **LCR (Liquidity Coverage Ratio)**: bank wajib punya aset likuid berkualitas tinggi untuk menahan tekanan 30 hari. **Intinya: tahan napas sebulan tanpa panik.** ([bis.org](#))
- **NSFR (Net Stable Funding Ratio)**: struktur pendanaan harus stabil untuk horizon setahun. **Tidak boleh hidup dari dana “mudah cabut”.** ([IFRS Foundation](#))
- **Finalisasi Basel III** juga merapikan risiko kredit & operasional agar ukuran modal lebih mencerminkan risiko sebenarnya. **Tujuannya: modal tidak “tipis semu”.** ([bis.org](#))

Mengapa relevan ke *cyber*? Gangguan TI besar bisa jadi *liquidity event* (nasabah *rush* digital). LCR/NSFR memberi waktu bagi bank dan regulator untuk menstabilkan situasi—asal tata kelola insiden rapi.

IFRS — “bahasa keuangan” yang *forward-looking*

IFRS membuat laporan bank **lebih jujur dan lebih cepat merespons risiko**:

- **IFRS 9 – Expected Credit Loss (ECL)**: rugi kredit dihitung berbasis ekspektasi ke depan, bukan menunggu *default*. Ini terbukti mempercepat pengakuan kerugian dibanding model lama. **Transparansi naik, kejutan turun.** ([IFRS Foundation](#))
- **IFRS 7 – Risk Disclosures**: mewajibkan *maturity analysis*, kebijakan manajemen likuiditas, dan paparan risiko pasar/kredit. **Investor bisa “melihat” di mana rapuhnya.** ([IFRS Foundation](#))

Kaitannya dengan *cyber*? Data kebocoran dan *downtime* bisa memicu lonjakan *ECL* (fraud, *forbearance*), sementara pengungkapan IFRS 7 menuntut cerita yang jelas soal ketahanan likuiditas saat insiden.

GCG — “otak dan nurani” organisasi

Prinsip **GCG** (transparansi, akuntabilitas, tanggung jawab, independensi, kewajaran) dalam panduan OECD/G20 adalah *payung* untuk semua risiko—termasuk digital:

- **Peran Dewan:** memastikan strategi risiko digital, *tone at the top*, dan *oversight* atas investasi keamanan data.
- **Hak Pemangku Kepentingan:** nasabah & investor berhak atas informasi yang jelas tentang insiden, perlindungan data, dan rencana pemulihan.
- **Transparansi:** laporan yang konsisten (IFRS), plus metrik operasional (insiden, *mean time to recover*, *patching cadence*) sebagai materi GCG modern. ([OECD](#))

Hasilnya: **digital trust** bukan hanya urusan CISO, tetapi mandat *board*. Keamanan data = kebijakan korporat, bukan proyek IT.

“Menjembatani” ke OJK CyberTrust & Data Privacy Ranking Framework

Agar mudah diadopsi industri, *ranking* nasional sebaiknya **menyatukan** tiga pilar ini:

- **Dari Basel III → CyberTrust**
 - *Signal* stabilitas: **hubungkan skor CyberTrust** dengan **penilaian profil risiko bank** (likuiditas, operasional). Insiden *cyber* besar harus tercermin sebagai *Pillar 2 add-on* atau *buffer* manajerial. ([bis.org](#))
- **Dari IFRS → CyberTrust**
 - Wajibkan **pengungkapan kuantitatif** dampak *cyber* ke **ECL** dan **likuiditas** (format mirip IFRS 7). Ini memudahkan pasar menilai *resilience*. ([IFRS Foundation](#))
- **Dari GCG → CyberTrust**
 - *Score uplift* bila **komite risiko/IT** aktif, *board* punya *cyber literacy*, dan *playbook* insiden diuji berkala. Standar acuan: prinsip OECD/G20. ([OECD](#))

Praktik internasional: pelajaran cepat

- **Eropa/UK:** pengawasan perbankan menautkan *operational resilience* ke modal & likuiditas. Laporan risiko operasional makin granular pasca finalisasi Basel III. ([bis.org](#))
- **Global accounting:** *post-implementation review* IFRS 9 menilai ECL memang mempercepat pengakuan rugi dan memperbaiki *loss provisioning*. ([IFRS Foundation](#))
- **Governance global:** pembaruan **OECD/G20 Principles (2023)** menekankan *sustainability & risk oversight*, termasuk risiko digital—relevan untuk bank yang makin digital. ([OECD](#))

Ringkasnya

- **Basel III = modal & likuiditas kuat** → penahan guncangan *cyber-induced run*. ([bis.org](#))

- **IFRS (9 & 7)** = laporan *forward-looking* dan pengungkapan risiko → pasar paham risiko digital dan dampaknya ke rugi kredit & likuiditas. ([IFRS Foundation](#))
- **GCG (OECD/G20)** = mandat *board* atas risiko digital → *tone at the top* untuk *privacy-by-design* dan *security-by-default*. ([OECD](#))
- **CyberTrust Ranking**: jadikan tiga standar ini **bahasa bersama**: skor yang tinggi = bank **aman, transparan, dan tertata**, bukan sekadar “lulus audit IT”.

Bab 6: Kewenangan OJK dalam Pengawasan Siber & Data Privacy

Penilaian risiko digital sebagai bagian dari stabilitas sistem keuangan

Keamanan siber kini bukan isu IT semata. Ia sudah masuk ranah stabilitas keuangan. Satu insiden besar bisa mengganggu layanan pembayaran, menekan likuiditas bank, dan memicu *loss of confidence*. Karena itu, penilaian risiko digital harus duduk sejajar dengan risiko kredit, pasar, dan likuiditas. IMF bahkan menempatkan risiko siber sebagai faktor yang dapat menular lintas lembaga dan negara. ([E-Library IMF](#))

Intinya sederhana: tanpa *digital trust*, biaya modal naik, biaya operasional membengkak, dan akses layanan terganggu. Dampaknya dirasakan nasabah, bank, dan pasar. Kerangka penilaian yang konsisten akan membantu OJK melihat potensi guncangan lebih dini, lalu bertindak cepat sebelum gangguan melebar ke sistem. FSB juga mendorong pelaporan insiden yang seragam agar otoritas bisa membaca pola dan mengambil tindakan terkoordinasi. ([IMF](#))

Mengapa wajib dinilai, bukan sekadar diawasi

- **Sifatnya sistemik.** Insiden siber besar bisa melompat antarlembaga lewat *interconnected systems* dan vendor bersama. Ini mempercepat transmisi risiko ke pasar uang dan pembayaran. IMF menekankan sifat *spillover* ini dalam analisis stabilitas keuangan global. ([E-Library IMF](#))
- **Eksposur meningkat.** Digitalisasi dan geopolitik menaikkan frekuensi dan *severity*. Tren global menunjukkan kerugian yang dilaporkan industri melonjak sejak 2020. Artinya, *loss distribution* makin “gemuk di ekor”. ([E-Library IMF](#))
- **Dampak nyata pada operasi kritikal.** Gangguan *core banking*, RTGS, atau *card switching* bisa memicu *cash hoarding* nasabah dan penarikan dana serentak—risiko likuiditas nyata. Basel Committee menempatkan ketangguhan operasional sebagai pilar yang langsung terkait kelangsungan fungsi kritikal bank. ([Bank for International Settlements](#))

Apa yang harus diukur dalam rating risiko digital (versi singkat)

- **Paparan (*exposure*):** aset TI kritikal, ketergantungan pada *cloud* dan vendor, jalur integrasi dengan lembaga lain.
- **Kerentanan (*vulnerability*):** *patching gap*, *identity & access*, enkripsi data, *backup/restore* teruji.
- **Kontrol (*controls effectiveness*):** SOC/MDR, *threat hunting*, *E2E monitoring*, dan *table-top exercise*.
- **Kepatuhan & kesiapsiagaan:** *incident response*, *mandatory reporting*, uji *crisis playbook* bersama otoritas. FSB mendorong konvergensi format pelaporan agar otoritas bisa membandingkan antar lembaga dan lintas negara. ([IMF](#))
- **Dampak ke stabilitas:** metrik *time-to-recovery*, *service availability*, dan *payment continuity*—langsung dihubungkan ke indikator pasar (likuiditas, *settlement risk*).

Cara memasukkan ke kerangka stabilitas (praktis dan *actionable*)

1. **Skor risiko digital** → **profil risiko bank**. Gabungkan skor dengan *ICAAP* dan *risk appetite*. Bank dengan skor rendah wajib menambah *capital buffer* operasional dan rencana perbaikan berjangka. Pedoman ketahanan operasional Basel memberi rambu penerapan ini. ([Bank for International Settlements](#))
2. **Systemically Important Functions (SIF)**. Petakan layanan yang “tak boleh jatuh” (pembayaran, kliring, KYC). Terapkan target *RTO/RPO* ketat dan uji serangan terarah (*threat-led testing*)—mengacu praktik Eropa/Inggris. ([protechtgroup.com](#))
3. **Cyber stress test**. Simulasikan skenario: serangan *ransomware* serentak ke 3 bank besar + gangguan *cloud region*. Ukur dampak ke likuiditas harian, *payment queue*, dan kebutuhan *intraday credit*. IMF menekankan pentingnya simulasi semacam ini untuk melihat efek *spillover*. ([E-Library IMF](#))
4. **Pelaporan insiden berstandar**. Gunakan taksonomi dan *data fields* FSB agar data insiden bisa dianalisis lintas bank/vendor, memudahkan *early warning* OJK dan koordinasi antara otoritas. ([IMF](#))
5. **Operational resilience dashboard**. Satukan indikator TI (uptime, *patch SLA*, *attack surface*) dengan indikator pasar (spread pendanaan, arus keluar dana ritel) untuk mendeteksi krisis kepercayaan dini.

Manfaat langsung bagi stabilitas

- **Menurunkan risiko contagion**. Kesenjangan kontrol di satu bank cepat terlihat dan bisa ditangani sebelum menular. IMF menilai peningkatan ketahanan siber akan memperkecil peluang gangguan sistemik. ([E-Library IMF](#))
- **Kepastian bagi pasar**. Adanya *rating* dan *disclosure* terukur menenangkan investor dan memperbaiki penetapan harga risiko.
- **Pengambilan keputusan berbasis data**. OJK dapat mengaitkan *rating* dengan pengawasan intensif, *P2SK* yang lebih presisi, hingga insentif GCG.

Tantangan yang perlu dijawab

- **Data kualitas tinggi**. Tanpa *data lineage* dan pelaporan insiden yang konsisten, *risk intelligence* akan bias. Di sini standar FSB membantu. ([IMF](#))
- **Ketertanggung vendor**. *Third-party risk* perlu *contractual control*, uji pemulihan bersama, dan *exit plan* untuk *cloud*. Prinsip Basel menuntut bank menjaga fungsi kritikal tetap berjalan meski pemasok terganggu. ([Bank for International Settlements](#))
- **Koordinasi lintas otoritas**. *Threat intel* perlu alur cepat antara OJK, BSSN, BI, dan pelaku industri agar respons bersifat *whole-of-system*.

Ajakan bertindak (ringkas)

- Tetapkan *digital risk rating* sebagai komponen resmi profil risiko bank.
- Lakukan *cyber stress test* minimal tahunan untuk fungsi pembayaran dan kliring.
- Terapkan pelaporan insiden berformat FSB dan *threat-led testing* bergaya TIBER/CBEST untuk bank sistemik. ([protechtgroup.com](#))
- Kaitkan peringkat dengan insentif dan *supervisory intensity*.

Dengan langkah-langkah ini, “penilaian risiko digital” bukan hanya *checklist* TI. Ia menjadi instrumen makroprudensial—menjaga kepercayaan, memastikan layanan esensial tetap hidup, dan meredam guncangan sebelum menjadi krisis. Itu inti stabilitas keuangan di era digital. ([E-Library IMF](#))

Integrasi hasil rating ke dalam *profil resiko bank*

Keamanan siber bukan isu IT. Ini isu **ketahanan operasional** dan **stabilitas bank**. Saat layanan digital terganggu, arus kas macet, nasabah panik, dan biaya pemulihan melonjak. Regulator dunia kini menilai *cyber posture* sebagai bagian dari **SREP/ICAAP** dan **modal risiko operasional**. Contoh: otoritas Singapura mengenakan **tambahan modal operasional (Pillar 2 add-on)** dan pembatasan perubahan IT pada bank yang berulang kali mengalami gangguan layanan digital. Tambahan modal itu bisa dicabut setelah bank membuktikan keandalan yang konsisten. ([The Wall Street Journal](#))

Intinya: **rating siber = sinyal risiko kuantitatif** yang harus “terkabel” ke risk appetite, modal, dan prioritas manajemen.

Prinsip global yang relevan (sebagai pagar tepi)

- **Operational resilience** jadi standar di banyak yurisdiksi; bank diminta mendesain, menguji, dan memulihkan *critical services* secara berkesinambungan. ([regulationtomorrow.com](#))
- **SREP di Eropa** memasukkan risiko TIK/keamanan ke penilaian pengawasan; hasilnya mempengaruhi tindakan pengawas dan kebutuhan perbaikan. ([asbasupervision.org](#))
- **DORA (Uni Eropa)** mewajibkan manajemen risiko TIK yang terukur, uji ketahanan, dan *third-party oversight*; pelanggaran dapat berujung tindakan pengawas, termasuk langkah kuantitatif. ([executiveitforums.org](#))
- **Pedoman EBA** tentang manajemen risiko TIK jadi referensi penilaian pengawas atas kontrol bank terhadap insiden, akses, dan perubahan. ([eba.europa.eu](#))
- **PRA/BoE** mengikat ketahanan operasional ke *impact tolerances* dan pengawasan berkelanjutan. ([riskxchange.co](#))

Cara teknis “menyambung” rating → profil risiko

1. Risk Appetite & KPI

- Tetapkan *risk appetite* digital berdasarkan **rating** (mis. target $\geq A$).
- Kaitkan ke **KRI**: *mean time to recover (MTTR)* layanan kritikal, jumlah *severe incidents*, tingkat *phishing click*, *patch compliance*.
- Jika rating turun 1 level, aktifkan *playbook* eskalasi: *war room*, *freeze* perubahan non-esensial, dan laporan Dewan.

2. ICAAP & Modal Risiko Operasional

- Peta rating ke **stress factor** operasional:

- AAA–AA: faktor 1.0–1.1
- A–BBB: 1.2–1.4
- BB ke bawah: 1.5+ + **buffer manajemen**
- Kenaikan faktor diterapkan ke kerangka **SA-OR** / model internal. Ini sejalan dengan praktik pengawas yang dapat menambah **Pillar 2 add-on** saat ketahanan digital lemah. ([The Wall Street Journal](#))

3. SREP/Internal Risk Profile

- Masukkan metrik rating ke **Self-Assessment SREP** bank.
- Tautkan ke *heatmap* risiko operasional & TIK: *likelihood* × *impact* mengikuti *operational resilience principles*. ([regulationtomorrow.com](#))

4. Pricing & Limit Counterparty

- Gunakan rating untuk menilai **vendor TIK** dan **mitra pembayaran**.
- Terapkan *margin* biaya risiko di kontrak, atau kurangi eksposur jika vendor berperingkat rendah. Ini selaras dengan praktik global yang menekan risiko *outsourcing* kritikal.

5. GCG & Kompensasi Manajemen

- Jadikan *target rating* sebagai **KPI Direksi/Komisaris**.
- Kegagalan berulang → penyesuaian remunerasi dan rencana remediasi—praktik akuntabilitas publik yang mulai diterapkan di pasar maju. ([The Wall Street Journal](#))

6. Pelaporan ke Regulator

- *Quarterly pack* ke OJK/BSSN memuat: skor rating, tren 12 bulan, *root cause*, status remediasi, hasil *scenario testing*.
- Struktur dan *taxonomy* insiden mengikuti praktik Eropa (DORA) dan EBA agar mudah dibandingkan. ([executiveitforums.org](#))

Alur data yang simpel (dan bisa di-audit)

1. **Koleksi otomatis**: insiden, *vulnerability*, kebocoran, *attack surface*, *vendor posture*.
2. **Skoring & normalisasi**: konversi ke **rating (AAA–D)**.
3. **Orkestrasi risiko**: dorong ke **ERM, ICAAP, Treasury limits**, dan **Vendor Management**.
4. **Dasbor eksekutif**: lampu merah/kuning/hijau per layanan kritikal; *drill-down* ke kontrol yang gagal.
5. **Evidencing**: simpan bukti uji pemulihan, *table-top exercise*, *red team*, sesuai kerangka ketahanan operasional. ([regulationtomorrow.com](#))

Contoh “aturan main” praktis (siap pakai)

- **Trigger modal**: rating jatuh < *BBB* → tambah *management buffer* 25–50 bps atas *operational risk capital*. (Selaras pendekatan pengawas saat resiliensi dinilai kurang.) ([The Wall Street Journal](#))

- **Trigger perubahan IT:** rating turun 1 level → *change freeze* non-esensial 30 hari + *senior management attestation*. (Sejalan dengan pola intervensi pengawas pada gangguan digital). ([The Wall Street Journal](#))
- **Trigger vendor:** vendor *tier-1* berperingkat < A → *enhanced monitoring*, uji pemulihan bersama, atau *exit plan*. (Konsisten dengan pengetatan risiko *outsourcing*).

Penutup

Rating siber bukan sekadar *score*. Ia adalah **tuas manajemen risiko**. Dengan memasukkan rating ke **risk appetite**, **ICAAP**, **SREP**, **limit vendor**, dan **governance**, bank mengubah keamanan dari biaya menjadi **perlindungan modal dan reputasi**. Ini garis besar praktik yang sudah berjalan di yurisdiksi maju—dari Eropa (SREP/DORA), Inggris (PRA), sampai Singapura (tambahan modal operasional untuk gangguan digital). ([asbasupervision.org](#))

Tantangan untuk industri: beranikan diri menetapkan **target rating minimum** dan *consequence management* yang nyata. Jadikan *digital trust* bagian resmi dari **profil risiko bank**—bukan lampiran IT.

Bagian III — Konsep dan Pikiran Besar Framework

Bab 7: Paradigma Baru: Data = Uang, Keamanan = Kepercayaan

Dari *financial rating* ke *digital trust rating*

Selama ini bank dinilai dari rasio keuangan. *Capital adequacy*. Likuiditas. Profit. Namun dunia berubah. Serangan siber dan kebocoran data langsung memukul biaya, reputasi, dan kepercayaan pasar. Regulator global juga bergerak. Eropa menerapkan **DORA** untuk ketahanan operasional digital di sektor keuangan. AS mewajibkan emiten mengungkapkan insiden siber material. Bank sentral Eropa bahkan melakukan **cyber stress test**. Semua ini mendorong lahirnya **rating kepercayaan digital**. (ma.moodys.com)

Intinya: *digital trust rating* jadi “mata uang kepercayaan” baru. Ia mempengaruhi *cost of funds*, akses pasar, hingga stabilitas sistemik.

Apa itu *digital trust rating*?

Gambaran singkat, mudah dicerna:

- **Skor kesiapan siber + privasi data:** proses, teknologi, *people*.
- **Kepatuhan & transparansi:** seberapa patuh pada UU PDP, pelaporan insiden, dan *disclosure* ke publik.
- **Ketahanan operasional:** kemampuan *prevent–detect–respond–recover* agar pelayanan tetap jalan.
- **Higiene rantai pasok:** kontrol vendor *critical* dan *cloud*.
- **Track record insiden:** frekuensi, waktu pulih, dampak finansial.

Perbedaan utama: *financial rating* melihat *ability to pay*. *Digital trust rating* melihat *ability to stay secure and reliable*.

Mengapa pasar peduli?

Lembaga pemeringkat sudah memasukkan risiko siber dalam penilaian tata kelola dan kualitas kredit.

- **S&P Global Ratings** menilai praktik manajemen & tata kelola, termasuk keamanan siber, sebagai faktor kredit lintas sektor. ([S&P Global](https://www.spglobal.com))
- **Moody’s** menempatkan *cyber attacks* sebagai ancaman besar bagi kesehatan finansial perusahaan—artinya dapat memicu dampak kredit negatif bila kontrol lemah. ([moodys.com](https://www.moodys.com))

Artinya: skor digital yang buruk bisa *price in* jadi premi risiko, denda, dan biaya modal lebih tinggi.

Menghubungkan dua dunia: dari angka ke kepercayaan

Bayangkan jembatan antara *financial rating* dan *digital trust rating*:

- **DORA** → **Operasional bank lebih tahan gangguan** → pendapatan *fee-based* lebih stabil → profil risiko operasional turun. (ma.moodys.com)
- **Kewajiban cyber disclosure SEC** → transparansi insiden meningkat → asimetri informasi turun → volatilitas harga saham berkurang. ([Financial Stability Board](#))
- **Uji ketahanan siber oleh bank sentral** → bukti objektif ke pasar → memperkuat *investor confidence*.

Kerangka pikir sederhana untuk bank

Tujuan: naik kelas dari *financially sound* menjadi *digitally trusted*.

1. **Ukur yang penting**
 - Tetapkan *digital trust KPI*: *mean time to detect* (MTTD), *mean time to recover* (MTTR), *patch compliance*, *phishing resilience rate*.
 - Kaitkan dengan uang: biaya insiden/pendapatan (%), denda/regulatory findings, *downtime* per juta transaksi.
2. **Masukkan ke Risk Appetite**
 - Taruh ambang digital di *Risk Appetite Statement*: contoh “MTTR kritikal ≤ 4 jam”, “*critical vulnerabilities* tersisa $\leq X$ dalam 30 hari”.
 - Link-kan ke *economic capital* untuk risiko operasional.
3. **Satukan ke ICAAP & profil risiko**
 - Kuantifikasi skenario siber ke dampak modal: *loss distribution*, *stress loss*, dan *reverse stress*.
 - Rekonsiliasi dengan *financial rating drivers*: pendapatan, biaya, likuiditas.
4. **Transparansi cerdas (*smart disclosure*)**
 - Publikasikan metrik ketahanan kunci di laporan tahunan dan *investor deck*.
 - Ikuti praktik pengungkapan SEC: insiden material, tata kelola siber di dewan, dan proses manajemen risiko. ([Financial Stability Board](#))
5. **Latih & uji seperti fire drill**
 - *Tabletop exercise* lintas fungsi: TI, *risk*, hukum, komunikasi.
 - Ikuti pola *cyber stress test* ala bank sentral untuk bukti ke pasar.

What good looks like — sinyal ke pasar

Tanda-bank-ini-layak-dipercaya secara digital:

- **Dewan terlibat aktif**: ada komite risiko digital, *dashboard* rutin, dan *challenge* nyata pada manajemen.
- **Kepatuhan standar**: kontrol sejalan DORA dan praktik pengawasan global (FSB/BIS) untuk pelaporan insiden dan ketahanan.

- **Vendor disiplin:** kontrak *SLA* siber jelas, tes *failover* berkala, *exit plan cloud*.
- **Respons cepat & jujur:** insiden diumumkan tepat waktu, rencana pemulihan jelas, pelajaran dipublikasikan.
- **Metrik membaik dari waktu ke waktu:** MTDD/MTTR turun, *phishing fail rate* turun, temuan audit menurun.

Manfaat bisnis yang langsung terasa

- **Biaya modal turun:** persepsi risiko mengecil → *spread* yang lebih murah.
- **Akses pasar lebih mudah:** *investor* melihat disiplin operasional → kepercayaan naik.
- **Daya saing digital:** pelanggan merasa aman → *adoption* kanal digital naik.
- **Perlindungan nilai saham:** saat ada insiden, pemulihan cepat → *drawdown* saham terbatas.

Tantangan yang harus ditaklukkan

- **Data berantakan:** tanpa *data lineage* dan *asset inventory*, skor digital rapuh.
- **Budaya:** keamanan masih dianggap urusan tim TI, bukan bisnis.
- **Rantai pasok:** risiko vendor kerap jadi *single point of failure*.
- **Transparansi:** ketakutan *disclosure* vs tuntutan pasar.

Langkah 90 hari (ringkas, nyata)

- **Hari 0–30:** *baseline* risiko digital; tentukan 8–10 KPI; aktifkan *executive cyber dashboard*.
- **Hari 31–60:** *tabletop* insiden material; *gap analysis* terhadap DORA/FSB *toolkit* pelaporan; siapkan *smart disclosure* template. (ma.moodyys.com)
- **Hari 61–90:** masukkan ambang digital ke *Risk Appetite*; tautkan ke ICAAP; siapkan *investor one-pager* “*Digital Trust at a Glance*”.

Penutup

Financial rating tetap penting. Tapi tanpa *digital trust rating*, cerita bank tidak lengkap. Keuangan yang sehat butuh operasi yang tangguh. Kepercayaan publik butuh keamanan dan keterbukaan. Saat pasar menilai *digital trust*, pemenangnya adalah bank yang bisa **mengukur, memperbaiki, dan menjelaskan**—dengan data.

Analogi antara Moody's/S&P dan CyberRank

Di dunia perbankan dan keuangan, kita terbiasa melihat lembaga seperti Moody's dan S&P yang memberikan *rating kredit* untuk negara, bank, atau perusahaan. Sedangkan di era digital, muncul alat baru seperti CyberRank.ai yang memberi *rating keamanan siber dan kepatuhan data*. Analogi antara keduanya bisa sangat berguna untuk memahami mengapa keamanan siber dan data adalah bagian penting dari stabilitas keuangan.

Apa yang dilakukan Moody's / S&P?

- Moody's dan S&P adalah lembaga pemeringkat kredit yang besar dan dikenal dunia. ([Wikipedia](#))
- Fungsi utama mereka: menilai **kemampuan suatu entitas** (negara, bank, perusahaan) untuk membayar kewajiban utang. ([Investopedia](#))
- Mereka menggunakan skala seperti AAA, AA, A, BBB, ... hingga D (atau Aaa, Aa, A di Moody's) untuk menunjukkan tingkat risiko gagal bayar. ([Fidelity](#))
- Hasil rating ini memengaruhi: biaya pinjaman (interest rate), kepercayaan investor, profil risiko institusi. ([S&P Global](#))
- Untuk bank dan lembaga keuangan: jika ratingnya turun, bisa jadi mereka harus membayar biaya dana lebih tinggi, atau investor jadi lebih hati-hati.

Apa yang dilakukan CyberRank.ai?

- CyberRank.ai adalah suatu alat teknologi yang memberikan *rating keamanan siber dan kepatuhan data* untuk organisasi, termasuk vendor/mitra, secara eksternal dan real-time. ([cyberrank.ai](#))
- Ia mengumpulkan data publik: sertifikasi keamanan, kerentanan yang terpapar, kebocoran data, eksposur vendor, aset publik, kebijakan privasi. ([cyberrank.ai](#))
- Dengan demikian, ia memberi semacam "skor" atau "peringkat" untuk melihat seberapa kuat organisasi dalam aspek keamanan siber dan kepatuhan data. ([iisri.com](#))
- Untuk bank, fintech, vendor teknologi — ini berarti Anda bisa memetakan risiko digital dan keamanan siber yang selama ini kurang terlihat.

Analogi Antara Moody's/S&P dan CyberRank.ai

- Moody's/S&P → *rating kredit*: menilai kesehatan keuangan dan risiko gagal bayar.
- CyberRank.ai → *rating siber/privasi*: menilai kesehatan keamanan data dan risiko kebocoran atau gangguan.
- Keduanya menggunakan pendekatan: analisis data + skala penilaian yang memudahkan perbandingan antar institusi.
- Dalam perbankan: bank yang mendapat rating kredit rendah oleh Moody's/S&P harus menghadapi tantangan keuangan; demikian juga bank yang punya rating siber/privasi rendah lewat CyberRank.ai akan menghadapi tantangan digital dan kepercayaan.
- Sebagaimana investor atau regulator melihat rating kredit untuk menilai risiko keuangan, regulator keamanan siber (atau bank sendiri) dapat melihat rating keamanan siber sebagai *indikator risiko digital*.

Kenapa Analogi Ini Penting untuk Industri Perbankan Indonesia

- Bank bukan hanya menjalankan bisnis keuangan tradisional, tapi juga bisnis digital & data. Data nasabah adalah aset yang sangat berharga.
- Jika suatu bank memiliki keamanan siber yang lemah → risiko tinggi kebocoran, denda regulator, hilangnya kepercayaan nasabah → bisa menimbulkan kerugian finansial dan reputasi.
- Dengan menggunakan analogi rating kredit, regulator seperti Otoritas Jasa Keuangan (OJK) bisa memperkenalkan konsep *rating siber & privasi* yang mudah dipahami: sama seperti “berapa sehat bank Anda dari sisi keuangan”, sekarang “berapa sehat bank Anda dari sisi keamanan siber & data”.
- Alat seperti CyberRank.ai bisa menjadi sarana untuk mengukur secara objektif dan terus-menerus — bukan hanya pengawasan periodik tradisional saja.

Tantangan dan Peluang

Tantangan:

- Banyak bank mungkin belum terbiasa dengan konsep “rating keamanan siber / privasi” seperti dengan rating kredit.
- Data eksternal yang digunakan oleh alat seperti CyberRank.ai bisa saja terbatas atau belum sempurna untuk semua jenis institusi keuangan di Indonesia.
- Regulasi dan kerangka nasional (seperti yang disusun dalam naskah Anda) perlu mengintegrasikan konsep ini agar menjadi bagian pengawasan resmi.

Peluang:

- Bank yang mendapatkan “rating siber/privasi” tinggi bisa mendapatkan keunggulan kompetitif: kepercayaan nasabah lebih tinggi, mungkin insentif dari regulator, biaya vendor atau mitra lebih rendah.
- Regulator bisa menjalankan pengawasan yang lebih modern: *data-driven supervision*, bukan hanya laporan manual.
- Dengan analogi rating kredit, komunikasi risiko kepada dewan, pemangku kepentingan, dan publik menjadi lebih mudah: “Jika kita mendapatkan peringkat siber tinggi, maka kita dianggap ‘AAA’ dalam keamanan digital”.

Kesimpulan

Analogi antara Moody's/S&P dengan CyberRank.ai memperjelas satu hal: **keamanan siber dan privasi data sudah menjadi bagian dari risiko keuangan.**

- Jika dulu bank dinilai dari *kemampuan membayar utang*, sekarang juga harus dinilai dari *kemampuan melindungi data dan sistemnya*.
- Framework yang Anda buat — “CyberTrust & Data Privacy Rating Framework” di bawah OJK — akan mendapatkan makna lebih luas dengan mengadopsi gaya pemeringkatan seperti rating kredit.
- Dengan demikian, bank tidak hanya berlomba mendapatkan rating kredit bagus, tetapi juga rating siber/privasi yang bagus — agar kepercayaan publik, regulator, dan pasar tetap tinggi.

Bab 8: Definisi dan Tujuan *Cyber & Privacy Rating Framework*

Penilaian objektif kesiapan siber dan kepatuhan PDP

Bank butuh cara yang **objektif** untuk mengukur dua hal:

1. **Kesiapan siber** (*cyber readiness*).
2. **Kepatuhan PDP** (UU No. 27/2022).

Objektif artinya **berbasis bukti**, terukur, dan konsisten. Bukan opini. Bukan sekadar *checklist*. Ia memakai standar global (mis. *NIST CSF 2.0*, *ISO/IEC 27001*) dan kewajiban nasional (UU PDP, POJK TI, Peraturan BSSN). ([NIST Technical Series Publications](#))

Kenapa harus objektif? (bahasa keuangan)

- **Risiko nyata & mahal:** rata-rata biaya kebocoran global 2024 = **USD 4,88 juta**; sektor keuangan lebih tinggi ≈ **USD 6,08 juta** per insiden. Ini memukul laba, CAR, dan biaya dana. ([IBM Newsroom](#))
- **Regulator makin ketat:** OJK mewajibkan manajemen risiko TI; UU PDP mewajibkan perlindungan & pelaporan; BSSN mensyaratkan standar keamanan untuk sistem strategis. Penilaian objektif memudahkan *compliance proof*. ([OJK](#))
- **Bahasa bersama:** NIST CSF 2.0 memperkenalkan fungsi **Govern** di samping Identify-Protect-Detect-Respond-Recover → memudahkan direksi membaca skor risiko seperti membaca rasio keuangan. ([NIST Technical Series Publications](#))

Apa itu “penilaian objektif” versi perbankan?

Bayangkan *credit rating*, tapi untuk **ketahanan siber & privasi data**. Bahan bakunya: **data bukti** yang dapat diaudit.

Sumber bukti (contoh konkret):

- **Kepatuhan hukum:** Pasal-pasal kewajiban pengendali data (UU PDP), bukti SOP pelaporan insiden, *consent* dan *DPIA*. ([Peraturan BPK](#))
- **Kontrol teknis:** sertifikasi/implementasi **ISO/IEC 27001:2022** (ISMS), pemetaan kontrol ke **NIST CSF 2.0** (termasuk fungsi Govern). ([ISO](#))
- **Kepatuhan OJK:** *risk governance* TI sesuai **POJK 38/2016** dan perubahannya. ([OJK](#))
- **Kewajiban BSSN:** pengamanan PSE, termasuk penerapan standar & audit untuk sistem strategis. ([Peraturan BPK](#))
- **Bukti operasional:** catatan latihan *incident response*, *backup/restore* teruji, *patching* SLA, MTTR/MTTD, hasil *vulnerability scan/pentest*, uji *phishing*. (Dipetakan ke NIST CSF 2.0). ([NIST Technical Series Publications](#))

Matriks nilai yang mudah dibaca manajemen

Gunakan skala huruf (mis. **AAA–D**) agar mudah dikomunikasikan ke Direksi, Komite Manrisk, dan OJK.

Contoh ringkas interpretasi (ilustratif):

- **AAA-AA**: ISMS tersertifikasi & hidup; *governance* kuat; pelaporan PDP rapi; uji pemulihan lulus; *third-party risk* terkendali.
- **A-BBB**: kontrol inti ada, namun *governance* dan *supply-chain* belum konsisten; sebagian KPI deteksi-respon belum stabil.
- **BB-B**: banyak kontrol reaktif; pelatihan & *patching* tidak merata; bukti PDP belum lengkap.
- **CCC-D**: *gaps* serius; tidak ada uji pemulihan; tidak patuh PDP; risiko denda & gangguan layanan tinggi.

Skala ini **harus ditopang metrik** (lihat bagian berikut) agar objektif, bukan penilaian subjektif.

Metrik yang membuatnya objektif (contoh KPI “inti 12”)

1. **Govern**: ada kebijakan PDP & ISMS disetujui Direksi (ya/tidak). ([NIST Technical Series Publications](#))
2. **ISMS**: status sertifikasi ISO/IEC 27001:2022 (valid/expired). ([ISO](#))
3. **DPIA** untuk proses berisiko tinggi (persentase proses kritikal yang punya DPIA). ([Peraturan BPK](#))
4. **Pelaporan insiden PDP**: waktu rata-rata dari deteksi ke pelaporan (*hours to notify*). ([Peraturan BPK](#))
5. **MTTD/MTTR** insiden siber (jam). ([NIST Technical Series Publications](#))
6. **SLA patching** kerentanan kritikal (hari). ([NIST Technical Series Publications](#))
7. **Uji DR/BCP** lulus per tahun (jumlah/scope). ([NIST Technical Series Publications](#))
8. **Pelatihan karyawan** dan *phishing fail rate* (%). ([NIST Technical Series Publications](#))
9. **Klasifikasi & enkripsi data** (cakupan aset kritikal). ([ISO](#))
10. **Manajemen vendor**: % vendor kritikal yang diaudit keamanan & PDP. ([NIST Technical Series Publications](#))
11. **Deteksi kebocoran**: temuan *data leak* eksternal tertutup (waktu penanganan). ([IBM Newsroom](#))
12. **Kepatuhan POJK TI**: pemenuhan kontrol kunci & *risk register* TI (skor). ([OJK](#))

Catatan: KPI di atas disusun agar **map** ke NIST CSF 2.0 (termasuk fungsi **Govern**) dan **ISO 27001** (konteks ISMS), sekaligus memenuhi UU PDP/POJK/BSSN. Ini yang membuat penilaian **terstandar** dan **audit-ready**. ([NIST Technical Series Publications](#))

Cara menilai harian–tahunan (alur singkat)

- **Harian / mingguan**: kumpulkan indikator otomatis (log SIEM, patch, *phishing test*, *asset inventory*).
- **Bulanan**: *score refresh + trend* (naik/turun), *exception* untuk Direksi.
- **Triwulan**: *table-top exercise* insiden, uji DR, audit vendor.
- **Tahunan**: *assurance review* (internal/eksternal), validasi kepatuhan PDP, *red team/pentest*, sertifikasi/ *surveillance* ISO 27001. ([NIST Technical Series Publications](#))

“Reality check” kondisi global

- Biaya kebocoran naik; sektor finansial tetap di papan atas. Konsekuensinya: denda, *downtime*, hilangnya nasabah, revisi rating & biaya modal. Penilaian objektif membantu *prioritize* investasi kontrol paling berdampak. ([IBM Newsroom](#))
- Tren standar: **NIST CSF 2.0 (2024)** menekankan **Govern** dan *supply-chain risk*; **ISO 27001:2022** memperbarui kontrol dan *continuous improvement*. Ini jadi acuan *benchmark* global. ([NIST Technical Series Publications](#))

Aksi 90 hari untuk bank (praktis & terukur)

- **Minggu 1–4:** *baseline assessment* pakai peta NIST CSF 2.0 ↔ ISO 27001 ↔ UU PDP/POJK/BSSN; tetapkan **12 KPI** inti dan target minimal. ([NIST Technical Series Publications](#))
- **Minggu 5–8:** tutup *gap* terbesar: *patch backlog*, *IAM/MFA* untuk akses kritikal, *backup* teruji, *incident playbook* + *table-top*. ([NIST Technical Series Publications](#))
- **Minggu 9–12:** lakukan *DR drill* penuh; audit vendor kritikal; finalisasi bukti PDP (DPIA, *consent*, pelaporan insiden); siapkan *scorecard* direksi + *trendline*. ([Peraturan BPK](#))

Nilai tambah untuk OJK (arah “OJK CyberTrust”)

Dengan penilaian objektif, OJK bisa memperoleh **scorecard nasional** yang konsisten lintas bank:

- **Transparan:** angka yang dapat dipertanggungjawabkan.
- **Se-irama standar global:** NIST CSF 2.0 & ISO 27001.
- **Reg-tech friendly:** *data-driven supervision*; integrasi dengan pelaporan rutin. ([NIST Technical Series Publications](#))

Ringkasnya

- **Objektif = berbasis bukti + standar + hukum.**
- **Skor yang jelas** membuat dewan dan regulator cepat paham.
- **Dampak finansial nyata** mendorong prioritas yang tepat.
- **Goal:** bank siap siber, patuh PDP, dan dipercaya nasabah—setara pentingnya dengan kesehatan keuangan.

Dukungan terhadap *transparency & accountability* perbankan

Mengapa *transparency & accountability* perlu diperkuat?

Kepercayaan nasabah lahir dari **bukti yang terlihat**, bukan janji. Di era digital, biaya kebocoran data makin mahal; sektor finansial termasuk yang tertinggi. Ini memukul laba, harga saham, dan reputasi. Karena itu, bank perlu cara yang **terukur** untuk menunjukkan “kami aman, kami patuh.” ([IBM](#))

Prinsip dasar

- **Standar jelas:** peta ke **NIST CSF 2.0** (termasuk fungsi **Govern**) dan **ISO/IEC 27001:2022** (ISMS). Ini fondasi tata kelola dan kontrol keamanan yang diakui global. ([NIST Technical Series Publications](#))
- **Kepatuhan hukum:** sejajarkan bukti dengan **UU No. 27/2022 (PDP)**, **POJK 38/2016** (manajemen risiko TI), dan **POJK 55/2016** (Tata Kelola Bank Umum). Ini menjadikan transparansi bukan pilihan, tetapi kewajiban. ([Peraturan BPK](#))
- **Ketahanan operasional:** ikuti prinsip **Basel Committee** tentang *operational resilience* agar bank tetap beroperasi saat terjadi gangguan siber. ([Bank for International Settlements](#))

Apa wujud *transparency* yang bermakna?

Bukan *slogan*, tapi **data yang dapat diverifikasi**.

Contoh wujudnya:

- **Scorecard direksi triwulanan:** menampilkan tren *MTTD/MTTR*, tingkat *patching*, hasil uji *phishing*, status *backup/restore*, serta kepatuhan pelaporan insiden PDP. Ringkas 1 halaman, dengan lampu **hijau/kuning/merah**. Dipetakan ke fungsi **Govern–Identify–Protect–Detect–Respond–Recover** (NIST CSF 2.0). ([NIST Technical Series Publications](#))
- **Laporan kepatuhan PDP tahunan:** bukti *consent*, *DPIA* untuk proses berisiko tinggi, dan SLA pelaporan insiden. Tautkan ke pasal-pasal UU PDP agar audit mudah. ([Peraturan BPK](#))
- **Sertifikasi & *surveillance* ISO 27001:** tunjukkan status terkini (aktif/kedaluwarsa), ruang lingkup, dan temuan mayor/minor beserta rencana perbaikan. ([ISO](#))
- **Pengungkapan risiko pihak ketiga:** daftar vendor kritikal, hasil *due diligence*, dan rencana mitigasi—selaras dengan prinsip ketahanan operasional Basel. ([Bank for International Settlements](#))

Apa wujud *accountability* yang nyata?

Akhirnya harus ada yang bertanggung jawab dan ada jejak tindak lanjut.

Contoh wujudnya:

- **Pernyataan tahunan dewan** (*board attestation*): menandatangani kepatuhan ke POJK TI & GCG, plus target perbaikan 12 bulan ke depan. ([OJK](#))
- **RUPS & komite risiko**: memasukkan *cyber & privacy score* sebagai agenda tetap, berdampingan dengan rasio keuangan.
- **Issue-to-closure log**: setiap temuan audit siber/PDP punya PIC, tenggat, dan status penutupan—ditrack sampai selesai.
- **Latihan incident response & DR terjadwal**: minimal 2x setahun, dengan *after-action report* dan perbaikan nyata. Diselaraskan dengan NIST CSF 2.0 dan praktik ketahanan operasional. ([NIST Technical Series Publications](#))

Bagaimana *framework* ini mendorong keterbukaan yang sehat?

- **Skor yang mudah dibaca** (mis. **AAA–D**): ringkas untuk investor dan publik, namun berbasis metrik yang diaudit (bukan *marketing*).
- **RegTech-friendly**: OJK dapat *dashboard* nasional untuk melihat tren risiko lintas bank secara *real-time*. Ini memperkuat pengawasan berbasis data dan menekan *blind spots*. ([OJK](#))
- **Pengungkapan terarah**: tidak semua detail dibuka. Yang dibuka adalah **indikator kunci** (mis. status sertifikasi, *mean time to recover*, tingkat kepatuhan PDP). Hasilnya: publik mendapat **key facts**, musuh tidak diberi peta lengkap.

Dampak finansial (kenapa penting untuk CFO & investor)

Ketika metrik dan *closure* dibuktikan, tiga hal terjadi:

1. **Biaya insiden turun** (lebih cepat deteksi & pulih). Data global menunjukkan biaya kebocoran naik; disiplin transparansi dan otomasi membantu menahan biaya. ([IBM](#))
2. **Biaya modal bisa membaik** (kepercayaan investor meningkat saat *governance* jelas dan konsisten). ([OJK](#))
3. **Risiko sistemik berkurang** (resiliensi operasional—bukan hanya keamanan—naik). ([Bank for International Settlements](#))

Paket aksi 90 hari (praktis untuk mulai sekarang)

- **Minggu 1–4**: tetapkan **indikator kunci** (maks. 12 KPI) yang memetakan NIST CSF 2.0 ↔ ISO 27001 ↔ UU PDP/POJK. Buat *scorecard* 1 halaman. ([NIST Technical Series Publications](#))
- **Minggu 5–8**: jalankan *table-top exercise* insiden, finalisasi *issue-to-closure log*, dan siapkan draf **board attestation**. ([NIST Technical Series Publications](#))
- **Minggu 9–12**: publikasikan **laporan transparansi siber & PDP bank** (versi eksternal singkat), dan integrasikan umpan balik ke rencana kerja tahun berjalan. ([Peraturan BPK](#))

Ringkasan

Transparency = **angka & bukti yang bisa dilihat**; *accountability* = **siapa yang bertanggung jawab sampai tuntas**. Dengan standar global (NIST CSF 2.0, ISO 27001), hukum nasional (UU PDP, POJK), dan prinsip ketahanan Basel, bank Indonesia bisa menunjukkan—secara sederhana namun kuat—bahwa keamanan data dan layanan digital **serius dijaga**. ([NIST Technical Series Publications](#))

Bab 9: Dimensi Penilaian Utama

Ketahanan siber (*cyber resilience*)

Ketahanan siber adalah kemampuan bank untuk tetap menjalankan operasi kritikal saat diserang, lalu pulih cepat dengan kerusakan minimal. Ini bukan sekadar *firewall* atau antivirus. Ini menyatukan **tata kelola, proses, orang, dan teknologi**. Basel Committee menyebutnya sebagai kemampuan bank **menjaga layanan kritikal** di tengah disrupsi seperti insiden siber, kegagalan teknologi, atau bencana. ([Bank for International Settlements](#))

Kenapa krusial untuk dunia perbankan?

- **Biaya insiden mahal.** Rata-rata global 2024: **USD 4,88 juta** per *data breach*; sektor keuangan lebih tinggi **≈ USD 6,08 juta**. Ini memukul laba, modal, dan reputasi. ([IBM](#))
- **Serangan makin kompleks.** Laporan WEF 2024 menyoroti kesenjangan kesiapan dan dampak teknologi baru pada risiko siber lintas ekonomi. ([World Economic Forum](#))
- **Regulasi global bergerak.** NIST CSF 2.0 (2024) menambah fungsi **Govern**—menekankan peran direksi dan *risk appetite*—agar keamanan benar-benar dikelola sebagai risiko bisnis, bukan teknis semata. Uni Eropa mulai menerapkan **DORA (2025)** untuk ketahanan operasional keuangan. ([NIST Technical Series Publications](#))

Tujuan penilaian ketahanan siber (untuk *rating* bank)

- **Objektif & berbasis bukti.** Mengukur kesiapan, bukan opini.
- **Sejalan standar global.** Dipetakan ke **NIST CSF 2.0** dan **ISO/IEC 27001:2022 (ISMS)** agar konsisten dan dapat diaudit. ([NIST Technical Series Publications](#))
- **Selaras prinsip Basel.** Fokus pada **kelangsungan layanan kritikal** dan **resiliensi operasional** end-to-end. ([Bank for International Settlements](#))

Apa saja yang dinilai? (kerangka sederhana untuk direksi)

Gunakan 6 fungsi **NIST CSF 2.0** sebagai “rangka” *scorecard*: **Govern – Identify – Protect – Detect – Respond – Recover**. Semua poin di bawah harus punya **indikator (KPI)** dan **bukti**. ([NIST Technical Series Publications](#))

1. **Govern** (*paling atas*):
 - Kebijakan risiko siber disetujui dewan, *risk appetite* jelas, peran CISO kuat.
 - *Board attestation* tahunan terkait kepatuhan UU PDP/POJK dan *closure* temuan audit. ([NIST Technical Series Publications](#))
2. **Identify**:
 - Inventaris aset lengkap (on-prem, cloud, SaaS), klasifikasi data nasabah, peta proses kritikal.

- Daftar vendor kritikal + *third-party risk* (kontrak, audit, *exit plan*)—area yang disorot Basel & otoritas perbankan. ([Bank for International Settlements](#))
3. **Protect:**
- Kontrol akses kuat (*MFA, least privilege*), enkripsi data sensitif, *hardening, patching SLA* jelas.
 - ISMS aktif dan tersertifikasi **ISO/IEC 27001:2022** (status sertifikat, ruang lingkup, temuan mayor/minor). ([ISO](#))
4. **Detect:**
- *Telemetry* menyatu (SIEM/EDR), deteksi anomali, uji *phishing* berkala.
 - **MTTD** (Mean Time to Detect) dipantau dan ditarget. (Semakin cepat, semakin kecil biaya insiden). ([IBM](#))
5. **Respond:**
- *Playbook* insiden, *table-top exercise* triwulanan, pelaporan insiden PDP sesuai UU.
 - **MTTR** (Mean Time to Respond/Recover) turun dari waktu ke waktu. ([NIST Technical Series Publications](#))
6. **Recover:**
- *Backup* teruji, *restore drill* rutin, target RTO/RPO terpenuhi untuk layanan kritikal (core banking, pembayaran).
 - Laporan *after-action* dan *lessons learned* terintegrasi ke perbaikan kebijakan. ([Bank for International Settlements](#))

KPI inti yang mudah dibaca manajemen (contoh)

- **Status ISO 27001** (aktif/kedaluwarsa + ruang lingkup). ([ISO](#))
- **Waktu pelaporan insiden PDP** (jam/hari sesuai aturan internal/regulator). ([NIST Technical Series Publications](#))
- **MTTD / MTTR** untuk insiden prioritas-1. ([NIST Technical Series Publications](#))
- **Patch compliance** untuk CVE kritikal ($\leq X$ hari). ([NIST Technical Series Publications](#))
- **Uji DR/BCP** lulus ($\geq 2x$ /tahun untuk layanan kritikal). ([Bank for International Settlements](#))
- **Vendor kritikal diaudit** (% vendor dengan kontrol ICT & PDP yang diverifikasi). ([Bank for International Settlements](#))
- **Tingkat kegagalan uji *phishing*** (turun konsisten kuartal ke kuartal). ([World Economic Forum](#))

Nilai bisnisnya: bank dengan MTTD/MTTR cepat, *patching* disiplin, dan latihan pemulihan teratur—cenderung **menekan biaya insiden** yang saat ini termasuk tertinggi di sektor finansial. ([IBM](#))

90 hari pertama: langkah praktis (*no-nonsense*)

- **Minggu 1–4** — *Baseline*: petakan layanan kritikal, definisikan RTO/RPO, tetapkan KPI di atas, dan *gap analysis* NIST CSF 2.0 ↔ ISO 27001 ↔ PDP. ([NIST Technical Series Publications](#))
- **Minggu 5–8** — *Quick wins*: tutup *patch backlog*, aktifkan MFA menyeluruh, *table-top* insiden (termasuk skenario *ransomware*), bekukan kebijakan *backup immutable*. ([TechRadar](#))
- **Minggu 9–12** — *Resilience drill*: uji *restore* penuh untuk satu layanan prioritas, audit vendor kritikal, finalisasi *board attestation & issue-to-closure log*. ([Bank for International Settlements](#))

Bagaimana ini diterjemahkan ke *rating*?

Gunakan skala huruf (mis. **AAA–D**) yang ditopang KPI dan bukti audit:

- **AAA–AA**: layanan kritikal tahan guncang; MTTD/MTTR rendah; ISO 27001 aktif; *governance* kuat; *third-party risk* terkendali.
- **A–BBB**: kontrol inti ada; latihan & *vendor oversight* belum konsisten; KPI stabil tapi belum unggul.
- **BB–B**: kontrol reaktif; *patching* lambat; latihan pemulihan minim; risiko gangguan layanan tinggi.
- **CCC–D**: *gaps* besar; tidak patuh; potensi denda dan *downtime* signifikan.

Ringkasan

Ketahanan siber adalah “asuransi operasi” bank. Ia mengurangi **biaya insiden**, **mendukung kepatuhan**, dan **menjaga layanan tetap berjalan** saat krisis. Dengan berpegang pada **NIST CSF 2.0**, **ISO/IEC 27001:2022**, dan **prinsip Basel** tentang resiliensi operasional, penilaian ketahanan siber bisa dibuat **objektif, terukur, dan dipercaya**—oleh dewan, OJK, dan pasar. ([NIST Technical Series Publications](#))

Kepatuhan UU PDP dan pelaporan insiden

Data nasabah adalah “darah” bank. Bocor, operasi terganggu. Biaya membengkak. Kepercayaan turun. Karena itu, kepatuhan **UU PDP** dan disiplin **pelaporan insiden** harus jadi **indikator inti** dalam *rating* keamanan digital bank. UU PDP sudah berlaku penuh sejak Oktober 2024 dan mewajibkan tanggung jawab jelas pada pengendali data. ([JDIH Kabupaten Tanah Laut](#))

Apa kewajiban kunci menurut UU PDP?

- **Wajib melindungi data pribadi** dengan langkah teknis dan administratif yang memadai. Ada hak subjek data dan kewajiban pengendali/prosesor. ([ABNR - Counsellors at Law](#))
- **Bila terjadi kebocoran/kegagalan pelindungan**, pengendali **wajib memberitahu secara tertulis maksimal 3×24 jam** kepada:
 1. **Subjek data** yang terdampak; dan
 2. **Lembaga pengawas** (otoritas). Pemberitahuan memuat jenis data, waktu/cara terjadinya, dan langkah pemulihan. ([JDIH Komdigi](#))

Intinya: bank tak boleh menunda. 3×24 jam adalah *hard deadline* di UU PDP. ([JDIH Komdigi](#))

Kewajiban pelaporan insiden ke ekosistem siber nasional

Selain ke otoritas PDP, ada aturan **BSSN** tentang **pengelolaan insiden siber**.

- Organisasi harus punya **Tim Tanggap Insiden (CSIRT)**.
- **Setiap insiden siber wajib dilaporkan** ke CSIRT sektoral **dengan tembusan ke CSIRT nasional**.
- **Batas awal pelaporan: 1×24 jam** setelah insiden ditemukan. ([Peraturan BPK](#))

Artinya: jalur pelaporan ada **dua**: *privacy regulator* (UU PDP) **dan nasional CSIRT channel** (BSSN). Keduanya wajib. ([JDIH Komdigi](#))

Kaitan dengan aturan sektor keuangan (OJK)

- **POJK 38/2016** mewajibkan bank menerapkan **manajemen risiko TI** termasuk tata kelola vendor TI dan pengembangan TI yang aman. Ini *payung* untuk *control* dan proses insiden di bank. ([OJK](#))
- Praktiknya: bank harus menunjukkan bukti kontrol, *escalation path*, dan uji berkala untuk insiden digital. Ini menyatu dengan GCG dan *risk appetite*. ([OJK](#))

Standar rujukan agar “objektif” dan “audit-ready”

- **NIST SP 800-61 Rev.3 (2025)**: panduan *incident response* modern, selaras dengan *NIST CSF 2.0*. Cocok untuk menyusun prosedur deteksi–respon–pemulihan. (csrc.nist.gov)

- **ISO/IEC 27035-1:2023:** kerangka *incident management* terstruktur dari persiapan, deteksi, pelaporan, penanganan, hingga *lessons learned*. ([ISO](#))

Bagaimana menilainya dalam *rating bank*?

Fokus ke **bukti** dan **angka**. Hindari penilaian berbasis opini.

KPI inti yang sederhana namun kuat:

- **Kepatuhan 3×24 jam:** persentase insiden PDP yang **dilaporkan ≤ 72 jam** ke subjek data dan otoritas. (Target: 100%). ([JDIH Komdigi](#))
- **Pelaporan 1×24 jam (BSSN):** persentase insiden siber yang **dilaporkan ≤ 24 jam** ke CSIRT sektoral/nasional. (Target: 100%). ([Peraturan BPK](#))
- **Waktu notifikasi rata-rata:** *mean hours to notify* (semakin kecil, semakin baik). ([JDIH Komdigi](#))
- **Kelengkapan notifikasi:** ada tiga elemen wajib (data yang bocor; *timeline/mode*; upaya pemulihan). (Target: 100% lengkap). ([JDIH Komdigi](#))
- **Pencatatan & closure:** % temuan insiden dengan *root cause* jelas, tindakan perbaikan (*corrective action*), dan *closure date*. (Target: ≥95%). (Selaras POJK 38/2016). ([OJK](#))
- **Kesiapan tim:** ketersediaan **CSIRT organisasi** (legal, IT, keamanan, *privacy*, komunikasi) + latihan *table-top* triwulanan. (Rujuk NIST/ISO). ([csrc.nist.gov](#))

Playbook pelaporan insiden yang mudah dipraktekkan

1. **Deteksi & klasifikasi cepat** (*detect & triage*).
2. **Aktifkan jalur ganda pelaporan:**
 - **PDP:** siapkan *template* notifikasi 3×24 jam (isi wajib 3 poin). ([JDIH Komdigi](#))
 - **BSSN:** kirim laporan awal 1×24 jam melalui kanal CSIRT sektoral/nasional. ([Peraturan BPK](#))
3. **Koordinasi dengan OJK** terkait dampak operasional dan *service continuity* (POJK 38/2016). ([OJK](#))
4. **Komunikasi nasabah** yang jujur dan *actionable*: apa yang terjadi, dampak, langkah proteksi (mis. blokir kartu sementara), dan *hotline*. (Sejalan NIST/ISO untuk *response & recovery*). ([csrc.nist.gov](#))
5. **Audit trail lengkap:** semua keputusan, waktu, dan pihak yang terlibat terdokumentasi.

90 hari pertama: target minimal patuh & tangguh

- **Minggu 1–4:** bentuk/kuatkan **CSIRT**; susun *RACI* insiden; petakan jalur pelaporan PDP (3×24 jam) dan BSSN (1×24 jam). ([Peraturan BPK](#))
- **Minggu 5–8:** lakukan **simulasi notifikasi** end-to-end (termasuk *draft e-mail/SMS* ke nasabah); ukur waktu; perbaiki *bottle-neck*. (Rujuk NIST/ISO). ([csrc.nist.gov](#))
- **Minggu 9–12:** integrasikan metrik ke *board scorecard*; tetapkan **SLA pelaporan** sebagai *KRI*; lakukan *table-top* lintas fungsi (IT, Legal, PR, Operasi, Kepatuhan). ([csrc.nist.gov](#))

Dampaknya bagi nilai bisnis

- **Mengurangi risiko denda dan gugatan** (patuh UU PDP, jalur pelaporan jelas). ([JDIH Komdigi](#))
- **Mempercepat pemulihan layanan** karena koordinasi formal dengan CSIRT nasional. ([Peraturan BPK](#))
- **Menjaga kepercayaan nasabah & investor** karena proses transparan dan tepat waktu (selaras POJK 38/2016). ([OJK](#))

Ringkasan

*Kepatuhan UU PDP + pelaporan insiden yang disiplin = **fondasi reputasi bank** di era digital. Aturannya jelas: **3×24 jam** ke subjek data & otoritas (UU PDP) **dan 1×24 jam** ke CSIRT (BSSN). Tinggal dieksekusi dengan *playbook* yang rapi, metrik yang terukur, dan latihan rutin. Itulah yang akan mengangkat *rating* keamanan digital bank Anda—bukan jargon, tapi **bukti**. ([JDIH Komdigi](#))*

Manajemen risiko vendor dan rantai pasok

Bank modern itu “terhubung”. Banyak layanan inti berjalan di atas vendor: *cloud*, *core banking module*, *file transfer*, *KYC*, *SOC*, sampai *outsourcing* operasional. Artinya: **risiko Anda = risiko vendor Anda**. Karena itu, *rating* keamanan bank **wajib** menilai **manajemen risiko vendor & rantai pasok** secara ketat—dari pemilihan, kontrak, pemantauan, hingga *exit*. Standar global menekankan ini: **NIST CSF 2.0** memasukkan *supply chain risk* di fungsi **Govern**; **ISO/IEC 27036** memberi panduan keamanan relasi pemasok. ([NIST Technical Series Publications](#))

Kenapa ini krusial untuk perbankan?

- **Serangan rantai pasok meningkat.** Kasus **MOVEit** (2023–2024) menunjukkan satu *zero-day* di perangkat *file transfer* bisa menular ke ribuan organisasi—termasuk sektor finansial. Dampaknya luas karena data mengalir lintas vendor. ([CybelAngel](#))
- **Regulator memperketat.** Komite Basel menerbitkan prinsip **third-party risk** dan **operational resilience**; EBA dan ECB mengeluarkan panduan *outsourcing* dan *cloud*; di AS, **OCC/FDIC/Fed** menerbitkan panduan gabungan *third-party risk*. Intinya: dewan direksi memikul akuntabilitas akhir. ([Bank for International Settlements](#))
- **Bahasa keuangan yang sederhana:** gangguan vendor = **downtime layanan**, **biaya insiden**, **denda**, **kehilangan nasabah**, bahkan **risiko sistemik**. Pengendalian vendor adalah *asuransi operasional*.

Apa yang dinilai? (kerangka *lifecycle* yang mudah diukur)

Gunakan siklus 5 tahap: **Plan** → **Due Diligence** → **Contract** → **Monitor** → **Exit**. Setiap tahap harus punya bukti dan *KPI*.

1. **Plan** (*perencanaan & klasifikasi layanan*)
 - Tetapkan apakah layanan termasuk “**kritis/important**” (mis. pembayaran, *core*, *KYC*, *cloud*).
 - Identifikasi konsentrasi vendor (satu *hyperscaler* untuk banyak sistem?) dan risiko lokasi/yurisdiksi. ([eba.europa.eu](#))
2. **Due Diligence** (*uji kelayakan keamanan & kepatuhan*)
 - Tinjau **sertifikasi** (ISO/IEC 27001:2022), kontrol akses, *logging*, *BCP/DR*, dan rekam insiden.
 - Rujuk **ISO/IEC 27036** untuk cakupan kontrol pada relasi pemasok; padankan ke kontrol **ISO 27001 Annex A** yang relevan. ([ISO](#))
3. **Contract** (*kontrak yang security-by-design**)
 - Klausul **SLA keamanan & privasi**, hak audit, lokasi data, *sub-processor approval*, *breach notification window* (sinkron dengan **UU PDP** 3×24 jam & kanal CSIRT nasional).
 - Kewajiban *vulnerability disclosure* dan *patching SLA* untuk komponen pihak ketiga. (Belajar dari MOVEit). ([CybelAngel](#))

4. **Monitor** (*pemantauan berkelanjutan*)
 - *Scorecard* vendor: **MTTD/MTTR**, *patch latency*, hasil uji *restore*, *phishing fail rate* staf vendor yang mengelola data bank.
 - *Attack-surface monitoring* dan pemantauan peristiwa rantai pasok (lihat sumber FFIEC/OCC untuk ekspektasi pengawasan berkelanjutan). (ffiec.gov)
5. **Exit** (*terminasi & portabilitas data*)
 - Rencana *exit* diuji: pemindahan layanan/data aman, penghapusan (*secure deletion*), dan *handover* bukti.
 - Hindari *vendor lock-in* yang menghambat pemulihan saat krisis (ditekankan regulator Eropa & Basel). (eba.europa.eu)

KPI inti (singkat, tajam, bisa dicek)

- **Klasifikasi vendor kritikal** selesai & *owner* jelas (target 100%). (eba.europa.eu)
- **Due diligence** keamanan & PDP *pre-contract* untuk seluruh vendor kritikal (target 100%). ([ISO](https://iso.org))
- **SLA notifikasi pelanggaran** pada kontrak selaras UU PDP ($\leq 3 \times 24$ jam) dan kanal CSIRT ($\leq 1 \times 24$ jam). (target 100%). ([OCC.gov](https://occ.gov))
- **Patch SLA** untuk CVE kritikal yang menimpa komponen vendor (mis. produk *file transfer*): $\leq X$ hari (diset via kontrak). (Belajar dari MOVEit). ([CybelAngel](https://cybelangel.com))
- **Uji DR/BCP** bersama vendor kritikal minimal 2×/tahun, memenuhi **RTO/RPO** layanan prioritas. ([Bank for International Settlements](https://bankforinternationalsettlements.com))
- **Audit & pemantauan berkelanjutan** (kontrol ISO 27001 aktif, laporan insiden, *pen-test* bersama) — *coverage* $\geq 95\%$. (dataguard.com)
- **Rencana exit** diuji & bukti *data destruction* tersedia untuk vendor yang berakhir kontraknya (target 100%). (eba.europa.eu)

“Red flags” yang menurunkan *rating*

- Kontrak tanpa **hak audit**, tanpa **SLA notifikasi** yang jelas, atau tanpa batas **sub-processor**. ([OCC.gov](https://occ.gov))
- Ketergantungan berlebih pada satu *cloud region* tanpa *failover*. (bankingsupervision.europa.eu)
- Tidak ada *table-top exercise* gabungan untuk skenario *ransomware/data exfiltration*. (MOVEit jadi contoh nyata). ([CybelAngel](https://cybelangel.com))

90 hari pertama: *playbook* praktis

- **Minggu 1–4:** *Vendor census* (daftar lengkap), tandai **kritikal/important**, tetapkan *owner*, dan *gap analysis* terhadap NIST CSF 2.0 (fungsi **Govern** untuk SCRM). ([NIST Technical Series Publications](https://nist.gov/technical-series/publications))
- **Minggu 5–8:** *Rapid due-diligence* untuk 10 vendor paling kritikal; tambahkan klausul kontrak: **hak audit**, **notifikasi ≤ 72 jam**, **patch SLA**, **sub-processor approval**, **data location**. ([OCC.gov](https://occ.gov))
- **Minggu 9–12:** *Joint DR drill* dengan 2 vendor prioritas; uji *restore* penuh; susun **exit plan** dan bukti *secure deletion*. Laporkan ke Komite Manrisk dalam *scorecard* 1 halaman. ([Bank for International Settlements](https://bankforinternationalsettlements.com))

Bagaimana ini diterjemahkan ke *rating*?

Skala huruf (mis. **AAA–D**) berbasis bukti:

- **AAA–AA**: *lifecycle* lengkap, kontrak kuat, pemantauan real-time, *DR drill* rutin, *exit plan* teruji, kepatuhan PDP solid.
- **A–BBB**: proses ada namun belum konsisten; *patch latency* vendor kadang melewati SLA; *drill* belum menyentuh semua layanan kritikal.
- **BB–B**: *due diligence* minim; kontrak lemah; tidak ada uji gabungan; ketergantungan tinggi ke satu vendor/region.
- **CCC–D**: *blind spot* besar; tidak patuh notifikasi; banyak insiden vendor tak tertangani.

Ringkasan

Manajemen risiko vendor & rantai pasok adalah **penopang ketahanan operasional** bank. Standar global (NIST CSF 2.0, ISO/IEC 27036), prinsip Basel, dan panduan EBA/OCC menuntut **lifecycle lengkap** dengan *KPI* yang bisa diverifikasi. Belajar dari kasus **MOVEit**, satu kelemahan di sisi pemasok bisa mengalir jadi **biaya** dan **krisis kepercayaan**. Kuncinya: **kontrak yang tepat, pemantauan yang hidup, dan rencana exit yang siap jalan**—bukan sekadar *paper compliance*. ([NIST Technical Series Publications](#))

Keamanan data nasabah dan transaksi digital

Intinya

Keamanan data nasabah = **modal kepercayaan**.

Keamanan transaksi digital = **denyut bisnis**.

Keduanya harus **terukur, terbukti, dan selaras standar**. Bukan opini.

Rujukan utama: **NIST CSF 2.0** (fungsi

Govern–Identify–Protect–Detect–Respond–Recover) dan **ISO/IEC 27001:2022 (ISMS)**.

([NIST Technical Series Publications](#))

Kenapa urgensinya tinggi?

- **Biaya kebocoran data naik.** Rata-rata global 2024 = **USD 4,88 juta**; sektor keuangan lebih mahal ≈ **USD 6,08 juta** per insiden. Ini langsung menggerus laba dan reputasi. ([IBM](#))
- **Transaksi digital makin jadi sasaran.** Serangan *phishing* dan *account takeover* meningkat; regulator dan komunitas standar mendorong *phishing-resistant MFA* (*FIDO2/passkeys*). ([FIDO Alliance](#))
- **Standar pembayaran ikut naik kelas.** **PCI DSS v4.0.1 (2024)** menguatkan kontrol data kartu dan *logging/monitoring* untuk mencegah kebocoran di jalur pembayaran. ([PCI Security Standards Council](#))

Apa yang dimaksud “keamanan data nasabah” (ringkas & praktis)?

Fokus pada **data pribadi** dan **data finansial** di semua siklus hidup: dikumpulkan, diproses, disimpan, dipindahkan, dan dimusnahkan. Komponen kunci yang dinilai:

- **Inventaris & klasifikasi data.** Tahu *di mana* data sensitif berada, siapa yang akses, dan untuk apa. (Pilar **Identify** di NIST CSF 2.0). ([NIST Technical Series Publications](#))
- **Kontrol akses & least privilege.** Wajib **MFA**; dorong *phishing-resistant MFA* seperti *FIDO2/passkeys*. ([FIDO Alliance](#))
- **Enkripsi & tokenization.** Data sensitif *at rest* dan *in transit* harus terenkripsi; data kartu mengikuti **PCI DSS**; data sangat sensitif sebaiknya di tokenisasi. ([middlebury.edu](#))
- **Standar manajemen keamanan.** **ISO/IEC 27001:2022** untuk *ISMS* aktif, dengan kontrol **Annex A** (93 kontrol) sebagai *guardrail*. ([ISO](#))
- **Pemantauan & logging.** *Telemetry* terpadu untuk deteksi anomali dan *forensics* (selaras PCI DSS v4 dan NIST). ([middlebury.edu](#))

Apa yang dimaksud “keamanan transaksi digital”?

Menjaga **kerahasiaan**, **integritas**, dan **keaslian** transaksi end-to-end — dari *onboarding* sampai *settlement*.

- **Proteksi kanal.** *End-to-end encryption*, *HSTS*, pinning sertifikat. (Praktik baik PCI DSS & ISO). (middlebury.edu)
- **Autentikasi kuat.** *Phishing-resistant MFA*, *device binding*, *behavioral biometrics* untuk cegah *session hijacking* dan *account takeover*. ([FIDO Alliance](https://fidoalliance.org))
- **Deteksi anomali real-time.** Skor risiko transaksi, *velocity checks*, dan *challenge* adaptif. (Selaras fungsi **Detect/Respond** di NIST CSF 2.0). ([NIST Technical Series Publications](https://nist.gov/technical-series-publications))
- **Kepatuhan pembayaran.** Untuk data kartu, penuhi **PCI DSS v4.0.1** (12 persyaratan: segmentasi, *logging*, *testing*, kebijakan). (middlebury.edu)

KPI inti yang mudah dibaca direksi (contoh, bisa langsung dipakai)

Data nasabah

- **Cakupan enkripsi *at rest/in transit*** (% sistem yang patuh). Target $\geq 99\%$. (ISO 27001/Annex A). ([ISO](https://iso.org))
- **Akurasi inventaris data sensitif** (% aset terpetakan). Target 100%. (NIST CSF – Identify). ([NIST Technical Series Publications](https://nist.gov/technical-series-publications))
- **Akses berisiko tinggi dengan MFA** (% akun admin/privileged). Target 100%. (FIDO2 rekomendasi regulator). ([FIDO Alliance](https://fidoalliance.org))

Transaksi digital

- **Tingkat adopsi *phishing-resistant MFA*** di kanal prioritas (% pengguna aktif). Target naik QoQ. ([FIDO Alliance](https://fidoalliance.org))
- **False positive/false negative** sistem deteksi penipuan (%). Target turun. (NIST CSF – Detect/Respond). ([NIST Technical Series Publications](https://nist.gov/technical-series-publications))
- **Waktu deteksi & tanggap** (MTTD/MTTR) untuk insiden transaksi prioritas-1 (jam). Target turun. ([NIST Technical Series Publications](https://nist.gov/technical-series-publications))
- **Kepatuhan PCI DSS v4.0.1** (status & temuan mayor/minor). Target: *clean* audit. (middlebury.edu)

Kenapa penting? Data IBM menunjukkan biaya kebocoran di finansial paling tinggi. KPI di atas lah yang menurunkannya, karena mempercepat deteksi, menahan dampak, dan memotong *fraud loss*. ([IBM](https://ibm.com))

90 hari pertama: *playbook* tanpa basa-basi

- **Minggu 1–4 — Baseline & *quick fixes***
 - Petakan **inventaris data** + klasifikasi sensitif.
 - Nyalakan **MFA** untuk semua akun berisiko tinggi; mulai *pilot FIDO2/passkeys* di kanal digital. ([FIDO Alliance](#))
 - Audit kepatuhan **PCI DSS** pada komponen pembayaran; tutup temuan kritikal. ([middlebury.edu](#))
- **Minggu 5–8 — Proteksi & pemantauan**
 - Terapkan **enkripsi wajib** dan **tokenization** untuk data yang sering berpindah. (PCI DSS & ISO). ([middlebury.edu](#))
 - Integrasikan *telemetry* ke pusat *logging/SIEM*; aktifkan deteksi anomali transaksi real-time. (NIST CSF – Detect). ([NIST Technical Series Publications](#))
- **Minggu 9–12 — Uji & latih**
 - Gelar **uji pemulihan** (*restore drill*) untuk satu *payment flow* ujung-ke-ujung.
 - Lakukan **table-top exercise** untuk skenario *account takeover* + *card data exfiltration*; ukur MTBD/MTTR; perbaiki *playbook*. (NIST CSF – Respond/Recover). ([NIST Technical Series Publications](#))

Red flags yang menurunkan *rating*

- **Tidak ada inventaris data sensitif** yang akurat; tidak tahu data ada di mana. (NIST – Identify). ([NIST Technical Series Publications](#))
- **MFA hanya SMS/OTP** tanpa rencana menuju *phishing-resistant MFA*. ([FIDO Alliance](#))
- **Audit PCI DSS gagal** atau temuan mayor berulang. ([middlebury.edu](#))
- **MTBD/MTTR tinggi** dan tidak ada *after-action review*. (NIST – Detect/Respond). ([NIST Technical Series Publications](#))

Bagaimana masuk ke *rating* (AAA–D)?

- **AAA–AA**: ISMS aktif; enkripsi & *tokenization* luas; *phishing-resistant MFA* dominan; PCI DSS *clean*; MTBD/MTTR rendah; *drill* rutin.
- **A–BBB**: kontrol ada tapi belum merata; *passkeys* baru pilot; beberapa temuan PCI minor; *drill* belum menyentuh semua *journey*.
- **BB–B**: inventaris data lemah; MFA tidak konsisten; deteksi lambat; temuan PCI berulang.
- **CCC–D**: *gaps* besar; tidak ada *governance*; banyak insiden transaksi tanpa perbaikan tuntas.

Ringkasan

Keamanan data nasabah dan transaksi digital **bukan proyek IT**. Ini **bahasa laba rugi**. Pegang **NIST CSF 2.0** untuk kerangka, **ISO/IEC 27001:2022** untuk tata kelola, dan **PCI DSS v4.0.1** untuk pembayaran. Perbanyak bukti, kurangi jargon. Naikkan *rating* dengan tiga kunci: **inventaris data yang rapi**, **MFA tahan-phishing**, dan **deteksi-respon yang cepat**. Biaya insiden turun. Kepercayaan naik. Bisnis aman. ([NIST Technical Series Publications](#))

Bagian IV — Framework & Arsitektur Penilaian

Bab 10: Struktur IISRI CyberRank Framework

Penjelasan IISRI CyberRank: Kriteria Ranking dari AAA hingga D

IISRI (Independent Information Security Rating Institute) CyberRank adalah sistem penilaian eksternal berbasis AI yang menilai tingkat kematangan keamanan informasi dan/atau privasi suatu organisasi berdasarkan data publik yang tersedia pada waktu tertentu. Penilaian ini mirip dengan rating kredit di sektor keuangan, tetapi fokus pada efektivitas kontrol keamanan siber. Skala rating berkisar dari **AAA** (tertinggi, paling aman) hingga **D** (terendah, paling berisiko).

Setiap tingkat rating memiliki **kriteria utama** (deskripsi tentang kecukupan kontrol keamanan, rekomendasi perbaikan, dan tingkat risiko). Berikut adalah penjelasan lengkap untuk masing-masing tingkat, disusun dalam tabel untuk kemudahan pemahaman:

Rating	Kriteria Utama (Deskripsi dan Rekomendasi)	Penilaian Kualitatif	Tingkat Risiko
AAA	Semua kontrol keamanan informasi dan/atau privasi memadai, tepat, dan efektif untuk memberikan jaminan wajar bahwa risiko keamanan dan privasi dikelola dengan baik serta tujuan tercapai. Tidak ada rekomendasi perbaikan signifikan.	Excellent (Sangat Baik)	Tidak ada hingga minimal
AA	Hampir semua kontrol keamanan informasi dan/atau privasi memadai, tepat, dan efektif untuk memberikan jaminan wajar bahwa risiko keamanan dan privasi dikelola dengan baik serta tujuan tercapai.	Very good (Sangat Baik)	Sangat rendah
A	Hampir semua kontrol keamanan informasi dan/atau privasi memadai, tepat, dan efektif untuk memberikan jaminan wajar bahwa risiko keamanan dan privasi dikelola dengan baik serta tujuan tercapai. Beberapa kelemahan kontrol spesifik dicatat; disarankan pekerjaan tambahan minor pada keamanan atau privasi.	Good (Baik)	Rendah
BBB	Kontrol utama keamanan informasi dan/atau privasi memadai, tepat, dan efektif untuk memberikan jaminan wajar bahwa risiko keamanan dan privasi dikelola dengan baik serta tujuan tercapai. Beberapa kelemahan kontrol	Satisfactory (Cukup Memuaskan)	Rendah

spesifik dicatat; disarankan pekerjaan tambahan minor pada keamanan atau privasi.

BB	Kontrol utama keamanan informasi dan/atau privasi memadai, tepat, dan efektif untuk memberikan jaminan wajar bahwa risiko keamanan dan privasi dikelola dengan baik serta tujuan tercapai. Beberapa kelemahan kontrol spesifik dicatat; disarankan pekerjaan tambahan sedang pada keamanan atau privasi.	Sufficient (Cukup)	Sedang
B	Beberapa kontrol keamanan informasi dan/atau privasi memadai, tepat, dan efektif untuk memberikan jaminan wajar bahwa risiko keamanan dan privasi dikelola dengan baik serta tujuan tercapai. Banyak kelemahan kontrol spesifik dicatat; sangat disarankan pekerjaan tambahan besar pada keamanan atau privasi.	Moderate (Sedang)	Sedang
CCC	Kontrol utama keamanan informasi dan/atau privasi tidak mungkin memberikan jaminan wajar bahwa risiko keamanan dan privasi dikelola dengan baik serta tujuan tercapai. Sangat disarankan pekerjaan besar pada keamanan atau privasi.	Insufficient (Tidak Cukup)	Tinggi
CC	Hampir semua kontrol keamanan informasi dan/atau privasi tidak mungkin memberikan jaminan wajar bahwa risiko keamanan dan privasi dikelola dengan baik serta tujuan tercapai. Sangat disarankan pekerjaan besar pada keamanan atau privasi.	Very insufficient (Sangat Tidak Cukup)	Tinggi
C	Hampir semua kontrol keamanan informasi dan/atau privasi tidak mungkin memberikan jaminan wajar bahwa risiko keamanan dan privasi dikelola dengan baik serta tujuan tercapai. Diperlukan pekerjaan besar atau program baru lengkap pada keamanan atau privasi.	Poor (Buruk)	Sangat tinggi
D	Semua kontrol keamanan informasi dan/atau privasi tidak memberikan jaminan apa pun bahwa risiko keamanan dan privasi dikelola dengan baik serta tujuan tercapai. Diperlukan program baru lengkap pada keamanan atau privasi.	Very poor (Sangat Buruk)	Hampir pasti

Catatan Tambahan:

- **Pembaruan:** Rating ini diperbarui secara harian oleh sistem CyberRank IISRI berdasarkan data publik seperti sertifikasi (misalnya ISO 27001, SOC 2), insiden keamanan, dan praktik vendor risk management.
- **Manfaat:** Organisasi dengan rating tinggi (AAA hingga A) sering diakui dalam IISRI CyberRank Awards, yang meningkatkan kredibilitas mereka di industri.
- **Sumber:** Penjelasan ini didasarkan pada kerangka resmi IISRI CyberRank.

Komponen hukum, teknis, dan tata kelola

Kenapa struktur ini penting?

Bank butuh kerangka yang **adil, terukur, dan bisa diaudit**. IISRI CyberRank menyatukan tiga komponen agar keputusan tidak pakai *feeling*, tapi **bukti**:

1. **Hukum (legal).**
2. **Teknis (controls & operasi).**
3. **Tata kelola (governance).**

Hasilnya: perlindungan data nasabah, transaksi tetap jalan, dan bank **patuh regulasi**.
Rujukan utama: **UU PDP, POJK 38/2016, BSSN 8/2020, NIST CSF 2.0, dan ISO/IEC 27001:2022**. ([Peraturan BPK](#))

1. Komponen Hukum (Legal)

Tujuan: pastikan semua praktik digital **selaras regulasi** Indonesia dan standar sektor.

- **UU No. 27/2022 (PDP).** Mengatur hak subjek data, kewajiban pengendali/prosesor, dasar pemrosesan, hingga kewajiban **pemberitahuan insiden**. Di sini CyberRank menilai **bukti penerapan**, bukan sekadar kebijakan di kertas. ([Peraturan BPK](#))
- **POJK 38/POJK.03/2016.** Bank **wajib** menerapkan manajemen risiko TI: pengawasan aktif Direksi/Dekom, kebijakan–prosedur, proses identifikasi–pemantauan risiko, dan *internal control*. *Clause* ini jadi *anchor* penilaian. ([OJK](#))
- **BSSN 8/2020.** Untuk *PSE strategis*, wajib merujuk **SNI ISO/IEC 27001** dan standar keamanan lain; ada koridor **CSIRT** dan pengamanan sistemik. Ini mengikat praktik keamanan agar tidak lepas dari standar nasional. ([Peraturan BPK](#))

Ringkasnya: komponen hukum membuat langkah teknis bank **defensible** di mata regulator—jelas pasal, jelas bukti. ([OJK](#))

2. Komponen Teknis (Controls & Operasi)

Tujuan: kontrol nyata di lapangan yang menjaga **kerahasiaan, integritas, ketersediaan**.

- **NIST CSF 2.0** sebagai tulang punggung *checklist*: **Govern – Identify – Protect – Detect – Respond – Recover**. Versi 2.0 menegaskan fungsi **Govern** dan *supply chain risk*. Cocok untuk memetakan kontrol ke *outcome* yang mudah dipahami bisnis. (csrc.nist.gov)
- **ISO/IEC 27001:2022** untuk *ISMS*: persyaratan dan kontrol **Annex A** (93 kontrol) mencakup organisasi, manusia, fisik, dan teknologi. Status sertifikasi, lingkup, dan *non-conformity* jadi poin skor. ([ISO](#))
- **Praktik pendukung** (contoh yang dinilai):
 - *Asset & data inventory*, klasifikasi data sensitif.
 - **MFA** (idealnya *phishing-resistant*), segmentasi jaringan, enkripsi *at rest/in transit*.
 - *Logging/SIEM*, deteksi anomali, uji *restore*, dan *table-top exercise*.

- Untuk data kartu: **PCI DSS v4.0.1** (*segmentation, logging, testing*). ([NIST Technical Series](#))

Intinya: komponen teknis memastikan bank **do it right**—kontrol berjalan, terukur, dan siap diuji.

3. Komponen Tata Kelola (*Governance*)

Tujuan: siapa bertanggung jawab, bagaimana akuntabilitas dijaga, dan bagaimana keputusan risiko dibuat.

- **NIST CSF 2.0 – Govern.** Menetapkan peran, otoritas, *risk appetite*, dan *oversight* dewan/manajemen. Termasuk pengawasan risiko **pihak ketiga/outsourcing**. ([csrc.nist.gov](#))
- **Keterkaitan dengan POJK.** POJK menuntut pengawasan aktif Direksi/Dekom, pelaporan berkala, dan *issue closure* yang terdokumentasi—ini diterjemahkan ke *board scorecard* siber. ([OJK](#))
- **Artefak tata kelola yang dinilai:**
 - *Cyber risk appetite statement* yang disetujui dewan.
 - *Board attestation* tahunan atas kepatuhan UU PDP/POJK.
 - *Issue-to-closure log* dengan SLA dan *owner* jelas.
 - Agenda Komite Risiko/Audit yang rutin meninjau metrik siber.

Intinya: tata kelola membuat **do it right** menjadi **keep doing it right**—konsisten dan akuntabel.

Cara skoringnya (singkat, lugas)

- **Pemetaan silang:** setiap kontrol teknis ditautkan ke **pasal UU/POJK** dan **pemilik tata kelola** → mudah ditelusuri saat audit. ([Peraturan BPK](#))
- **Skor berbasis bukti:**
 - **Legal:** kepatuhan pasal dan mekanisme pelaporan.
 - **Teknis:** performa kontrol & temuan audit.
 - **Governance:** keputusan dewan, *closure rate*, dan frekuensi *challenge*.
- **Transparan & *audit-trail*:** dari *rating* ke bukti lapangan bisa dibuka balik tanpa drama.

90-hari implementasi (aksi cepat)

- **Minggu 1–4 | *Baseline* hukum.** *Compliance mapping* UU PDP–POJK–BSSN; pastikan alur pelaporan insiden dan *data subject request* berjalan. ([Peraturan BPK](#))
- **Minggu 5–8 | Teknis prioritas.** Terapkan kontrol NIST/ISO yang berdampak besar: inventaris aset & data, MFA, enkripsi, *logging/SIEM*, uji *restore*. ([NIST Technical Series](#))
- **Minggu 9–12 | Tata kelola hidup.** Tetapkan *risk appetite*, aktifkan *board scorecard*, dan lakukan *table-top* lintas fungsi dengan *after-action review*. ([csrc.nist.gov](#))

Ringkasan

Legal memastikan *do the right thing*. **Teknis** memastikan *do it right*. **Governance** memastikan *keep doing it right*. Dengan rujukan **UU PDP**, **POJK 38/2016**, **BSSN 8/2020**, **NIST CSF 2.0**, dan **ISO/IEC 27001:2022**, Struktur IISRI CyberRank memberi **peta jalan yang jelas** untuk bank: patuh, aman, dan tangguh—berbasis **bukti**, bukan jargon. ([Peraturan BPK](#))

Kalau diinginkan, saya bisa susun **matriks pemetaan 1 halaman** (kolom: regulasi → kontrol → bukti → pemilik → SLA) agar siap dibawa ke rapat Komite Manrisk.

Indikator risiko siber & privasi (berbasis 33 pasal UU PDP + ISO 27001 + NIST CSF)

Intinya: bank butuh ukuran yang jelas dan objektif. Bukan opini. Bukan *checklist* seadanya. Indikator di bawah ini langsung terhubung ke tiga rujukan utama: **UU PDP**, **ISO/IEC 27001:2022 (Annex A – 93 kontrol)**, dan **NIST CSF 2.0**. ([Peraturan BPK](#))

A. Indikator Berbasis Hukum (UU PDP)

Tujuan: pastikan hak nasabah dilindungi, insiden dilaporkan cepat, dan proses data tertib.

- **Hak Subjek Data terpenuhi**
 - *Service level* respons akses/koreksi data $\leq 3 \times 24$ jam tercatat di *log* (acu Pasal akses/permintaan data). ([ABNR - Counsellors at Law](#))
 - Tersedia kanal mudah: *web form*, cabang, *contact center*. Bukti: tiket & metrik bulanan. ([Peraturan BPK](#))
- **Dasar pemrosesan & minimisasi**
 - Setiap *dataset* punya *record of processing* (tujuan, dasar hukum, retensi). Minimal 95% sistem kritikal sudah punya *record*. ([Peraturan BPK](#))
- **Pemberitahuan insiden ke regulator & nasabah**
 - *Timer* pelaporan insiden aktif. Bukti: *runbook* & *notifikasi template*. *Drill* triwulan. (Kewajiban perlindungan & pemberitahuan kegagalan). ([Peraturan BPK](#))
- **Kontrak dengan processor**
 - 100% vendor yang menyentuh data pribadi punya klausul PDP: tujuan, larangan *secondary use*, *Breach Notification*, *sub-processor* transparan. ([Peraturan BPK](#))

Skor cepat:

- 4 = semua bukti lengkap & teruji drill
- 3 = bukti ada tapi drill terbatas
- 2 = prosedur ada tapi bukti kurang
- 1 = belum terdokumentasi

B. Indikator Berbasis Standar (ISO/IEC 27001:2022)

Tujuan: kontrol teknis dan organisasi berjalan, bukan hanya sertifikat di dinding.

- **Kelengkapan kontrol Annex A (93 kontrol)**
 - *Coverage* kontrol per sistem kritikal (pembayaran, *mobile banking*, *core*). Target $\geq 90\%$ *implemented* (empat tema: organisasi, manusia, fisik, teknologi). ([itgovernance.co.uk](#))
- **Manajemen risiko berulang**

- Siklus *risk assessment* dan *treatment* minimal 2×/tahun pada aset kritikal. Ada *risk owner* & *target residual risk*. (itgovernance.co.uk)
- **Uji ketahanan & *hardening***
 - *Vulnerability scanning* mingguan, *patch SLA*: kritikal ≤ 7 hari. Uji *penetration* 2×/tahun untuk aplikasi berisiko tinggi. (Bagian kontrol teknologis & operasional Annex A). (itgovernance.co.uk)
- **Kesiapan SDM & *awareness***
 - Pelatihan *phishing simulation* triwulan; tingkat klik < 5% untuk unit layanan nasabah & operasional. (Kontrol People). (ISMS.online)

Skor cepat (per domain ISO):

- 4 = kontrol efektif + metrik
- 3 = kontrol jalan tapi metrik belum stabil
- 2 = kontrol sebagian
- 1 = gap mayor.

C. Indikator Berbasis *Framework* (NIST CSF 2.0)

Tujuan: ketahanan ujung-ke-ujung. Bukan hanya *prevent*, tapi juga *detect–respond–recover*.
Fungsi NIST: *Govern, Identify, Protect, Detect, Respond, Recover*. (NIST Technical Series)

- **GOVERN — Tata kelola risiko siber**
 - Dewan menerima *cyber risk dashboard* per kuartal: 5–10 metrik kunci, termasuk *loss events* & *near-miss*. (NIST Technical Series)
- **IDENTIFY — Inventaris aset & *crown jewels***
 - ≥ 98% aset kritikal terinventarisir; *data flow map* untuk data pribadi & transaksi. (NIST Technical Series)
- **PROTECT — *Zero trust* dasar & kontrol akses**
 - MFA untuk semua *admin* dan kanal nasabah; *network segmentation* untuk sistem pembayaran. (NIST Technical Series)
- **DETECT — *Telemetry* & *use case***
 - *Mean Time to Detect (MTTD)* < 24 jam untuk anomali prioritas-1; *use case* SIEM meliputi *account takeover* & *fraud*. (NIST Technical Series)
- **RESPOND — *Playbook* insiden PDP**
 - *Tabletop exercise* lintas unit (TI, hukum, *contact center*) minimal 2×/tahun. (NIST Technical Series)
- **RECOVER — Pemulihan layanan**
 - RTO/RPO disetujui bisnis; *restore test* triwulan untuk *core banking* & *mobile*. (NIST Technical Series)

Skor cepat (fungsi NIST):

- 4 = terukur & konsisten
- 3 = terukur sebagian
- 2 = prosedural
- 1 = ad-hoc.

D. Indikator Spesifik Transaksi Kartu (opsional namun penting)

Untuk bank penerbit/acquirer, tambahkan indikator *PCI DSS v4.0.1* (aktif per 1 Jan 2025). Contoh: *scope* kartu jelas, *encryption* data PAN, *logging* transaksi, uji tahunan. (blog.pcisecuritystandards.org)

E. Contoh Scorecard (ringkas dan tajam)

Gunakan skala **AAA–D** per dimensi, lalu gabungkan.

- **Privasi (UU PDP):** hak & notifikasi — AAA / AA / A / BBB / ... / D
- **ISO 27001 (Annex A):** kontrol & kedewasaan — AAA–D
- **NIST CSF 2.0:** kesiapan G–I–P–D–R–R — AAA–D
- **Tambah PCI (bila relevan):** *Compliant* / *Minor Gap* / *Major Gap*

Aturan agregasi sederhana:

- Nilai akhir = *weighted average*, dengan bobot: Privasi 35%, ISO 35%, NIST 30%.
- *Floor rule*: bila salah satu < **BB**, rating akhir turun satu tingkat (untuk lindungi nasabah).

F. Metrik yang Mudah Dipahami CFO & Komite Risiko

Bahasa sederhana. Angka nyata. Dampak ke bisnis.

- **MTTD / MTTR insiden prioritas-1** (jam) → efek ke *downtime* layanan. ([NIST Technical Series](#))
- **Rasio insiden terlapor sesuai SLA PDP** (%) → risiko denda & reputasi. ([Peraturan BPK](#))
- **Coverage kontrol Annex A pada *crown jewels*** (%) → risiko kebocoran data & fraud. (itgovernance.co.uk)
- **Tingkat klik *phishing*** (%) pada unit frontliner → risiko *account takeover*. ([ISMS.online](#))
- **Kepatuhan PCI (jika relevan)** → risiko *chargeback* & biaya kepatuhan. ([PCI Security Standards Council](#))

G. Kenapa relevan sekarang?

- UU PDP sudah berlaku dan menuntut proses yang rapi dan dapat dibuktikan. ([Peraturan BPK](#))
- NIST CSF 2.0 memperkuat fungsi **GOVERN** agar manajemen puncak memegang kendali risiko siber, bukan hanya tim TI. ([NIST Technical Series](#))
- ISO 27001:2022 menyederhanakan ke **93 kontrol** agar bank fokus pada kontrol yang berdampak. ([itgovernance.co.uk](#))
- Bagi transaksi kartu, PCI **v4.0.1** sudah menggantikan v4.0 mulai **1 Jan 2025**; penting untuk *issuer/acquirer*. ([blog.pcisecuritystandards.org](#))

H. Cara Pakai di Bank (langkah cepat)

1. Petakan *crown jewels* (data pribadi, *core*, *mobile*, *payment*).
2. *Gap assessment* terhadap UU PDP, Annex A 93 kontrol, dan NIST CSF 2.0.
3. Tetapkan target *MTTD/MTTR*, cakupan kontrol, dan SLA pelaporan PDP.
4. Jalankan *tabletop & drill* triwulan; perbarui *risk register*.
5. Publikasikan *scorecard* ke komite risiko & OJK sebagai bagian profil risiko digital. ([OJK](#))

Penutup

Transparansi butuh angka. Akuntabilitas butuh bukti. Dengan indikator di atas, *digital trust* naik, risiko turun, dan biaya kebocoran bisa ditekan sebelum terjadi.

Catatan: ringkasan ini merujuk langsung ke UU PDP, NIST CSF 2.0, ISO/IEC 27001:2022, serta PCI DSS v4.0.1 (untuk transaksi kartu). Gunakan sebagai *baseline*. Sesuaikan bobot dan ambang sesuai profil risiko bank Anda. ([Peraturan BPK](#))

Bab 11: Model Skor dan Interpretasi Rating (AAA–D)

Tabel penilaian dan deskripsi tingkat risiko

Ide besar

- Skor menggambarkan **ketahanan siber** dan **kepatuhan UU PDP** dalam satu pandangan.
- Rujukan praktik baik: *NIST CSF 2.0* (fungsi *Govern–Identify–Protect–Detect–Respond–Recover*) ([NIST Technical Series](#)), **ISO/IEC 27001:2022** (93 kontrol *Annex A*) ([ISO](#)), **PCI DSS v4.0.1** untuk data kartu pembayaran ([PCI Security Standards Council](#)), dan **BCBS Principles for Operational Resilience** untuk ketahanan operasional perbankan ([Bank for International Settlements](#)).
- Kewajiban lokal: **UU No. 27/2022 (PDP)** termasuk notifikasi insiden dan perbaikan dalam kerangka waktu yang ditentukan hukum ([JDIH Komdigi](#)).

Cara membaca rating

- **AAA–AA–A** = kuat. Risiko rendah.
- **BBB–BB–B** = moderat. Ada celah yang harus ditutup.
- **CCC–CC–C** = lemah. Risiko tinggi. Perlu perbaikan cepat.
- **D** = gagal. Ada pelanggaran berat atau *control breakdown*.

Prinsipnya mirip *credit rating*. Bedanya, ini menilai *digital trust*: tata kelola, kontrol teknis, dan bukti kepatuhan.

Komponen skor (ringkas)

Skor total = 100. Bobot seimbang agar adil dan praktis:

1. **Governance & PDP Compliance (30%)**
 - Struktur *governance*, peran CISO/DPO, *policy* dan bukti kepatuhan UU PDP, *breach notification* sesuai aturan.
 - Selaras *NIST CSF – Govern* dan klausul ISO 27001. ([NIST Technical Series](#))
2. **Technical Controls & Secure Architecture (30%)**
 - Implementasi kontrol ISO 27001:2022 *Annex A*, *hardening*, enkripsi, *IAM*, pemantauan, *secure SDLC*.
 - Untuk data kartu: keselarasan PCI DSS v4.0.1. ([itgovernance.co.uk](#))
3. **Detection & Incident Response (20%)**
 - *Threat detection*, *SIEM/SOC*, uji *playbook*, MTTR, kedisiplinan pelaporan insiden ke regulator/otoritas terkait.
 - *NIST CSF – Detect/Respond*. ([NIST Technical Series](#))
4. **Operational Resilience (20%)**

- *Business continuity, disaster recovery*, uji skenario lintas vendor, *stress test* layanan kritikal.
- Mengacu BCBS *operational resilience*. ([Bank for International Settlements](#))

Tabel rating yang “bicara”

Ratin g	Skor	Kondisi singkat	Makna risiko	Contoh sinyal kunci
AAA	95–100	<i>World-class</i> . Tata kelola matang. <i>Controls</i> menyeluruh.	Sangat rendah	ISO 27001 tersertifikasi, SOC 24/7, uji krisis rutin, patuh PDP & PCI, <i>zero critical findings</i> . (ISO)
AA	90–94	Kuat dan konsisten. <i>Gap</i> kecil.	Rendah	<i>Penetration test</i> triwulan, <i>automated patching</i> , notifikasi insiden siap jalan.
A	85–89	Baik. Masih ada <i>legacy risk</i> .	Rendah–Moderat	Beberapa kontrol manual, <i>vendor</i> kritikal sudah ditata, latihan IR tahunan.
BBB	80–84	Cukup. <i>Coverage</i> kontrol belum merata.	Moderat	Sebagian aset belum di- <i>inventory</i> , korelasi log terbatas, <i>DR drill</i> belum tahunan.
BB	75–79	Rapuh di area tertentu.	Moderat–Tinggi	<i>Patch latency</i> panjang, <i>MFA</i> belum penuh, kontrak <i>vendor</i> kurang klausul PDP.
B	70–74	Banyak <i>gap</i> .	Tinggi	<i>Logging</i> parsial, SOP pelaporan insiden belum jelas.
CCC	60–69	Kontrol dasar lemah.	Sangat tinggi	Tidak ada <i>threat hunting</i> , enkripsi tidak konsisten.

CC	50–59	Risiko kritikal terbuka.	Ekstrem	<i>Known critical vuln</i> tidak ditutup, pelatihan minim.
C	40–49	Hampir gagal.	Ekstrem	Audit temukan pelanggaran materiil PDP.
D	< 40	Gagal. Pelanggaran serius / <i>major incident</i> tanpa tata kelola.	Kegagalan	Tidak patuh UU PDP, <i>outage</i> berkepanjangan, <i>control breakdown</i> . (JDIH Komdigi)

Catatan: ambang skor dapat disesuaikan OJK berdasar profil risiko bank dan *regulatory appetite*.

Mengapa model ini relevan dengan kondisi keuangan sekarang?

- Serangan siber berdampak ke **kepercayaan pasar**, biaya modal, dan biaya operasional. *Downtime* berarti hilangnya fee, potensi *liquidity stress*, dan denda kepatuhan.
- Standar global makin ketat. *NIST CSF 2.0* menambahkan fungsi *Govern* untuk menekankan tanggung jawab manajemen puncak. *PCI DSS v4.0.1* memperbarui kontrol pembayaran dan tenggat adopsi. ISO 27001:2022 merapikan kontrol jadi 93 butir agar lebih fokus pada *risk/outcome*. Semua ini menekan bank untuk *continuous improvement*. ([NIST](#))
- Regulator perbankan global mendorong **operational resilience** agar layanan kritikal tetap berjalan saat krisis digital. Ini bukan sekadar *IT hygiene*, tapi pilar stabilitas sistem keuangan. ([Bank for International Settlements](#))

“Skor ke aksi” — interpretasi yang menantang

- **AAA–AA**
 - Pertahankan. Jadikan *benchmark* industri. Buka *bug bounty* dan *red team* eksternal.
- **A–BBB**
 - Tutup *gap* yang berdampak pada PDP, *detection coverage*, dan *vendor lock-in*. Target **naik 1 level** dalam 12 bulan.
- **BB–B**
 - Masuk *improvement plan* resmi. Prioritaskan *MFA*, *patching SLA*, *asset inventory*, dan *SIEM correlation*.
- **CCC–C**

- Aktifkan *war room*. *Freeze* perubahan non-esensial. *Rapid remediation* pada kontrol dasar: enkripsi, logging, *IR playbook*.
- D
 - *Regulatory escalation*. Rencana pemulihan menyeluruh, *board oversight*, dan *external assurance*.

Bukti yang dinilai (contoh singkat)

- *Policy* dan bukti implementasi ISO 27001:2022 (daftar kontrol relevan, risiko, *statement of applicability*). ([ISO](#))
- *Mapping* kapabilitas ke *NIST CSF 2.0* (GOV-ID-PR-DE-RS-RC) dan metrik kinerja IR/BCP. ([NIST Technical Series](#))
- Kepatuhan PCI DSS v4.0.1 untuk seluruh *payment flows*. Bukti *compensating controls* jika ada. ([PCI Security Standards Council](#))
- Artefak PDP: *consent record*, DPIA, SLA pelaporan insiden, *data subject rights* & bukti pemenuhan tenggat di UU PDP. ([JDIH Komdigi](#))
- Bukti *resilience*: hasil uji DR, *RTO/RPO*, uji skenario BCBS (gangguan siber, *third-party failure*). ([Bank for International Settlements](#))

Ringkasan

Rating ini membuat *digital trust* terlihat dan terukur. Bahasa bisnisnya sederhana: **skor naik → biaya risiko turun → kepercayaan naik**. Tantangannya jelas: **buktikan kontrol, bukan janji**. Dengan rangka kerja yang mengacu ke standar global dan hukum nasional, bank Indonesia bisa tumbuh **aman** dan **pasti patuh**.

Batas minimal rating per kategori bank (BUKU 2 – 4)

Tujuan singkat: memberi *benchmark* yang jelas, adil, dan bisa diaudit. Supaya tiap bank tahu “ambang bawah” keamanan siber dan kepatuhan data. Mudah dicek. Mudah ditindaklanjuti. Dampaknya langsung ke kepercayaan nasabah, stabilitas, dan biaya modal.

Catatan istilah: OJK sudah mengganti klasifikasi **BUKU** menjadi **KBMI** lewat POJK 12/2021. Banyak pelaku masih memakai istilah BUKU. Framework ini mengikuti penyebutan BUKU (sebagai jembatan), sambil merujuk perubahan OJK terbaru.

Prinsip penetapan ambang (ringkas)

- **Semakin besar bank → ambang makin tinggi.** Karena dampak sistemiknya lebih besar (*too interconnected to fail*). Ini sejalan dengan prinsip *operational resilience* Basel Committee.
- **Kepatuhan bukan kertas.** Harus nyata: kontrol berjalan, log rapi, *alerting* hidup, *table-top exercise* rutin, dan *red team* berkala.
- **Selaras regulasi & standar.** Rujukan: UU PDP (UU 27/2022), POJK TI & SEOJK Ketahanan Siber, ISO/IEC 27001:2022, dan NIST CSF 2.0 (*Govern* function). ([OJK](#))

Usulan ambang minimal rating (wajib dipenuhi)

Skala rating: **AAA, AA, A, BBB, BB, B, C, D**

AAA = sangat kuat & proaktif

A = memadai tapi masih ada gap

BBB ke bawah = rawan dan perlu perbaikan cepat.

- **BUKU 4 (bank besar, aset/volume transaksi tertinggi)**
Minimal: AA.
Kenapa? Risiko sistemik tinggi, *24x7 critical services*, eksposur pihak ketiga luas, dan target utama serangan. Basel mendorong ketahanan end-to-end lintas pihak.
Jika < AA: larangan peluncuran produk digital baru, peningkatan frekuensi audit, *remediation plan* ≤ 90 hari, dan *executive attestation* ke OJK.
- **BUKU 3 (menengah-besar, penting secara regional/nasional)**
Minimal: A.
Kenapa? Volume tinggi, banyak integrasi *API*, dan ketergantungan *cloud/VPN* lintas lokasi. **Jika < A:** cap pertumbuhan pengguna digital sampai *finding* kritikal ditutup, *table-top exercise* insiden PDP triwulanan, dan penguatan kontrol prioritas ISO 27001 Annex A (*identity, logging, crypto, supplier security*).
- **BUKU 2 (menengah)**
Minimal: BBB.
Kenapa? Skala lebih kecil, tapi tetap mengelola data pribadi dan pembayaran ritel.
Jika < BBB: *moratorium* kerja sama baru dengan *vendor* berisiko, *patching SLA* ketat, *phishing drill* bulanan, serta pendampingan *SupTech* dari OJK. Rujuk SEOJK 29/2022 untuk ketahanan & keamanan siber. ([OJK](#))

Transisi BUKU → KBMI. Ketika bank berpindah kelas (modal/aktivitas naik), ambang rating ikut naik otomatis. Dasar klasifikasi terbaru ada di POJK 12/2021.

Cara menilai pemenuhan ambang (praktis)

- **Bukti “jalan” (bukan dokumen):** *attack surface* terkendali, *MFA* wajib, *EDR/SIEM* aktif, *alert-to-respond* < 15 menit, *RTO/RPO* sesuai skala layanan.
- **Pelaporan insiden PDP:** *Breach* terkonfirmasi → notifikasi ke regulator & subjek data sesuai UU PDP, dengan *root cause* & rencana perbaikan.
- **Kesiapan tata kelola:** Dewan komisaris mendapat *risk dashboard* kuartalan; fungsi *Govern* (NIST CSF 2.0) jelas: kebijakan, peran, *risk appetite*, dan pengawasan.
- **Kesesuaian standar:** Kontrol kunci ISO/IEC 27001:2022 (Annex A) terlacak ke risiko; ada *evidence* audit dan *continuous monitoring*.

Early-warning & sanksi bertahap (contoh mekanisme)

- **Skor jatuh 1 level dari ambang:** *Action plan* 90 hari + audit *follow-up*.
- **Jatuh 2 level:** pembatasan produk/kanal berisiko tinggi + *on-site review*.
- **Jatuh ≥3 level atau *material breach* PDP:** publikasi status pemulihan di *CyberTrust Report Card*, dan kewajiban *executive attestation* triwulanan ke OJK.

Apa untungnya bagi bank?

- **Biaya insiden turun.** Respon cepat = kerugian finansial menurun.
- **Akses insentif GCG.** Bank dengan rating di atas ambang dapat prioritas *regulatory fast-track* untuk inovasi.
- **Kepercayaan pasar.** Rating tinggi mempermudah kerja sama *cross-border* dan *wholesale funding*.

Ringkasan

- **BUKU 4 ≥ AA**
- **BUKU 3 ≥ A**
- **BUKU 2 ≥ BBB**
- Patuh UU PDP & SEOJK 29/2022; kelola risiko sesuai ISO 27001:2022 & NIST CSF 2.0. ([OJK](#))
- Jika di bawah ambang → *remediation*, pembatasan aktivitas digital, dan pengawasan intensif.
- Target 12 bulan: **naik ≥ 1 level** untuk semua bank di bawah ambang.

Dengan ambang yang jelas, pengawasan jadi *data-driven*, bank fokus pada kontrol yang berdampak, dan nasabah mendapat perlindungan nyata—bukan janji.

Bab 12: Proses Audit dan Sertifikasi Tahunan

Pengumpulan data otomatis (*data leak, domain risk, vendor exposure*)

Inti idenya sederhana: jangan menunggu insiden. Tarik data otomatis. Baca sinyal risiko harian. Jadikan bukti audit. Dengan cara ini, rating *CyberTrust* tidak lagi sekadar kertas. Ia hidup, terukur, dan bisa ditindaklanjuti.

Kenapa harus otomatis?

- Serangan makin cepat. Proses manual terlambat.
- Jejak risiko tersebar: internet, *cloud*, aplikasi, dan vendor.
- Bukti audit harus objektif, *timestamped*, dan bisa diverifikasi.
- Bank butuh *early warning* untuk menghindari biaya forensik, denda, dan *downtime*.

Tiga sumber data utama (ditarik harian)

1. *Data leak* (kebocoran data di luar)

Apa yang ditarik:

- Ekspos akun *email korporat* di dump publik/gelap.
- Kredensial bocor (*username/password*), *token*, *API key*, *session cookie*.
- Contoh *pattern* data sensitif: NIK, nomor kartu, *secret key* dalam *repo*.

Cara kerja singkat:

- *Crawler* + *feed threat intelligence*.
- *Regex/ML* untuk deteksi pola data sensitif.
- *De-duplication* + *hashing* untuk bukti.

Metrik & SLA aksi:

- *Mean Time to Triage (MTTT)*: ≤ 4 jam.
- *Credential exposure rate*: turun $\geq 50\%$ per kuartal.
- *Auto-reset password & token revoke* ≤ 6 jam.

Bukti audit:

- *Evidence hash*, tautan sumber, *screenshot* ter-anonimisasi, *playbook* perbaikan.

2. *Domain risk* (risiko merek & kanal digital)

Apa yang ditarik:

- *Attack surface*: domain/subdomain aktif, *open ports*, *expired certs*.
- *Brand abuse*: *phishing*, *typosquatting*, situs palsu, APK palsu.

- *Misconfiguration: TLS weak ciphers, HSTS hilang, SPF/DKIM/DMARC gagal.*

Cara kerja singkat:

- *Passive DNS + certificate transparency log.*
- *Scanning berkala non-intrusif.*
- *Brand monitoring untuk nama bank & varian ejaan.*

Metrik & SLA aksi:

- *Unknown subdomain ratio: → 0% (semua harus tercatat di asset inventory).*
- *Phishing takedown TTR: ≤ 24 jam sejak deteksi.*
- *TLS/Email security score: ≥ “strong” untuk kanal kritikal.*

Bukti audit:

- Daftar temuan, status *takedown*, perubahan *DNS/TLS*, log verifikasi.

3. Vendor exposure (paparan dari pihak ketiga)

Apa yang ditarik:

- *Security rating vendor (kebijakan, insiden publik, patch cadence).*
- *SBOM/software bill of materials* untuk aplikasi kritikal.
- *Bukti kontrol wajib: MFA, encryption at rest/in transit, logging, access review.*
- *Kontrak: klausul breach notification & hak audit.*

Cara kerja singkat:

- *Questionnaire otomatis + evidence upload.*
- *API ke portal vendor untuk compliance attestation.*
- *Continuous control monitoring (CCM) untuk endpoint yang dioperasikan vendor.*

Metrik & SLA aksi:

- *% vendor tier-1 tanpa kontrol wajib = 0%.*
- *Breach notification latency vendor: ≤ 72 jam.*
- *Remediation deadline temuan kritikal: ≤ 30 hari.*

Bukti audit:

- *Attestation bertanda tangan, control screenshots, log akses, ticket closure.*

Arsitektur pengumpulan

- **Konektor:** *API/feeds* ke sumber *threat intel*, *asset inventory*, *ticketing*.
- **Collector:** *agentless* bila mungkin; *agent* hanya untuk sistem kritikal.
- **Normalizer:** ubah semua data ke skema tunggal (*JSON schema*).
- **Scorer:** hitung skor pertemuan → indikator *data leak*, *domain risk*, *vendor exposure*.
- **Evidence Vault:** *WORM storage* dengan *hash* dan *immutability* untuk forensik.
- **Dashboard OJK/Bank:** status harian, tren bulanan, *drill-down* ke bukti.
- **Alerting:** *webhook* ke *SIEM/SOAR* untuk *auto-response*.

Prinsip *privacy by design*: tarik **minim data** yang perlu; *masking* data pribadi; akses dibatasi; semua *query* berjejak.

Skor & pembobotan (contoh praktis)

- *Data leak* = 40% (dampak langsung ke nasabah).
- *Domain risk* = 35% (pintu masuk serangan & reputasi).
- *Vendor exposure* = 25% (risiko *supply chain*).

Penalti instan: bila ada *material breach* PDP yang *unreported*, skor total turun 2 level sampai *remediation* lulus verifikasi.

Frekuensi & kalender kerja

- **Harian:** *crawl* kebocoran, pemantauan domain/sertifikat, *brand abuse*.
- **Mingguan:** validasi *false positive*, uji *takedown*, *patch compliance* sampel.
- **Bulanan:** *vendor attestation* terpilih, *table-top exercise* mini.
- **Triwulan:** *red team/phishing drill*, uji *incident communication*.
- **Tahunan (sertifikasi):** *evidence review*, *on-site/remote audit*, tanda tangan *executive attestation*.

Playbook aksi cepat (contoh)

- **Kredensial bocor terdeteksi:** *auto-reset* + *user notify* + pantau anomali transaksi 72 jam.
- **Phishing domain aktif:** *legal takedown* + blokir di DNS, WAF, dan *mail gateway*.
- **Vendor gagal kontrol wajib:** hentikan akses *prod*, alihkan trafik, *hotfix* 30 hari.

Bukti untuk sertifikasi (yang disukai auditor)

- *Timeline* deteksi → triase → mitigasi → *closure*.
- *Ticket ID* dan *owner* yang jelas.
- *Before–after* konfigurasi.
- *Hash* bukti & *chain of custody*.
- *Management sign-off* per insiden material.

Anti-window dressing (agar tak bisa “diakali”)

- Sumber data wajib lintas pihak (internal + eksternal).
- Sampling acak oleh auditor setiap bulan.
- *Challenge test*: auditor memancing *phishing* terkontrol; lihat respons.
- Korelasi silang: *SIEM log* vs laporan unit bisnis.
- *Penalty* bila temuan berulang tidak tuntas sesuai *SLA*.

Manfaat ke bisnis (bukan hanya “compliance”)

- Mengurangi *fraud loss* dan *chargeback*.
- Mempercepat izin peluncuran produk digital (bukti kuat).
- Meningkatkan *trust* nasabah dan mitra *wholesale*.
- Menjadi *insurance-ready* untuk polis *cyber*.

Ajakan bertindak (12 minggu eksekusi cepat)

1. Pasang *connector* ke 3 sumber data.
2. Tetapkan *SLA* & *runbook* respon 24/7.
3. Bangun *dashboard* + *evidence vault*.
4. Uji takedown *phishing* end-to-end.
5. Lakukan *mini-audit* bulanan dan *gap closure*.

Dengan pengumpulan data otomatis, audit tahunan berubah jadi proses yang ringan. Sertifikasi bukan “acara setahun sekali”, tapi hasil dari kerja harian yang konsisten—terlihat, terukur, dan dapat dipertanggungjawabkan.

Audit forensik, self-assessment, dan validasi oleh OJK

Tujuan bab ini: memastikan rating *CyberTrust* bukan sekadar dokumen. Harus ada bukti. Ada proses. Ada akuntabilitas. Hasilnya jelas: bank tahu risikonya, OJK yakin pengendalian jalan, nasabah merasa aman.

Gambaran besar alur tahunan

1. **Self-assessment** oleh bank
2. **Audit forensik** untuk bukti mendalam
3. **Validasi OJK** sebagai *independent assurance*
4. **Penerbitan sertifikat & rating** + *follow-up* perbaikan

Prinsip kunci: sederhana, terukur, dan berbasis data. Ikuti hukum (UU PDP), standar (ISO/IEC 27001, NIST CSF), dan *good governance*.

1. **Self-assessment (SA): jujur, cepat, berbukti**

Apa itu SA? Penilaian mandiri oleh bank terhadap kontrol siber dan privasi. Bukan *checklist* “ya/tidak”. Harus ada bukti.

Ruang lingkup minimal:

- Kepatuhan UU PDP: dasar pemrosesan, hak subjek data, *breach notification*.
- Kontrol ISO/IEC 27001: kebijakan, *asset inventory*, *access control*, *logging*, *incident management*.
- NIST CSF: *Identify–Protect–Detect–Respond–Recover*.
- *Third-party risk* dan *cloud security*.

Output yang wajib:

- **SAQ** (*self-assessment questionnaire*) terisi penuh + tautan bukti.
- **Gap list:** temuan → risiko → rencana perbaikan → *due date*.
- **Executive attestation:** ditandatangani Direktur Kepatuhan/CISO.

Tips praktis agar SA bermakna:

- Tunjukkan *evidence* konkret: *policy doc*, *config screenshot*, *SIEM log*, tiket insiden.
- Hindari jawaban “sedang disusun”. Tulis jadwal, pemilik, dan *milestone*.
- Gunakan bahasa sederhana. Auditor suka jelas.

2. Audit forensik: membuktikan, bukan menebak

Tujuan: memverifikasi SA dan menemukan celah tersembunyi. Fokus pada bukti teknis & *root cause*.

Kapan dilakukan:

- Minimal setahun sekali.
- Lebih cepat bila ada insiden material atau perubahan besar (mis. migrasi *core banking*, *cloud*, *M&A*).

Teknik yang umum dan aman untuk bank:

- **Log & timeline analysis:** *endpoint*, *server*, *WAF*, *EDR*, *mail gateway*.
- **Memory & artifact review:** jejak *malware/phishing* tanpa mengganggu operasi.
- **Configuration diff:** sebelum–sesudah insiden/patch.
- **Credential & data-leak trace:** *dark web* dan *paste site* (ter-anonimisasi).
- **Table-top exercise:** simulasi insiden untuk menguji *playbook* tim.

Hal yang diperiksa auditor:

- *Chain of custody* bukti: *hash*, *timestamp*, akses terbatas.
- Konsistensi cerita: log, tiket, *post-incident report*.
- Kecepatan respon: *MTTD/MTTR* dibanding *SLA* internal.
- Kepatuhan PDP saat insiden: *containment*, pemberitahuan, pemulihan.

Deliverable audit forensik:

- **Forensic Report:** kronologi, bukti kunci, dampak, *lessons learned*.
- **Remediation Plan:** tindakan, pemilik, tenggat.
- **Verification Notes:** cara auditor memvalidasi perbaikan.

3. Validasi OJK: *independent assurance* yang tegas

Apa yang dilakukan OJK:

- **Desk review:** cek konsistensi SA + laporan forensik + bukti.
- **Spot check:** *sampling* kontrol kritikal (mis. *MFA*, *backup restore*, *phishing takedown*).
- **Wawancara eksekutif:** Direksi, CISO, DPO. Menilai *tone at the top*.
- **Uji komunikasi insiden:** simulasi pemberitahuan ke regulator & nasabah.

Kriteria umum lulus/tidak:

- Bukti sah dan dapat diverifikasi.
- Temuan kritikal ditutup sesuai tenggat.
- Kepatuhan PDP saat insiden terbukti (termasuk *breach notification* tepat waktu).
- Tidak ada *repeat finding* yang dibiarkan.

Hasil validasi:

- **Sertifikat kepatuhan tahunan + rating CyberTrust.**
- **Surat tindakan korektif** bila ada celah besar.
- **Pemantauan intensif** bila risiko sistemik teridentifikasi.

Mekanisme skor yang transparan

Bobot contoh (untuk bab ini):

- *Self-assessment* berkualitas + bukti lengkap: **30%**
- Audit forensik & *remediation effectiveness*: **50%**
- Validasi OJK (konsistensi, *spot check*, *executive oversight*): **20%**

Penalti otomatis:

- *Material breach* yang tidak dilaporkan → turun **2 level** rating sampai *remediation* lulus.
- *Repeat finding* kritikal dua kali berturut → *enhanced supervision*.

Kalender kerja 12 bulan (ringkas)

- **Q1:** SAQ, pengumpulan bukti, *table-top* insiden PDP.
- **Q2:** Audit forensik putaran 1, perbaikan cepat, verifikasi.
- **Q3:** *Spot check* internal, uji pemulihan, *red-team/phishing drill*.
- **Q4:** Audit forensik putaran 2 (final), *desk review* OJK, terbit sertifikat & rating.

Catatan: untuk bank besar/BUMN, tambahkan *continuous control monitoring* agar bukti selalu segar.

Artefak yang “disukai auditor”

- **Matriz bukti:** kontrol → bukti → lokasi → pemilik → tanggal.
- **RACI:** siapa *Responsible, Accountable, Consulted, Informed*.
- **Runbook insiden:** singkat, *step-by-step*, kontak 24/7.
- **Before–After config:** tunjukkan perubahan nyata.
- **Dashboard metrik:** *MTTD, MTTR, patch SLA, phishing TTR*, tren 12 bulan.

Guardrail anti *window dressing*

- Bukti dari **multi-sumber** (internal + eksternal).
- **Sampling acak** oleh auditor & OJK.
- **Cross-correlation:** tiket vs log vs laporan bisnis.
- **Independensi:** auditor tidak boleh menilai kontrol yang mereka bangun.
- **Retensi bukti:** *WORM/immutable storage* sesuai kebijakan.

Manfaat langsung ke bisnis

- Waktu *downtime* turun, biaya forensik berkurang.
- Kepercayaan nasabah naik → *churn* turun.
- Lebih siap hadapi pemeriksaan lintas otoritas.
- Memperkuat *investment case* dan *wholesale partnerships*.

Ajakan bertindak: 30–60–90 hari

- **30 hari:** tuntaskan SAQ + kumpulkan bukti prioritas.
- **60 hari:** audit forensik putaran 1 + *quick wins* (MFA, *backup restore test*, *takedown phishing*).
- **90 hari:** *close* temuan kritikal + *management attestation* + *mock review* ala OJK.

Pesan penutup: audit forensik, *self-assessment*, dan validasi OJK adalah satu rangkaian. Tujuannya bukan mencari salah, tetapi mengamankan uang masyarakat. Dengan proses yang jelas dan bukti yang kuat, rating *CyberTrust* menjadi kompas yang dipercaya semua pihak.

Bab 13: Integrasi dengan GCG & Profil Risiko Digital Bank

Penilaian Digital Maturity Index

Inti bab ini: tata kelola yang baik (GCG) butuh ukuran yang jelas. Kematangan digital (*Digital Maturity*) harus terukur, terbukti, dan terhubung ke **profil risiko digital** bank. Hasil akhirnya: keputusan bisnis lebih cepat, risiko lebih terkendali, kepercayaan publik naik.

Mengapa DMI penting untuk bank

- **Transaksi digital tumbuh cepat.** Risiko ikut naik: *fraud, phishing, ransomware, data leak*.
- **Regulator & investor** menilai kesiapan digital bank, bukan hanya rasio keuangan.
- **GCG yang kuat** butuh *dashboard* yang objektif, bukan opini.

Acuan ringkas yang relevan: UU PDP (prinsip perlindungan data), ISO/IEC 27001 (kontrol keamanan), NIST CSF (kerangka siber), dan praktik *risk governance* per Basel (peran Dewan, tiga lini pertahanan). Semua ini menyatu di **DMI** agar mudah dibaca Direksi–Komisaris.

Struktur DMI: 6 dimensi, 0–5 skala kematangan

Gunakan bahasa sederhana. Bukti nyata. Skor 0 (belum ada) s.d. 5 (unggul & berkelanjutan).

1. Strategi & Tata Kelola Digital

- Ada strategi digital 3–5 tahun, disetujui Dewan?
- Ada *risk appetite* digital? *KPI* terhubung ke bonus manajemen?
- **Bukti:** risalah rapat Dewan, *risk appetite statement*, *scorecard* eksekutif.

2. Arsitektur & Keamanan Teknologi

- *Zero trust, MFA, EDR, backup immutable*, segmentasi jaringan.
- *Cloud security baseline* dan *hardening* diterapkan?
- **Bukti:** *config baseline*, hasil *vulnerability scan*, log SIEM.

3. Data & Kepatuhan (PDP)

- *Data inventory* lengkap? *Data lineage* jelas? *Privacy by design*?
- Mekanisme *breach notification* dan hak subjek data berjalan?
- **Bukti:** *RoPA* (record of processing), DPO report, tiket insiden PDP.

4. Proses Bisnis & Otomasi

- *Straight-through processing, RPA*, kualitas data, *SLAs* stabil.
- Uji pemulihan rutin (*DR test*), *RTO/RPO* tercapai?
- **Bukti:** laporan *DR drill*, metrik kegagalan proses, *post-mortem*.

5. Talenta & Budaya Risiko

- Peran CISO/DPO kuat? *Upskilling* rutin? Simulasi *phishing* periodik?
- *Three lines of defense* berjalan?

- **Bukti:** matriks kompetensi, tingkat kelulusan pelatihan, hasil kampanye *phishing*.

6. Ketahanan Operasional & Respon Insiden

- *Playbook* insiden diuji? *MTTD/MTTR* membaik?
- *Third-party outage* tertangani? *Failover* diuji?
- **Bukti:** *table-top exercise*, laporan forensik, *service resilience* test.

Skor akhir DMI = rata-rata tertimbang (mis. dimensi 2,3,6 berbobot lebih tinggi untuk bank inti digital).

Pemetaan DMI → GCG & Profil Risiko Digital

Tujuan: skor bukan sekadar angka. Harus memandu keputusan GCG dan risiko.

- **Dewan Komisaris/Direksi (GCG):**
 - Menetapkan *risk appetite* digital berbasis DMI.
 - Menyetujui *remediation plan* untuk dimensi berskor rendah.
 - Memasukkan DMI ke **agenda rapat triwulanan**.
- **Profil Risiko Digital (Regulator):**
 - **DMI $\geq 4,0$** → Risiko *Low–Moderate*, pengawasan normal.
 - **DMI 3,0–3,9** → Risiko *Moderate*, perlu *action plan* dan *milestone* per kuartal.
 - **DMI $< 3,0$** → Risiko *Moderate–High/High*, *enhanced supervision*, uji *stress* tambahan.
- **Three Lines of Defense:**
 - **Line 1** (unit bisnis/TI): jalankan kontrol & bukti.
 - **Line 2** (manajemen risiko/kepatuhan): kalibrasi skor & konsistensi.
 - **Line 3** (audit internal): uji keandalan data & *sampling* bukti.

Contoh rubrik skor (singkat & tajam)

- **Skor 5 – Unggul:** kontrol otomatis, metrik turun-naik di monitor real-time, *continuous testing*, *posture* selaras standar global, *supplier* diawasi ketat.
- **Skor 4 – Mapan:** kebijakan lengkap, uji berkala, insiden kecil tertangani cepat, kesenjangan minor.
- **Skor 3 – Cukup:** dasar ada, pelaksanaan belum konsisten, beberapa kontrol manual.
- **Skor 2 – Rentan:** kebijakan parsial, pelatihan jarang, *backlog* perbaikan panjang.
- **Skor 1 – Minimum:** *ad-hoc*, bergantung pada individu, bukti lemah.
- **Skor 0 – Tidak ada:** belum terbentuk.

KPI ringkas yang langsung nyambung ke bisnis

- **Keamanan & operasi:** *MTTD, MTTR, tingkat patch compliance, backup success rate, DR RTO/RPO.*
- **PDP & data:** waktu *breach notification*, SLA hak subjek data, *data quality index*.
- **Manusia & budaya:** tingkat kelulusan pelatihan, *phishing fail rate*, rotasi peran kunci.
- **Vendor & cloud:** persentase vendor berisiko tinggi sudah diaudit, *control coverage* di *cloud*.
- **Konsumen & pendapatan:** *fraud loss per 1.000 trx, app uptime, NPS* kanal digital.

Cara menghitung: sederhana tapi ketat

1. Skor tiap indikator (0–5) + bobot per dimensi.
2. **Normalisasi** ke 0–100 → tampilkan sebagai **DMI Index**.
3. Tetapkan **ambang risiko** (mis. <60 = *High*, 60–79 = *Moderate*, ≥80 = *Low*).
4. Tautkan ke **rencana perbaikan** dan **anggaran**; turunkan ke KPI individu.

Dashboard untuk Dewan (yang mudah dicerna)

- **Heatmap DMI** per dimensi (merah–kuning–hijau).
- Tren 12 bulan: *MTTR, fraud loss, phishing fail rate*.
- **Top 5 gap** + biaya & dampak bila tidak ditutup.
- Status vendor kritikal dan *cloud posture*.

Satu halaman. Satu cerita. Satu keputusan anggaran.

Red flags yang menurunkan skor DMI

- *Repeat finding* audit pada kontrol yang sama.
- *Breach* tidak dilaporkan tepat waktu.
- *Phishing fail rate* > 10% selama 2 kuartal.
- *DR test* gagal mencapai RTO/RPO.
- Vendor kritikal tanpa *assessment* tahunan.

30–60–90 hari: jadwal eksekusi yang realistis

- **30 hari:** tetapkan bobot DMI, kumpulkan bukti minimal, bangun *draft dashboard*.
- **60 hari:** lakukan *gap assessment*, tutup *quick wins* (MFA, *backup test, log retention*), latih Dewan membaca dashboard.
- **90 hari:** integrasikan DMI ke **rapat risiko**, tautkan ke **profil risiko digital & rencana anggaran** tahun berjalan.

Penutup

DMI bukan perlombaan teknologi. Ini alat untuk **GCG yang efektif**. Dengan DMI, bank tahu **di mana posisi hari ini**, risiko apa yang paling mahal besok, dan **berapa investasi yang tepat** untuk menjaga kepercayaan nasabah. Sederhana, objektif, dan *audit-ready*.

Hubungan dengan OJK *CyberTrust Scorecard*

Inti pesan: *CyberTrust Scorecard* bukan sekadar formulir. Ini “bahasa bersama” antara bank dan OJK. Tujuannya jelas: tata kelola kuat (GCG), risiko digital terukur, kepercayaan publik naik.

Apa itu *CyberTrust Scorecard* bagi GCG

- Ringkas. Terstruktur. *Audit-ready*.
- Menyatukan bukti keamanan siber, kepatuhan PDP, dan ketahanan operasi.
- Menjadi kompas bagi Dewan Komisaris/Direksi saat mengambil keputusan.

Manfaat langsung untuk bank:

- Satu *dashboard* untuk rapat risiko.
- Prioritas investasi TI lebih tepat.
- Jalur komunikasi ke OJK lebih cepat dan berbasis data.

Prinsip hubungan: Scorecard ↔ GCG ↔ Profil Risiko Digital

Bayangkan tiga roda gigi yang saling mengunci.

1. **Scorecard sebagai data inti**
 - Berisi metrik, bukti, dan *trend*.
 - Diisi rutin, minimal triwulan.
 - Terhubung dengan *incident register* dan daftar vendor.
2. **GCG sebagai pengarah**
 - Dewan menetapkan *risk appetite* digital.
 - Komite Risiko mengawasi eksekusi dan *remediation*.
 - Insentif manajemen link ke capaian pada Scorecard.
3. **Profil Risiko Digital sebagai output ke regulator**
 - Menarik ringkasan dari Scorecard.
 - Mengkategorikan: *Low / Moderate / High*.
 - Menentukan intensitas pengawasan OJK.

Isi ringkas *CyberTrust Scorecard* (yang dibaca Dewan)

- **Postur Keamanan:** *MFA coverage*, kepatuhan *patch*, *EDR* aktif, *SIEM* berjalan.
- **Kepatuhan PDP:** *RoPA*, *privacy by design*, SLA permintaan subjek data, waktu *breach notification*.
- **Ketahanan Operasional:** *RTO/RPO*, hasil *DR test*, *backup success rate*, *failover* kritikal.
- **Fraud & Kanal Digital:** *fraud loss per 1.000 transaksi*, *app uptime*, keluhan nasabah, *NPS* kanal.
- **Vendor & Cloud:** jumlah vendor kritikal diaudit, temuan terbuka, *cloud baseline* terpenuhi.

- **Budaya & Talenta:** tingkat kelulusan pelatihan, *phishing fail rate*, sertifikasi peran kunci.

Semua pakai definisi sederhana. Satuan jelas. Bukti tersimpan.

Cara Scorecard menerapkan GCG (alur singkat)

- **Bulanan:** manajemen memutakhirkan Scorecard + *trend*.
- **Triwulanan:** Komite Risiko meninjau *gap* teratas dan biaya penutupan.
- **Semesteran:** Dewan menetapkan ulang *risk appetite* digital berdasarkan data terbaru.
- **Tahunan:** target *Key Risk Indicators (KRI)* masuk RKAP. Bonus manajemen terkait.

Hasilnya: keputusan berbasis angka, bukan asumsi.

Pemetaan otomatis ke Profil Risiko Digital

Gunakan ambang sederhana agar mudah dipahami dan konsisten.

- **Skor Scorecard $\geq 80/100$** → Risiko *Low*.
Aksi: pengawasan normal, *continuous improvement*.
- **Skor 60–79/100** → Risiko *Moderate*.
Aksi: *remediation plan* 90 hari, pelaporan progres ke OJK.
- **Skor $< 60/100$** → Risiko *High*.
Aksi: *enhanced supervision*, *stress test* tambahan, jadwal rapat khusus dengan OJK.

“Aturan main” data dan bukti

- Setiap angka punya **sumber bukti**: tiket insiden, laporan *scan*, hasil *DR drill*, log SIEM.
- Bukti sampel oleh Audit Internal.
- DPO dan CISO menandatangani keabsahan data.
- *Versioning* dijaga. Tidak ada “copy–paste” manual yang rawan salah.

Mekanisme eskalasi yang sehat

- Bila *MTTR* insiden melewati ambang → eskalasi ke Komite Risiko ≤ 48 jam.
- Bila temuan prioritas-1 belum tertutup > 30 hari → Dewan minta *corrective action*.
- Bila vendor kritikal belum *assessed* → pembatasan *go-live* proyek terkait.

Sederhana. Tegas. Terukur.

Contoh pertanyaan Dewan yang dijawab oleh Scorecard

- “Apakah *fraud loss* turun seiring kenaikan *app usage*?”
- “Berapa persen data sensitif sudah *tokenized*?”
- “Vendor *cloud* kita memenuhi *baseline*? Ada *gap* besar?”
- “Kalau satu *datacenter* gagal, berapa menit layanan pulih?”

Jawaban datang dari satu sumber: *CyberTrust Scorecard*.

Integrasi ke siklus kinerja manajemen

- KPI eksekutif mencantumkan 3–5 indikator Scorecard (mis. *phishing fail rate*, *patch compliance*, *breach notification SLA*).
- Anggaran TI diprioritaskan untuk *gap* dengan dampak risiko tertinggi.
- *Quick wins* 90 hari: aktifkan *MFA* penuh, bersihkan *admin shadow*, uji *backup restore*, tingkatkan *logging* kritikal.

Red flags yang menurunkan nilai Scorecard

- *Repeat finding* audit pada kontrol yang sama.
- Laporan insiden PDP terlambat.
- *DR test* gagal memenuhi RTO/RPO.
- *Phishing fail rate* > 10% dua kuartal berturut.
- Vendor kritikal tanpa *due diligence* mutakhir.

Ringkas eksekusi 30–60–90 hari

- **30 hari:** sepakati definisi metrik, ambang risiko, dan format Scorecard.
- **60 hari:** isi data awal, validasi bukti, tampilkan *heatmap* untuk Dewan.
- **90 hari:** kunci *remediation plan*, link-kan ke RKAP dan bonus manajemen.

Penutup

CyberTrust Scorecard menyederhanakan hal yang rumit. Bank berbicara data. OJK menilai dengan adil. Publik merasa aman. GCG jadi hidup karena angka yang jujur, bukti yang rapi, dan aksi yang cepat.

Bagian V — Strategi Implementasi Nasional

Bab 14: Tahapan Implementasi Framework di OJK

Fase 1: Pilot Test (bank Buku 4 dan BUMN)

1. Mengapa Pilot Test itu Penting

Sebelum penerapan penuh dari kerangka kerja *CyberTrust & Data Privacy Ranking Framework*, OJK ingin memastikan bahwa sistem berjalan dengan baik, relevan dan bisa diukur. Oleh karena itu, dipilih **fase pilot** sebagai langkah awal.

- Pilot test memungkinkan pengujian nyata di bank-besar (Bank Buku 4) dan bank milik negara (BUMN) sebelum diterapkan ke semua bank.
- Dengan menggunakan institusi besar terlebih dahulu, potensi risiko kegagalan bisa dipantau dan dikendalikan — jika ada kelemahan bisa diperbaiki.
- Di skala internasional, banyak regulator menggunakan konsep *sandbox* atau pilot, agar regulasi baru bisa “didalami” sebelum diberlakukan secara penuh.
- Di Indonesia, regulasi terkini seperti POJK 11/POJK.03/2022 tentang Penyelenggaraan Teknologi Informasi oleh Bank Umum sudah menetapkan kerangka manajemen risiko TI dan keamanan siber bagi bank. ([OJK](#))
- Hal ini menunjukkan bahwa pilot test bukan hanya “luar biasa” tapi menjadi jalan realistis agar regulasi dan framework bisa dijalankan secara efektif.

2. Siapa yang Terlibat dalam Fase 1

Fase 1 mencakup bank-besar dan BUMN sebagai peserta awal.

- Bank Buku 4: ini adalah bank yang sudah memiliki modal besar, infrastruktur digital relatif matang, dan sistem TI yang berkembang.
- BUMN perbankan: bank yang kepemilikan negara atau sebagian besar negara, artinya memiliki cakupan nasional yang luas dan pengaruh besar terhadap stabilitas sistem keuangan.
- OJK sebagai regulator mengkoordinasi pilot: memastikan bahwa bank-peserta mengimplementasikan kerangka kerja dengan benar, mengumpulkan data, mengukur hasil, dan mempelajari pelaksanaan.
- Stakeholder tambahan: mungkin vendor teknologi, auditor internal/eksternal, tim keamanan siber bank, dan tim data privacy (perlindungan data pribadi).
- Internasional juga menunjukkan bahwa bank-besar sering dipilih untuk pilot karena mereka punya kompleksitas tinggi dan sehingga hasilnya bisa menjadi “best practice” untuk bank yang lebih kecil.

3. Apa yang Dilakukan dalam Pilot Test

Tahapan konkret dari pilot test bisa dijabarkan sebagai berikut.

- **Persiapan awal:**
 - Bank-peserta memahami kerangka kerja rating yang ditetapkan oleh OJK (skor, indikator, dimensi seperti keamanan siber, kepatuhan data pribadi).
 - Penetapan tim internal yang akan bertanggung jawab (unit keamanan siber, unit privasi data, audit TI).
 - Pemetaan infrastruktur TI-bank dan proses yang berisiko (misalnya penggunaan cloud, vendor outsourcing, koneksi digital).
- **Pengumpulan data dan baseline:**
 - Bank melakukan *self-assessment* untuk mengetahui posisi saat ini (maturity level, risiko inheren) sesuai regulasi seperti SEOJK 29/SEOJK.03/2022 yang mengatur ketahanan dan keamanan siber bagi bank umum. ([Spentera](#))
 - Bank mengumpulkan data yang diperlukan: insiden siber sebelumnya, vendor TI yang digunakan, arsitektur TI, prosedur privasi data nasabah, dsb.
- **Uji coba kerangka penilaian (rating framework):**
 - OJK bersama bank menjalankan proses penilaian: indikator teknis, tata kelola, kepatuhan data pribadi, rantai pasok vendor, dll.
 - Menggunakan bank-besar sebagai “laboratorium” untuk men-trial model skor, interpretasi rating (misalnya AAA–D), dan melihat bagaimana hasilnya di lapangan.
 - Melakukan *gap analysis* — di mana bank belum memenuhi standar, di mana kelemahan, dan bagaimana perbaikannya.
- **Review dan evaluasi:**
 - Hasil pilot dikumpulkan, dianalisis OJK dan bank-peserta bersama-sama.
 - Identifikasi hambatan penerapan: misalnya keterbatasan TI, kurangnya kompetensi SDM, vendor yang belum memenuhi standar, data yang belum rapi.
 - Perbaikan framework: berdasarkan feedback pilot, OJK bisa melakukan revisi indikator, proses audit, atau mekanisme penilaian agar lebih cocok dengan kondisi bank Indonesia.
- **Persiapan peningkatan skala:**
 - Setelah pilot sukses, bank-lain akan dipersiapkan untuk fase berikut (integrasi ke sistem pengawasan OJK digital, kemudian implementasi nasional).
 - Bank-peserta pilot akan menjadi contoh (benchmark) bagi bank lainnya.
 - OJK akan menetapkan timeline, pelatihan, pendampingan, serta mekanisme publikasi hasil rating.

4. Tantangan yang Mungkin Dihadapi

Pelaksanaan pilot test ini bukan tanpa hambatan — berikut beberapa yang perlu diperhatikan.

- Kompetensi internal bank: tidak semua bank memiliki tim keamanan siber atau privasi data yang matang. Padahal regulasi menuntut tim yang mandiri dan kapabel. ([ASEAN Briefing](#))
- Kualitas data dan dokumentasi: bank harus memiliki data sistem TI yang rapi, catatan insiden, vendor outsourcing yang terdokumentasi, proses audit. Tanpa itu, penilaian akan sulit.
- Vendor dan rantai pasok: banyak bank menggunakan vendor TI atau cloud. Standar keamanan vendor belum selalu seragam. Ini bisa menjadi titik lemah dalam penilaian.
- Pembebanan biaya dan sumber daya: uji penetrasi, simulasi insiden (*table-top exercise*), audit forensik memerlukan biaya dan tenaga — bank harus siap.
- Harmonisasi dengan standar internasional: bank besar Indonesia juga harus selaras dengan standar global seperti ISO/IEC 27001 atau NIST Cybersecurity Framework, agar ratingnya dapat dipercaya secara internasional.
- Penyesuaian budaya dan proses: perubahan mindset dari “aman sebentar” menjadi “keamanan siber dan privasi data adalah bagian dari bisnis” membutuhkan waktu.

5. Dampak yang Diharapkan dari Fase 1

Jika pilot ini berjalan baik, maka manfaatnya dapat terasa luas, tidak hanya bagi bank-peserta sebagai “uji coba”.

- Bank-peserta akan punya **benchmark internal**: mereka tahu posisi mereka dalam keamanan siber dan privasi data dibanding standar yang ditetapkan OJK.
- OJK akan memiliki data nyata untuk memperbaiki framework: berdasarkan pilot akan muncul revisi yang lebih siap diterapkan nasional.
- Bank yang berhasil akan meningkatkan kepercayaan publik: jika bank dapat menunjukkan punya rating baik dalam kerangka keamanan siber & data pribadi, maka reputasi meningkat.
- Industri perbankan nasional akan semakin tangguh terhadap ancaman siber: pilot memperkuat sistem, sehingga ketika tahap nasional berlangsung, bank-lain lebih siap.
- Ini membantu menjaga **stabilitas sistem keuangan nasional**: karena jika bank besar gagal dalam keamanan siber, risikonya bisa sistemik. Pilot membantu mencegah itu.
- Regulasi dan pengawasan OJK akan menjadi lebih berbasis data (*data-driven supervision*), bukan hanya regulasi “di atas kertas”.

6. Pesan Penting untuk Bank dan Pemangku Kepentingan

Beberapa hal praktis yang perlu diingat oleh bank (terutama yang termasuk peserta pilot) dan pemangku kepentingan:

- Anggaplah pilot bukan sebagai beban tambahan, tetapi sebagai investasi jangka panjang untuk reputasi, kepercayaan nasabah, dan keberlanjutan bisnis.
- Siapkan dokumentasi sedini mungkin: data insiden, vendor, audit, prosedur keamanan, pelatihan SDM.
- Libatkan seluruh lapisan organisasi—kepala TI, keamanan siber, data privacy, auditor internal—agar proses berjalan solid.
- Jangan hanya memenuhi persyaratan formal, namun evaluasi secara nyata bagaimana sistem TI dan proses operasional bank berfungsi dalam kondisi serangan atau gangguan.
- Gunakan hasil pilot untuk memperkuat pemain lain: berbagi pengalaman, menjadi leader dalam keamanan siber perbankan Indonesia.
- Pantau dan siapkan perubahan regulasi: OJK telah memperketat regulasi seperti POJK 11/2022 dan SEOJK 29/2022 terkait TI dan keamanan siber.
(assets.kpmg.com)

Dengan narasi tersebut, maka fase pertama – pilot test – dari implementasi framework di OJK menjadi lebih nyata, menantang namun juga sangat penting bagi dunia perbankan Indonesia. Bila Anda ingin, saya bisa membuat “timeline detail”, “checklist bank peserta pilot”, atau “kriteria sukses pilot” secara lebih terstruktur. Mau saya buat?

Fase 2: Integrasi dengan Sistem Pengawasan OJK Digital

1. Inti gagasan

Fase ini menghubungkan **hasil rating CyberTrust & Data Privacy** ke **mesin pengawasan digital OJK**. Tujuannya jelas: **pengawasan berbasis data** (*data-driven supervision*) yang real-time, konsisten, dan bisa ditindaklanjuti.

- Dari manual → otomatis.
- Dari reaktif → *early warning*.
- Dari kepatuhan kertas → *SupTech* yang *actionable*.
- Selaras dengan kewajiban TI & siber di **POJK 11/2022** dan panduan **SEOJK 29/2022** untuk perbankan. ([OJK](#))

2. Kenapa sekarang?

- OJK sudah mendorong transformasi digital pengawasan (*SupTech*), termasuk peluncuran **OSIDA** untuk otomasi pengumpulan dan analitik data sektor keuangan. Integrasi CyberTrust masuk ke arus utama ini. ([lab.ccaf.io](#))
- Tren global: otoritas memakai *SupTech* agar pengawasan lebih cepat dan tajam. Survei BIS/FSI menunjukkan mayoritas regulator kini telah menerapkan alat *SupTech* di “produksi”, bukan sekadar eksperimen. ([Bank for International Settlements](#))
- Internasional juga mengarah ke **harmonisasi pelaporan insiden siber** (FSB), termasuk format umum seperti **FIRE** agar pelaporan lintas lembaga makin seragam dan cepat. ([Financial Stability Board](#))

3. Apa yang diintegrasikan?

Bayangkan tiga “pipa data” utama ke **data platform OJK** (*data lake/warehouse*).

1. Pipa Kepatuhan & Tata Kelola

- Bukti kepatuhan **POJK 11/2022 & SEOJK 29/2022**: kebijakan, struktur *governance*, *risk register*, kontrol teknis, uji berkala.
- Output: **skor CyberTrust** per dimensi (ketahanan siber, PDP, vendor, data nasabah). ([OJK](#))

2. Pipa Risiko Operasional & Insiden Siber

- *Feeds* insiden siber terstandar (kategori, *severity*, waktu pemulihan, *root cause*).
- Diselaraskan dengan rekomendasi FSB soal **konvergensi pelaporan** agar efisien dan bisa dipakai lintas otoritas. ([Financial Stability Board](#))

3. Pipa *Threat Intelligence* & Vendor/Rantai Pasok

- Paparan pihak ketiga, temuan kerentanan, kebocoran data yang terverifikasi, dan status *patching*.
- Menjawab fokus global pada risiko *outsourcing* dan pihak ketiga di sektor keuangan. ([Bank for International Settlements](#))

4. Cara kerja integrasi (versi singkat)

- **Standarisasi skema data:** definisi kolom, *taxonomy* insiden, *reference data*—supaya semua bank bisa kirim data dengan format seragam. Selaras arah FSB untuk penyamaan istilah dan struktur pelaporan. ([Financial Stability Board](#))
- **Konektor & API terautentikasi:** *push/pull* data berkala dan *event-driven* atas insiden material. Audit-trail wajib.
- **Validasi otomatis:** *schema check*, *logic check*, *outlier detection* sebelum data masuk *data lake*.
- **Skoring & analytics:** mesin OJK menghitung **CyberTrust score** dan memetakan tren risiko (bank, grup usaha, industri).
- **Dashboard early warning:** pemeringkatan, *heatmap*, *trendline*, *drill-down* insiden, dan *benchmark* industri.
- **Alerting & workflow:** jika skor turun atau ada insiden kritis, sistem membuat *case* dan *tasking* untuk *supervisory review*.
- **Pelaporan periodik:** ringkas, konsisten, siap diekspor untuk rapat komite risiko, rapat Dewan Komisiner, atau koordinasi antar-otoritas.

5. Peran & tanggung jawab

- **Bank**
 - Menyediakan *data feed* yang akurat dan tepat waktu.
 - Menjaga kualitas bukti kontrol (kebijakan, uji, log).
 - Menetapkan PIC lintas fungsi: CISO, DPO, TI, Kepatuhan, *Internal Audit*.
- **OJK**
 - Menyediakan spesifikasi teknis, *API*, *playbook* insiden, dan *service window*.
 - Menjalankan *SupTech analytics* (termasuk OSIDA) untuk *profil risiko digital* dan pengawasan berbasis prioritas. ([lab.ccaf.io](#))
- **Vendor/third-party**
 - Mendukung *evidence* kepatuhan, *hardening*, dan pelaporan insiden sesuai kontrak.
 - Siap dengan bukti *due diligence* dan *right to audit*.

6. Standar & referensi yang dirujuk

- **POJK 11/2022** — kewajiban tata kelola TI dan manajemen risiko TI bank. ([OJK](#))
- **SEOJK 29/2022** — praktik terbaik ketahanan & keamanan siber bank. ([Spentera](#))
- **FSB** — rekomendasi konvergensi pelaporan insiden siber untuk stabilitas sistemik. ([Financial Stability Board](#))
- **BIS/FSI** — bukti adopsi *SupTech* oleh banyak otoritas, dari uji coba ke produksi. ([Bank for International Settlements](#))
- **OSIDA (OJK SupTech)** — contoh konkret otomasi pengumpulan dan analitik data pengawasan. ([lab.ccaf.io](#))

7. Output yang diharapkan

- **Satu sumber kebenaran** (*single source of truth*) untuk risiko siber & privasi.
- **Skor CyberTrust** terhubung ke **profil risiko bank** dan memandu prioritas pengawasan.
- **Early warning yang bisa ditindak**: bukan hanya angka, tetapi *alert* dengan konteks.
- **Efisiensi pemeriksaan**: bukti digital, *traceable*, dan siap audit.
- **Koordinasi lintas lembaga** lebih lancar karena struktur data insiden makin seragam. ([Financial Stability Board](#))

8. Tantangan praktis (dan cara mengatasinya)

- **Kualitas & konsistensi data**: atasi dengan *data contract*, *schema registry*, dan *data quality rules*.
- **Beban integrasi TI bank**: sediakan *SDK/connector* referensi dan *sandbox* uji integrasi.
- **Isu privasi & kerahasiaan**: enkripsi ujung-ke-ujung, kontrol akses berbasis peran, *pseudonymization* untuk data sensitif.
- **Beragamnya vendor/arsitektur**: gunakan standar *API* terbuka dan *mapping* minimalis yang fleksibel.
- **Perubahan budaya**: latih tim bank & pengawas agar nyaman dengan *RegTech/SupTech*—bukan sekadar pelaporan *compliance*.

9. Quick-wins yang realistis

- Mulai dengan **insiden siber material** dan **indikator minimum** (mis. *patch latency*, *mean time to recover*, kasus kebocoran).
- **Auto-ingest skor CyberTrust + evidence links** ke dashboard OSIDA/monitoring. ([lab.ccaf.io](#))
- Pilot **alert FIRE-like fields** untuk memudahkan harmonisasi pelaporan insiden. ([xbrl.org](#))
- Terapkan **SLA pengiriman data** dan uji **playbook** bulanan (table-top exercise).

Ringkasan

Fase 2 adalah **menyambung data ke pengawasan digital**. Agar OJK tidak hanya “menerima laporan”, tetapi **melihat risiko lebih cepat, bertindak lebih tepat, dan menjaga kepercayaan sistem keuangan**. Ini sejalan dengan arah global *SupTech*, standar pelaporan insiden FSB, dan kewajiban TI/siber di Indonesia. ([Bank for International Settlements](#))

Fase 3: Implementasi Nasional dan Public Disclosure

1. Tujuan besar

Fase ini membawa kerangka **CyberTrust & Data Privacy Rating** ke level nasional. Semua bank ikut. Hasilnya terhubung ke pengawasan digital OJK, dan bagian intinya **dipublikasikan** secara terukur.

- **Nasionalisasi:** dari pilot → seluruh perbankan.
- **Transparansi:** dari laporan internal → *public disclosure* yang terarah.
- **Kepercayaan:** pasar, nasabah, dan investor dapat membaca sinyal risiko digital bank, seperti membaca *credit rating*.
- **Selaras dunia:** tren global mendorong *operational resilience* dan pelaporan insiden siber yang konsisten. ([Bank for International Settlements](#))

2. Apa yang dipublikasikan? (ringkas, bermakna, aman)

Tujuannya bukan membuka “buku dapur”, tapi memberi **sinyal risiko** yang berguna.

- **Peringkat agregat** CyberTrust (mis. AAA–D) + **kategori risiko** (rendah/sedang/tinggi).
- **Indikator ringkas:** tren insiden material per tahun, waktu pulih rata-rata, kepatuhan PDP, dan kesiapan vendor.
- **Keterangan kebijakan:** *governance* keamanan siber dan privasi di tingkat dewan/direksi.
- **Catatan insiden material** yang sudah *disclose* publik sesuai aturan pasar modal (bila emiten). (AS mewajibkan emiten umumkan insiden siber material dalam 4 hari kerja setelah penentuan materialitas—ini jadi pembelajaran praktik transparansi bagi kita). ([SEC](#))

Prinsipnya: publik mendapat **sinyal kualitas dan ketahanan**, tanpa mengekspos taktik teknis yang bisa dimanfaatkan penyerang.

3. Belajar dari praktik internasional

- **SEC (AS):** mengatur pengungkapan insiden siber material via Form 8-K dalam 4 hari kerja setelah penentuan materialitas, serta pengungkapan tata kelola risiko siber dalam laporan tahunan—ini mendorong disiplin pengungkapan dan akuntabilitas ke investor. ([SEC](#))
- **FSB – FIRE:** format umum global untuk pelaporan insiden operasional (termasuk siber) agar **seragam** lintas otoritas—mendukung konsistensi data dan koordinasi. ([Financial Stability Board](#))
- **DORA (Uni Eropa):** menstandarkan *operational resilience*, pelaporan insiden, uji ketahanan, serta pengawasan *third-party* ICT. Ini menguatkan logika *public signal* tentang kesiapan digital entitas keuangan. ([eur-lex.europa.eu](#))
- **Basel Committee – Operational Resilience:** menegaskan ketahanan operasi sebagai kemampuan inti bank menghadapi gangguan besar, termasuk insiden siber dan kegagalan teknologi. ([Bank for International Settlements](#))

4. Arsitektur pelaksanaan nasional (versi sederhana)

Bayangkan tiga lapisan:

1. Pengumpulan & Standarisasi

- Semua bank mengirim data terstruktur (insiden, kontrol, vendor, kepatuhan PDP) ke platform *SupTech* OJK (OSIDA dan turunannya).
- Skema mengikuti kamus data OJK serta *mapping* ke elemen umum FIRE untuk memudahkan harmonisasi dan koordinasi lintas lembaga. ([OJK](#))

2. Skoring & Analitik

- Mesin OJK menghitung **CyberTrust score** nasional, *benchmark* per segmen bank, dan tren risiko industri.
- *Early-warning* otomatis untuk penurunan tajam skor atau insiden besar.

3. Publikasi & Engagement

- **Laporan Tahunan CyberTrust**: peringkat ringkas tiap bank, tren industri, dan rekomendasi nasional.
- **Dashboard publik**: *heatmap* industri dan agregat sektoral (tanpa detail sensitif).
- **Dialog pasar**: *briefing* berkala untuk investor, analis, dan media, agar sinyal risiko dipahami dengan benar.

Catatan: OSIDA sudah menjadi kanal *SupTech* OJK untuk analitik dan otomasi pengawasan; penguatan OSIDA memudahkan fase nasional. ([OJK](#))

5. Tahapan implementasi (praktis dan bertahap)

- **T-0**: Tetapkan **aturan main publikasi** (format, frekuensi, konten, *safe-harbor wording*). Selaraskan dengan hukum pasar modal & PDP.
- **T-1**: *Dry-run* nasional (tanpa publikasi) selama 1–2 siklus pelaporan untuk menstabilkan kualitas data.
- **T-2**: Rilis **Laporan Industri** (agregat, tanpa nama bank) untuk pemanasan pasar.
- **T-3**: *Public disclosure* terbatas—mis. top-tier dan bottom-tier, atau publikasi **rentang peringkat** per bank.
- **T-4**: *Full roll-out*—**Report Card per bank** + agregat industri, diselaraskan dengan kalender pelaporan pengawasan tahunan.

6. Risiko *public disclosure* dan *mitigations*

- **Risiko keamanan**: publikasi berlebihan memberi “peta” bagi penyerang → batasi ke indikator agregat, gunakan rentang, tunda *timing* publikasi insiden teknis.
- **Risiko legal & pasar**: salah tafsir peringkat → sertakan *methodology note*, *peer comparison*, dan *FAQ* untuk investor.
- **Risiko kualitas data**: *inconsistency* → terapkan *data contract*, validasi otomatis, dan *issue management* lintas bank.
- **Koordinasi multi-otoritas**: gunakan elemen **FIRE** agar pelaporan konsisten dan efisien lintas lembaga. ([Financial Stability Board](#))

7. Konten *Public Disclosure* yang disarankan (minimalis namun kuat)

- **Peringkat CyberTrust + status tren** (naik, turun, stabil).
- **3–5 KPI inti**: jumlah insiden material per tahun, *mean time to recover*, *patch latency*, *vendor criticality index*, dan *compliance attestation* PDP.
- **Pernyataan dewan/direksi** tentang *oversight* risiko siber & data.
- **Ringkasan insiden material** yang sudah wajib *disclose* sesuai aturan pasar modal (bagi emiten)—meniru praktik SEC soal transparansi insiden material untuk kepentingan investor. ([SEC](#))

8. Manfaat yang diharapkan

- **Kepercayaan pasar meningkat**: investor bisa menilai ketahanan digital bank secara objektif. (Di AS, aturan SEC mendorong keterbukaan kepada investor; efeknya adalah disiplin tata kelola dan *market discipline*). ([Reuters](#))
- **Disiplin industri**: publikasi memicu *peer pressure* positif untuk naik kelas.
- **Efisiensi pengawasan**: OJK fokus ke bank berisiko tinggi berdasarkan data yang sama dengan yang dilihat publik.
- **Koherensi global**: sejalan dengan DORA (UE) dan prinsip Basel, memudahkan kolaborasi internasional saat terjadi insiden lintas batas. ([eur-lex.europa.eu](#))

9. “Checklist siap *go-public*” untuk bank

- **Data siap audit**: pelaporan insiden, *root cause*, dan *lessons learned* terdokumentasi.
- **Vendor terkelola**: *due-diligence* dan *right-to-audit* aktif untuk penyedia ICT kritikal. (Isu *outsourcing/cloud* jadi sorotan regulator global). ([Reuters](#))
- **Governance kuat**: peran dewan, komite risiko, CISO, dan DPO jelas.
- **Narasi konsisten**: sejalan antara laporan OJK, pengumuman publik, dan keterbukaan ke investor.

Ringkasan

Fase 3 memastikan **semua bank terukur** dan **publik mendapatkan sinyal yang jelas** tentang ketahanan digital perbankan. Formatnya ringkas, aman, dan bermanfaat—selaras dengan arah global: **Basel** (ketahanan operasional), **FSB-FIRE** (format insiden), **DORA** (resiliensi digital), dan **SEC** (keterbukaan insiden material bagi investor). Indonesia sudah punya pondasi *SupTech* (OSIDA); tinggal **menyambungkan, menstandarkan, dan mempublikasikan** dengan cerdas. ([Bank for International Settlements](#))

Bab 15: Sinkronisasi dengan BSSN dan Kemenkominfo

Pertukaran data ancaman siber nasional

Tujuan singkat: menyambungkan *intelijen ancaman* dari bank ke **BSSN** dan **Kemenkominfo**, lalu balik lagi ke industri secara cepat, terstruktur, dan bisa ditindaklanjuti (*actionable*). Hasil akhirnya: **perbankan lebih kebal serangan**, dan **OJK** punya gambaran risiko nasional yang *real-time*.

1. Peran lembaga: jelas dan saling menguatkan

- **BSSN:** *national cyber lead* — mengoordinasikan *situational awareness* nasional (Pusat Operasi/“Pusopskamsinas”), mendorong pembentukan CSIRT, dan menerbitkan strategi serta kajian ketahanan siber. ([Antara News](#))
- **Kemenkominfo:** *policy & compliance rail* — mengatur PSTE melalui **PP 71/2019** dan turunannya (PSE, sertifikat elektronik, tata kelola operator). Ini jalur hukum penting untuk kewajiban pelaporan dan interkoneksi data. ([Peraturan BPK](#))
- **ID-SIRTII/CC** (hosted by BSSN): *national/sectoral incident response hub* untuk pertukaran indikator dan koordinasi teknis insiden. Terdaftar di jaringan FIRST. ([ID-SIRTI](#))
- **OJK:** *sectoral supervisor* — mengikat data ancaman ke pengawasan sektor keuangan (SupTech/OSIDA) dan kewajiban ketahanan siber perbankan (POJK/SEOJK) agar bisa jadi **peringatan dini** dan **profil risiko**. (OJK juga merilis pedoman keamanan FSTI dengan data ancaman BSSN sebagai konteks nasional). ([OJK](#))

2. Mengapa sinkronisasi ini mendesak?

- **Volume serangan tinggi** dan menysasar layanan keuangan: BSSN mencatat ratusan juta serangan/tahun; insiden bernuansa finansial (phishing, *credential theft*, *mobile malware*) terus naik. ([OJK](#))
- **Waktu respon makin sempit:** bank global menilai jeda dari *zero-day* ke eksploit kini hitungan jam—*sharing* harus otomatis dan seketika. ([fsisac.com](#))
- **Praktik global:** sektor keuangan dunia memakai **FS-ISAC** untuk *real-time sharing* lintas bank—model gotong royong intelijen ancaman. ([fsisac.com](#))

3. Prinsip desain *threat intel sharing* (sederhana tapi kuat)

- **Standar terbuka:** gunakan **STIX 2.1** (bahasa CTI) dan **TAXII 2.1** (protokol transport) agar *feed* bisa otomatis, interoperabel, dan aman. ([OASIS Open](#))
- **Mesin-ke-mesin (M2M):** dorong *push/pull* indikator via *client TAXII* seperti praktik **CISA AIS** (Amerika). Belajar juga dari evaluasi OIG agar partisipasi dan kualitas *feed* tetap tinggi. ([CISA](#))
- **Segmentasi data:** pisahkan *tactical IOCs* (hash, IP, domain), *operational TTPs* (MITRE ATT&CK), dan *strategic intel* (tren sektor) — supaya tepat sasaran dan tidak membanjiri tim SOC. (FS-ISAC menyarankan kurasi/penyaringan sinyal-vs-noise). ([fsisac.com](#))

- **Privasi & legal:** patuhi PDP dan PP 71/2019; minimalkan data pribadi, gunakan *pseudonymization*, dan *need-to-know access*.

4. Alur pertukaran data (versi ringkas)

1. **Bank → OJK/BSSN/ID-SIRTII/CC**
 - Kirim indikator prioritas tinggi (*high-confidence IOCs, exploited CVEs, observed TTPs*) via **TAXII**.
 - Laporan insiden material mengikuti jalur pengawasan (OJK) + notifikasi teknis (BSSN/ID-SIRTII/CC). ([ID-SIRTI](#))
2. **BSSN/ID-SIRTII/CC → Industri (melalui OJK/komunitas sektor)**
 - *Fan-out* indikator terverifikasi ke bank lain (dengan TTL, *sighting*, tingkat kepercayaan).
 - Terbitkan *early warning* nasional bila ada kampanye *phishing/banking malware* berskala. ([Antara News](#))
3. **Interkoneksi lintas standar**
 - *Mapping playbook* lokal ke kerangka **FIRE/NIS2-style CSIRTs network**: memudahkan koordinasi regional dan *cross-border*. ([digital-strategy.ec.europa.eu](#))
4. **Loop balik**
 - OJK menelan *feed* ke *SupTech* (OSIDA) untuk *risk scoring* sektor, lalu mengembalikan **sectoral advisories** ke bank agar tindakan mitigasi seragam. (Pedoman OJK untuk FSTI mencontohkan integrasi konteks ancaman BSSN). ([OJK](#))

5. Apa yang dipertukarkan? (paket minimum yang berguna)

- **IOC prioritas:** IP/domain *command-and-control*, hash *malware* aktif, *phishing kit* yang sedang beredar.
- **Konteks CVE yang dieksploitasi:** versi produk terdampak, *patch guidance*, *exploit maturity*.
- **TTPs:** *initial access vectors, lateral movement, exfiltration* — agar tim SOC tahu *behavior*.
- **Sector watch FS-ISAC-like:** ringkasan tren serangan *credential stuffing, OTP-stealing, SIM-swap* pada layanan finansial digital. ([fsisac.com](#))

6. Pelajaran dari luar negeri (yang bisa langsung dipakai)

- **FS-ISAC** menunjukkan *collective defense* itu nyata: ribuan institusi, 75 negara, *sharing* harian. Kita bisa meniru model *trust group* dan *fusion call*. ([fsisac.com](#))
- **CISA AIS** membuktikan *machine-readable sharing* skala nasional mungkin dilakukan—pakai **STIX/TAXII**, *open-source client, server connection guide*. (Catatan: kualitas & partisipasi harus dijaga). ([CISA](#))

- **NIS2/CSIRTs Network (UE)** menekankan *interoperable feeds* dan kerja sama operasional lintas negara—relevan untuk koordinasi kita di ASEAN/mitra global. (csirtsnetwork.eu)

7. Tata kelola & *guardrails* (agar aman dan patuh)

- **MoU teknis OJK–BSSN–Kominfo**: cakupan data, SLA, kanal darurat, dan *liability shield* untuk *good-faith sharing*.
- **Klasifikasi & *traffic light protocol* (TLP)**: atur siapa yang boleh lihat/teruskan.
- **Anonymization & minimization**: jangan kirim PII kecuali wajib hukum; jika wajib, gunakan enkripsi ujung-ke-ujung dan *access control*.
- **Quality gate**: *schema validation*, *confidence score*, *duplicate check*, dan *feedback loop* (bank memberi *sighting* agar intel makin tajam).
- **Audit & metrics**: *time-to-share*, *patch latency*, *mean time to mitigate*, jumlah *detections* dari IOC nasional—semua dilaporkan berkala ke komite bersama.

8. Quick wins 90 hari (realistis untuk sektor bank)

- **TAXII pilot**: 10–15 bank besar kirim/terima IOC harian → *blocking rules* otomatis di email/web/SIEM.
- **Playbook *phishing* finansial**: *template* nasional (STIX bundle) untuk kampanye *credential theft* terhadap *mobile banking*.
- **Fusion digest mingguan**: ringkasan *top CVEs exploited* di sektor keuangan Indonesia + rekomendasi *patching window*.
- **Latihan *table-top*** OJK–BSSN–Kominfo–Bank: simulasi kebocoran kredensial massal; ukur *time-to-alert* dan *time-to-mitigate*.

9. Risiko & cara menanganinya

- **Over-disclosure** (membuka taktik internal): pakai ringkasan tanpa *runbook* sensitif; gunakan TLP.
- **Data quality rendah**: tetapkan *submission guide* (contoh AIS 2.0) dan *lint review* otomatis sebelum *fan-out*. ([CISA](#))
- **Fragmentasi alat**: wajibkan **STIX/TAXII** sebagai *common rail*; sediakan *reference client* agar UMKM bank tidak tertinggal. ([OASIS Open](#))
- **Kepatuhan hukum**: *align* dengan PP 71/2019 & PDP; buat *legal gateway* khusus *incident sharing* agar bank nyaman berbagi. ([Peraturan BPK](#))

Ringkasan

Sinkronisasi OJK–BSSN–Kemenkominfo adalah **urat nadi *defense-in-depth* nasional**: **bank berbagi cepat**, **BSSN mengorkestrasi nasional**, **Kominfo memastikan rilenya hukum/teknologi**, dan **OJK menyalurkan kembali intel menjadi tindakan pengawasan yang presisi**. Modelnya tidak asing: **FS-ISAC**, **CISA AIS**, dan **NIS2/CSIRTs Network** sudah membuktikan bahwa *collective defense* itu bekerja—asal **standar (STIX/TAXII)**, **peran**, dan **kualitas data** dijaga. (fsisac.com)

Harmonisasi standar penilaian PDP

1. Tujuan

Kita butuh **satu bahasa** untuk menilai kepatuhan Pelindungan Data Pribadi (PDP) di sektor keuangan. Artinya, standar OJK untuk bank harus **selaras** dengan:

- **UU 27/2022 tentang PDP** (hak subjek data, kewajiban pengendali/pemroses, sanksi),
- **PP 71/2019** (PSE, kewajiban keamanan & keandalan layanan elektronik),
- Pedoman teknis dan peran koordinatif **BSSN** di keamanan siber nasional. ([Peraturan BPK](#))

Hasil akhirnya: penilaian PDP bank **konsisten**, bisa diaudit, mudah dipetakan ke risiko operasional, dan kompatibel dengan standar internasional (agar dipercaya investor/mitra global).

2. Prinsip desain harmonisasi (mudah diingat)

- **Satu kerangka, banyak pemakai:** OJK menetapkan *baseline*; BSSN memberi konteks keamanan siber nasional; Kominfo memastikan *compliance rail* PSE & tata kelola data. ([JDIH Komdigi](#))
- **Hak & kewajiban sebagai poros:** *checklist* harus menurunkan pasal-pasal UU PDP (hak akses, koreksi, penghapusan; dasar pemrosesan; DPIA; pelaporan insiden) ke kontrol yang terukur. ([Peraturan BPK](#))
- **Teknis mengikuti standar terbuka:** gunakan **ISO/IEC 27701 (PIMS)** sebagai mesin manajemen privasi dan **NIST Privacy Framework** sebagai *playbook* manajemen risiko privasi. ([ISO](#))
- **Interoperable lintas batas:** dukung **Global/APEC CBPR** untuk transfer data lintas negara secara akuntabel. ([Global CBPR Forum](#))

3. Apa yang diselaraskan? (konten inti *assessment*)

A. Tata Kelola & Akuntabilitas

- Peran dewan/direksi, DPO, kebijakan privasi, *record of processing*, kontrak dengan pemroses pihak ketiga.
- *Mapping* ke klausul UU PDP + klausa ISO 27701 (kontrol PII controller/processor). ([Peraturan BPK](#))

B. Hak Subjek Data & Dasar Pemrosesan

- Mekanisme persetujuan, akses, koreksi, *erasure*, *portability*; SLA penanganan permintaan.
- Selaras *function* di NIST PF (Identify-P, Control-P, Communicate-P). ([NIST](#))

C. *Privacy by Design* & DPIA

- Uji dampak privasi pada fitur *mobile banking*, *fraud analytics*, *cloud outsourcing*.
- Format DPIA dirujuk ke NIST PF + ISO 27701 agar seragam. ([NIST](#))

D. Insiden & Pelaporan

- Prosedur deteksi, *containment*, notifikasi regulator/pengguna; *evidence* yang diaudit.
- Sinkron dengan jalur PSE (Kominfo/PP71) dan orkestrasi nasional BSSN/CSIRT. ([Peraturan BPK](#))

E. Third-Party Risk

- *Due diligence* vendor, klausul data-processing, *right to audit*, lokasi pemrosesan (data residency PP71). ([Peraturan BPK](#))

F. Transfer Lintas Negara

- Opsi kontrak standar + sertifikasi **CBPR/PRP**; ini meningkatkan kepercayaan dagang dan mengurangi friksi lintas yurisdiksi. ([Global CBPR Forum](#))

4. Belajar dari praktik internasional (agar “nyambung” ke pasar)

- **NIST Privacy Framework 1.1** → alat sukarela, banyak dipakai lintas industri untuk menyetarakan risiko privasi dengan risiko perusahaan. Cocok jadi “bahasa bersama” bank-regulator. ([ansi.org](#))
- **ISO/IEC 27701** → PIMS yang menempel ke ISO 27001/27002; memudahkan audit gabungan keamanan-privasi. ([ISO](#))
- **Global/APEC CBPR** → skema sertifikasi lintas negara untuk arus data; memperkuat *market trust* ketika bank bermitra global. ([Global CBPR Forum](#))
- **Model konsistensi ala GDPR** → otoritas privasi Eropa memakai *consistency mechanism* agar penegakan seragam. Ini inspirasi tata kelola lintas lembaga di Indonesia (OJK–BSSN–Kominfo–Lembaga PDP). ([gdpr-info.eu](#))

5. Cara eksekusi (singkat, praktis)

1. **MoU Metodologi OJK–BSSN–Kominfo**: ruang lingkup penilaian PDP bank, *data dictionary* bukti, SLA, dan *appeal process*.
2. **Kamus Kontrol Nasional**: *mapping* Pasal UU PDP ↔ kontrol ISO 27701 ↔ fungsi NIST PF (satu tabel, satu nomor kontrol). ([Peraturan BPK](#))
3. **Template DPIA & Insiden**: format standar (termasuk *root cause*, data terdampak, *time-to-notify*).
4. **Uji Konsistensi**: *peer review* lintas lembaga untuk menilai keseragaman putusan (meniru *consistency mechanism*). ([gdpr-info.eu](#))
5. **Jalur Lintas Negara**: panduan penggunaan **CBPR/PRP** + klausul kontrak standar saat *cross-border processing*. ([Global CBPR Forum](#))

6. *Quick wins* untuk 6–12 bulan

- **Skor PDP Minimum** nasional: hak subjek data + DPIA + insiden + *third-party*; jadi *entry bar* semua bank.
- **Checklist terharmonisasi** (10–12 butir) untuk *on-site/desk review*—mengurangi beban audit ganda.
- **Pelatihan gabungan** (OJK–BSSN–Kominfo): *case clinic* kebocoran nyata, latihan *table-top* notifikasi insiden sesuai UU PDP + PP71. ([Peraturan BPK](#))
- **Cross-border playbook**: contoh kontrak + jalur sertifikasi CBPR untuk *data sharing* dengan mitra internasional. ([Global CBPR Forum](#))

7. Risiko yang perlu dijaga (dan cara meredam)

- **Standar tumpang tindih** → selesaikan lewat *kamus kontrol nasional* dan *one-stop guidance*.
- **Eksekusi tidak konsisten** → terapkan *review panel* lintas lembaga ala *consistency mechanism*. ([gdpr-info.eu](#))
- **Friksi lintas negara** → gunakan **CBPR/PRP** + ISO 27701 sebagai bukti akuntabilitas. ([Global CBPR Forum](#))

Ringkasan

Harmonisasi penilaian PDP adalah **jembatan** antara hukum, tata kelola, dan praktik teknis. Dengan **UU 27/2022** dan **PP 71/2019** sebagai landasan, **ISO 27701** dan **NIST PF** sebagai mesin, serta **CBPR** untuk lintas batas—OJK, BSSN, dan Kemenkominfo dapat memberikan **satu standar yang jelas, konsisten, dan diakui global**. Itu yang dibutuhkan industri perbankan agar *privacy = trust = nilai ekonomi*. ([Peraturan BPK](#))

Bab 16: Keterlibatan Ekosistem: Bank — Fintech — Vendor Teknologi

Program kemitraan dan kolaborasi open audit

1. Inti gagasan

Kita butuh cara audit yang tidak jalan sendiri-sendiri. Bank, *fintech*, dan vendor teknologi harus **bekerja bareng**. Konsepnya: **open audit** — audit yang **terstruktur, transparan, kolaboratif**, dan **berbagi bukti** secara aman.

- Tujuan: mempercepat kejelasan *control*, menurunkan biaya audit ganda, dan menaikkan **ketahanan digital** industri.
- Ini sejalan dengan praktik global: *collective defense* lewat komunitas sektor keuangan seperti **FS-ISAC**, dan pengujian ketahanan bersama ala **TIBER-EU/CBEST**. ([FSISAC](#))

2. Mengapa sekarang?

- Regulasi internasional makin tegas soal **risiko pihak ketiga**. **DORA** di Uni Eropa bahkan menempatkan *critical ICT providers* di bawah pengawasan sektor keuangan. ([EIOPA](#))
- Komite **Basel** mengusulkan prinsip pengawasan *outsourcing* yang menegaskan **tanggung jawab direksi** dan *due diligence* sebelum kontrak. ([Reuters](#))
- Tren Asia juga sama: **RBI (India)** mendorong program ketahanan operasional dan pengendalian *outsourcing TI* lintas entitas. ([Reuters](#))
- Artinya, kolaborasi audit bukan opsi tambahan. Ini **arus utama** di dunia keuangan.

3. Prinsip *open audit* (ringkas dan mudah diikuti)

- **Satu peta kontrol, banyak pemakai**: *mapping* ke UU/POJK + standar internasional agar bukti vendor **bisa dipakai ulang** oleh beberapa bank (tanpa audit berulang).
- **Berbagi bukti secara aman**: gunakan *portal* berbasis *secure evidence room*; hak akses berlapis; jejak audit lengkap.
- **Uji bareng yang bermakna**: *threat-led testing* seperti **TIBER-EU/CBEST** untuk proses penting (*payment, mobile banking, core*) — hasilnya dibagi ke pihak terkait dengan batasan yang jelas. ([European Central Bank](#))
- **Fokus risiko pihak ketiga**: integrasikan *supplier risk* mengikuti panduan **NIST SP 800-161** (C-SCRM). ([NIST Computer Security Resource Center](#))
- **Budaya *collective defense***: berbagi *intelijen* dan pola serangan melalui jejaring seperti **FS-ISAC** (informasi terstandar, *real-time sharing*). ([FSISAC](#))

4. Bentuk program *open audit* (siap dieksekusi)

A. Konsorsium Audit Sektor Keuangan

- Anggota: bank, *fintech* berizin, dan vendor ICT strategis (cloud, core, switching, KYC).
- Produk: *control library* bersama → *questionnaire* standar → *evidence pack* terverifikasi.
- Manfaat: satu kali asesmen vendor dapat **di-leverage** oleh beberapa bank (hemat waktu & biaya).

B. *Threat-Led Test* lintas pihak (simulasi terkendali)

- Ikuti pola **TIBER-EU/CBEST**: ada *threat-intel provider*, *red team*, *white team*, dan pengawas.
- Cakupan: layanan kritikal yang dipakai bersama (mis. *cloud-based payments*) → hasil rekomendasi **lintas organisasi**. ([European Central Bank](#))

C. Program *Vendor Transparency*

- *Scorecard* minimum vendor: *patch latency*, *vuln backlog*, hasil uji *backup/restore*, dan bukti *DR test*.
- *Right-to-audit* yang jelas, termasuk *sub-processor* berlapis (rantai pasok).
- Rujukan *best practice*: **DORA** (oversight ICT), **Basel** (prinsip *outsourcing*), **NIST 800-161** (C-SCRM). ([EIOPA](#))

D. *Collective Defense Playbook*

- Kanal berbagi *Indicators of Compromise* (IOC) sektor keuangan via komunitas seperti **FS-ISAC**.
- *Release* rutin: *top exploited CVEs* + *mitigation* singkat untuk SOC bank/*fintech*. ([FSISAC](#))

5. Governance & peran

- **OJK**: tetapkan *baseline control* dan format *evidence*; pastikan hasil *open audit* bisa langsung masuk ke *supervision dashboard*.
- **Bank**: jadi *anchor tenant*; mengangkat standar ke vendor inti dan *fintech* mitra.
- **Fintech/Vendor**: menyediakan *evidence pack* standar; ikut uji *threat-led*; menutup *gap* yang ditemukan.
- **Forum industri** (mis. asosiasi): *operasionalisasi* konsorsium, *calendar* audit, dan pelatihan.

6. Manfaat langsung untuk industri

- **Cepat**: waktu dari temuan ke perbaikan lebih pendek karena bukti dan rekomendasi dibagi.
- **Efisien**: audit tidak berulang; *once tested, many trusted*.

- **Akurat:** *threat-led test* memotret *real-world attack path* pada proses kritikal. (CBEST/TIBER-EU dipakai regulator Eropa/UK untuk tujuan ini). ([Bank of England](#))
- **Kuat di vendor:** mengurangi *blind spot* rantai pasok sesuai **NIST 800-161**. ([NIST Computer Security Resource Center](#))
- **Selaras global:** konsisten dengan **DORA** (UE) dan dorongan **Basel**. ([EIOPA](#))

7. Risiko & *guardrails* (supaya aman)

- **Kebocoran info sensitif** → pakai *traffic light protocol*, *need-to-know*, dan *redaction* pada laporan publik.
- **Ketergantungan pihak ketiga** → kontrak harus memuat *right-to-audit*, *exit plan*, dan kewajiban *resilience test*. (Sejalan DORA & Basel). ([EIOPA](#))
- **Tes yang “mengganggu” produksi** → pakai metode **TIBER-EU/CBEST**: uji terencana, terkendali, berkoordinasi dengan pengawas. ([European Central Bank](#))

8. Quick wins 6 bulan (realistis)

- **Control Library 50 butir:** gabungan *security + privacy + third-party*; *questionnaire* tunggal untuk semua vendor prioritas.
- **Pilot open audit:** 10 vendor kritikal → *evidence pack* dibagi ke 5–7 bank.
- **Mini TIBER-style test** pada proses pembayaran digital → hasil koreksi *cross-org*. ([European Central Bank](#))
- **FS-ISAC weekly digest** ke SOC bank/*fintech*: *IOC* dan *patch advice* yang *actionable*. ([FSISAC](#))

9. Cara menjual program ini ke manajemen (narasi bisnis)

- **Biaya turun:** satu asesmen, banyak pemakai; audit vendor jadi hemat.
- **Waktu *time-to-trust*** lebih cepat: *onboarding* mitra tak tersendat.
- **Risiko sistemik turun:** *attack path* bersama tertutup lebih dini (uji bergaya TIBER/CBEST).
- **Kepatuhan terjaga:** selaras **DORA**, **Basel**, dan praktik C-SCRM **NIST** — kredibel di mata investor global. ([EIOPA](#))

Ringkasan

Open audit mengubah audit dari “beban” menjadi **kemitraan**. Kuncinya: **berbagi bukti, menguji bersama, dan menutup celah bersama**. Model dunia sudah ada: **FS-ISAC** untuk berbagi ancaman, **TIBER-EU/CBEST** untuk uji ketahanan, **DORA/Basel** untuk tata kelola pihak ketiga, dan **NIST 800-161** untuk rantai pasok. Tinggal kita **adopsi, sederhanakan, dan jalankan** sesuai konteks Indonesia. ([FSISAC](#))

Bagian VI — Analisis Risiko dan Dampak Ekonomi

Bab 17: Kerugian Finansial dan Reputasional dari Breach

Dampak langsung: forensik, denda, hilangnya nasabah

Kebocoran data itu mahal. Bukan hanya *hacker* yang untung, tapi biaya di pihak bank meledak di hari-hari pertama. Riset global IBM/Ponemon menunjukkan biaya rata-rata pelanggaran data dunia **~USD 4,4–4,9 juta** per insiden. Di industri keuangan, angkanya lebih tinggi, **~USD 6,08 juta**. Ini termasuk biaya teknis, hukum, kompensasi nasabah, dan gangguan bisnis. ([IBM](#))

1, Forensik & pemulihan (*digital forensics & incident response – DFIR*)

Yang terjadi di 0–90 hari pertama:

- **Isolasi & containment:** memutus akses penyerang, menonaktifkan akun, *network segmentation*.
- **Forensik:** tim DFIR menelusuri *log*, *artifacts*, dan *malware*; mengukur *scope* data yang bocor.
- **Pemulihan layanan:** *restore* dari *backup*, uji integritas sistem, *hardening*.
- **Biaya operasional tambahan:** *call center*, monitor kredit/identitas untuk nasabah, *public relations*. IBM mencatat komponen pasca-insiden ini nyata membengkak. ([cdn.table.media](#))

Catatan: tren 2024–2025 sempat naik tajam, lalu turun tipis secara global karena deteksi & *containment* makin cepat. Namun biaya di AS justru rekor tinggi, menekan bank yang beroperasi di sana. ([Axios](#))

Pelajaran praktis

- *Playbook* insiden harus siap: siapa menghubungi siapa, 24/7, tanpa debat.
- Automasi deteksi (*AI/automation*) mempercepat *mean time to contain* → biaya turun. ([Axios](#))

2. Denda & sanksi regulator

Dampak ini langsung terasa, apalagi untuk bank dan perusahaan jasa keuangan yang tunduk pada banyak rezim.

- **AS (Capital One):** denda **USD 80 juta** dari OCC terkait pengendalian risiko *cloud*; juga penyelesaian gugatan konsumen **USD 190 juta**. ([OCC.gov](#))
- **AS (Equifax):** *settlement* global **USD 575–700 juta** akibat kebocoran 2017 (147 juta orang). Termasuk dana bantuan untuk konsumen. ([Federal Trade Commission](#))
- **Uni Eropa (GDPR):** otoritas rutin mengenakan denda besar untuk kegagalan perlindungan data. *Tracker* publik menampilkan daftar denda—termasuk kasus di sektor layanan keuangan. ([enforcementtracker.com](#))

- **Ingggris (2025, Capita):** denda **£14 juta** dari ICO karena kelemahan keamanan yang berujung kebocoran data jutaan individu. Biaya total kasusnya jauh di atas angka denda. ([Financial Times](#))

Intinya: denda bukan satu-satunya biaya. Ada biaya hukum, audit tambahan, kompensasi, dan investasi ulang keamanan yang wajib dilakukan.

3. Hilangnya nasabah (*customer churn*)

Ini sering jadi “biaya tersembunyi” yang paling berat.

- Setelah *breach*, sebagian nasabah **pindah bank**. Survei industri menyebut **~38%** nasabah bersedia pindah lembaga keuangan jika datanya bocor. *Lost business* ini bisa lebih mahal dari denda. ([PKWARE®](#))
- IBM menempatkan “kehilangan bisnis” (turunnya akuisisi, *customer turnover*, penurunan *lifetime value*) sebagai komponen biaya terbesar pada banyak insiden. ([cdn.table.media](#))

Sinyal keuangan yang sering tampak:

- Naik-turunnya harga saham pascainsiden.
- Kenaikan *customer acquisition cost* untuk mengembalikan kepercayaan.
- Pengeluaran *remediation* (monitor kredit, *identity protection*) untuk menjaga loyalitas. ([zscaler.com](#))

4. Tiga *driver* biaya yang paling menentukan

- **Kecepatan deteksi & *containment***. Makin cepat, makin murah. Organisasi yang menerapkan *AI/automation* dan *playbook* matang, biaya turun nyata. ([Axios](#))
- **Jenis data yang bocor**. *Customer PII* dan data finansial paling sering dicuri dan mahal ditangani. ([cdn.table.media](#))
- **Kepatuhan lintas yurisdiksi**. Operasi multi-negara berarti multi-regulator, multi-denda, multi-kewajiban *disclosure* (contoh: aturan SEC mewajibkan *public company* melaporkan insiden *material* dengan cepat). ([SEC](#))

5. Checklist aksi 30 hari untuk menekan dampak langsung

Singkat. *Actionable*. Fokus tiga area di atas.

Forensik & pemulihan

- Kontrak DFIR *on-retainer*. Latih *table-top* triwulan.
- Standarkan *evidence handling*; pastikan *logging* 12–18 bulan tersimpan.

Denda & kepatuhan

- *One-pager* kewajiban notifikasi: OJK, PDP, pasar modal, *card schemes*, mitra internasional.
- Tunjuk juru bicara, siapkan *FAQ* publik; kurangi risiko salah ucap yang berdampak hukum.

Hilangnya nasabah

- Paket *goodwill* nasabah: *credit monitoring*, hotline khusus, SLA pemrosesan klaim.
- Kampanye *trust rebuild* sederhana: apa yang terjadi, apa yang diperbaiki, kapan selesai—tanpa jargon.

Ringkasan

Dampak langsung *breach* di perbankan = **tiga pukulan beruntun**:

1. **Forensik & pemulihan** yang mahal dan menyita fokus operasi.
2. **Denda/regulatory actions** lintas otoritas, dari OJK sampai GDPR/ICO/FTC—angka bisa menembus ratusan juta dolar dalam kasus besar. ([Federal Trade Commission](#))
3. **Hilangnya nasabah** yang berakibat jangka panjang pada pendapatan.

Kuncinya: *deteksi cepat*, *respons terlatih*, *transparansi yang pas*, dan paket pemulihan kepercayaan sejak hari pertama. Dengan itu, bank memang tidak bisa “membatalkan” *breach*, tapi bisa **memotong biaya langsung** dan **menahan arus nasabah keluar**.

Dampak tidak langsung: penurunan nilai saham & kepercayaan publik

Kebocoran data bukan hanya urusan *IT*. Pasca *breach*, dua hal sering terjadi: **harga saham turun** dan **kepercayaan publik jatuh**. Efeknya bisa berbulan-bulan, bahkan tahunan. Studi *event study* menunjukkan *cumulative abnormal returns* negatif di sekitar pengumuman insiden. Ini artinya pasar menghukum emiten karena melihat risiko tata kelola dan operasional meningkat. ([ScienceDirect](#))

1. Penurunan nilai saham: pola yang berulang

- **Reaksi cepat pasar.** Banyak kasus menunjukkan penurunan harga saham di hari pengumuman dan beberapa minggu sesudahnya. Contoh, pada kasus besar di AS: setelah pengumuman *breach*, saham turun signifikan; beberapa studi mencatat penurunan *3-day window* sekitar **-4% CAAR** untuk serangan besar. ([istari-global.com](#))
- **Kinerja tertinggal setahun.** Analisis bisnis menyebut perusahaan yang terkena *data breach* dapat **underperform** indeks teknologi **~8–9% setelah 1 tahun**—indikasi luka reputasi yang belum sembuh. ([Harvard Business Review](#))
- **Kasus ikonik.** Insiden besar di biro kredit AS memicu penurunan tajam di awal dan memakan waktu lama untuk pulih; kasus ini sering jadi rujukan dampak reputasi terhadap valuasi. ([The Guardian](#))

Kenapa saham turun? Investor menilai: biaya pemulihan membesar, risiko denda naik, potensi *customer churn* tinggi, dan manajemen dianggap gagal mengelola risiko *cyber*. Ini menekan *earning multiple*.

2. Kepercayaan publik: aset tak terlihat, dampaknya sangat nyata

- **“Lost business” membengkak.** Komponen biaya terbesar dalam banyak insiden adalah **kehilangan bisnis**: nasabah pindah, penjualan baru seret, *brand* rusak. Laporan IBM tahunan menegaskan porsi “lost business” tinggi dalam total biaya *breach*. ([IBM](#))
- **Tren global.** Jumlah *data breach* meningkat dari tahun ke tahun; publik makin sensitif terhadap perlindungan data. Ketika transparansi dan kontrol pengguna lemah, kepercayaan runtuh lebih cepat. ([Harvard Business Review](#))

Efek keuangan dari trust yang jatuh

- *Customer acquisition cost* naik, promosi “pemulihan” jadi mahal.
- *Cross-sell* gagal; nasabah menahan aktivitas.
- Mitra global lebih ketat memberi akses data maupun kerjasama lintas negara.

3. Jalur penularan ke valuasi & likuiditas bank

- **Ekspektasi denda & gugatan** → *earnings* tergerus → *price/earnings* turun. ([Financial Stability Board](#))
- **Tekanan kepatuhan lintas negara** → kewajiban pelaporan lebih cepat (*FIRE*, SEC, GDPR) → biaya kepatuhan bertambah → margin tertekan. ([Financial Stability Board](#))

- **Sentimen kredit & pasar modal** → *risk premium* naik; biaya pendanaan bisa terdampak.

4. **Playbook sederhana untuk menahan kerusakan (30–90 hari)**

A. Atur narasi publik (transparan, faktual, tanpa drama)

- Rilis *timeline* yang jelas: apa yang terjadi, data apa terdampak, langkah perbaikan.
- Janji yang konkret: *credit monitoring*, *hotline*, SLA. Ini *signal* kuat untuk pasar.

B. Lindungi valuasi dengan aksi nyata

- *Containment* cepat dan bukti perbaikan: *patch*, *hardening*, *third-party review*.
- Sampaikan *leading indicators*: waktu deteksi/penanganan membaik, *penetration test* selesai, audit independen berjalan. Investor butuh angka, bukan slogan.

C. Pulihkan *trust*

- Terapkan *privacy by design* pada fitur utama (*mobile banking*, *onboarding*).
- Tonjolkan *governance*: peran *board*, DPO, dan *risk committee*; pastikan keterlibatan mereka terlihat.

5. **Metrik yang wajib dilaporkan ke pasar (dan ke OJK)**

- **Waktu deteksi & *containment*** (menit/jam, bukan hari). Percepatan ini berkorelasi dengan turunnya biaya dan meredam sentimen negatif pasar. ([IBM](#))
- **Besaran data terdampak** + jenis PII finansial.
- **Tingkat *customer churn*** dan *win-back rate*.
- **Kemajuan *remediation***: *patch rate*, hasil uji *red team*, status audit eksternal.
- **Kepatuhan pelaporan** (kerangka *FIRE* untuk insiden operasional/ siber di sektor keuangan). ([Financial Stability Board](#))

6. **Apa pelajaran untuk bank di Indonesia?**

- **Siapkan *market response kit***: *press Q&A*, *investor deck*, dan *risk disclosure* standar—selaras dengan praktik konvergensi pelaporan insiden global yang didorong FSB. ([Financial Stability Board](#))
- **Latih skenario pasar**: simulasi *table-top* bukan hanya teknis, tapi juga komunikasi ke publik, analis, dan otoritas.
- **Bangun *trust equity*** sebelum krisis: audit berkala, *certification* relevan, dan *transparency report* tahunan membuat pasar memberi “diskon hukuman” saat terjadi insiden.

Ringkasan

Penurunan nilai saham dan kepercayaan publik adalah **biaya tak kasat mata** namun paling lama membekas. Pasar menghukum ketidakpastian; publik menghukum kurangnya empati dan perbaikan. Resepnya: **deteksi cepat, laporan rapi (standar global), aksi perbaikan nyata, dan komunikasi jujur**. Dengan itu, bank bisa **memotong dampak valuasi** dan **mengembalikan kepercayaan** lebih cepat daripada pesaing yang lambat. ([Harvard Business Review](#))

Bab 18: Efek Sistemik terhadap Stabilitas Keuangan Nasional

Simulasi skenario “crisis of confidence”

Dalam serangan siber besar, masalahnya bukan hanya server mati. Yang lebih berbahaya adalah **krisis kepercayaan**. Nasabah panik. Dana ditarik. *Payment* tersendat. Pasar uang tegang. Jika tidak cepat diatasi, gangguan bisa menyebar ke sistem keuangan nasional. Lembaga internasional sudah mengingatkan: insiden siber besar dapat mengganggu *financial market infrastructure* dan memicu risiko stabilitas sistemik. ([Financial Stability Board](#))

Kerangka global sebagai acuan

- **FSB** mendorong *cyber resilience* lintas negara, *incident reporting* yang selaras, serta praktik respons/pemulihan agar gangguan tidak meluas. ([Financial Stability Board](#))
- **IMF**: *cyber risk* kini masuk radar *macrofinancial stability*. IMF menerbitkan panduan penggunaan simulasi untuk *cyber stress testing*. Ada contoh gangguan pembayaran antar bank yang berkepanjangan di beberapa negara. ([IMF](#))
- **ECB – TIBER-EU**: kerangka *threat-intelligence-based red teaming* untuk menguji ketahanan sistem produksi yang kritikal. Bisa diadopsi sebagai referensi uji sektor keuangan. ([European Central Bank](#))
- **Bank of England**: melakukan *cyber stress test* sektor keuangan dan mempublikasikan temuan tematik untuk perbaikan kolektif. ([Bank of England](#))
- **The Fed/OCC**: menegaskan pentingnya ketahanan operasional FMU (*financial market utilities*) yang menopang *clearing/settlement*. Jika FMU terganggu, efeknya sistemik. ([Federal Reserve](#))

Intinya: Indonesia perlu simulasi yang tidak hanya *technical*, tapi juga *macroprudential*—menguji perilaku pasar, likuiditas, dan koordinasi antar-otoritas.

Model simulasi 3 babak: dari insiden ke sistemik

Bayangkan ini seperti *war-game* selama 72 jam. Ada **pemicu**, **saluran penularan**, dan **tindakan penahan**.

Babak 1 — Pemicu (*trigger*)

- *Data breach* di bank besar → publikasi media.
- *Payment switch* dan *RTGS* tetap jalan, tapi terjadi *degradation* layanan digital.
- *Rumor* menyebar di media sosial tentang hilangnya dana.

Asumsi teknis

- *Malware* menonaktifkan sebagian *core banking API*.
- *Mean time to detect/contain* belum optimal.

Indikator

- Lonjakan *mobile login failure*.
- Kenaikan *call-center queue*.
- Antrian penarikan tunai.

Babak 2 — Penularan (*contagion channels*)

- **Likuiditas ritel:** *bank run* digital; *switching* dana ke bank pesaing/uang tunai.
- **Pasar antarbank:** lawan transaksi menaikkan *haircut* atau menahan *limit* intrahari.
- **FMI/FMUs:** *clearing/settlement* melambat → risiko gagal serah.
- **Reputasi sistem:** bank sehat ikut terdampak karena *herd behavior*.

FSB dan IMF menekankan bahwa gangguan di FMI atau *payment* dapat menimbulkan implikasi stabilitas luas bila tidak segera dikandung. ([Financial Stability Board](#))

Babak 3 — Aksi penahan (*containment*)

- **Teknis:** isolasi segmen jaringan, *failover* ke *clean site*, prioritas layanan kritikal.
- **Likuiditas:** otoritas aktifkan fasilitas likuiditas intrahari; perluasan *eligible collateral*.
- **Komunikasi:** *joint statement* OJK–BI–BSSN. Satu narasi. *Status page* publik.
- **Koordinasi:** *incident reporting* cepat dan seragam ke otoritas (selaras rekomendasi FSB). ([Financial Stability Board](#))

Cara mendesain simulasi OJK (praktis dan terukur)

1. Skenario inti (yang dites)

- **Gangguan 48–72 jam** pada *digital channels* bank sistemik.
- **Degradasi 20–40%** kapasitas *payment* ritel dan keterlambatan *clearing* antarbank.
- **Kebocoran PII** terkonfirmasi, *media coverage* intens.

2. Metrik kunci (harian & intrahari)

- **Kecepatan pemulihan:** *MTTD/MTTC*, waktu *failover*, *service availability*.
- **Likuiditas:** arus keluar dana ritel (net-outflow), *LCR* intrahari, *haircut* dan *limit* pasar uang.
- **FMI:** *settlement finality delay*, jumlah instruksi tertunda.
- **Perilaku publik:** *call volume*, *complaint spike*, *social sentiment* negatif.
- **Kepercayaan pasar:** *CDS spread* (jika ada), *interbank rate* vs *policy rate*.

3. *Decision points* yang harus muncul

- Kapan mengaktifkan **fasilitas likuiditas darurat**?
- Kapan melakukan **public disclosure minimal** agar tidak menambah panik, namun tetap patuh?
- Bagaimana **traffic shaping pembayaran** agar prioritas ekonomi (gaji, kesehatan, pangan) tetap jalan?

4. Bukti *readiness* yang diminta dari bank

- *Board-approved cyber playbook + table-top* 2x setahun.
- Hasil *red-team* berbasis intelijen ala *TIBER-EU* untuk sistem kritikal.
- *Service mapping* → daftar *critical business services* dan *impact tolerance* (berapa lama aman terganggu). ([European Central Bank](#))

Rancangan “skor simulasi” untuk menilai stabilitas

Sederhana. Skor 0–100. Tiga komponen sama bobot:

1. **Teknis** (*operational resilience*): *detection/containment, failover, data integrity*.
2. **Likuiditas & pasar**: kebutuhan pendanaan darurat, *market confidence*, disiplin antarbank.
3. **Transparansi & koordinasi**: kepatuhan pelaporan, kualitas *public messaging*, kolaborasi dengan FMI/FMUs.

Skor <60 = *watchlist*. 60–80 = *improve*. >80 = *resilient*.

Pendekatan ini sejalan dengan dorongan IMF/FSB untuk memasukkan siber ke *stress testing* dan *macroprudential toolkit*. ([IMF](#))

Peran OJK saat simulasi (dan saat krisis nyata)

- **Komando**: pusat koordinasi insiden sektor keuangan, *single source of truth*.
- **Kepatuhan**: format *incident reporting* terstandar, waktu pelaporan ketat, *taxonomy* seragam—mengacu rekomendasi FSB tentang konvergensi pelaporan. ([Financial Stability Board](#))
- **Konektivitas**: kanal cepat ke BI (likuiditas & pembayaran), BSSN (teknis & *threat intel*), Kominfo (komunikasi publik).
- **Pembelajaran**: setelah simulasi, keluarkan *thematic findings* sektor, seperti praktik Bank of England, agar semua bank—termasuk yang tidak ikut uji—ikut memperbaiki. ([Bank of England](#))

Penutup

Crisis of confidence bisa menyebar lebih cepat daripada *malware*. Kuncinya ada di **kecepatan pemulihan layanan kritikal**, **ketersediaan likuiditas**, dan **narasi publik yang jernih**. Dengan simulasi terstruktur dan metrik yang jelas—mengacu praktik FSB, IMF, ECB, dan Bank of England—Indonesia dapat **menahan guncangan**, menjaga **stabilitas**, dan memulihkan **kepercayaan** sebelum krisis menjadi sistemik. ([Financial Stability Board](#))

Peran OJK dalam pencegahan efek berantai

Inti gagasan: kalau ada *cyber breach* besar di satu bank, kepercayaan bisa runtuh, dana keluar, pasar panik. Tugas OJK adalah “memutus rantai” sebelum guncangan menyebar ke bank lain, ke *payment system*, lalu ke ekonomi riil.

Kenapa ini krusial?

- IMF menegaskan: insiden siber makin sering dan semakin mahal. Risiko “kejadian ekstrem” bisa memicu hilangnya kepercayaan dan gangguan layanan kritikal. Ini bisa berdampak makro—bukan hanya teknis TI. ([IMF](#))
- Standar global menuntut **ketahanan operasional**. Bukan hanya mencegah serangan, tapi memastikan layanan inti tetap jalan saat krisis. Basel Committee mendorong *principles for operational resilience*. ([Bank for International Settlements](#))
- Untuk infrastruktur pasar (*FMI*—RTGS, kliring, CSD), pedoman CPMI-IOSCO menargetkan *two-hour RTO* agar layanan pulih cepat dan mencegah kepanikan sistemik. ([Bank for International Settlements](#))

Peran OJK: lima garis pertahanan sistemik

1. **Peringatan dini (*early warning*) lintas-bank**
 - Bangun *fusion center* pengawasan digital: kumpulkan *telemetry* insiden, anomali pembayaran, dan *threat intel* sektor.
 - Wajibkan pelaporan insiden siber yang ringkas, seragam, dan cepat—mengacu rekomendasi FSB soal harmonisasi *incident reporting*. Tujuannya: bahasa sama, metrik sama, waktu laporan jelas. ([Financial Stability Board](#))
2. **Pengujian ketahanan terarah**
 - Terapkan uji *threat-intel led red teaming* ala **TIBER-EU** pada bank sistemik, *payment switch*, dan *e-channels* kritikal. Fokus pada skenario yang paling mungkin memicu *bank run digital*. ([European Central Bank](#))
 - Kaitkan hasil uji ke **rating** CyberTrust. Bank yang gagal pada skenario sistemik wajib *remediasi* sebelum musim puncak transaksi (Lebaran, akhir tahun).
3. **Protokol *stabilization* saat krisis**
 - *Playbook* nasional yang disepakati regulator: OJK (prudensial), BI/BI-FAST/RTGS (pembayaran), BSSN (respon teknis).
 - Tombol *circuit breaker* operasional: *transaction throttling*, perpanjangan jam kliring, *read-only mode* untuk layanan non-kritis, plus *communications control* agar publik dapat info cepat dan konsisten. Pedoman CPMI-IOSCO mendukung pemulihan cepat di FMI untuk cegah transmisi guncangan. ([Bank for International Settlements](#))
4. **Proteksi dari *third-party concentration risk***

- IMF mengingatkan keterkaitan bank-penyedia TI dapat jadi jalur rambatan. OJK perlu *vendor registry* kritikal, uji *failover* antar-region, dan kewajiban *exit plan* multi-cloud. ([IMF](#))
- Tetapkan *impact tolerance* dan *severe but plausible scenarios* seperti di aturan ketahanan operasional UK/BCBS. Tenggat uji dan *mapping* layanan harus jelas. ([nortonrosefulbright.com](#))

5. Transparansi terukur, tanpa memicu panik

- Terapkan *tiered disclosure*: laporan cepat ke otoritas (menit–jam), pengumuman publik terarah saat layanan aman, dan *post-mortem* terbuka setelah pemulihan. IMF menilai hilangnya kepercayaan adalah kanal utama risiko sistemik—komunikasi yang jujur menahan eksodus dana. ([IMF](#))

Arsitektur operasional OJK saat “efek berantai” mengancam

- **Command center regulatori**
War room lintas-lembaga (OJK-BI-BSSN-Kemenkominfo). Satu *dashboard* risiko real-time: kesehatan kanal pembayaran, *incident tickets*, ketersediaan *core banking*, antrean kliring, dan sentimen publik.
- **Metrik pemutus rantai**
 1. *Time to detect, time to contain, time to recover (TTR)*.
 2. *Deposit outflow velocity* ritel/korporat sebagai indikator kepercayaan.
 3. *FMI's health index* (RTGS/kliring) untuk melihat potensi *liquidity gridlock*. (Selaras dengan CPMI-IOSCO yang menempatkan FMI sebagai “penyalur guncangan” jika tidak tahan banting). ([Bank for International Settlements](#))
- **Intervensi bertahap**
 1. *Supervisory nudge*: instruksi penguatan *DDoS shielding*, *traffic shaping*, dan *customer comms*.
 2. *Temporary relief*: kelonggaran operasional/likuiditas berkoordinasi dengan BI untuk jaga kepercayaan, tanpa mengorbankan integritas pasar.
 3. *Public assurance*: pesan satu suara. Jelaskan layanan yang aman, SLA pemulihan, dan langkah kompensasi terbatas. (IMF: kejelasan mengurangi *run dynamics*). ([IMF](#))

Apa yang wajib dilakukan bank sekarang?

- **Buktikan *impact tolerance*** untuk layanan inti: *mobile banking*, ATM, RTGS interface.
- **Latihan *crisis comms*** bersama OJK: *media drill* 90 menit, *dark site* siap tayang.
- **Uji *live failover* terjadwal** dengan skenario lintas-vendor, mengikuti semangat *two-hour RTO* di dunia FMI. ([Bank for International Settlements](#))
- **Penuhi format laporan insiden yang diseragamkan** (FSB 16 rekomendasi). *Template* ini mempercepat analisis dan koordinasi lintas-regulator. ([Financial Stability Board](#))

Ukur keberhasilan OJK (indikator sederhana)

- Waktu deteksi-ke-respon di bank sistemik turun $\geq 50\%$ dalam 12 bulan.
- Tak ada *spillover* ke RTGS/kliring pada tiga insiden besar berturut-turut.
- *Deposit outflow velocity* kembali normal < 72 jam pasca insiden.
- Kepatuhan uji *red team* ala TIBER-EU di seluruh bank BUKU 4 dan FMI prioritas. ([European Central Bank](#))

Penutup

Cyber breach bukan sekadar isu TI. Ini isu **kepercayaan**. Dengan *early warning* yang seragam (FSB), ketahanan operasional berstandar global (BCBS, CPMI-IOSCO), dan uji serangan realistis (TIBER-EU), OJK bisa menahan guncangan agar tidak berubah menjadi **krisis sistemik**. Itulah inti pencegahan efek berantai—teknologi siap, tata kelola kuat, komunikasi jernih. ([Financial Stability Board](#))

Istilah asing yang digunakan: early warning, incident reporting, threat-intel led red team, TTR/TTR, two-hour RTO, circuit breaker, impact tolerance, stress scenario, public assurance.

Bagian VII — Roadmap Peningkatan & Mitigasi

Bab 19: Roadmap Peningkatan Tahunan bagi Bank

Target kenaikan rating per tahun (> 1 level)

Intinya: naikkan *digital trust* bank setiap tahun. Minimal lompat lebih dari satu tingkat rating. Lakukan dengan rencana yang jelas, metrik yang terukur, dan disiplin eksekusi. Ikuti praktik global. Sesuaikan dengan konteks Indonesia.

Mengapa target >1 level itu realistis

- Standar global makin jelas. **NIST CSF 2.0** sudah menambah fungsi *Govern* untuk tata kelola risiko siber. Ini memudahkan bank membangun *baseline* yang kuat dan naik cepat dari tahun ke tahun.
- **ISO/IEC 27001:2022** menyederhanakan kontrol (93 kontrol baru), sehingga program peningkatan bisa lebih fokus dan cepat dieksekusi.
- Regulator internasional mendorong *operational resilience* yang terukur (Basel, UK PRA). Artinya, ada *benchmark* yang bisa langsung dipakai untuk *gap closing*. (service.betterregulation.com)
- Tekanan ekonomi nyata: laporan **IBM Cost of a Data Breach 2024** menunjukkan biaya rata-rata pelanggaran data naik dan sektor keuangan termasuk yang paling mahal. Naik rating = turunkan biaya insiden.

Prinsip eksekusi tahunan (sederhana dan tegas)

1. **Fokus 12 bulan.** Bagi jadi 4 kuartal. Tiap kuartal harus ada *quick wins* dan *hardening* yang terlihat.
2. **Data-driven.** Semua aksi harus punya metrik: *MTTD/MTTR*, tingkat *patching*, *phishing fail rate*, temuan audit, *vendor risk score*.
3. **Governance dulu.** Perkuat *board oversight* dan peran CISO/DPO. Ini kunci di NIST CSF 2.0 fungsi *Govern*.
4. **Resilience, bukan cuma compliance.** Uji *impact tolerance* layanan penting, seperti anjuran Basel dan UK PRA. (service.betterregulation.com)
5. **Transparan ke OJK.** Kirimkan progres per kuartal ke dashboard pengawasan OJK dalam format standar, selaras inisiatif harmonisasi pelaporan insiden (FSB *FIRE*). ([Financial Stability Board](https://financialstabilityboard.org))

Peta jalan 12 bulan untuk loncat >1 level

Q1 — Baseline & Quick Wins

- Tentukan **baseline rating** dengan *self-assessment* yang memetakan kontrol ISO 27001:2022 ↔ NIST CSF 2.0. Prioritaskan kontrol *Govern/Identify/Protect*.

- **Perkuat *governance*.** Bentuk komite risiko siber lintas unit. Set *risk appetite* dan *impact tolerance* per layanan (pembayaran, *mobile banking*, *treasury*). (service.betterregulation.com)
- **Quick wins.** Patch backlog, aktifkan MFA di semua akun istimewa, *email security* (DMARC), *endpoint hardening*.
- **Vendor tiering.** Kelompokkan *critical vendors*. Masukkan klausul pelaporan insiden dan *right to audit* ala DORA/operational resilience.

Q2 — Control Build-out

- **Konsolidasikan kontrol ISO 27001:2022.** Tutup celah pada *access control*, *logging*, *encryption at rest/in transit*.
- **Latihan *table top*.** Simulasikan skenario *ransomware* dan kebocoran data. Ukur *MTTD/MTTR*, keputusan eskalasi, dan *customer comms*.
- **Lengkapi *playbook* pelaporan insiden** mengacu pada elemen umum FSB *FIRE*. Ini memudahkan koordinasi antar-otoritas dan bank. ([Financial Stability Board](https://financialstabilityboard.org))

Q3 — Resilience Proof

- **Uji *impact tolerance*.** Lakukan *stress test* gangguan pada layanan penting (ATM, *real-time payments*). Target: tetap di bawah ambang toleransi seperti panduan PRA/ Basel. (service.betterregulation.com)
- **Third-party testing.** Minta *attestation* pihak ketiga (penetration test, *red team*). Fokus ke *crown jewels* dan *critical vendors*.
- **Otomasi pemantauan.** Integrasi telemetri ke *SIEM/SOAR* untuk menurunkan *MTTR*. *Dashboard* siap disinkronkan ke portal OJK.

Q4 — Assurance & Kenaikan Rating

- **Audit internal + external assurance.** Gunakan *evidence* satu tahun untuk menunjukkan perbaikan skor.
- **Tutup *residual risk*.** Terbitkan rencana 90 hari untuk isu sisa.
- **Publikasikan ringkas progres** (ke OJK dan internal manajemen). Tautkan hasil ke target tahun depan.

Metrik keberhasilan (yang bank bisa hitung cepat)

- **Kenaikan rating:** naik ≥ 2 level (contoh: dari *BB* ke *A*).
- **Mean Time to Detect (MTTD) & Recover (MTTR):** turun $\geq 30\%$.
- **Kepatuhan kontrol ISO 27001:2022:** $\geq 90\%$ kontrol prioritas tuntas.
- **Uji *impact tolerance* lulus** untuk ≥ 3 layanan kritikal. (service.betterregulation.com)
- **Vendor kritikal tersertifikasi** atau punya *attestation* setara DORA/TRM.
- **Kerugian insiden:** *trend* menurun; targetkan penghematan sejalan temuan biaya kebocoran data global (rujukan IBM).

Pilar kebijakan yang menyokong kenaikan >1 level

- **Govern first.** Dewan komisaris menerima *risk dashboard* siber tiap kuartal—ini sejalan dengan NIST CSF 2.0 fungsi *Govern*.
- **Resilience berbasis prinsip.** Ikuti **Basel Principles for Operational Resilience** untuk layanan penting dan ketergantungan *third-party*.
- **Kesiapan regulasi lintas yurisdiksi.** *Playbook* insiden dan pengelolaan TIK mengacu **EU DORA**—relevan bagi bank yang terhubung ke pasar Eropa.
- **Harmonisasi pelaporan.** Elemen pelaporan insiden mengikuti **FSB FIRE** agar mudah dibaca lintas otoritas. ([Financial Stability Board](#))

Paket tindakan ringkas (siap dieksekusi)

- **30 hari:** *baseline* + *quick wins* teknis (MFA, patch, DMARC).
- **90 hari:** *governance charter*, *risk appetite*, *vendor tiering*, *tabletop exercise*.
- **180 hari:** kontrol ISO 27001:2022 prioritas selesai; integrasi *SIEM/SOAR* dasar.
- **270 hari:** uji *impact tolerance* layanan penting; *remediation sprint*. ([service.betterregulation.com](#))
- **360 hari:** audit, *external assurance*, bukti kenaikan rating, dan target tahun berikutnya.

Penutup

Naik >1 level tiap tahun itu **bisa**. Kuncinya *governance yang tajam*, eksekusi kuartalan, dan keberanian mengukur *impact tolerance*. Bank yang bergerak cepat bukan hanya patuh. Mereka **lebih tahan banting**, **lebih dipercaya**, dan **lebih efisien biaya**—sejalan dengan arah global dari NIST, Basel, UK PRA, DORA, dan best practice biaya insiden. ([service.betterregulation.com](#))

Catatan istilah: baseline, quick wins, playbook, benchmark, stress test, tabletop exercise, impact tolerance, governance, attestation, operational resilience, SOAR — digunakan apa adanya karena sudah lazim di industri.

Program “PDP Compliance Improvement Plan”

Target: setiap bank naik >1 level rating per tahun

Tujuan singkat: Program ini membantu bank menutup celah kepatuhan UU PDP dan standar internasional. Caranya terukur, bertahap, dan langsung ke inti risiko. Hasilnya: *privacy by design* jalan, insiden turun, dan rating naik cepat.

Prinsip main yang sederhana

- **Fokus pada risiko terbesar dulu.** Mulai dari data yang paling sensitif: KTP, biometrik, kredensial login, transaksi.
- **Otomatisasi bukti kepatuhan.** Kurangi *spreadsheet*. Pakai *control library* dan *evidence collector* otomatis.
- **Perbaiki berkelanjutan.** Setiap kuartal ada *gap* yang ditutup, bukan menunggu audit tahunan.
- **Selaras standar global.** Mapping ke ISO/IEC 27001:2022, ISO/IEC 27701, NIST CSF 2.0 & NIST Privacy Framework. ([ISO](#))

Paket kerja 12 bulan (ringkas tapi tajam)

Q1 — “Kenali dan amankan mahkota data”

- **Data inventory & data flow mapping** untuk seluruh *customer journey* digital.
- **Klasifikasi & retention policy:** pisahkan *golden record* vs. data turunan.
- **Kontrol dasar kuat:** *MFA*, *hardening cloud*, *secrets management*, enkripsi *at rest/in transit*.
- **Hasil:** *Data map* resmi bank + *risk register* PDP prioritas tinggi.
- **Rujukan:** ISO/IEC 27701 (Sistem Manajemen Informasi Privasi) menekankan *roles*, *PII lifecycle*, dan bukti penerapan. ([NIST](#))

Q2 — “Buktikan kontrol berjalan”

- **Uji bukti otomatis:** *log akses PII*, *DLP alert*, *backup restore test* terdokumentasi.
- **Consent management & privacy notice** seragam di mobile/web.
- **Penilaian dampak privasi (DPIA)** untuk fitur berisiko tinggi: *e-KYC*, *fraud analytics*, *biometric*.
- **Rujukan:** NIST Privacy Framework & NIST CSF 2.0 (fungsi *Govern* memperkuat tata kelola dan akuntabilitas). ([NIST](#))

Q3 — “Latih dan latih ulang”

- **Simulasi insiden:** *tabletop exercise* kebocoran data end-to-end (deteksi → notifikasi → pemulihan).
- **Uji teknis:** *red team*, *phishing drill*, uji *ransomware recovery* RTO/RPO.
- **Vendor due diligence:** *right-to-audit*, *breach clause*, dan *data processing agreement* minimum ISO 27001/27701.

- **Pelajaran global:** bank yang gagal menjaga ketersediaan dan *operational resilience* bisa dikenai sanksi/penalti pengawasan. Contoh dari Singapura menunjukkan pengawas dapat memberi *capital add-on* untuk kegagalan teknologi. ([Wall Street Journal](#))

Q4 — “Tutup gap & naik kelas”

- **Remediasi tersisa:** *privileged access, shadow IT, orphan data* di *data lake*.
- **Audit internal mandiri + external assurance** terarah ke kontrol PDP kritikal.
- **Public assurance narrative:** siapkan ringkasan yang bisa dibaca publik tanpa membuka rahasia, selaras *OJK CyberTrust & Data Privacy Ranking*.
- **Rujukan:** ISO/IEC 27001:2022 menyederhanakan kontrol jadi 93 *Annex A* dengan tema *Govern, Protect, Detect, Respond, Recover* — memudahkan pelaporan dan pengujian. ([ISO](#))

Playbook kenaikan rating >1 level: metrik yang harus “hijau”

- **Waktu deteksi insiden (MTTD)** < 24 jam dan **waktu respon (MTTR)** < 72 jam pada insiden berdampak PII.
- **Tingkat kepatuhan *consent & purpose limitation*** ≥ 99% untuk produk ritel (cek *event log & API gateway*).
- **Backup immutability & ransomware drill** lulus 2x setahun.
- **Vendor kritikal:** 100% punya *DPA*, uji *restore*, dan *breach SLA*.
- **DPIA:** semua fitur berisiko tinggi selesai sebelum *go-live*.
- **Pelatihan anti-phishing:** tingkat klik < 5% pada simulasi Q3.
- **Pembuktian biaya:** gunakan *control mapping* ke standar agar investasi terbaca regulator dan auditor.
- **Catatan tren global:** rata-rata biaya *data breach* terus tinggi di sektor keuangan; temuan tahunan menekankan deteksi cepat dan otomatisasi sebagai pengurang biaya terbesar. ([IBM](#))

Komponen wajib dokumen (mudah dicek, mudah diaudit)

1. **Register aktivitas pemrosesan** (siapa, data apa, tujuan, dasar pemrosesan, retensi).
2. **Katalog kontrol** yang dipetakan ke ISO 27001:2022 / 27701, NIST CSF 2.0, dan UU PDP. ([ISO](#))
3. **Rencana respons insiden PDP** termasuk *playbook* notifikasi regulator/nasabah.
4. **Consent evidence & DSAR log** (permintaan akses/hapus/data portability).
5. **Third-party risk file:** peringkat risiko vendor + rencana mitigasi.
6. **Laporan testing:** *restore test, red team, phishing drill, dan tabletop*.

Insentif & sanksi yang mendorong perubahan nyata

- **Insentif:** *capital relief* terbatas untuk kontrol yang terbukti menurunkan *loss expectancy* operasional, pengurangan *supervisory findings*, dan akses prioritas ke *regulatory sandbox* untuk *privacy tech*.
- **Sanksi progresif:** *heightened monitoring*, pembatasan fitur baru sampai kontrol PDP lulus, dan eskalasi ke tindakan pengawasan operasional sebagaimana praktik pengawas internasional pada kasus gangguan sistemik. ([Wall Street Journal](#))

Praktik bagus yang bisa langsung ditiru (*quick wins*)

- **Satu *privacy dashboard*** untuk CISO/DPO: *consent rate*, *DPIA status*, *DSAR SLA*, *vendor risk heatmap*.
- ***Data minimization by default*** di aplikasi mobile/web.
- ***Tokenization*** untuk PII di data analitik dan *test environment*.
- ***Just-in-time privacy notice***: singkat, jelas, muncul saat data dikumpulkan.
- ***Kill switch*** integrasi pihak ketiga di *API gateway* saat ada anomali.

Kenapa program ini “bankable”

- **Selaras praktik pengawas global.** NIST CSF 2.0 dan ISO 27001/27701 memberi bahasa kontrol yang diterima luas. ([NIST Publikasi Teknik](#))
- **Terukur dan bisa diaudit.** Setiap kuartal ada artefak: *data map*, *DPIA*, *test report*, *vendor file*.
- **Efek finansial nyata.** Deteksi cepat + otomatisasi respons terbukti menurunkan biaya *breach* dan durasi *downtime*. ([IBM](#))

Call-to-action untuk manajemen bank

- **Tetapkan *owner eksekusi*:** DPO untuk *governance*, CISO untuk kontrol teknis, CIO untuk *platform*.
- **Kunci anggaran 12 bulan** fokus ke *privacy engineering*, *log & monitoring*, dan *vendor risk*.
- **Komitmen rapat bulanan *Risk & Compliance*** hanya 30 menit: lihat metrik, putuskan remediasi.
- **Tujuan akhir tahun:** semua *gap high-risk* PDP tertutup, bukti kontrol siap, rating naik minimal satu tingkat.

Sederhana, konkret, dan terbukti di pasar global. Kita tidak perlu menebak-nebak. Kita jalankan *PDP Compliance Improvement Plan* secara disiplin—dan kita naik kelas.

Bab 20: Taktik *Empowerment* untuk Bank Berperingkat Rendah

Capacity building CISO dan DPO

Tujuan bab ini sederhana: menaikkan kemampuan *CISO* dan *DPO* di bank berperingkat rendah agar cepat naik kelas. Fokusnya praktik. Bahas hal yang bisa langsung dilakukan. Bahasa lugas. Tanpa jargon berlebihan.

Kenapa harus ngebut?

- Biaya *data breach* di sektor keuangan termasuk yang tertinggi di dunia. Setiap jam terlambat memperbaiki kontrol, biaya makin bengkak. Laporan global terbaru juga menekankan pentingnya *response playbook* yang teruji. ([ISO](#))
- Standar internasional sudah lebih jelas. *NIST CSF 2.0* menambah pilar *govern* agar peran manajemen dan *board* tegas. Ini selaras dengan kebutuhan bank: jelas peran, jelas indikator, jelas akuntabilitas. ([NIST Publikasi Teknik](#))
- Untuk privasi, *ISO/IEC 27701* memberi kerangka kerja praktis membangun *Privacy Information Management System (PIMS)*—pas dengan mandat DPO. ([Otoritas Perbankan Eropa](#))

Peran kunci: CISO & DPO (ringkas dan tegas)

- **CISO:** jaga *cyber resilience*. Tanggung jawab utama: *risk register*, arsitektur *zero trust*, *incident response*, dan latihan rutin.
- **DPO:** jaga kepatuhan PDP. Tanggung jawab utama: *privacy by design*, *record of processing*, *data subject rights*, *breach notification*. Pedoman regulator Eropa menekankan independensi, akses pada *board*, dan sumber daya memadai—prinsip yang bisa diadopsi OJK. ([ISO](#))

Paket 100 Hari: “Naik 1 Level Dulu”

Target: bank bisa naik >1 level rating dalam 12 bulan; 100 hari pertama bikin fondasi kuat.

Hari 0–30 — Stabilkan pondasi

- Bentuk **Cyber & Privacy War Room**. Rapat 30 menit tiap pagi. Agenda tetap: *open risks*, insiden, *SLA*.
- Kunci 10 kontrol duluan (prioritas tinggi):
 1. *MFA* untuk semua admin, 2) *EDR* aktif, 3) *backup immutable*, 4) *patching* 14 hari, 5) *email security (DMARC/SPF/DKIM)*,
 2. *privileged access* dibatasi, 7) *vendor access* lewat *bastion*, 8) *DLP* kanal sensitif, 9) *log* terkonsolidasi, 10) *crisis comms template*.
- DPO mulai **data mapping** cepat: sistem apa, data apa, tujuan apa, dasar hukum apa. Pakai *RACI* sederhana.
- Tetapkan **5 KRI** minimal: *phishing click rate*, *patch age*, jumlah *critical findings*, *mean time to detect*, dan *overdue DPIA*.

- Sinkronkan kerangka dengan **NIST CSF 2.0** (fungsi *Identify–Protect–Detect–Respond–Recover + Govern*) dan **ISO/IEC 27701** untuk privasi. ([NIST Publikasi Teknik](#))

Hari 31–60 — Melatihrespons

- Jalankan **tabletop exercise** lintas fungsi (CISO, DPO, Legal, Operasi, *call center*, PR). Skenario: *ransomware* + kebocoran data nasabah.
- Uji **alur notifikasi** PDP: siapa eskalasi, *deadline*, bukti *forensik*, dan pesan ke publik.
- Bentuk **Security Champions** di unit bisnis. Tugas: cek *privacy by design* di fitur baru dan edukasi cepat.
- Mulai **penilaian vendor kritikal** berbasis pedoman perbankan Eropa soal risiko *ICT & security*. Fokus: *access control*, *logging*, lokasi data, dan *incident clause* di kontrak. ([edpb.europa.eu](#))

Hari 61–100 — Kunci keberlanjutan

- Adakan **mini red team** 2 minggu. Tujuan: buktikan kontrol prioritas benar-benar bekerja.
- Terapkan **DPIA cepat** untuk 3 proses berisiko tinggi (mis. *mobile onboarding*, *credit scoring*, *fraud analytics*).
- Tautkan **OKR CISO/DPO** ke **insentif manajemen**: bonus terhubung ke penurunan *critical risk* dan kepatuhan *SLA* pelaporan insiden.
- Siapkan **laporan ke board** triwulanan: *risk heat map*, *loss estimate*, kesiapan *playbook*.
- Sinkronkan format pelaporan insiden dengan **arah global** menuju harmonisasi *cyber incident reporting* untuk kurangi beban dan percepat respons lintas regulator. ([xbri.org](#))

Kurikulum Singkat 6 Bulan untuk CISO & DPO

Gaya *bootcamp*. Jam belajar singkat. Banyak praktik.

- **Bulan 1 — Governance & Metrics**
OKR/KRI, risk appetite, board reporting. Case study biaya kebocoran di sektor finansial. ([ISO](#))
- **Bulan 2 — Zero Trust & Identity**
Segmentasi, MFA, privileged access, just-in-time access.
- **Bulan 3 — Detection & Response**
Use case SIEM, EDR, playbook, tabletop, forensics basics. Rujukan struktur Respond/Recover dari NIST CSF 2.0. ([NIST Publikasi Teknik](#))
- **Bulan 4 — Privacy by Design**
Data mapping, DPIA, dasar hukum pemrosesan, data subject rights. Ambil garis besar peran DPO dari panduan regulator Eropa. ([ISO](#))

- **Bulan 5 — *Third-Party & Cloud Risk***
Contract clause, right to audit, exit plan, resilience. Selaras dengan pedoman EBA ICT & security risk. (edpb.europa.eu)
- **Bulan 6 — *Operational Resilience Drills***
Latihan failover, backup restore, communications. Tambahkan opsi *bug bounty* atau *vulnerability disclosure program (VDP)*.

10 Quick Wins minim biaya, dampak besar

1. Aktifkan *MFA* 100% untuk admin & *remote access*.
2. *Disable* akun *dormant* dan *default*.
3. Terapkan *geo-blocking* untuk akses *admin*.
4. *Auto-patch internet-facing* 14 hari.
5. *DMARC quarantine/reject*.
6. *Security banner* dan *session timeout* di aplikasi internal.
7. *Awareness* mikro: video 3 menit mingguan.
8. *DLP* aturan sederhana: cegah kirim NIK/Norek lewat email eksternal.
9. *Honeytoken* untuk deteksi kebocoran cepat.
10. *After-action review* 24 jam setelah insiden.

Mekanisme akuntabilitas yang bikin “nempel”

- **Skor bulanan CISO/DPO:** 60% kinerja teknis (KRI), 40% kepatuhan & edukasi.
- **Kontrak vendor** wajib ada *incident disclosure window* (mis. 24 jam) dan *right to audit*. Selaras tren internasional yang mendorong pelaporan insiden makin seragam. (xbrl.org)
- **Komite Risiko Digital** di level direksi. Agenda tetap: *top 10 risks, loss estimate, status remediation*.
- **Simulasi median** biaya insiden berdasarkan *benchmarks* global untuk mengukur manfaat investasi keamanan. ([ISO](https://iso.org))

Sinkron ke Regulasi & Standar (ringkas)

- *NIST CSF 2.0:* tambahkan *Govern* → kuatkan mandat CISO, jalur eskalasi, dan metrik. ([NIST Publikasi Teknik](https://nist.gov/publications))
- *ISO/IEC 27701:* jadikan DPO punya *toolkit* PIMS yang rapi—kebijakan, *record, DPIA, training*. ([Otoritas Perbankan Eropa](https://otoritasperbankan.europa.eu))
- *EBA Guidelines* (ICT & security): cek vendor dan *outsourcing* TIK kritikal. (edpb.europa.eu)
- Panduan DPO Eropa/ICO: jaga independensi, hindari konflik kepentingan, akses ke *board*. ([ISO](https://iso.org))

Output yang harus terlihat dalam 3 bulan

- **Risk Register** 20 risiko teratas, dengan penanggung jawab dan *due date*.
- **Playbook insiden** 1–2 halaman per skenario.
- **Daftar vendor kritikal** + status *remediation*.
- **Peta aliran data** sederhana + *records of processing*.
- **Laporan ke *board*** yang singkat, visual, dan *actionable*.

Penutup

Bangun kapasitas CISO dan DPO itu soal disiplin harian. Bukan proyek satu kali. Pakai *framework* global, ambil *quick wins*, dan kunci akuntabilitas. Saat kontrol dasar solid, rating akan naik. Kepercayaan publik ikut naik. Dan biaya kebocoran bisa ditekan drastis.

Hibah teknologi & pendampingan oleh BSSN/OJK

Garis besar: bank berperingkat rendah butuh dorongan cepat. Alatnya dua: *hibah teknologi* dan *pendampingan intensif*. Tujuan akhir: naik kelas rating, turunkan risiko kebocoran, dan jaga kepercayaan publik. Bahasa sederhana. Langkah konkret. Bisa dieksekusi.

Kenapa model hibah + pendampingan?

- Investasi keamanan itu mahal. Bank kecil sering tertinggal.
- Regulator di banyak negara mendorong *shared capability* dan *cost-effective controls*. Intinya: alat standar, proses rapi, hasil terukur.
- Dengan *hibah* dan *coaching*, perbaikan bisa cepat. Risiko sistemik turun. *Confidence* pasar naik.

Prinsip desain program (ringkas)

- **Terarah:** fokus 10 kontrol kritikal.
- **Netral vendor:** pilih alat berstandar terbuka, hasil *portable*.
- **Berbasis hasil:** pencairan hibah bertahap sesuai *milestone*.
- **Cepat & ringan:** *paperwork* minimal, *delivery* maksimal.
- **Transparan:** metrik jelas, laporan singkat, mudah diaudit.

Paket Hibah Teknologi (contoh isi)

Tujuan: tutup celah yang paling sering dipakai attacker. Biaya rendah, dampak tinggi.

- **Keamanan identitas & akses**
 - *MFA* untuk admin & *remote access*.
 - *Privileged Access Management (PAM)* sederhana.
- **Deteksi & respons**
 - *Endpoint Detection & Response (EDR)* terkelola.
 - *Log centralization + alerting* dasar.
- **Email & web**
 - *DMARC/SPF/DKIM* aktif (*policy: reject/quarantine*).
 - *Secure Web Gateway* ringan.
- **Backup & pemulihan**
 - *Immutable backup* + uji *restore* terjadwal.
- **Perlindungan data pribadi**
 - *Data discovery & tagging* dasar.
 - *DLP* aturan minimal (NIK, norek, OTP).
- **Uji keamanan**
 - *External attack surface monitoring*.
 - *Vulnerability scan* bulanan.

Format: lisensi 12 bulan + layanan terkelola 6–9 bulan. Target: bank mampu *operasional mandiri* setelah itu.

Skema pendampingan oleh BSSN/OJK

Model *coach–embed–handover*. Tim gabungan turun tangan, lalu serah terima.

1. **Assessment kilat (2 minggu)**
 - *Gap analysis* terhadap kontrol kritikal.
 - Peta aliran data nasabah.
 - *Risk register* awal (20 risiko teratas).
2. **Playbook & quick wins (1 bulan)**
 - *Incident response playbook* 1–2 halaman per skenario: *phishing*, *ransomware*, *data leak*.
 - *Tabletop exercise* lintas fungsi (TI, DPO, legal, PR, *call center*).
 - Aktifkan *controls* paling penting dulu (MFA, DMARC, patch 14 hari).
3. **Implementasi berjenjang (2–3 bulan)**
 - Pasang EDR, *log*, *backup immutable*.
 - Jalankan *DPIA* cepat untuk proses berisiko tinggi (*onboarding*, *credit scoring*, *fraud analytics*).
 - *Third-party check*: akses vendor, *logging*, lokasi data, *incident clause*.
4. **Handover & upskilling (1 bulan)**
 - *Runbook* operasional harian.
 - *Security champions* per unit bisnis.
 - *Retained advisory* ringan selama 3 bulan.

Siapa berhak dapat?

- Bank BUKU 2/3, bank daerah, BPR/BPRS yang ratingnya rendah.
- Prioritas: ada riwayat insiden, *attack surface* besar, atau ketergantungan vendor tinggi.
- Komitmen manajemen: menunjuk *owner* proyek, hadir di *tabletop*, dan *reporting* ke direksi.

Cara kerja pendanaan (sederhana)

- **Model *tiered grant***
 - *Tier A* (paling rendah): hibah 80% + *coaching* intensif.
 - *Tier B*: hibah 60% + *coaching* moderat.
 - *Tier C*: hibah 40% + fokus audit & *red team*.
- **Pencairan bertahap**
 - 40% saat *baseline controls* aktif.
 - 40% setelah *tabletop* + uji *restore* lulus.
 - 20% setelah audit verifikasi & pelaporan insiden *mock*.
- **Kontribusi bank**
 - *In-kind*: tim *project*, waktu *champions*, *training hours* wajib.
 - Biaya operasional setelah 12 bulan.

Target 6 bulan (terukur)

- *MFA coverage* admin dan *remote* $\geq 100\%$.
- *Patch internet-facing* ≤ 14 hari.
- *Phishing click rate* turun $\geq 50\%$.
- *Mean Time to Detect* (MTTD) < 24 jam untuk *high severity*.
- 100% *DMARC* pada *policy* aktif.
- 3 *DPIA* selesai untuk proses paling kritis.
- *Tabletop 2x*, *after-action review* ≤ 48 jam.

Tata kelola & akuntabilitas

- **Komite Program** (BSSN, OJK, perwakilan industri): set *priorities* & *vendor pool*.
- **Panel Teknis**: jaga standar, QA, dan *blueprint* teknis.
- **Audit acak**: cek konfigurasi, *log*, *evidence* pelaksanaan *playbook*.
- **Publikasi ringkas**: *scorecard* agregat (tanpa sebut nama bank), agar pasar melihat progres nasional.

Mengadopsi praktik internasional (tanpa ribet)

- **Shared services**: *threat intel*, *phishing simulation*, dan *attack surface monitoring* secara terpusat; bank tinggal *consume*.
- **Harmonized reporting**: format pelaporan insiden yang sama untuk semua bank, sehingga respons lintas lembaga cepat.
- **Outcome-based funding**: dana cair jika *outcome* tercapai (bukan sekadar beli alat).
- **Vendor-neutrality**: beberapa pilihan produk; *interoperable*, bisa pindah tanpa *lock-in*.
- **Operational resilience drills**: uji *failover*, *restore*, dan komunikasi krisis secara berkala.

Contoh “paket siap kirim” (Siap dipakai minggu ini)

- **Starter Pack 90 Hari**
 - MFA admin, DMARC *reject*, EDR 200 endpoint, *log* inti ke *collector*, *backup immutable* 1 sistem kritikal, *tabletop* 1x.
- **Privacy Pack**
 - *Data mapping* cepat, 2 *DPIA* prioritas, *DLP* aturan NIK/norek, *template* notifikasi insiden PDP, simulasi permintaan *data subject*.
- **Vendor Risk Pack**
 - *Checklist* kontrak TIK, *access review* vendor, *jump host* untuk akses pihak ketiga, *right-to-audit* aktif.

Risiko program & cara menghindarinya

- **Risiko:** *checkbox compliance*.
Mitigasi: *red team* ringan + *evidence-based audit*.
- **Risiko:** ketergantungan pada 1 vendor.
Mitigasi: *multi-vendor pool*, standar terbuka, klausul *exit*.
- **Risiko:** alat ada, tim belum siap.
Mitigasi: *embed coach*, *runbook*, *champions*, dan *handover* bertahap.

Dampak yang diharapkan

- Bank berperingkat rendah bisa naik >1 level dalam 12 bulan.
- *Incident rate* turun, *response time* membaik.
- Kepatuhan PDP makin kuat.
- Kepercayaan nasabah naik. Biaya risiko turun.
- Ekosistem perbankan makin tangguh. *Digital trust* tumbuh.

Intinya: hibah teknologi tanpa pendampingan itu setengah obat. Pendampingan tanpa target metrik itu setengah jalan. Gabungkan keduanya. Jalankan cepat. Ukur ketat. Hasilnya: bank lebih aman, nasabah lebih tenang, pasar lebih percaya.

Program “Cyber Resilience Bootcamp”

Tujuan singkat: menaikkan *cyber & privacy rating* bank berperingkat rendah secara cepat, terukur, dan hemat biaya. Fokus pada *people–process–technology*. Durasi 90 hari. Output jelas. Skor naik >1 level.

Kenapa *bootcamp*?

- Serangan siber makin canggih. Kecepatan perbaikan jadi kunci.
- Regulator global menekan ketahanan operasional digital: EU *DORA*, NIST *CSF 2.0*, FFIEC *CAT*, MAS *TRM*, dan TIBER-EU. Bank kecil–menengah perlu “*fast track*” agar tidak tertinggal. (eur-lex.europa.eu)

Desain *bootcamp* 90 hari (ramping, praktis, *hands-on*)

Hari 0–7: *Baseline & quick wins*

- *Rapid gap assessment* terhadap UU PDP, ISO 27001, NIST *CSF 2.0*.
- *Attack surface scan*: domain, *email security*, paparan *credential*.
- *Quick wins* 14 hari: aktifkan MFA, *privileged access*, *backup immutability*, *logging* kritikal.

Hari 8–30: *Fix the fundamentals*

- Kebijakan *data minimization* dan *record of processing*.
- *Patch management* mingguan, *hardening* server inti.
- Simulasi *phishing* + pelatihan *just-in-time* untuk unit operasional.

Hari 31–60: *Resilience engineering*

- *Tabletop exercise* insiden *ransomware* & kebocoran data.
- Uji *disaster recovery* 4 jam: RTO/RPO realistis.
- *Vendor risk sprint*: 10 pemasok teratas, *security addendum* standar.

Hari 61–90: *Prove & certify*

- *Purple-team exercise* ala TIBER-EU (*threat-intel led*).
- Perbaiki temuan *red team* paling berisiko dalam 2 minggu.
- Siapkan *evidence pack* untuk *rating re-assessment* OJK. ([European Central Bank](https://www.ecb.europa.eu/press/eng/2022/02/22022201_en.html))

Kurikulum inti (modul singkat, bahasa sederhana)

1. **Identitas & Akses:** MFA, *least privilege*, *break-glass account*.
2. **Proteksi Data PDP:** *lawful basis*, *consent*, *record retention*, *encryption at rest/in transit*.
3. **Ketahanan Operasional:** *backup 3-2-1*, *restore drill*, *network segmentation*.
4. **Deteksi & Respon:** *SIEM/SOC lite*, *playbook insiden 4 jam pertama*.
5. **Risiko Vendor:** *security questionnaire*, *right to audit*, *breach clause*.
6. **Budaya Aman:** *phishing drill* bulanan, *secure coding* dasar untuk tim *channel digital*.
7. **Uji Serangan Nyata:** *purple-team* berbasis skenario TIBER-EU, prioritas pada *payments* dan *mobile banking*. ([European Central Bank](#))

Paket *hibah teknologi* (fokus nilai tinggi, biaya rendah)

- *Email security & DMARC managed*.
- EDR ringan untuk *endpoint* kritikal.
- *Password manager* enterprise untuk unit sensitif.
- *Cloud backup* dengan *immutability + least privilege*.
- *Vulnerability scanner* terotomasi mingguan.
- *MFA token* bagi *privileged users*.
→ Selaras dengan praktik TRM MAS, FFIEC CAT, dan NIST CSF 2.0 yang menekankan kontrol akses, deteksi, dan pemulihan. ([ffiec.gov](#))

Peran BSSN/OJK di *bootcamp* (pendampingan aktif)

- **Standar target:** peta ke EU *DORA* (ketahanan operasional digital) agar bank siap menghadapi tuntutan lintas-negara. ([eur-lex.europa.eu](#))
- **Pelatih & asesor:** daftar pelatih tersertifikasi, *playbook insiden nasional*, dan contoh *policy kit*.
- **Threat-intel terkini:** *IOCs* dan taktik terbaru ke sektor bank.
- **Simulasi TIBER-style:** fasilitas *red team/purple team* terkoordinasi regulator. ([European Central Bank](#))
- **Fast-track audit:** kanal *evidence* digital untuk naik rating.

Target hasil (90 hari)

- **Skor naik >1 level** pada *CyberTrust & Data Privacy Rating*.
- **MFA 100%** untuk admin dan *remote access*.
- **RTO ≤ 4 jam** untuk 3 layanan kritikal.
- **Vendor top-10** memiliki *security addendum*.
- **Measurable culture:** tingkat *phish-click* turun ≥50% dari *baseline*.

KPI & metrik sederhana

- *Time-to-patch* kritikal: ≤ 7 hari.
- *Backup restore test* sukses bulanan.
- *Mean-time-to-detect/respond (MTTD/MTTR)* insiden prioritas-1.
- *Data processing inventory* 100% untuk unit ritel & SME.
- *TIBER-findings closure* $>80\%$ sebelum *re-rating*. ([European Central Bank](#))

Tata kelola program

- **Sponsor:** Direktur Manajemen Risiko.
- **Pemilik:** CISO (teknis) & DPO (PDP).
- **Ritme:** *stand-up* harian 15 menit; *war-room* mingguan.
- **Transparansi:** *dashboard traffic-light* ke direksi dan OJK.

Estimasi *budget* (arah, bisa disesuaikan)

- Lisensi *security stack* dasar + pelatihan: kecil–menengah.
- *Professional services* TIBER-style: paket bersama regulator/ asosiasi → biaya ditekan lewat *shared services*. ([European Central Bank](#))

Mengapa ini relevan global?

- **NIST CSF 2.0** menekankan “*Govern*” sebagai fungsi baru—artinya tata kelola keamanan harus terlihat sampai dewan.
- **FFIEC CAT** dipakai bank AS untuk *self-assessment* dan prioritas *controls*.
- **MAS TRM** menuntut kontrol ketat untuk akses istimewa dan uji ketahanan berkala.
- **EU DORA** mewajibkan uji ketahanan dan manajemen risiko TIK terpadu di sektor keuangan Eropa per 2025.

Bootcamp ini merangkum praktik-praktik itu dalam versi ringkas yang bisa langsung diterapkan bank Indonesia. ([eur-lex.europa.eu](#))

Call to action

Mulai dari yang paling berdampak: MFA, *backup immutability*, *tabletop* 4 jam, dan *vendor top-10*. Lakukan 90 hari, buktikan hasil, naikan rating. **Kepercayaan publik adalah modal.** *Bootcamp* ini membuatnya terukur, cepat, dan nyata.

Bab 21: Mitigasi & Pemberdayaan Ekosistem Keamanan Digital

Skema insentif OJK untuk bank dengan rating tinggi

Bank yang aman itu seperti bendungan kokoh. Menahan arus serangan. Menjaga aliran ekonomi tetap lancar. Karena itu, **rating tinggi** di *OJK CyberTrust & Data Privacy Ranking* harus **bernilai nyata**. Bukan sekadar label. Insentif yang tepat akan mendorong semua bank “naik kelas”, cepat, dan terukur.

Di bawah ini rancangan skema insentif yang sederhana, jelas, dan langsung terasa bagi bisnis—namun tetap **prudensial**.

Prinsip dasar insentif

- **Hadiah untuk konsistensi, bukan kebetulan.** Insentif keluar bila kinerja aman *persisten* (≥ 12 bulan), bukan hanya lolos audit musiman.
- **Pro-sistemik.** Insentif memperkuat ketahanan sektor, sejalan dengan standar global soal *operational resilience* dan pengelolaan risiko TIK/pihak ketiga. ([Financial Stability Board](#))
- **Tidak mengurangi kehati-hatian.** Semua manfaat berada dalam koridor Basel (khususnya *Pillar 2/supervisory review*) dan regulasi ketahanan operasional. ([eur-lex.europa.eu](#))

Siapa yang berhak?

Ambang pemicu (*triggers*) yang mudah dicek:

- Rating **AAA/AA** selama ≥ 12 bulan.
- **0** insiden *material* ($\text{loss} \geq \text{ambang OJK}$) atau pelanggaran **UU PDP** dalam 12 bulan.
- *Mean Time to Detect (MTTD)* ≤ 24 jam dan *Mean Time to Recover (MTTR)* ≤ 4 jam untuk insiden kritis.
- Skor risiko pihak ketiga di bawah **ambang 20/100** pada portofolio vendor inti (*cloud, core banking, pembayaran*). Rujukan praktik global: *operational resilience* dan pengawasan pihak ketiga. ([Financial Stability Board](#))

Menu insentif yang terasa di bisnis

1. *Supervisory fast lane*

- **Prioritas** pada persetujuan produk digital, *open API*, dan *pilot* inovasi.
- **Pengurangan frekuensi** *on site inspection* (diganti *continuous monitoring* berbasis data).
- Sejalan dengan arah global menuju *digital operational resilience* dan *tech risk management*. ([Flofr](#))

2. Pengaturan berbasis kinerja (*performance-based supervision*)

- Jika kontrol kuat, **beban pelaporan** bisa disederhanakan (format *regtech* standar, integrasi API ke *SupTech* OJK).
- Fokus pada indikator ketahanan: pengujian krisis TIK, *incident response*, dan pembinaan vendor esensial—praktik yang ditekankan di DORA/NIST. (torontocentre.org)

3. Pillar 2 relief yang terukur (non-otomatis)

- **Penyesuaian add-on risiko operasional** dapat dipertimbangkan untuk bank berketahanan sangat tinggi, **setelah** *stress test* dan *supervisory review*.
- Bukan hak, tapi **opsional dan proporsional**, mengacu praktik *Pillar 2* internasional. (eur-lex.europa.eu)

4. Akses prioritas ke fasilitas nasional

- **Kursi prioritas** di *threat-intel sharing hub* nasional (OJK–BSSN–BI).
- **Kouta gratis/bersubsidi** untuk *red teaming*, *table-top exercise*, dan *sector-wide crisis simulation* (selaras agenda *operational resilience* internasional). ([Financial Stability Board](https://financialstabilityboard.org))

5. Public trust booster

- **Lencana “CyberTrust Gold”** di situs bank dan *OJK Report Card*.
- **Pengungkapan ringkas** (1 halaman) tentang praktik terbaik bank: *patching cadence*, latihan *IR*, jangkauan enkripsi.
- Transparansi yang tepat meningkatkan akuntabilitas dan kepercayaan pasar—garis besar ada di FFIEC/NIST. ([Banking Supervision](https://www.fdic.gov/banking-supervision/))

6. Insentif biaya kepatuhan

- **Diskon biaya** untuk evaluasi berkala jika bank menyalurkan data *telemetry* real-time ke *dashboard* OJK (mengurangi biaya pengawasan manual).
- **Kredit pelatihan** untuk DPO/CISO pada kurikulum resmi (berbasis TRM/BCM). ([Monocle Solutions](https://monocle-solutions.com))

Cara menilai dan menjaga kualitas (anti *window dressing*)

- **Verifikasi independen.** Bukti teknis: *audit trail*, *forensic-ready logging*, hasil *penetration test*.
- **Pengujian acak (*spot check*)** dan *sector-wide exercises*.
- **Aturan *clawback*.** Jika setelah insentif muncul pelanggaran material, manfaat ditarik dan *capital add-ons* dapat **naik** kembali.
- **Keselarasan standar.** Kontrol dipetakan ke **NIST CSF 2.0**, **DORA** (tata kelola TIK, manajemen insiden, pengawasan *critical third parties*), dan **TRM/BCM**. ([Elofr](https://eflor.fr))

Contoh paket insentif “ringkas tapi tajam”

- **Gold (AAA):** *fast lane* + simplifikasi pelaporan + akses prioritas simulasi krisis + potensi *Pillar 2 relief* terbatas.
- **Silver (AA):** *fast lane* + pelatihan bersertifikat + subsidi *red team*.
- **Bronze (A):** pelatihan inti + *threat-intel feed* dasar + rute percepatan untuk *bug bounty* terkoordinasi.

Metrik sederhana untuk *scorecard* insentif

- *Patch lead time* kritikal: median ≤ 7 hari.
- *Phishing resilience rate* karyawan: $\geq 98\%$ tidak klik.
- *Back-up recovery* teruji: RPO ≤ 15 menit, RTO ≤ 2 jam untuk layanan inti.
- *Third-party concentration risk*: eksposur ke penyedia “kritis” $\leq X\%$ dari beban transaksi—isu yang disorot regulator global. ([Financial Stability Board](#))

Kenapa ini relevan secara internasional?

- **UE (DORA)** mendorong ketahanan operasional digital menyeluruh, termasuk insiden TIK, uji ketahanan, dan pengawasan pihak ketiga penting. Insentif lokal harus mendorong kesiapan ke arah ini. ([torontocentre.org](#))
- **NIST CSF 2.0** menekankan *governance* dan *supply-chain risk*, cocok sebagai tulang punggung kontrol teknis yang dinilai OJK. ([Flofr](#))
- **MAS (Singapura)** menekankan TRM/BCM dan ketangguhan layanan kritikal; pelatihan dan simulasi rutin menjadi *best practice* regional. ([Monocle Solutions](#))
- **FSB/BCBS** menyoroti risiko konsentrasi pihak ketiga pada sektor keuangan—maka insentif harus mendorong *vendor diversification* dan uji ketergantungan. ([Financial Stability Board](#))

Ringkasan

Insentif adalah “gas”, pengawasan adalah “rem”. Keduanya perlu. Dengan *fast lane*, *performance-based supervision*, akses fasilitas nasional, dan opsi *Pillar 2 relief* yang terukur, bank ber-rating tinggi akan **semakin kuat**, kompetitif, dan dipercaya publik. Efek gandanya: standar industri naik, risiko sistemik turun, stabilitas keuangan makin kokoh.

Kolaborasi industri untuk shared cyber intelligence

Intinya: serangan datang cepat. Sendirian, bank kalah cepat. Bersama, bank bisa menang. *Shared cyber intelligence* = saling berbagi peringatan, *indikator ancaman (IOCs)*, taktik penyerang, dan langkah mitigasi. Tujuan akhirnya sederhana: kurangi kerugian, jaga kepercayaan, dan stabilkan sistem keuangan.

Mengapa harus kolaborasi sekarang?

- Penjahat siber berbagi alat dan data di *underground*. Kita harus lebih kompak dari mereka.
- Praktik global membuktikan: berbagi intel membuat deteksi lebih dini dan *respon* lebih cepat. Contoh paling dikenal: **FS-ISAC** untuk sektor keuangan dunia. Organisasi ini memfasilitasi peringatan dini lintas bank dan *payment firms*.
- Di Eropa, regulasi **DORA** mendorong *financial entities* membentuk pengaturan berbagi informasi dan intelijen, demi kesiapsiagaan siber bersama.
- Inggris mengoperasikan platform **CiSP** (NCSC) untuk berbagi info ancaman secara aman antara pemerintah dan industri, termasuk sektor keuangan. ([FIRST](#))

Prinsip desain *shared intelligence* yang sederhana

1. **Aman secara hukum dan privasi**
 - Gunakan *Traffic Light Protocol (TLP)* untuk menandai tingkat kerahasiaan info (TLP: CLEAR/AMBER/RED). Ini standar global. ([FIRST](#))
 - Selaras dengan UU PDP: hanya berbagi *threat indicators*, bukan data pribadi nasabah.
2. **Standar teknis yang sama**
 - Kirim/terima intel dengan format **STIX** dan kanal **TAXII**. Ini memudahkan mesin ke mesin, otomatis, dan cepat. ([FIRST](#))
 - Pakai **MISP** sebagai platform *open-source* untuk kurasi, korelasi, dan *enrichment* IOCs. Banyak komunitas bank di dunia memakainya. ([NCSC](#))
3. **Nilai langsung untuk bank**
 - Dapat *early warning* kampanye *phishing*, *credential stuffing*, *ransomware*.
 - Dapat *playbook* respon yang sudah terbukti.
 - *Dwell time* turun, *false positive* berkurang, biaya insiden menyusut.

Model operasional versi Indonesia (ringkas dan bisa jalan cepat)

Nama: *Indonesia Financial ISAC (IF-ISAC)* — difasilitasi OJK & BSSN.

- **Anggota:** bank umum, BPD, BPR/BPRS besar, *switching*, *payment gateway*, fintech berizin.
- **Hub & Spoke:** satu *hub* (SOC Nasional) untuk kurasi pusat; *spoke* di tiap bank (SOC bank).
- **Kanal berbagi:**
 - *Real-time feed* STIX/TAXII (otomatis ke SIEM/SOAR bank).

- *Daily brief* intel prioritas (email + portal).
- *Threat hunting sprint* mingguan (room kolaborasi tertutup).
- **Konten minimal harian:**
 - IOCs (IP/domain/hash), TTPs *MITRE ATT&CK*, *phishing kits*, *brand abuse*, *dark web chatter*.
 - *Use case* korelasi siap pakai untuk SIEM.
- **Red teaming terarah:** sinkron dengan uji **TIBER-style** agar intel dipakai untuk latihan nyata, bukan arsip. (TIBER-EU adalah kerangka uji ketahanan berbasis intel di Eropa). (misp-project.org)

Peran OJK: pengarah, penjamin, pemberi insentif

- **Kebijakan “safe harbor” berbagi intel:** selama mengikuti TLP dan tidak memuat data pribadi, anggota terlindungi dari risiko hukum ketika berbagi info teknis ancaman.
- **Selaraskan dengan DORA-style:** dorong *arrangements* berbagi intel antarlembaga sebagai bagian dari kepatuhan operasional digital.
- **Harmonisasi pelaporan insiden:** ikut rekomendasi **FSB** agar format pelaporan antar-otoritas selaras, beban bank berkurang, dan data agregat kualitasnya naik. ([Financial Stability Board](https://www.fsb.go.id/))
- **Kaitkan ke rating OJK CyberTrust:** bank yang aktif berbagi dan memanfaatkan intel mendapat poin plus di *scorecard*.

Paket insentif yang terasa manfaatnya

- **Regulatory credit:** pengurangan frekuensi *thematic inspection* siber untuk bank berkontribusi tinggi di IF-ISAC.
- **Biaya lebih murah:** akses *feed* intel premium nasional disubsidi untuk bank kecil/menengah.
- **Prioritas fast-track sandbox:** untuk proyek deteksi ancaman bersama (contoh: *brand monitoring*, *account takeover*).
- **Pengakuan publik:** *CyberTrust Leaderboard* tahunan untuk partisipasi intel terbaik (mendorong *market trust*).

Playbook 90 hari pertama (mulai dulu, sambil sempurnakan)

0–30 hari

- Tetapkan *charter*, aturan TLP, *code of conduct*.
- Pasang MISP nasional (BSSN) + TAXII gateway; buat *onboarding kit* (API, contoh *mapping* ke SIEM). ([NCSC](https://ncsc.nl/))

31–60 hari

- Mulai *pilot feed* harian: *phishing domain*, *botnet C2*, *brand impersonation*.
- Jalankan *weekly intel stand-up* 30 menit: *what's new* → *what to hunt* → *what to patch*.

61–90 hari

- *Threat hunting* lintas bank (1 use case/minggu), ukur temuan & *mean time to detect (MTTD)*.
- Simulasikan *coordinated disclosure & rapid alert* ala CiSP/FS-ISAC untuk satu kampanye *phishing* besar. ([FIRST](#))

Metrik sederhana untuk mengukur dampak

- **Kecepatan:** waktu dari *intel published* ke *rule deployed* di SIEM bank (target <24 jam).
- **Efektivitas:** jumlah *blocked indicators* & temuan *threat hunting* lintas bank per minggu.
- **Kualitas:** *precision* intel (rasio *false positive*).
- **Kontribusi:** skor partisipasi (jumlah kiriman intel, validasi silang, *after-action review*).

Rambu keamanan & tata kelola

- **Privasi & PDP:** hanya *threat metadata*; kalau ada data pribadi, wajib dianonimkan.
- **Kepatuhan:** rujuk panduan **CPMI-IOSCO** untuk ketahanan siber FMI—menekankan koordinasi dan berbagi info; jadikan referensi tata kelola IF-ISAC. ([Bank of Canada](#))
- **Audit jejak berbagi:** semua kiriman intel otomatis *logged* untuk *traceability*.
- **Minimum-viable-sharing:** lebih baik berbagi cepat dengan data cukup, daripada sempurna tapi terlambat.

Penutup

Kolaborasi intel bukan proyek IT. Ini *risk management* bersama. Dunia sudah melakukannya—FS-ISAC, CiSP, DORA mendorong itu. Indonesia bisa punya versi yang relevan, hemat, dan cepat jalan. Mulai kecil, rutin berbagi, ukur dampaknya. Kepercayaan publik dan stabilitas sistem keuangan adalah hadiahnya.

Bagian VIII — Pemantauan dan Evaluasi Berkelanjutan

Bab 22: Dashboard OJK CyberTrust Monitoring

Visualisasi real-time status rating seluruh bank

Bayangkan satu layar. Sederhana. Penuh arti. OJK bisa melihat kesehatan *cyber* perbankan Indonesia dalam hitungan detik.

Warna hijau—aman
Kuning—waspada
Merah—aksi cepat.

Itu inti *Dashboard OJK CyberTrust*.

Kenapa *real-time* penting? Karena serangan tidak menunggu rapat mingguan. Regulator global juga bergerak ke arah pengawasan digital (*SupTech*), penggunaan *analytics*, dan pelaporan insiden yang makin terstandar. (adb.org)

Apa yang tampil di layar (versi yang mudah dibaca)

- **Peta rating nasional (AAA–D).**
Satu *heatmap* status seluruh bank. Bisa difilter per kategori (BUKU), aset, dan kompleksitas operasi. Klik satu bank → *drill-down*.
- **Tren risiko 30–90 hari.**
Grafik naik-turun skor *CyberTrust* dan *PDP compliance*. *Sinyal awal* bila tren turun beruntun 3 minggu.
- **Indikator kunci (KPI) singkat.**
 - Rata-rata *patching window* kritikal (hari).
 - Jumlah insiden material 30 hari terakhir.
 - *Mean Time to Detect/Respond (MTTD/MTTR)*.
 - Kepatuhan *mandatory controls* (contoh: *logging, backup, multi-factor authentication*). Banyak otoritas—seperti MAS dan UE lewat DORA—mendorong kontrol teknologi dan pelaporan insiden yang konsisten. ([Kementerian Kewangan](http://KementerianKewangan))
- **Peta paparan pihak ketiga.**
Vendor bersama yang dipakai banyak bank. Jika satu vendor *down*, terlihat potensi efek berantai.
- **Watchlist & early warning.**
Daftar bank dengan degradasi skor paling besar minggu ini. Notifikasi otomatis ke tim pengawas.

Dari mana datanya?

- **Laporan insiden terstandarisasi.**
Mengadopsi *format* pertukaran yang direkomendasikan global agar data konsisten

dan bisa ditukar cepat (contoh inisiatif FSB **FIRE** untuk *incident reporting* lintas yurisdiksi). (esma.europa.eu)

- **Telemetry keamanan dan kepatuhan.**

Ringkas, teragregasi, dan *privacy-preserving*:

- Status *endpoint*, *patch*, *vulnerability*.
- Hasil uji *phishing* internal.
- Status *backup* dan *restore test*.
- *Data Loss Prevention* (jumlah *policy hits*, tanpa konten).

- **Sumber intelijen ancaman.**

Umpan *threat intelligence* industri melalui standar *STIX/TAXII* untuk *indicator* serangan terbaru. (Note: disajikan sebagai skor risiko, bukan data mentah yang sensitif).

- **Integrasi regulasi internasional.**

Mapping kontrol ke **NIST CSF** untuk *benchmark* kematangan dan *governance*; cocok untuk banding lintas negara. (esma.europa.eu)

Desain pengalaman yang “ramah regulator”

- **Aturan 5 detik.**

Dalam 5 detik, pengawas tahu: siapa hijau, siapa kuning, siapa merah.

- **Aturan 2 klik.**

Klik 1: bank mana yang turun. Klik 2: *root cause* paling mungkin.

- **SLA visual.**

Gauge sederhana—misal, *MTTR* target 24 jam. Jarum melewati batas → *alert*.

- **Bahasa non-teknis.**

Hindari jargon. Pakai istilah bisnis: “paparan denda”, “potensi *downtime* layanan”, “jumlah nasabah terdampak”.

Arsitektur data (ringkas, aman, dan audit-ready)

1. **Konektor API bank → Data Lake OJK.**

Data sudah disaring dan di-*hash*. Tidak memuat data pribadi.

2. **Lapisan rules engine.**

Menghitung skor *CyberTrust* dan *PDP*.

3. **Lapisan analytics dan anomali.**

Mencari pola “tak wajar” (misal, lonjakan *blocked attacks* + kenaikan *phishing success rate*).

4. **Lapisan visual.**

Dashboard interaktif untuk pengawas dan *executive view* untuk pimpinan.

5. **Jejak audit otomatis.**

Semua perubahan skor dan *override* tercatat.

Pengawasan modern seperti ini sejalan dengan tren *SupTech* global—regulator memanfaatkan data dan *analytics* untuk respons cepat dan kebijakan berbasis bukti. (adb.org)

Minimum Viable Dashboard (bisa jalan dalam 100 hari)

- **M1–M2 (Fondasi).**
 - 20 *KPI* inti.
 - *Heatmap* rating nasional.
 - *Watchlist* mingguan otomatis.
- **M3 (Pengayaan).**
 - *Early warning model* sederhana.
 - Panel vendor bersama.
 - *What-if view*: dampak jika satu kontrol kritikal gagal.

Contoh alur kerja pengawas

1. *Alert* merah pada Bank X → skor turun dari A ke BBB.
2. Klik *drill-down* → *MTTD* melewati batas + vendor SOC alami gangguan.
3. Sistem memunculkan **daftar tindakan**: aktifkan *contingency*, percepat *patch* CVE kritikal, lakukan *table-top exercise*.
4. *Timer SLA* berjalan. Jika tak ada perbaikan, notifikasi naik ke pimpinan pengawasan.

Tata kelola & etika data

- **Privacy by design.**
Hanya data agregat. Tidak ada data nasabah yang tampil.
- **Hak akses berjenjang.**
Pengawas hanya melihat yang relevan.
- **Transparansi metodologi.**
Rumus skor dipublikasikan. Bisa diaudit.
- **Keselarasan standar internasional.**
Mapping ke DORA/NIST agar kompatibel dengan praktik global dan memudahkan *cross-border benchmarking*. (eiopa.europa.eu)

Tantangan yang harus diatasi

- **Kualitas data tidak merata.**
Solusi: *schema* pelaporan yang konsisten + *validation rules*.
- **Beban pelaporan bank kecil.**
Solusi: *agent* ringan + *upload* berkala; fokus pada 20 *KPI* inti.
- **Risiko kebocoran informasi sensitif.**
Solusi: agregasi, *tokenization*, kontrol akses ketat.
- **Change management.**
Pelatihan bagi pengawas dan bank agar membaca *dashboard* dengan cara yang sama.

Kenapa ini menantang sekaligus penting?

- Mempercepat deteksi risiko sistemik.
- Menurunkan biaya pengawasan manual.
- Mendorong *race to the top*—bank berlomba naik kelas rating.
- Selaras dengan arah dunia: pengawasan berbasis data, pelaporan insiden yang harmonis, dan *operational resilience* digital. (adb.org)

Call to action

Mulai dari yang sederhana. Tampilkan yang paling penting. Bangun *dashboard* yang jujur, cepat, dan bisa ditindaklanjuti. Dengan *real-time CyberTrust Monitoring*, OJK dan industri bisa melihat badai sebelum tiba—dan meneduhkannya sebelum berdampak ke publik.

Bab 23: Audit Ulang Tahunan dan Sertifikasi Kepatuhan

Mekanisme penurunan atau kenaikan rating

Audit ulang tahunan itu seperti *check-up* kesehatan bank. Tujuan utamanya sederhana: memastikan kontrol keamanan dan kepatuhan PDP benar-benar bekerja, bukan sekadar di atas kertas. Hasil audit langsung memengaruhi rating. Naik jika disiplin, turun jika lengah. Format ini mengikuti praktik global: *operational resilience* Basel, *NIST CSF 2.0*, dan aturan Eropa *DORA*. [Bank for International Settlements+2Financial Stability Board+2](#)

Prinsip inti penilaian ulang

- **Bukti, bukan janji.** Semua klaim harus didukung *log* dan bukti kontrol berjalan 24/7 (*continuous monitoring*). Standar ini sejalan dengan *NIST CSF 2.0* yang menekankan pengukuran dan perbaikan berulang. [Financial Stability Board](#)
- **Ketahanan operasional sebagai sasaran.** Fokus pada kemampuan bank bertahan saat gangguan: serangan siber, kegagalan TI, bencana. Ini mengikuti prinsip *operational resilience* Basel Committee. [Bank for International Settlements](#)
- **Pelaporan insiden yang cepat.** *DORA* di UE mewajibkan tata kelola risiko TIK, uji ketahanan, dan pelaporan insiden ke regulator. Semangatnya sama: respons cepat, transparan, dan terdokumentasi. [eiopa.europa.eu](#)

Kapan rating bisa naik

Rating naik ketika bank menunjukkan kontrol bekerja secara konsisten selama periode audit—bukan hanya saat *pre-audit rush*. Indikator yang mudah dipahami:

1. **Zero critical findings berulang**
 - Tidak ada temuan *critical* pada dua kuartal berturut-turut.
 - Semua temuan *major* ditutup ≤ 60 hari dengan bukti perbaikan.
 - Sejalan dengan dorongan *NIST CSF 2.0* untuk *improvement cycle*. [Financial Stability Board](#)
2. **MTTD/MTTR membaik signifikan**
 - *Mean Time to Detect* turun $\geq 30\%$, *Mean Time to Respond* turun $\geq 30\%$ dalam 12 bulan.
 - Dibuktikan lewat SIEM/SOAR dan *incident postmortem*.
 - Selaras dengan *operational resilience*—tujuan akhirnya memperkecil dampak. [Bank for International Settlements](#)
3. **Uji ketahanan lulus dengan *impact tolerance* terjaga**
 - Hasil *crisis playbook drill* dan *table-top exercise* menunjukkan layanan kritikal tetap di bawah *impact tolerance*.
 - Praktik ini sejalan dengan tren pengawasan ketahanan layanan inti di Inggris/EU. [NIST Publications](#)
4. **Kepatuhan PDP konsisten**

- DPIA dilakukan untuk semua produk baru, *privacy by design* terdokumentasi, dan *data subject request* dipenuhi tepat waktu.
- *DORA/ICT risk oversight* mendorong tata kelola vendor dan data lintas pihak. eiopa.europa.eu

Contoh keputusan:

- Dari **BBB** → **A** jika 3 dari 4 indikator di atas tercapai dan tidak ada pelanggaran PDP *material* 12 bulan terakhir.
- Dari **A** → **AA** jika bank juga menunjukkan integrasi penuh ke program *red-teaming* dan *threat intelligence* lintas industri.

Kapan rating bisa turun

Turun itu bukan hukuman; ini sinyal risiko sistemik yang harus segera dikelola. *Triggers* yang jelas:

- **Insiden material tidak dilaporkan tepat waktu**
Keterlambatan atau pelaporan tidak lengkap ke regulator/CSIRT akan memicu peninjauan khusus. Kerangka global menekankan harmonisasi pelaporan insiden demi respon lintas lembaga yang cepat. [Bank for International Settlements](#)
- **Gagal menjaga layanan kritikal**
Outage melebihi *impact tolerance* pada layanan pembayaran/kredit tanpa rencana pemulihan yang efektif. Ini inti dari prinsip *operational resilience*. [Bank for International Settlements](#)
- **Temuan *critical* berulang**
Kontrol akses lemah, *patching* tertunda, enkripsi tidak konsisten. Dua siklus audit masih *open* → langsung evaluasi penurunan.
- **Kepatuhan PDP cacat**
Tidak ada DPO aktif, tidak ada DPIA pada produk baru, atau *third-party processor* tidak diawasi. *DORA/EBA* menuntut pengawasan TIK pihak ketiga yang ketat. [NIST Publications](#)

Contoh keputusan:

- Dari **A** → **BBB** jika terjadi 1 insiden material + keterlambatan pelaporan + rencana perbaikan tidak meyakinkan.
- Dari **BBB** → **BB** jika ada kebocoran data berulang dan *root cause* yang sama muncul kembali dalam 6 bulan.

Alur keputusan audit & sertifikasi (ringkas dan tegas)

1. **Pra-audit (T-60 hari).** Bank mengirim *evidence pack* standar: kebijakan, logs, metrik MTBD/MTTR, hasil uji, DPIA, dan pengawasan vendor. *Template* mengikuti *NIST CSF 2.0 quick start* agar konsisten. [Financial Stability Board](#)
2. **On-site/remote review (T-0).** Tim OJK/BSSN memverifikasi bukti, mewawancarai CISO/DPO, dan melakukan *sampling* kontrol.
3. **Skoring & keputusan (T+14).** Panel menetapkan naik/turun/tetap, plus *remediation order* bila perlu.

4. **Sertifikasi & public note (T+30).** Sertifikat kepatuhan diterbitkan. Catatan publik singkat membantu pasar memahami posisi risiko, sejalan dengan dorongan transparansi di Eropa lewat *DORA oversight*. eiopa.europa.eu
5. **Follow-up kuartalan.** Bank wajib mengirim metrik ketahanan dan status perbaikan. Jika tren memburuk, dapat dipanggil *extra review* walau di luar siklus tahunan—praktik yang juga diberlakukan pengawas di UE dan UK. [NIST Publications](https://www.nist.gov/publications)

Fast track naik rating: bukti yang “mengunci” keputusan

- Uji *red team* independen lulus terhadap skenario *ransomware* dan *data exfiltration*.
- Simulasi *failover* antar *data center* di bawah *RTO/RPO* target.
- Kontrak vendor TIK sudah selaras dengan klausa *DORA-style* (hak audit, *incident notification*, *exit strategy*). eiopa.europa.eu
- Metodologi *baselined* ke *NIST CSF 2.0*: ada peta kontrol → *gaps* → rencana perbaikan → metrik hasil. [Financial Stability Board](https://www.fsb.gov/)

Safeguards agar penurunan tidak jadi krisis

- Masa *grace period* 30–60 hari untuk temuan non-material, dengan *milestone* per minggu.
- Pengawasan intensif bagi bank yang turun ≥ 2 tingkat; wajib *weekly dashboard* ke OJK.
- Rencana komunikasi publik yang jujur dan ringkas agar kepercayaan nasabah terjaga—praktik yang menjadi bagian dari *resilience playbook* di banyak yurisdiksi. [Bank for International Settlements](https://www.bis.org/)

Apa artinya bagi bank

- **Jelas dan terukur.** Bank tahu persis syarat naik atau risiko turun.
- **Sejalan standar global.** Kerangka audit memadukan *NIST CSF 2.0*, prinsip Basel, dan semangat *DORA*—memudahkan kolaborasi lintas batas dan akses pasar. [Financial Stability Board](https://www.fsb.gov/)+2[Bank for International Settlements](https://www.bis.org/)+2
- **Hadiah utama: kepercayaan.** Rating bukan hanya angka. Ini *signal* ke pasar, investor, dan nasabah bahwa bank Anda siap menghadapi guncangan digital.

Singkatnya: audit ulang tahunan + sertifikasi kepatuhan adalah “rem” dan “gas” sekaligus. Naik jika siap dan disiplin. Turun jika abai. Dengan aturan yang tegas dan selaras internasional, kita menjaga stabilitas dan *digital trust* industri perbankan Indonesia.

Bab 24: Pelaporan Publik dan Transparansi Data

CyberTrust Report Card tahunan (OJK–BSSN–Bank Indonesia)

Pelaporan publik dan transparansi data bukan sekadar formalitas. Dalam dunia keuangan yang makin digital, **kepercayaan (trust)** menjadi komoditas yang tak bisa diabaikan. Regulasi, audit, dan rating saja tidak cukup — publik dan stakeholder harus melihat hasil nyata. Maka muncul gagasan *CyberTrust Report Card* tahunan yang dikeluarkan oleh OJK-BSSN-Bank Indonesia sebagai alat ukur integritas keamanan siber dan pengelolaan data pribadi di sektor perbankan.

Mengapa perlu “Report Card” tahunan

- Meningkatnya frekuensi dan kecanggihan serangan siber menuntut bank dan lembaga keuangan untuk bergerak dari “kami aman” ke “kami dapat dibuktikan aman”. Misalnya, di Indonesia tercatat ada miliaran traffic anomali dalam lima tahun terakhir. ([GovInsider](#))
- Data nasabah kini adalah “mata uang baru” dalam sektor keuangan — ketika bocor, biaya tak hanya teknis, tetapi reputasi dan kepercayaan publik ikut rusak.
- Dengan publikasi terbuka (“*public disclosure*”) dari rating keamanan siber dan kepatuhan data, industri bisa dipacu untuk kompetisi ke arah yang lebih baik, bukan sekadar ‘memenuhi regulasi’.
- Transparansi membantu regulator (OJK), badan siber (BSSN) dan bank sentral (BI) untuk menjalankan pengawasan yang berbasis data (*data-driven supervision*).

Apa yang harus dilaporkan dan dipublikasikan

Dalam *Report Card* ini, minimal ada unsur-unsur berikut:

- Skor/rating keamanan siber dan privasi data setiap bank (misalnya tingkat AAA hingga D).
- Tren tahunan: apakah ada peningkatan atau penurunan dari bank ke bank.
- Insiden keamanan yang telah terjadi (jenis, dampak, mitigasi) — tentu dalam batas kerahasiaan yang wajar.
- Kepatuhan terhadap regulasi seperti UU PDP, POJK terkait TI dan keamanan siber.
- Rencana perbaikan yang sudah/akan dijalankan oleh bank-bank berperingkat rendah.
- Penggunaan indikator kuantitatif + kualitatif: misalnya jumlah vendor dengan akses data, frekuensi latihan skenario insiden, dan integrasi sistem respons.

Manfaat untuk industri perbankan dan publik

Untuk bank:

- Mendapat “tolak ukur eksternal” yang jelas: bukan hanya internal audit tapi juga penilaian terbuka.

- Bank yang punya skor bagus bisa mendapatkan keunggulan kompetitif: kepercayaan nasabah lebih tinggi, bisa jadi insentif regulasi publik.
- Bank dengan skor rendah mendapat sinyal kuat bahwa perbaikan harus cepat — bukan menunda sampai insiden terjadi.

Untuk publik/investor:

- Transparansi membuat nasabah bisa memilih bank yang tidak hanya menawarkan produk bagus, tetapi juga *aman secara digital*.
- Investor bisa melihat profil risiko digital bank — bukan hanya laporan keuangan.
- Regulator memperkuat kredibilitas sistem keuangan nasional: ketika pelaporan publik dijalankan, investor asing dan lokal makin yakin bahwa sistem punya mekanisme kontrol.

Tantangan dan catatan penting

- Data yang dilaporkan harus **andalan dan valid** — jika hanya sebatas angka yang “diberi” oleh bank sendiri tanpa verifikasi independen, maka kredibilitas akan lemah.
- Skor yang dipublikasikan harus punya makna dan konteks: publik perlu memahami apa artinya “Skor B” vs “Skor A”.
- Transparansi tidak boleh membuat bank takut melaporkan kelemahan — sebaliknya, budaya “mengaku dulu, lalu perbaiki” harus dibangun.
- Publikasi tahunan harus diikuti tindakan: jika bank terus nilai buruk tapi tidak ada efek, maka sistem bisa dianggap sekadar “sampul bagus”.
- Keterkaitan internasional juga penting: trend global menunjukkan bahwa regulator mulai menuntut pelaporan insiden, keamanan dan privasi data menjadi regulasi utama. ([HBT](#))

Langkah konkret yang diharapkan untuk Bab 24

- Penyusunan template *CyberTrust Report Card* yang standar — mencakup indikator yang ditetapkan oleh OJK-BSSN-BI.
- Bank-bank wajib menyerahkan data ke regulator dan menerima verifikasi reguler.
- Hasil rating tahunan dipublikasikan ke publik: website regulator, laporan industri, etc.
- Penggunaan hasil publikasi sebagai input dalam pengawasan bank: bank dengan skor rendah akan dibina, bank bagus bisa mendapat insentif.
- Edukasi kepada nasabah/publik: menjelaskan arti rating-rating tersebut, agar transparansi benar-benar berdampak ke kepercayaan dan keputusan mereka.

Bagian IX — Manfaat dan Dampak Nasional

Bab 25: Bagi OJK & Regulator

Efisiensi pengawasan dan *data-driven regulation*

Mengapa OJK perlu *data-driven regulation*

Pengawasan perbankan makin kompleks. Serangan siber makin sering. Data makin besar. Tanpa pendekatan berbasis data, pengawasan menjadi lambat dan reaktif. *SupTech* (supervisory technology) memberi kemampuan baru: pengumpulan data otomatis, analitik real-time, dan prioritasasi risiko. Hasilnya: pengawasan lebih cepat, konsisten, dan hemat sumber daya. (BIS—*suptech* meningkatkan efisiensi dan kualitas pengawasan). ([Bank for International Settlements](#))

Prinsip kunci: dari manual ke otomatis

Intinya sederhana: “kurangi kerja rutin, tingkatkan keputusan berbasis risiko.”

- Otomasi *regulatory reporting*. Data masuk sekali, dipakai berkali-kali oleh berbagai fungsi pengawasan. ([Financial Stability Board](#))
- Analitik untuk memetakan bank mana yang paling berisiko hari ini, bukan minggu depan. ([Bank for International Settlements](#))
- Alat bantu *inspection* berbasis data agar tim lapangan fokus ke temuan bernilai tinggi. (Contoh: MAS mengembangkan analitik untuk otomatisasi analisis saat pemeriksaan). ([Bank for International Settlements](#))

Standar global yang memandu regulator

Agar efisien, OJK perlu selaras dengan praktik internasional:

- **Harmonisasi pelaporan insiden siber.** FSB mengeluarkan 16 rekomendasi untuk menyatukan format, istilah, dan alur laporan. Tujuannya: pengawas mendapat sinyal dini dan bisa bertindak cepat lintas lembaga. ([Financial Stability Board](#))
- **DORA (EU):** mulai berlaku 17 Jan 2025. Menuntut ketahanan operasional digital end-to-end (termasuk manajemen risiko *third-party*). Pelajarannya untuk OJK: minta *register* vendor ICT yang konsisten dan bisa diaudit. ([eiopa.europa.eu](#))
- **TIBER-EU:** *threat-intel based ethical red-teaming*. Kerangka uji serangan terarah pada fungsi kritikal. Cocok jadi *gold standard* untuk uji ketahanan bank sistemik. ([European Central Bank](#))

Dampak langsung bagi efisiensi pengawasan OJK

Apa yang berubah bila OJK *data-driven*?

- **Waktu respon** insiden turun. Format pelaporan seragam → lebih sedikit bolak-balik klarifikasi → tindakan lebih cepat. (FSB dorong format bersama untuk memangkas beban & kebingungan pelaporan). (xbrl.org)
- **Prioritisasi risiko** yang objektif. *Dashboards* menyorot bank dengan paparan vendor kritikal, anomali trafik, atau *patching* tertunda. ([Bank for International Settlements](https://www.bankforinternationalsettlements.org))
- **Inspeksi lebih tajam.** Tim pengawas masuk dengan daftar *hypothesis-driven* berdasarkan analitik, bukan *checklist* generik. (stage.torontocentre.org)
- **Koordinasi antar-otoritas** (OJK–BSSN–BI) makin sinkron: insiden, *threat intel*, dan status remediasi berbagi satu kamus istilah dan satu paket metrik. ([Financial Stability Board](https://www.financialstabilityboard.org))

Paket kebijakan praktis (low-friction, high-impact)

1. **Format Pelaporan Insiden Nasional**
 - Adopsi kamus FSB (*Cyber Lexicon*) + *data fields* minimum.
 - Satu portal pelaporan, *auto-routing* ke OJK/BSSN/BI. ([Financial Stability Board](https://www.financialstabilityboard.org))
2. **Register Vendor ICT per Bank (gaya DORA)**
 - Nama vendor, layanan, data yang diakses, kontrol keamanan, dan SLA.
 - Wajib diperbarui per kuartal; *auto-flag* jika vendor berisiko tinggi. (eiopa.europa.eu)
3. **Program Uji Ketahanan Terarah (mirip TIBER)**
 - Untuk bank sistemik: uji *red-team* berbasis *threat intel* pada fungsi kritikal (pembayaran, *core banking*).
 - Hasil masuk ke skor pengawasan dan rencana remediasi. ([European Central Bank](https://www.europeancentralbank.org))
4. **SupTech Analytics Hub**
 - *Pipelines* untuk: deteksi anomali, *vendor risk*, keterlambatan *patch*, *open exposure*.
 - *Playbooks* otomatis untuk *onsite/remote inspection*. ([Bank for International Settlements](https://www.bankforinternationalsettlements.org))

Metrik kinerja (KPI) pengawasan yang mudah dipahami

- **TTR (Time-to-Respond)** insiden material ↓ 50% dalam 12 bulan. ([Financial Stability Board](https://www.financialstabilityboard.org))
- **Coverage vendor kritikal** (memiliki *register* lengkap) = 100% bank buku 4; 90% bank lainnya. (eiopa.europa.eu)
- **Siklus inspeksi berbasis data:** ≥70% temuan didahului *analytic alerts* (bukan temuan ad-hoc). ([Bank for International Settlements](https://www.bankforinternationalsettlements.org))
- **Rasio duplikasi permintaan data** → turun drastis pasca standarisasi *reporting*. ([Financial Stability Board](https://www.financialstabilityboard.org))

Tata kelola data untuk pengawas (*governance first*)

- **Satu kamus data** lintas OJK–BSSN–BI agar *interoperable*. (Sejalan dorongan FSB untuk istilah & format yang seragam). ([Financial Stability Board](#))
- **Privasi & need-to-know**: hanya data yang relevan untuk pengawasan yang dikumpulkan. (Pelajaran DORA: minimalisasi data + kontrol pihak ketiga). ([eba.europa.eu](#))
- **Auditability**: setiap *alert* dan keputusan pengawasan punya *data-trail*. (BIS: suptech membantu transparansi proses). ([Bank for International Settlements](#))

Narasi singkat untuk publik & DPR

“Kami (OJK) beralih dari pengawasan dokumen ke pengawasan berbasis data. Format laporan insiden kami seragam sesuai FSB, daftar vendor ICT mengikuti DORA, dan uji ketahanan mengacu TIBER-EU. Dengan ini, respon lebih cepat, koordinasi lebih rapi, dan keputusan lebih tepat.” ([Financial Stability Board](#))

Ringkasan eksekutif (langsung bisa dieksekusi)

- **Standarisasi**: adopsi *common format* pelaporan insiden + *register* vendor. ([Financial Stability Board](#))
- **Automasi**: bangun *SupTech Analytics Hub* untuk prioritisasi risiko. ([Bank for International Settlements](#))
- **Uji ketahanan**: jalankan *threat-intel red-teaming* untuk bank sistemik. ([European Central Bank](#))
- **KPI jelas**: ukur TTR, cakupan *register*, dan kontribusi analitik pada temuan. ([Financial Stability Board](#))

Dengan langkah-langkah ini, **pengawasan menjadi lebih efisien, terukur, dan *trust-building***. *Data-driven regulation* bukan sekadar jargon — ia adalah cara kerja baru yang menyelamatkan waktu pengawas, menurunkan beban kepatuhan bank, dan meningkatkan stabilitas sistem keuangan Indonesia.

Bab 26: Bagi Bank & Industri Keuangan

Kepercayaan nasabah dan akses insentif GCG

Inti pesannya

Di ekonomi digital, **kepercayaan** adalah mata uang. Nasabah akan pindah ke bank yang **aman, transparan, dan cepat pulih saat insiden**. Reputasi GCG yang kuat bukan sekadar *compliance*—ia menurunkan biaya risiko, memperbaiki akses pendanaan, dan membuka insentif dari regulator maupun pasar. *CyberTrust Rating* membantu bank membuktikan hal itu dengan data, bukan janji.

Apa yang paling dirasakan bank?

1. Kepercayaan nasabah naik → retensi dan *cross-sell* membaik

- Riset konsumen global menunjukkan bank yang membangun *advocacy* (rasa percaya + dilayani) tumbuh lebih kuat; keamanan dan kejelasan komunikasi jadi pendorong utama loyalitas. ([accenture.com](https://www.accenture.com))
- Insiden data mahal dan memicu *churn*; sektor finansial menanggung biaya pelanggaran tertinggi di atas rata-rata industri. *Takeaway*: mencegah lebih murah daripada memulihkan. ([IBM](https://www.ibm.com))

2. Nilai GCG meningkat → persepsi risiko investor membaik

- Lembaga pemeringkat kini memasukkan **paparan risiko siber** ke dalam analisis kredit. Eksposur tinggi = potensi tekanan pada *outlook* dan biaya pendanaan. Skor CyberTrust yang baik jadi sinyal disiplin GCG ke pasar modal. ([moody.com](https://www.moody.com))

3. Premi dan syarat *cyber insurance* lebih bersahabat

- Pasar asuransi menilai kontrol siber yang kuat secara positif: syarat lebih baik, limit naik, dan retensi bisa turun ketika kontrol dan *governance* terbukti. *Rating* yang jelas membantu negosiasi. ([marsh.com](https://www.marsh.com))

4. Kesiapan regulasi masa depan → biaya kepatuhan turun

- Arah global (UE **DORA**, UK **operational resilience**) menuntut uji ketahanan end-to-end, kontrol *third-party*, dan pelaporan insiden yang seragam. Bank yang sejak awal mengadopsi metrik & proses ala CyberTrust akan lebih gampang *comply* ketika aturan makin ketat. (eba.europa.eu)

“Insentif GCG” yang bisa diakses bank ber-rating tinggi

Bentuk insentif tidak selalu berupa uang tunai; banyak yang berbentuk **kelonggaran proses dan akses yang lebih baik**:

- **Keunggulan reputasi & pasar**
Lebih dipercaya nasabah, disukai mitra, dan dinilai lebih sehat oleh investor karena *operational resilience* dianggap bagian dari *safety & soundness*. ([Bank of England](#))
- **Leverage di pasar asuransi**
Portofolio kontrol yang tervalidasi (patching, uji *red-team*, *vendor risk register*) → peluang tarif lebih stabil/lebih rendah dan klausul yang lebih ramah. ([marsh.com](#))
- **Efisiensi kepatuhan**
Dengan pelaporan insiden yang **terstandar** (mengikuti rekomendasi FSB), duplikasi permintaan data dan *rework* berkurang; tim kepatuhan bisa fokus ke perbaikan nyata. ([Financial Stability Board](#))
- **Kelancaran dialog pengawasan**
Praktik yang selaras DORA (inventaris vendor ICT kritikal, uji skenario, *impact tolerance*) memudahkan diskusi berbasis bukti dengan pengawas, mempercepat *closure* temuan. ([eba.europa.eu](#))

Apa yang harus dilakukan bank (praktis, 6 langkah)

1. **Jadikan keamanan & privasi sebagai *value proposition***
Cantumkan komitmen dan metrik di *channels* publik. Saat insiden, komunikasikan jujur & cepat. (Ini mengubah krisis menjadi *trust-building moment*). ([accenture.com](#))
2. **Bangun *vendor risk register* ala DORA**
Daftar vendor, data yang diakses, kontrol, SLA, dan rencana *exit*. Perbarui kuartalan. ([eba.europa.eu](#))
3. **Uji ketahanan layanan kritikal (*payments, core banking*)**
Terapkan uji berkala sesuai prinsip *operational resilience* (identifikasi layanan penting, tetapkan *impact tolerance*, uji dan perbaiki). ([FCA](#))
4. **Siapkan *incident reporting* berformat FSB**
Satu *playbook*, satu kamus istilah, satu alur pelaporan ke regulator. Kurangi *back-and-forth*. ([Financial Stability Board](#))
5. **Kaitkan CyberTrust Score ke KPI manajemen risiko & GCG**
Ikat bonus manajemen ke penurunan paparan *critical findings* dan *time-to-respond*. (Sejalan arah pengawas menilai ketahanan operasional). ([Bank of England](#))
6. **Optimalkan *cyber insurance* dengan bukti kontrol**
Kirimkan ringkasan kontrol, hasil uji, dan tren perbaikan untuk negosiasi syarat yang lebih baik. ([marsh.com](#))

Narasi singkat untuk direksi & komisaris

“Skor CyberTrust yang tinggi bukan hanya compliance. Ia menurunkan biaya insiden, memperbaiki persepsi kredit, mempermudah dialog dengan regulator, dan menguntungkan saat menawar asuransi. Hasilnya: nasabah lebih percaya, biaya modal lebih efisien, dan GCG lebih kuat.” ([IBM](#))

Ringkasan

- **Trust = growth:** keamanan + komunikasi jujur → retensi & *advocacy* naik. ([accenture.com](https://www.accenture.com))
- **GCG yang kuat dibaca pasar:** risiko siber masuk radar pemeringkat & investor. ([moodys.com](https://www.moodys.com))
- **Insentif nyata:** syarat asuransi lebih baik, kepatuhan lebih efisien, dialog pengawas lebih lancar. ([marsh.com](https://www.marsh.com))
- **Selaras tren global:** DORA & *operational resilience*—siap lebih dulu, biaya kepatuhan turun. (eba.europa.eu)

Dengan begitu, **CyberTrust Rating** menjadi alat yang memadukan *customer trust* dan **insentif GCG**: meningkatkan loyalitas, menekan *cost of risk*, dan mengangkat daya saing bank Indonesia di mata nasabah, investor, dan regulator.

Bab 27: Bagi Publik dan Investor

Transparansi keamanan digital nasional

Keamanan digital bukan urusan teknis semata. Ia menyangkut **hak nasabah untuk tahu** dan **hak investor untuk menilai risiko**. Tanpa informasi yang jelas, publik menebak-nebak. Pasar pun meraba-raba. Negara-negara maju mendorong *disclosure* siber agar keputusan publik dan investasi lebih cerdas. Contoh di AS: **SEC** mewajibkan emiten mengungkapkan **insiden siber material** dalam 4 hari kerja, lengkap dengan dampak dan langkah pemulihan. Ini dibuat agar investor memperoleh informasi **tepat waktu** dan **relevan**. ([SEC](#))

Apa yang didapat publik dan investor?

1. Gambaran risiko yang nyata, bukan janji

- Laporan yang konsisten membuat masyarakat paham: bank mana yang **siap menghadapi serangan**, mana yang masih **rawan**. *Disclosure* yang jujur dan cepat membantu meminimalkan kepanikan saat insiden. ([Reuters](#))

2. Sinyal kualitas tata kelola

- Investor membaca keamanan digital sebagai bagian dari **GCG** dan **ketahanan operasional**. Tren global: lembaga pemeringkat mulai memasukkan **paparan risiko siber** ke analisis kredit. Artinya, transparansi bisa **memperbaiki persepsi pasar** dan menurunkan *cost of capital* bagi institusi yang kuat. ([moody's.com](#))

3. Keputusan investasi lebih akurat

- Ketika biaya *data breach* naik dari tahun ke tahun, investor butuh data untuk membedakan bank yang hanya “*compliant on paper*” vs yang benar-benar **tangguh**. Riset IBM menunjukkan biaya rata-rata pelanggaran data 2024 mencapai **USD 4,88 juta**, dan di sektor keuangan **lebih tinggi** dari rata-rata global. Informasi seperti ini penting untuk model valuasi dan penilaian risiko. ([IBM Newsroom](#))

Seperti apa bentuk transparansi yang ramah publik?

Gunakan prinsip *plain language* dan *comparable metrics* agar mudah dibaca oleh non-teknis:

- **Skor/rating keamanan & privasi** per bank (mis. AAA–D) + artinya bagi nasabah.
- **Ringkasan insiden material**: apa yang terjadi, dampak, waktu respon, langkah perbaikan. (Selaras praktik *disclosure* SEC). ([SEC](#))

- **Metrik ketahanan:** rata-rata *time-to-respond*, persentase layanan kritikal yang diuji, dan hasil uji pemulihan. (Sejalan dengan arah **DORA** di Uni Eropa tentang *operational resilience*). (eiopa.europa.eu)
- **Paparan pihak ketiga** (*third-party risk*) yang ringkas: jumlah vendor kritikal ICT dan status kontrolnya. (Ditekankan dalam DORA). (eba.europa.eu)
- **Tren tahunan:** naik/turun, serta target perbaikan tahun depan.

Dengan format ini, publik tidak perlu membaca *jargon*. Investor dapat **membandingkan** lintas bank dengan cepat.

Pelajaran dari standar internasional

- **AS — SEC Cyber Rules:** empat hari kerja untuk *material incident* + pengungkapan strategi manajemen risiko siber dalam laporan tahunan. Memberi **momentum transparansi** yang kuat ke pasar. ([SEC](https://sec.gov))
- **Uni Eropa — DORA:** berlaku mulai **17 Januari 2025**. Menuntut **resiliensi digital end-to-end**, termasuk tata kelola vendor ICT dan uji ketahanan layanan kritikal. Transparansi teknisnya membantu **kepercayaan lintas negara**. (eiopa.europa.eu)
- **NIS2 (UE):** menegaskan **kewajiban pelaporan insiden** dalam jangka waktu tertentu—mendorong kesiapan dan pelatihan krisis yang lebih baik. (comarch.com)

Intinya: dunia bergerak ke arah **pelaporan yang seragam, lebih cepat, dan lebih bisa dibandingkan**. Indonesia bisa mengadaptasi prinsipnya untuk konteks lokal.

“Apa untungnya buat saya?” — perspektif masyarakat

- **Sebagai nasabah:** Anda bisa memilih bank yang tidak hanya murah dan nyaman, tapi juga **aman**. Jika terjadi insiden, Anda tahu **apa yang sedang dilakukan** bank. Itu menumbuhkan *digital trust*. ([Reuters](https://reuters.com))
- **Sebagai UMKM/investor ritel:** Laporan yang jelas mengurangi *noise*. Anda bisa fokus ke bank yang **serius** terhadap proteksi data dan **tanggap** menghadapi insiden. ([IBM Newsroom](https://ibm.com))
- **Sebagai warga negara:** Transparansi mendorong **akuntabilitas**—bank berlomba memperbaiki kontrol, bukan sekadar *checklist*. Itu memperkuat **stabilitas keuangan** secara nasional. (eba.europa.eu)

Panduan singkat membaca *CyberTrust Report Card* (untuk publik & investor)

- Lihat **rating keseluruhan** dan **tren 3 tahun**: konsisten membaik atau fluktuatif?
- Cek **kecepatan respon** dan **rencana pemulihan**: adakah target waktu dan *milestones*? (Praktik baik *disclosure*). ([Reuters](https://reuters.com))
- Perhatikan **paparan vendor kritikal**: makin transparan, semakin baik tata kelolanya. (Sejalan DORA). (eba.europa.eu)
- Bandingkan **biaya insiden** vs **investasi pencegahan**: apakah bank mengalihkan biaya dari *remediasi* ke *prevention*? (Relevan dengan tren biaya pelanggaran data). ([IBM Newsroom](https://ibm.com))

Narasi publik yang kuat (contoh)

“Transparansi keamanan digital bukan menakut-nakuti, tetapi menguatkan kepercayaan. Dengan laporan yang jelas, publik tahu banknya aman, investor tahu risikonya terkelola, dan negara tahu sistem keuangannya tangguh.”

Ringkasan

- **Buat *report card* yang mudah dibaca:** ringkas, visual, bisa dibandingkan.
- **Selaraskan dengan praktik global:** *incident disclosure* ala SEC, resiliensi ICT ala DORA/NIS2. ([SEC](#))
- **Edukasi publik:** jelaskan arti skor dan apa yang bank lakukan untuk memperbaiki.
- **Jaga konsistensi tahunan:** transparansi yang **berkelanjutan** menciptakan *trust* yang **berkembang**.

Dengan begitu, **Transparansi Keamanan Digital Nasional** bukan sekadar wacana. Ia menjadi **alat lindung konsumen**, **kompas investor**, dan **penopang stabilitas** ekosistem perbankan Indonesia di era *digital trust economy*.

Lampiran 1: Template CyberRank Assessment Checklist

Tujuan singkat: daftar periksa yang ringkas, mudah dipakai, dan *audit-ready*. Fokus pada bukti, bukan opini. Gunakan kalimat pendek. Semua butir punya pemilik, frekuensi, dan skor.

Cara Pakai (3 langkah cepat)

1. **Isi** tiap butir: *Ya / Parsial / Tidak*, tulis bukti.
2. **Nilai** 0–3 (lihat rubrik skor).
3. **Rekap** di akhir: total skor, *gap*, dan rencana 90 hari.

Sumber acuan: UU PDP, POJK Manajemen Risiko TI, standar *ISO/IEC 27001*, *NIST CSF*. Konteks pasar: serangan ke sektor finansial terus naik; biaya *fraud* dan *downtime* langsung pukul NIM, fee-based revenue, serta kepercayaan nasabah. Jadikan checklist ini *living document*.

Rubrik Skor Tiap Butir

- **0 = Tidak ada** kontrol/bukti.
- **1 = Ada di atas kertas** (kebijakan) namun belum dijalankan.
- **2 = Berjalan** sebagian, ada bukti dan log, belum menyeluruh.
- **3 = Matang** dan rutin diuji; *metrics* stabil, *trend* membaik.

Kolom jawaban: **Ya / Parsial / Tidak • Skor (0–3) • Bukti • Pemilik • Frekuensi**

A. Identitas & Lingkup Penilaian

- Lingkup sistem kritikal (*core banking, mobile banking, internet banking, payment switch*) terdaftar jelas.
- Data klasifikasi: publik, internal, rahasia, sangat rahasia.
- *Asset inventory & data map* (termasuk *cloud & SaaS*) mutakhir ≤ 90 hari.

B. Kepatuhan PDP (*Privacy & Data Rights*)

- **RoPA** (Record of Processing Activities) lengkap & ditinjau tahunan.
- *Lawful basis* tiap proses data terdokumentasi.
- *Consent* tersimpan dan bisa ditarik (*withdraw consent*) oleh subjek data.
- *Data minimization* dan *purpose limitation* diberlakukan.
- Proses permintaan subjek data (akses, koreksi, hapus, *portability*) < SLA regulasi.
- *Privacy by design* pada proyek baru (template DPIA tersedia).
- Mekanisme *breach notification* ke OJK/Kominfo/nasabah, diuji lewat *tabletop exercise*.

C. Kontrol Teknis Inti (**Security Controls**)

- **MFA** 100% untuk admin, >95% untuk *remote access* staf.
- *Endpoint protection/EDR* aktif di server & laptop kritikal.
- *Vulnerability management*: scan rutin, *patching* < 14 hari untuk *critical*.
- *SIEM* mengumpulkan log dari sistem kritikal; *use case* deteksi prioritas jalan.
- *Network segmentation & zero trust* untuk akses antar zona.
- *Secrets management* (kredensial, API key) terpusat, tidak di kode.
- Enkripsi data *at rest* dan *in transit* (TLS modern, *HSM* untuk kunci).
- *Tokenization / data masking* untuk data sensitif di non-produksi.
- *Secure SDLC + SAST/DAST* untuk *mobile/web banking*.
- *API security*: gateway, rate limiting, schema validation, *mTLS* jika perlu.

D. Ketahanan Operasional (**Operational Resilience**)

- **RTO/RPO** disetujui Dewan untuk tiap *business service* kritikal.
- *Backup* terenkripsi, diuji *restore* triwulan; *immutable backup* tersedia.
- Uji **DR/Failover** minimal 1x/tahun dengan hasil dan *lesson learned*.
- *Capacity & performance monitoring* (uptime kanal digital, *latency*, *error rate*).
- *Incident response* 24/7; *playbook ransomware & DDoS* diuji.

E. Manajemen Vendor & **Third Party Risk**

- **Daftar vendor kritikal** lengkap (termasuk *cloud*).
- *Due diligence* keamanan & PDP sebelum kontrak (*pre-contract*).
- *Contractual clauses*: data residency, sub-processor, hak audit.
- *Continuous monitoring*: security attestation, penetration test vendor, attack surface.
- *Exit plan & data return/destruction* saat kontrak berakhir, diuji.

F. Kanal Digital & **Fraud Control**

- *Transaction monitoring* berbasis risiko (anomaly, device, lokasi, velocity).
- *Proteksi account takeover*: device binding, behavioural biometrics, risk-based auth.
- *App hardening & runtime protection* untuk *mobile banking*.
- Rasio **fraud loss per 1.000 transaksi** dilacak, trend turun.
- Mekanisme edukasi nasabah (*in-app*) dan *anti-phishing* berjalan.

G. Tata Kelola, Peran, & Budaya (**GRC & People**)

- **CISO & DPO** ditetapkan, independen, lapor ke Komite Risiko/Dewan.
- *Risk appetite* digital disahkan Dewan; KRI/KPI ditetapkan.
- Program pelatihan berkala; **phishing simulation** dengan *fail rate* target < 5%.
- *Internal audit* men-sample bukti Scorecard; repeat finding turun.
- *Whistleblowing* untuk insiden PDP/keamanan tersedia, dilindungi.

H. Pemantauan Berkelanjutan & *Telemetry*

- *Continuous control monitoring* (CCM) untuk *MFA*, *patch*, *log coverage*.
- *Threat intelligence* terintegrasi (indikator BSSN/komunitas industri).
- *Attack surface monitoring* (domain, *certificate*, *exposed ports*).
- Deteksi *data leak* (paste site, *dark web*) dan *brand monitoring*.
- *Dashboard* eksekutif: 5–7 metrik inti dengan *trend* 12 bulan.

I. Pelaporan & Kepatuhan ke Regulator

- Laporan insiden tepat waktu dan lengkap sesuai format OJK/Kominfo.
- *CyberTrust Scorecard* triwulan ke Komite Risiko dan *profil risiko digital* ke OJK.
- Notulen keputusan Dewan terkait keamanan & PDP terdokumentasi.

J. Ringkasan Skor & *Heatmap* Risiko

Format rekap (contoh):

- **Total butir:** 60 • **Rata-rata skor:** 2,4/3
- **Zona merah (skor ≤1):** Patch kritikal, *DR drill*, *vendor exit plan*
- **Zona kuning (skor =2):** *API security*, *behavioural biometrics*
- **Zona hijau (skor =3):** *MFA admin*, enkripsi data, *backup restore*

Interpretasi cepat:

2,6–3,0 = matang;

2,0–2,59 = cukup, perlu fokus gap;

<2,0 = rawan, butuh enhanced supervision.

K. Rencana Perbaikan 30–60–90 Hari

- **30 hari:** tutup *quick wins* — aktifkan *MFA* penuh, perbaiki *admin shadow*, pastikan *backup restore* lulus.
- **60 hari:** *patching backlog* kritikal=0; *API gateway* aktifkan *rate limit* & *schema validation*.
- **90 hari:** uji **DR/Failover** untuk layanan mobile & core; *exit plan* 3 vendor kritikal diuji.

L. Tabel Template (siap di-copy/paste ke lembar kerja)

Domain	Kontrol/Bu tir	Ya/ Parsial/ Tidak	Skor (0–3)	Bukti/Log	Pemilik	Frekuen si
PDP	RoPA lengkap & up-to-date			Link dokumen	DPO	Tahunan
Teknis	MFA admin 100%			Laporan IdP	CISO	Bulanan
Resilien si	Uji DR memenuhi RTO/RPO			Hasil DR test	Head IT Ops	Tahunan
Vendor	Due diligence vendor <i>cloud</i>			Kuesioner+Attesta tion	Procurem ent	Tahunan
Fraud	Fraud loss /1.000 trx < target			Laporan AML/Fraud	Head Digital Risk	Bulanan
Budaya	Phishing fail rate <5%			Hasil simulasi	HR/CISO	Triwulan

M. Daftar Bukti Minimum (*Evidence Pack*)

- Kebijakan & SOP (*access control, incident response, backup, DR*).
- Log IdP/MFA, laporan *patch*, hasil *scan* kerentanan, *SIEM use case*.
- Hasil *penetration test, code review, mobile app hardening* report.
- DPIA, template *privacy by design*, catatan permintaan subjek data.
- Kontrak vendor (lampiran *security & privacy clauses*), *exit checklist*.
- Notulen Komite Risiko/Dewan, *risk register, remediation tracker*.

N. Ambang Kinerja (KRI) yang Direkomendasikan

- *Patch compliance* kritikal $\geq 95\%$ (≤ 14 hari).
- *Log coverage* aset kritikal $\geq 95\%$.
- *Phishing fail rate* < 5%.
- *Breach notification* $\leq 3 \times 24$ jam sesuai kebijakan.
- *Backup restore test* lulus 100% kuartalan.
- Vendor kritikal 100% *due diligence* tahunan.

Penutup

Checklist ini membantu bank berbicara dalam satu bahasa data: sederhana, tajam, dan *actionable*. Isi jujur. Simpan bukti. Gerak cepat pada *gap* yang paling berdampak ke nasabah dan stabilitas layanan.

Lampiran 2: Contoh Audit Summary Bank A – Buku 4

Catatan penting: ini contoh fiktif untuk ilustrasi. Angka dan temuan disusun agar mudah dipahami tim bisnis, risiko, TI, dan Dewan. Mengacu praktik baik *ISO/IEC 27001*, *NIST CSF*, UU PDP, dan POJK Manajemen Risiko TI. Bahasa sederhana. Fokus ke dampak bisnis.

1. Ringkasan Eksekutif (1 halaman)

- **Rating CyberRank: A-**
- **Status risiko:** *Moderate–Low* (terkendali, masih ada celah prioritas tinggi di *API* dan *third party*).
- **Apa artinya untuk bank?**
Layanan inti aman dan andal. Risiko *fraud* masih bisa ditekan. Perlu akselerasi kontrol vendor dan *app security* agar siap ekspansi digital.
- **3 temuan terbesar:**
 1. *API security* belum seragam (validasi *schema*, *rate limiting*).
 2. *Exit plan* vendor kritikal belum diuji (*data return/destruction*).
 3. Uji **DR/Failover** belum mencakup *mobile banking* penuh.
- **3 hal yang sudah kuat:**
 1. **MFA** admin 100% & *EDR* aktif.
 2. Enkripsi *at rest/in transit* konsisten; kunci dikelola via *HSM*.
 3. *SIEM* aktif dengan *use case* prioritas (*AIO*, *privilege misuse*, *ransomware*).

Estimasi dampak finansial jika celah prioritas tidak ditutup (12 bulan):

- Potensi *fraud loss* tambahan: Rp20–40 miliar.
- Potensi *downtime* + pemulihan: Rp5–10 miliar.
- Potensi denda kepatuhan (jika terjadi *breach*): signifikan.

Angka adalah proyeksi konservatif berbasis tren industri; bukan prediksi pasti.
Tujuan: bantu *prioritization*.

2. Ruang Lingkup & Metode

- **Sistem dinilai:** *core banking*, *internet banking*, *mobile banking*, *payment switch*, *API gateway*, *data warehouse*, *cloud workloads* terbatas.
- **Periode audit:** Jan–Mar 2025.
- **Metode:**
Self-assessment + bukti, *technical testing* (*SAST/DAST*, *config review*), *attack surface scan*, *threat intel*, *tabletop exercise*, dan *board interview*.
- **Acuan:** UU PDP, POJK 38/2016, *ISO 27001*, *NIST CSF*.
- **Skala skor** per kontrol: 0–3 (0 tidak ada, 3 matang), digabung menjadi rating (AAA–D).

3. Skor Domain Inti (ringkas)

- **PDP & Privacy: 2.6/3**
RoPA lengkap, *DPIA* rutin, *consent* terekam. Perlu otomatisasi SLA permintaan subjek data.
- **Kontrol Teknis: 2.7/3**
EDR, SIEM, enkripsi kuat. *Secrets management* baik. *API security* belum seragam → *gap* utama.
- **Ketahanan Operasional: 2.4/3**
RTO/RPO disetujui. *Backup* terenkripsi & *restore* lulus. Uji DR *mobile* belum penuh.
- **Vendor & Third Party Risk: 2.2/3**
Due diligence ada. *Exit plan* belum diuji. *Continuous monitoring* perlu diperluas.
- **Kanal Digital & Fraud: 2.5/3**
Transaction monitoring berbasis risiko. *Behavioural biometrics* bertahap. Target *fraud loss*/1.000 *trx* perlu pengetatan.
- **Tata Kelola & Budaya: 2.8/3**
CISO & DPO mandiri. Komite Risiko aktif. *Phishing fail rate* 3.8% (baik, terus tekan).

Rata-rata tertimbang: 2.53/3 → Rating: A-

4. Indikator Kinerja (KRI) — Q1 2025

- *Patch compliance* kritikal ≤14 hari: **96%** (target ≥95%) ✓
- Cakupan log SIEM aset kritikal: **94%** (target ≥95%) ⚠
- *Phishing fail rate* pegawai: **3.8%** (target <5%) ✓
- *Fraud loss* / 1.000 transaksi digital: **0,021** (target ≤0,018) ⚠
- Waktu deteksi insiden (MTTD): **45 menit** (baik) ✓
- Waktu pemulihan (MTTR) insiden prioritas 1: **4,5 jam** (target ≤6 jam) ✓

5. Temuan Kritis (Top 5) & Aksi

1. **API rate limiting tidak konsisten** pada 3 *microservice*—risiko *credential stuffing*.
→ *Action 30 hari*: aktifkan *rate limit* + *schema validation* di *gateway*.
2. **Exit plan vendor cloud** belum diuji pengembalian/penghancuran data.
→ *Action 60 hari*: uji end-to-end, simulasikan pemutusan kontrak.
3. **DR mobile banking** belum *failover* penuh lintas zona.
→ *Action 90 hari*: uji komprehensif, capai RTO 1 jam, RPO 15 menit.
4. **Cakupan log SIEM** belum 95% untuk semua aset prioritas.
→ *Action 30 hari*: onboard 25 server yang tertinggal, verifikasi *use case*.
5. **Fraud analytics** belum gunakan *device binding* di semua segmen.
→ *Action 60 hari*: perluas *behavioural biometrics* & *risk-based auth*.

6. Insiden & *Lessons Learned* (12 bulan terakhir)

- **Insiden signifikan:**
 - *Account takeover* skala kecil (terkendali). Tidak ada *data exfiltration*.
- **Pelajaran kunci:**
 - Edukasi nasabah *in-app* menurunkan eskalasi.
 - Korelasi SIEM + *fraud engine* mempercepat blokir.

7. Heatmap Risiko (setelah kontrol)

- **Merah:** *API abuse* terarah, kegagalan *vendor exit*.
- **Kuning:** Cakupan log 95%, *fraud loss ratio*.
- **Hijau:** MFA admin, enkripsi, *backup/restore*, *phishing*.

8. Rencana Perbaikan 30–60–90–180 Hari

30 hari

- Tutup *logging gap* 1% → 95%+ cakupan.
- Terapkan *rate limiting* & *schema validation* di semua *public API*.
- *Quick win* edukasi nasabah anti-*phishing* di *app*.

60 hari

- Uji **vendor exit plan** + bukti *data destruction*.
- Perluas *behavioural biometrics* ke segmen ritel berisiko tinggi.
- Selesaikan *patch backlog* kritikal jadi 0.

90 hari

- Uji **DR/Failover** *mobile banking* end-to-end (zona aktif–aktif).
- *Hardening* aplikasi: *SAST/DAST* terotomasi di *CI/CD*.
- Integrasi SIEM ↔ *fraud engine* untuk *real-time correlation*.

180 hari

- *Continuous control monitoring* (CCM) untuk MFA, *patch*, dan *log coverage*.
- Sertifikasi ulang *ISO 27001* lingkup digital channel.
- Target **rating naik ke A** melalui perbaikan vendor & *fraud analytics*.

9. Dampak ke GCG & Profil Risiko

- **GCG:** bukti pengawasan Dewan kuat (notulen, KPI). Perlu *deep dive* triwulanan soal vendor dan kanal digital.
- **Profil Risiko Digital:** tetap pada **Moderat–Rendah** dengan *trend* membaik jika rencana 90 hari tercapai.

10. Pernyataan Manajemen (Ringkas)

- Dewan meninjau laporan dan menyetujui *risk appetite* digital tahun berjalan.
- Komitmen anggaran: *API security uplift*, uji DR, dan *fraud analytics* lanjutan.
- Tenggat *regulatory reporting* dipenuhi.

11. Evidence Pack (tersedia)

- *Policies/SOP* terbaru, log IdP/MFA, laporan *patch*, hasil *scan* kerentanan, konfigurasi *API gateway*, hasil uji DR, bukti *vendor exit test*, laporan *fraud monitoring*, notulen Komite Risiko/Dewan.

Kesimpulan untuk Pemimpin Bisnis

- **Why it matters:** setiap 1 jam *downtime* dan 1 bps kenaikan *fraud loss* menekan laba.
- **Good news:** fondasi kuat; tinggal akselerasi di *API*, vendor, dan *fraud analytics*.
- **Ask to Board:** setuju prioritas 90 hari. Ukur hasilnya di *CyberTrust Scorecard* berikutnya.

Takeaway: amankan pertumbuhan digital, jaga kepercayaan nasabah, dan turunkan biaya risiko. Itu inti dari A- menuju **A**.

Lampiran 3: Panduan Teknis Integrasi API CyberRank ↔ OJK Portal

Tujuan dokumen ini: memandu bank agar *integrasi data* aman, rapi, dan patuh regulasi. Bahasa sederhana. Fokus ke langkah praktis. Selaras praktik *ISO/IEC 27001*, *NIST CSF*, UU PDP, dan POJK Manajemen Risiko TI.

1. Gambar besar: alur data yang aman

- **Dari Bank → OJK:** kirim metrik keamanan dan privasi (harian/mingguan/bulanan).
- **Dari OJK → Bank:** terima *feedback* skor, *findings*, dan *remediasi* prioritas.
- Semua lewat **API terproteksi**: *mTLS*, *OAuth 2.0 Client Credentials*, *JWT*, dan *IP allowlist*.
- **Prinsip minimisasi data:** kirim yang perlu saja. PII diminimalkan atau dipseudonimkan.

2. Lingkungan & konektivitas

- **Lingkungan:** *Sandbox* (uji), *Pre-prod* (staging), *Prod* (operasional).
- **Koneksi:** *VPN/MPLS* atau *private link*; fallback *TLS 1.2+* dengan *mTLS*.
- **Jam operasional API:** 24/7. **SLA** gateway 99,9% bulanan.
- **Rate limit awal:** 600 *requests* / menit / *client*. *Burst* disepakati saat *cut-off* pelaporan.

3. Skema otentikasi & otorisasi

- **mTLS:** sertifikat organisasi (CA terpercaya). Rotasi minimal tiap 12 bulan.
- **OAuth 2.0 – Client Credentials:**
 - *token endpoint:* `/oauth2/token`
 - *scope:* `cyberrank:write`, `cyberrank:read`, `alerts:read`
- **RBAC:** peran *Reporter*, *Reader*, *Admin*. Pisahkan *service account* dari akun manusia.
- **Secrets management:** simpan *client_id/secret* di *HSM/vault*. Jangan di *code repo*.

4. Model data ringkas (contoh JSON)

a) Metrik kerentanan (harian)

```
{
  "bankId": "B4-123",
  "reportDate": "2025-05-31",
  "vulnSummary": {
    "criticalOpen": 3,
    "highOpen": 17,
    "medianRemediationDays": 9
  },
  "coverage": {
    "siemLogCoveragePct": 94.5,
    "edrCoveragePct": 98.2,
    "mfaAdminPct": 100
  },
  "evidenceUri": "s3://bank-a/evidence/2025-05-31.zip"
}
```

b) Insiden terlapor (realtime atau H+1)

```
{
  "bankId": "B4-123",
  "incidentId": "INC-2025-00077",
  "classification": "UnauthorizedAccess",
  "severity": "High",
  "startTime": "2025-05-31T03:12:00Z",
  "status": "Contained",
  "exfilSuspected": false,
  "affectedRecords": 0,
  "regulatoryNotified": true
}
```

c) Paparan vendor (bulanan)

```
{
  "bankId": "B4-123",
  "month": "2025-05",
  "criticalVendors": [
    { "vendorId": "V-019", "function": "Cloud",
      "lastAudit": "2025-04-12", "exitPlanTested": true }
  ],
  "thirdPartyFindings": { "openHigh": 2, "openMedium": 5 }
}
```

Catatan: PII tidak dikirim, atau dikirim setelah dipseudonimkan. Jika wajib kirim PII (kasus khusus), lakukan *encryption-in-payload* + alasan hukum (UU PDP).

5. Endpoints utama (versi v1)

- **POST /v1/reports/vuln-daily** – kirim ringkasan kerentanan harian.
- **POST /v1/reports/incidents** – lapor insiden.
- **POST /v1/reports/vendor-monthly** – paparan vendor.
- **GET /v1/scorecards/latest** – ambil *CyberRank scorecard* terbaru bank.
- **GET /v1/findings/open** – daftar temuan terbuka + *due date*.
- **POST /v1/evidence/upload-url** – *pre-signed URL* untuk bukti audit.

Versi & kompatibilitas

- Versi di URL (**/v1/...**).
- Perubahan minor tambah *field* bersifat *backward compatible*.
- *Breaking change* → **/v2** + periode *dual-run* min. 6 bulan.

6. Validasi, idempotency, dan webhook

- **Schema validation:** *JSON Schema* wajib. *Reject* jika *field* wajib kosong.
- **Idempotency-Key:** *header* untuk mencegah *double submit*.
- **Webhook OJK** → **Bank:** notifikasi *score update* dan *regulatory deadlines*.
 - Daftarkan <https://api.bank.co.id/ojk/webhook>
 - Tanda tangani *payload* (HMAC) + verifikasi *source IP*.

7. Keamanan tingkat lanjut

- **Enkripsi:** *TLS 1.2+*, data sensitif di *payload* dienkripsi *AES-256* lalu dibungkus *JWE*.
- **Header keamanan:** *X-Content-Type-Options*, *X-Frame-Options*, *Content-Security-Policy* (untuk *portal*).
- **Anti-replay:** *timestamp* + *nonce*.
- **Anti-abuse:** *rate limit*, *WAF*, *schema enforcement*.
- **Rotasi kunci:** *TLS cert*, *JWT signing key*, dan *API secret* sesuai kebijakan kunci.

8. Observabilitas & pelaporan

- **Tracing:** *distributed tracing* (mis. *W3C Trace Context*).
- **Logging:** tanpa *PII*; *correlation-id* wajib.
- **Metrics minimal:** *latency p95/p99*, *error rate*, *throughput*, *webhook success*.
- **Dashboards:** *SLA uptime*, *delivery lag*, dan *retry*.
- **Alerting:** ke *SOC Bank* dan kontak *OJK* (24/7 untuk insiden prioritas 1).

9. Error handling standar

- **200/201:** sukses.
- **400:** *schema* salah / *field* hilang → perbaiki *payload*.
- **401/403:** token/otorisasi salah → cek *scope* & *clock skew*.
- **409:** duplikasi → gunakan *Idempotency-Key*.
- **429:** *rate limit* → *retry with backoff*.

- **5xx:** masalah sisi OJK → *retry* eksponensial, laporkan jika >15 menit.

Contoh respons kesalahan

```
{
  "errorCode": "SCHEMA_VALIDATION_FAILED",
  "message": "field 'reportDate' is required",
  "traceId": "9f2e..."
}
```

10. Tata kelola & kepatuhan (UU PDP)

- **Dasar hukum:** jelaskan dasar pemrosesan data pada perjanjian integrasi.
- **DPIA:** lakukan *Data Protection Impact Assessment* sebelum *go-live*.
- **Hak subjek data:** siapkan mekanisme *access/erasure* bila diperlukan.
- **Retensi:** tentukan *retention schedule*; hapus/anonimkan saat lewat masa simpan.
- **Audit trail:** simpan *who/what/when* untuk setiap kiriman.

11. Checklist go-live (ringkas & to-the-point)

Teknis

- Sertifikat *mTLS* aktif dan diuji *CRL/OCSP*.
- *OAuth token flow* berjalan; *clock drift* < 60 detik.
- Validasi *JSON Schema* lulus di *CI/CD*.
- *Idempotency-Key* diterapkan untuk semua **POST**.
- *Webhook* diverifikasi (HMAC + IP).
- *Rate limit* dan *retry policy* dikonfigurasi.

Keamanan

- Kunci/rahasia disimpan di *vault*.
- *Secrets rotation* terjadwal.
- Tanpa PII, kecuali ada dasar hukum + *encryption-in-payload*.
- *Penetration test* API selesai dan *remediation* kritikal ditutup.

Kepatuhan

- DPIA disetujui DPO.
- *Data sharing agreement* ditandatangani.
- *Retention & disposal* terdokumentasi.
- *Runbook* insiden & kontak 24/7 tersedia.

12. Rencana implementasi 30–60–90 hari

- **0–30 hari (foundation)**
 - *Network path* aman, *mTLS* & *OAuth* siap.
 - *CI/CD* menolak *payload* yang tidak sesuai *schema*.
 - *Sandbox* kirim **vuln-daily** & **incidents** contoh.

- **31–60 hari (stabilize)**
 - *Pre-prod dual-run* dengan data sintetis → uji *rate limit* & *webhook*.
 - Tutup temuan *pentest* prioritas tinggi.
 - Finalisasi DPIA dan *data mapping*.
- **61–90 hari (go-live)**
 - Aktifkan *Prod. Runbook* insiden dites (*tabletop*).
 - Nyalakan *dashboards* & *alerts*.
 - *Post-go-live* review, siapkan *capacity plan* kuartalan.

13. *Do's* & *Don'ts* yang sering terlewat

Do's

- Otomatiskan uji *schema* di *pipeline*.
- Gunakan *correlation-id* yang sama dari Bank ke OJK.
- Enkripsi bukti audit; kirim lewat *pre-signed URL* saja.

Don'ts

- Jangan kirim *raw logs* berisi PII.
- Jangan menaruh *client secret* di kode/variabel lingkungan tanpa *vault*.
- Jangan mengubah *field* wajib tanpa naik versi API.

14. Contoh *pseudo-code* singkat (kirim harian)

```
token = oauth2.client_credentials()
payload = build_vuln_daily()
resp = POST /v1/reports/vuln-daily
      headers: { Authorization: Bearer token, Idempotency-Key:
      uuid4() }
      body: payload
if resp.status in [200,201]: ok
elif resp.status == 429: sleep(backoff); retry
else: alert(SOC, resp.error)
```

15. Siapa mengerjakan apa (peran inti)

- **CISO / Risk:** set *risk appetite*, menyetujui cakupan data.
- **DPO / Legal:** cek dasar hukum, DPIA, *retention*.
- **Head of IT / Architecture:** desain koneksi & *security controls*.
- **SOC / SecOps:** *monitoring, alerting, incident response*.
- **DevOps:** *CI/CD, observability, capacity*.
- **Vendor Manager:** *due diligence* dan kontrol *third party* terkait integrasi.

Penutup

Integrasi **API CyberRank** ↔ **OJK Portal** bukan sekadar kewajiban. Ini *enabler* kepercayaan. Dengan desain yang aman, *observability* kuat, dan tata kelola jelas, bank dapat menurunkan biaya risiko, mempercepat respon insiden, dan menjaga reputasi.

Mulai dari dasar: *mTLS, OAuth, schema*, dan **minimasi data**. Lalu naikkan level: *automation, telemetry, dan continuous compliance*.

Glosarium Istilah Teknis dan Regulasi

A

- **AAA–D Rating** — Skala penilaian keamanan siber dan kepatuhan privasi, mirip sistem pemeringkatan kredit (AAA = sangat baik, D = buruk).
- **API (Application Programming Interface)** — Antarmuka yang memungkinkan sistem berbeda saling berkomunikasi.
- **Audit Forensik** — Pemeriksaan teknis mendalam terhadap sistem untuk mendeteksi, menganalisis, dan membuktikan pelanggaran keamanan.
- **Awareness Program** — Program edukasi untuk meningkatkan kesadaran keamanan siber pegawai dan pengguna.

B

- **Bank Buku 2–4** — Klasifikasi bank di Indonesia berdasarkan modal inti (POJK No. 6/2021).
- **Basel III** — Standar internasional untuk permodalan dan manajemen risiko perbankan.
- **BSSN (Badan Siber dan Sandi Negara)** — Lembaga pemerintah Indonesia yang bertanggung jawab atas keamanan siber nasional.
- **Breach** — Pelanggaran keamanan yang menyebabkan data pribadi atau sistem bocor.

C

- **Capital One Case** — Contoh kasus kebocoran data bank di AS akibat kesalahan konfigurasi *cloud*.
- **CCPA (California Consumer Privacy Act)** — Regulasi privasi di Amerika Serikat untuk perlindungan data konsumen.
- **CIA Triad (Confidentiality, Integrity, Availability)** — Tiga pilar utama keamanan informasi: kerahasiaan, integritas, dan ketersediaan.
- **Cloud Computing** — Model layanan komputasi berbasis internet yang fleksibel namun berisiko tinggi terhadap kebocoran data.
- **Cyber Resilience** — Ketahanan digital untuk mencegah, mendeteksi, dan pulih dari serangan siber.
- **CyberTrust Rating / Scorecard** — Sistem penilaian terpadu oleh OJK untuk menilai keamanan siber dan kepatuhan data pribadi perbankan.
- **Cyber Insurance** — Polis asuransi untuk melindungi organisasi dari kerugian akibat serangan siber.

D

- **Data Breach** — Kebocoran atau akses ilegal terhadap data pribadi atau finansial.
- **Data Governance** — Tata kelola data agar aman, akurat, dan sesuai hukum.
- **DORA (Digital Operational Resilience Act)** — Regulasi Uni Eropa yang menuntut ketahanan digital sektor keuangan.
- **Dashboard Monitoring** — Sistem visualisasi real-time untuk memantau status keamanan digital bank.

E

- **Encryption (Enkripsi)** — Proses pengubahan data menjadi format tidak terbaca untuk melindungi kerahasiaan.
- **Equifax Case** — Insiden besar kebocoran data di AS yang memicu reformasi regulasi kredit.
- **EU GDPR (General Data Protection Regulation)** — Regulasi privasi Uni Eropa yang menjadi acuan global.

F

- **Firewall** — Sistem keamanan jaringan yang memfilter lalu lintas masuk dan keluar.
- **Fintech (Financial Technology)** — Perusahaan teknologi di bidang keuangan yang sering menjadi mitra bank.
- **Framework** — Kerangka kerja sistematis untuk pengawasan, penilaian, dan sertifikasi keamanan siber.

G

- **GCG (Good Corporate Governance)** — Prinsip tata kelola perusahaan yang baik dan transparan.
- **GDPR** — Regulasi privasi data Uni Eropa (lihat EU GDPR).
- **Governance, Risk, and Compliance (GRC)** — Pendekatan terpadu untuk mengelola risiko, tata kelola, dan kepatuhan.

H

- **Heartland Payment Systems Case** — Kebocoran data besar akibat serangan malware di sistem pembayaran AS.
- **Hybrid Cloud** — Kombinasi *private* dan *public cloud* untuk fleksibilitas sistem bank.

I

- **Incident Reporting** — Pelaporan resmi insiden siber kepada regulator (OJK, BSSN, atau publik).
- **IndoBERT** — Model *Natural Language Processing* berbasis bahasa Indonesia (disebut dalam konteks AI).
- **Information Security Management System (ISMS)** — Sistem manajemen untuk menjaga keamanan informasi, merujuk pada ISO/IEC 27001.
- **ISO 27001** — Standar internasional untuk manajemen keamanan informasi.
- **ISO 31000** — Standar manajemen risiko internasional.
- **IT Governance** — Kerangka kerja pengelolaan TI agar selaras dengan tujuan bisnis dan regulasi.

J

- **JPMorgan Chase Case** — Contoh insiden *zero-day attack* yang menyebabkan kebocoran data besar.

K

- **Kepatuhan PDP (Personal Data Protection)** — Kesesuaian terhadap UU No. 27/2022 tentang Pelindungan Data Pribadi.
- **KYC (Know Your Customer)** — Proses verifikasi identitas nasabah dalam perbankan.

L

- **Leak Detection** — Proses identifikasi dini atas kebocoran data di jaringan atau sistem.
- **Laporan Publik (Public Disclosure)** — Publikasi tahunan tentang status keamanan digital perbankan.

M

- **Machine Learning (ML)** — Teknologi pembelajaran mesin yang digunakan untuk deteksi anomali atau serangan siber.
- **Mitigasi Risiko** — Langkah-langkah untuk mengurangi kemungkinan dan dampak risiko siber.
- **Moody's/S&P Analogy** — Perbandingan antara lembaga pemeringkat keuangan (seperti Moody's, S&P) dan sistem pemeringkatan keamanan siber.

N

- **NIST CSF (National Institute of Standards and Technology Cybersecurity Framework)** — Standar keamanan siber dari Amerika Serikat.
- **NIS2 Directive** — Aturan Uni Eropa tentang keamanan jaringan dan informasi, menggantikan NIS 2016.

O

- **OJK (Otoritas Jasa Keuangan)** — Regulator sektor jasa keuangan di Indonesia.
- **OJK CyberTrust & Data Privacy Ranking Framework** — Kerangka nasional untuk penilaian keamanan siber dan privasi data bank di bawah pengawasan OJK.
- **Operational Resilience** — Kemampuan lembaga keuangan untuk bertahan dan beroperasi dalam gangguan digital.

P

- **Penilaian Risiko Digital** — Evaluasi kemampuan bank menghadapi ancaman siber dan kebocoran data.
- **POJK (Peraturan OJK)** — Regulasi yang diterbitkan oleh OJK, misalnya POJK No. 38/POJK.03/2016 tentang Manajemen Risiko TI.
- **Privacy Impact Assessment (PIA)** — Proses untuk menilai dampak perlindungan data pribadi dalam sistem.
- **Public Disclosure** — Laporan terbuka kepada publik tentang keamanan dan privasi digital bank.

Q

- **Quantitative Risk Analysis** — Analisis risiko berbasis data numerik untuk menilai potensi kerugian.

R

- **RAG (Risk Assessment and Governance)** — Penilaian risiko yang terintegrasi dengan tata kelola.
- **RegTech (Regulatory Technology)** — Teknologi yang digunakan regulator untuk meningkatkan efisiensi pengawasan berbasis data.
- **Risk Intelligence** — Pemanfaatan data dan analitik untuk memahami dan memitigasi ancaman.

S

- **Self-Assessment** — Penilaian mandiri oleh bank terhadap kepatuhan dan kesiapan siber.
- **Sertifikasi Kepatuhan** — Proses audit resmi untuk mendapatkan pengakuan terhadap sistem keamanan siber yang memenuhi standar.
- **SupTech (Supervisory Technology)** — Teknologi pengawasan digital yang digunakan OJK untuk efisiensi dan deteksi dini risiko.
- **Supply Chain Risk (Vendor Risk)** — Risiko dari pihak ketiga atau mitra teknologi.
- **Sustainability Reporting** — Laporan tanggung jawab sosial dan lingkungan, kini mencakup aspek keamanan digital.

T

- **Third-Party Risk Management (TPRM)** — Pengawasan risiko terhadap vendor atau penyedia teknologi pihak ketiga.
- **Transparency Index** — Indeks keterbukaan keamanan digital nasional.

U

- **UU PDP (Undang-Undang Pelindungan Data Pribadi)** — UU No. 27 Tahun 2022, dasar hukum pelindungan data pribadi di Indonesia.
- **User Awareness** — Tingkat pemahaman dan perilaku aman pengguna terhadap ancaman siber.

V

- **Vendor Exposure** — Tingkat keterpaparan risiko akibat layanan pihak ketiga.
- **Vulnerability** — Kelemahan dalam sistem yang dapat dimanfaatkan oleh penyerang.

W

- **Wazuh** — Alat *open source* untuk deteksi ancaman, audit keamanan, dan kepatuhan TI.

Z

- **Zero-Day Attack** — Serangan yang memanfaatkan celah keamanan yang belum diketahui atau ditambal.

Referensi Hukum dan Standar Internasional

Bank for International Settlements. (2023). *SupTech applications in banking supervision: A review of global trends*. Retrieved from <https://www.bis.org>

Basel Committee on Banking Supervision. (2011). *Principles for the Sound Management of Operational Risk*. Bank for International Settlements. Retrieved from <https://www.bis.org/publ/bcbs195.htm>

Basel Committee on Banking Supervision. (2023). *Cyber-resilience: Range of practices*. Bank for International Settlements. Retrieved from <https://www.bis.org/bcbs/publ/d505.htm>

Badan Siber dan Sandi Negara (BSSN). (2020). *Peraturan BSSN Nomor 8 Tahun 2020 tentang Strategi Keamanan Siber Nasional*. Jakarta: BSSN.

European Commission. (2022). *Digital Operational Resilience Act (DORA)*. Official Journal of the European Union. Retrieved from https://finance.ec.europa.eu/regulation-and-supervision/financial-services-legislation/digital-operational-resilience_en

European Union Agency for Cybersecurity (ENISA). (2023). *NIS2 Directive Explained: Strengthening EU Cybersecurity*. Retrieved from <https://www.enisa.europa.eu>

Financial Stability Board. (2023). *Cyber Incident Reporting: Harmonisation of Incident Reporting Frameworks*. Retrieved from <https://www.fsb.org/2023/04/cyber-incident-reporting-harmonisation>

International Organization for Standardization. (2018). *ISO/IEC 27001:2018 Information Security Management Systems – Requirements*. Geneva: ISO.

International Organization for Standardization. (2018). *ISO 31000:2018 Risk Management – Guidelines*. Geneva: ISO.

International Organization for Standardization. (2015). *ISO/IEC 38505-1:2015 Governance of Data – Application of ISO/IEC 38500 to the Governance of Data*. Geneva: ISO.

National Institute of Standards and Technology (NIST). (2018). *Framework for Improving Critical Infrastructure Cybersecurity, Version 1.1*. Gaithersburg, MD: U.S. Department of Commerce. Retrieved from <https://www.nist.gov/cyberframework>

Otoritas Jasa Keuangan (OJK). (2016). *POJK No. 38/POJK.03/2016 tentang Penerapan Manajemen Risiko dalam Penggunaan Teknologi Informasi oleh Bank Umum*. Jakarta: OJK.

Otoritas Jasa Keuangan (OJK). (2020). *POJK No. 13/POJK.03/2020 tentang Penerapan Tata Kelola bagi Bank Umum*. Jakarta: OJK.

Pemerintah Republik Indonesia. (2022). *Undang-Undang Nomor 27 Tahun 2022 tentang Pelindungan Data Pribadi (UU PDP)*. Lembaran Negara Republik Indonesia Tahun 2022 Nomor 210.

Purbo, O. W. (2025). *Framework Peringkat Keamanan Siber & Kepatuhan Data Pribadi untuk Dunia Perbankan Indonesia: Menuju Sistem Nasional "OJK CyberTrust & Data Privacy Ranking Framework"*. Institut Teknologi Tangerang Selatan (ITTS) & OnnoCenter.

United States Securities and Exchange Commission (SEC). (2023). *Cybersecurity Risk Management, Strategy, Governance, and Incident Disclosure Rules*. Federal Register. Retrieved from <https://www.sec.gov>

World Bank. (2022). *Financial Sector's Digital Transformation and Cybersecurity Risk*. Washington, DC: World Bank. Retrieved from <https://www.worldbank.org>

Ringkas Tabel

Kategori	Regulasi / Standar	Keterangan Singkat	Referensi (APA Style)
A. Regulasi Nasional	Undang-Undang Nomor 27 Tahun 2022 tentang Pelindungan Data Pribadi (UU PDP)	Dasar hukum utama perlindungan data pribadi di Indonesia. Mengatur hak subjek data, kewajiban pengendali data, dan sanksi pidana/sipil.	Pemerintah Republik Indonesia. (2022). <i>Undang-Undang Nomor 27 Tahun 2022 tentang Pelindungan Data Pribadi</i> . Lembaran Negara Republik Indonesia Tahun 2022 Nomor 210.
	Peraturan OJK No. 38/POJK.03/2016	Tentang <i>Penerapan Manajemen Risiko dalam Penggunaan Teknologi Informasi</i> oleh bank umum. Menjadi dasar pengawasan OJK terhadap risiko TI dan siber.	Otoritas Jasa Keuangan (OJK). (2016). <i>POJK No. 38/POJK.03/2016 tentang Penerapan Manajemen Risiko dalam Penggunaan Teknologi Informasi oleh Bank Umum</i> . Jakarta: OJK.
	Peraturan OJK No. 13/POJK.03/2020	Mengatur <i>Tata Kelola (GCG)</i> bagi Bank Umum, termasuk aspek pengawasan risiko digital dan pelaporan insiden siber.	Otoritas Jasa Keuangan (OJK). (2020). <i>POJK No. 13/POJK.03/2020 tentang Penerapan Tata Kelola bagi Bank Umum</i> . Jakarta: OJK.
	Peraturan BSSN No. 8 Tahun 2020	Menetapkan <i>Strategi Keamanan Siber Nasional</i> dan panduan pelaksanaan koordinasi antar lembaga.	Badan Siber dan Sandi Negara (BSSN). (2020). <i>Peraturan BSSN Nomor 8 Tahun 2020 tentang Strategi Keamanan Siber Nasional</i> . Jakarta: BSSN.

Rencana Aksi SPBE Nasional 2023–2028 (KemenPANRB)

Mendorong integrasi keamanan siber dan tata kelola data dalam sistem pemerintahan digital.

Kementerian Pendayagunaan Aparatur Negara dan Reformasi Birokrasi (KemenPANRB). (2023). *Rencana Aksi SPBE Nasional 2023–2028*. Jakarta: KemenPANRB.

Kategori	Regulasi / Standar	Keterangan Singkat	Referensi (APA Style)
B. Standar & Regulasi Internasional	ISO/IEC 27001:2018	Standar global sistem manajemen keamanan informasi (<i>Information Security Management System</i>).	International Organization for Standardization. (2018). <i>ISO/IEC 27001:2018 Information Security Management Systems – Requirements</i> . Geneva: ISO.
	ISO 31000:2018	Pedoman manajemen risiko organisasi. Sering diintegrasikan dengan ISO 27001 dalam pengelolaan risiko TI dan data.	International Organization for Standardization. (2018). <i>ISO 31000:2018 Risk Management – Guidelines</i> . Geneva: ISO.
	ISO/IEC 38505-1:2015	Standar <i>Governance of Data</i> – tata kelola data yang selaras dengan ISO/IEC 38500.	International Organization for Standardization. (2015). <i>ISO/IEC 38505-1:2015 Governance of Data – Application of ISO/IEC 38500 to the Governance of Data</i> . Geneva: ISO.
	NIST Cybersecurity Framework (CSF) 1.1	Panduan dari NIST AS untuk mengelola risiko keamanan infrastruktur kritis.	National Institute of Standards and Technology (NIST). (2018). <i>Framework for Improving Critical Infrastructure Cybersecurity, Version 1.1</i> . Gaithersburg, MD: U.S. Department of Commerce.

Basel Committee Principles for Operational Risk (Basel III)	Prinsip global pengelolaan risiko operasional dan siber di sektor perbankan.	Basel Committee on Banking Supervision. (2011). <i>Principles for the Sound Management of Operational Risk</i> . Bank for International Settlements.
Basel Cyber-Resilience Practices (2023)	Praktik terbaik global untuk ketahanan siber lembaga keuangan.	Basel Committee on Banking Supervision. (2023). <i>Cyber-resilience: Range of practices</i> . Bank for International Settlements.
Digital Operational Resilience Act (DORA)	Regulasi Uni Eropa 2022 yang mewajibkan lembaga keuangan memastikan ketahanan digital, pelaporan insiden, dan kontrol vendor ICT.	European Commission. (2022). <i>Digital Operational Resilience Act (DORA)</i> . Official Journal of the European Union.
NIS2 Directive (2023)	Penguatan kerangka kerja keamanan jaringan dan informasi di Uni Eropa.	European Union Agency for Cybersecurity (ENISA). (2023). <i>NIS2 Directive Explained: Strengthening EU Cybersecurity</i> .
SEC Cybersecurity Disclosure Rule (2023)	Aturan baru SEC (Amerika Serikat) yang mewajibkan pelaporan insiden siber material oleh emiten dalam 4 hari kerja.	United States Securities and Exchange Commission (SEC). (2023). <i>Cybersecurity Risk Management, Strategy, Governance, and Incident Disclosure Rules</i> . Federal Register.
FSB Cyber Incident Reporting Framework (2023)	Harmonisasi global pelaporan insiden siber di sektor keuangan.	Financial Stability Board. (2023). <i>Cyber Incident Reporting: Harmonisation of Incident Reporting Frameworks</i> . Retrieved from https://www.fsb.org
World Bank Cybersecurity & Financial	Kajian peran keamanan siber dalam stabilitas	World Bank. (2022). <i>Financial Sector's Digital Transformation and</i>

**Sector Study
(2022)**

sistem keuangan
digital.

Cybersecurity Risk.
Washington, DC: World Bank.

Tentang Penulis



Onno W. Purbo, saat ini bertugas sebagai rektor di Institut Teknologi Tangerang Selatan (ITTS). Onno memperoleh gelar Ph.D bidang Electrical Engineering dari University of Waterloo, Canada, adalah seorang copyleft, educator dan ICT evangelist. Dia sudah mempublikasikan 50++ buku, termasuk free ICT ebook untuk sekolah tahun 2008. Beberapa buku terakhirnya adalah "Internet-TCP/IP: Konsep Dan Implementasi", 2018; "Sistem Operasi, Konsep Dan Membuat Linux OpenWRT Dan ROM Android", 2019; "IPv6 Untuk Mendukung Operasi Jaringan Dan Domain Name System", 2019; "Kubernetes untuk Pemula", 2024 dan "Membuat Operator Seluler 5G Sendiri", 2024. Dia memimpin sambungan pertama Internet di Institut Teknologi Bandung, tahun 1993-2000, dan menggunakannya untuk membuat jaringan Internet pendidikan yang pertama di

Indonesia. Dia membebaskan frekuensi WiFi, memperkenalkan RT/RW-net, antenna Wajanbolic dan jaringan selular OpenBTS dan private 5G sendiri. Dia memimpin jaringan telepon pertama di atas Internet, VoIP Merdeka, yang kemudian hari dikenal sebagai VoIP Rakyat berbasis SIP dan menggunakan kode area +62520 dan +62521. Dia saat ini aktif memperkenalkan e-Learning, dan menjalankan server e-Learning di <http://lms.onnocenter.or.id/moodle/> 66,000++ siswa / mahasiswa dan <https://opencourse.itts.ac.id> 38.000+ mahasiswa secara gratis. Email: onno@indo.net.id