fintech indonesia

CISSReC
LEMBAGA RISET SIBER INDONESIA

PEDOMAN KEAMANAN SIBER AFTECH

Cybersecurity Implementation Guidelines for AFTECH Members

VERSI

Versi	Tanggal	Perubahan	Keterangan
1.0	13 Desember 2025	● Versi Awal	Pedoman Keamanan Siber AFTECH dikembangkan bersama oleh AFTECH, BSSN dan CISSReC

DAFTAR ISI

BAB 1
PENDAHULUAN

1.1 LATAR BELAKANG

Ekosistem Fintech Indonesia berkembang sangat cepat, ditandai dengan meningkatnya penggunaan teknologi digital, pertumbuhan layanan keuangan berbasis aplikasi, serta pemanfaatan kecerdasan buatan, cloud computing, API ecosystem, open finance, dan model bisnis inovatif lainnya. Inovasi ini membawa manfaat signifikan berupa peningkatan efisiensi, akses keuangan, serta percepatan digitalisasi di masyarakat. Namun, transformasi tersebut diiringi oleh meningkatnya risiko keamanan siber, serangan digital, dan kebocoran data yang berpotensi mengganggu keandalan layanan Fintech.

Sejalan dengan ketentuan regulator termasuk Undang-Undang Penguatan Sektor Keuangan, UU Perlindungan Data Pribadi, Peraturan OJK terkait ITSK, SEOJK 29/SEOJK.03/2022 tentang Ketahanan dan Keamanan Siber, serta Peraturan Bank Indonesia Nomor 2 Tahun 2024 tentang Keamanan Sistem Informasi dan Ketahanan Siber pelaku industri Fintech wajib membangun cyber resilience yang kuat, adaptif, serta sejalan dengan praktik terbaik industri global.

Ancaman siber pada sektor keuangan terus meningkat setiap tahun, mulai dari serangan ransomware, kebocoran data, rekayasa sosial, credential stuffing, hingga ancaman rantai pasok (supply chain attack). Sektor Fintech dan layanan keuangan digital menjadi salah satu target utama karena tingginya nilai data yang dikelola, keterhubungan dengan infrastruktur finansial nasional, serta tingginya volume transaksi yang berlangsung secara real time.

Sebagai asosiasi yang menaungi penyelenggara Fintech di Indonesia, AFTECH memiliki peran strategis untuk menyediakan panduan praktis dan terstandarisasi guna memastikan anggotanya dapat mengimplementasikan keamanan siber secara efektif, terukur, dan sesuai dengan peraturan yang berlaku. Pedoman ini dirancang sebagai dokumen komprehensif yang dapat digunakan sebagai acuan dalam membangun, menerapkan, memelihara, dan meningkatkan keamanan siber bagi seluruh anggota AFTECH.

Dengan demikian, penyusunan Pedoman Keamanan Siber AFTECH menjadi kebutuhan mendesak untuk:

1. mendukung ketahanan layanan Fintech nasional,
2. melindungi konsumen dan data pengguna,
3. memastikan kesesuaian dengan regulasi,
4. meningkatkan kepercayaan publik, dan
5. mendorong terciptanya ekosistem digital yang aman dan berkelanjutan.

1.2 Maksud dan Tujuan

Pedoman ini disusun sebagai guideline (pedoman tidak bersifat wajib) untuk memberikan arah dan praktik terbaik dalam penerapan keamanan siber di sektor Fintech.

Namun demikian, setiap perusahaan tetap wajib mematuhi dan mengimplementasikan pengendalian keamanan siber sesuai dengan seluruh peraturan perundang-undangan dan regulasi yang berlaku, termasuk namun tidak terbatas pada ketentuan yang ditetapkan oleh OJK, Bank Indonesia, Kementerian Komunikasi dan Digital (Komdigi), BSSN, serta regulator atau otoritas lain yang relevan dengan model bisnis dan perizinan masing-masing perusahaan. Secara garis besar, pedoman ini disusun dengan tujuan untuk:

1. Memberikan kerangka kerja keamanan siber yang komprehensif

Sebagai referensi bagi penyelenggara Fintech dalam menerapkan praktik keamanan siber berbasis risk-based approach, zero trust, dan standar internasional.

2. Mendukung kepatuhan terhadap regulasi

Mengharmonisasikan persyaratan keamanan siber dari OJK, BI, BSSN, dan regulasi terkait lain sehingga anggota AFTECH dapat melakukan implementasi secara konsisten.

3. Meningkatkan ketahanan siber anggota AFTECH

Melalui panduan penguatan tata kelola, manajemen risiko, teknologi pengamanan, peningkatan kesadaran keamanan siber anggota, serta mekanisme deteksi, respons, dan pemulihan insiden.

4. Melindungi konsumen dan menjaga integritas layanan keuangan digital

Dengan memastikan data pribadi, transaksi, dan aset digital terlindungi dari serangan maupun penyalahgunaan.

5. Membangun standar minimum keamanan siber industri Fintech

Melalui definisi kontrol minimum, persyaratan audit, serta indikator evaluasi maturitas keamanan siber.

6. Mendorong kolaborasi keamanan siber dalam ekosistem Fintech

Termasuk information sharing, early warning system, dan mekanisme tanggap insiden lintas platform untuk mengurangi risiko sistemik.

1.3 Prinsip-Prinsip Dasar Keamanan Siber

Pedoman ini disusun berdasarkan prinsip berikut:

1. Risk-Based Approach

Setiap kontrol keamanan harus didasarkan pada tingkat risiko operasional, teknologi, dan bisnis masing-masing penyelenggara Fintech.

2. Zero Trust Architecture

Akses diberikan berdasarkan prinsip never trust, always verify, dengan autentikasi berlapis dan segmentasi ketat.

3. Proportionality & Scalability

Kontrol keamanan disesuaikan dengan ukuran, kompleksitas, dan model bisnis perusahaan, sehingga UMKM Fintech maupun perusahaan besar dapat mengimplementasikannya secara efektif.

4. Secure by Design & Privacy by Design

Keamanan dan privasi wajib menjadi bagian dari design phase, bukan sekadar tambahan di akhir.

5. Continuous Monitoring & Improvement

Keamanan siber merupakan proses tanpa akhir yang memerlukan pemantauan, evaluasi, dan peningkatan berkelanjutan.

6. Accountability & Transparency

Manajemen puncak bertanggung jawab penuh atas pengelolaan keamanan siber dan perlindungan data di organisasinya.

1.4 Ruang Lingkup Penerapan

Pedoman ini berlaku bagi seluruh anggota AFTECH, baik yang merupakan penyelenggara Inovasi Teknologi Sektor Keuangan (ITSK), penyelenggara sistem pembayaran berbasis Fintech, maupun inovator layanan keuangan digital lainnya, dengan penerapan yang disesuaikan berdasarkan profil risiko masing-masing perusahaan.

Penerapan pedoman ini tidak bersifat seragam (*one-size-fits-all*), melainkan harus mempertimbangkan karakteristik, kompleksitas layanan, eksposur risiko, skala

operasional, serta kewajiban regulasi yang melekat pada masing-masing perusahaan.

Pedoman ini disusun untuk bersifat implementatif, bukan hanya konseptual, dan dapat digunakan sebagai acuan praktis bagi penyelenggara Fintech dalam:

- menyusun kebijakan internal keamanan siber,
- mengembangkan SOP dan standar teknis, serta
- mendukung kesiapan audit, asesmen regulator, dan penguatan tata kelola keamanan siber secara berkelanjutan.

1.5 Definisi dan Istilah Kunci

Untuk keseragaman pemahaman, sejumlah istilah penting dalam pedoman ini adalah:

1. Keamanan Siber (Cyber security)
   Kondisi terjaganya kerahasiaan, integritas, dan ketersediaan data maupun sistem informasi dari serangan dan ancaman siber.
2. Ketahanan Siber (Cyber Resilience)
   Kemampuan organisasi untuk mencegah, mendeteksi, menanggulangi, dan memulihkan diri dari insiden siber.
3. Data Pribadi
   Setiap data yang dapat mengidentifikasi individu, sesuai ketentuan UU PDP.
4. Aset Informasi
   Data, aplikasi, sistem, perangkat keras, jaringan, dan seluruh komponen TI yang mendukung layanan Fintech.
5. Insiden Siber
   Kejadian yang berdampak pada keamanan layanan, operasional, data konsumen, atau keandalan sistem.
6. Penyedia Pihak Ketiga (Vendor/Third Party)
   Entitas eksternal yang menyediakan layanan TI, cloud, sistem pembayaran, API, pengembangan aplikasi, atau layanan lain yang memiliki akses ke sistem atau data.
7. Secure SDLC (Secure Software Development Life Cycle)
   Praktik integrasi keamanan dalam seluruh tahapan pengembangan perangkat lunak.
8. Zero Trust
   Model keamanan yang mengharuskan verifikasi identitas dan otorisasi secara terus-menerus terhadap setiap permintaan akses.

BAB 2
TATA KELOLA KEAMANAN SIBER (CYBERSECURITY GOVERNANCE)

Tata kelola keamanan siber merupakan fondasi utama yang memastikan seluruh pengelolaan keamanan siber dilakukan secara terarah, terukur, dapat dipertanggungjawabkan, dan terintegrasi dengan tujuan bisnis organisasi. Tata kelola yang baik diperlukan untuk menjamin bahwa penyelenggara Fintech memiliki struktur organisasi, kebijakan, dan mekanisme pengawasan yang memadai untuk melindungi data, layanan, dan proses bisnis dari ancaman siber.

Bab ini menetapkan prinsip, struktur, dan persyaratan tata kelola keamanan siber bagi anggota AFTECH.

2.1 Prinsip-Prinsip Tata Kelola Keamanan Siber

Tata kelola keamanan siber dalam pedoman ini disusun berdasarkan prinsip-prinsip berikut:

1. **Kepemimpinan dan Akuntabilitas**
   Manajemen puncak bertanggung jawab penuh terhadap implementasi keamanan siber, mulai dari kebijakan, pendanaan, hingga pengawasan efektivitas kontrol keamanan.
2. **Independensi Fungsi Keamanan Siber**
   Unit keamanan siber harus independen dari fungsi pengembangan atau pengoperasian sistem, sebagaimana disyaratkan dalam standar OJK dan PBI, untuk mencegah konflik kepentingan.
3. **Integrasi dengan Manajemen Risiko dan Bisnis**
   Keamanan siber harus menjadi bagian dari strategi bisnis, proses operasional, dan perencanaan teknologi, bukan fungsi tambahan yang berdiri sendiri.
4. **Transparansi, Kepatuhan, dan Auditabilitas**
   Seluruh aktivitas keamanan harus dapat diaudit, sesuai regulasi OJK–BI dan standar internasional.
5. **Prinsip “Security by Design” dan “Zero Trust”**
   Seluruh sistem, aplikasi, API, dan layanan wajib dirancang dengan pendekatan keamanan sejak awal serta mengadopsi model zero trust dalam pengelolaan identitas dan akses.

2.2 Struktur Tata Kelola Keamanan Siber

Setiap anggota AFTECH harus memiliki struktur tata kelola keamanan siber yang jelas, proporsional, dan disesuaikan dengan kompleksitas model bisnis masing-masing. Struktur minimum mencakup:

1. **Manajemen Puncak (Direksi/CEO)**

   Bertanggung jawab menetapkan arah strategis keamanan siber, menyetujui kebijakan utama, menyediakan sumber daya, serta memastikan adanya mekanisme pengendalian dan pelaporan berkala.

   Tanggung jawab meliputi :
   a) menyetujui risk appetite dan risk tolerance keamanan siber di level perusahaan,
   b) menyetujui kebijakan keamanan siber,
   c) mengesahkan struktur organisasi serta memastikan memastikan independensi keamanan siber,
   d) memastikan pelaksanaan audit internal dan eksternal,
   e) menerima dan memastikan tindak lanjut laporan insiden siber oleh semua tim yang terlibat.

2. **Chief Information Security Officer (CISO)**

   Atau pejabat yang setara.

   Tanggung jawab meliputi:
   a) Memimpin dan mengelola program keamanan siber sesuai arah strategis Direksi.
   b) Mengawasi penerapan kebijakan dan standar keamanan siber yang telah disetujui manajemen puncak.
   c) Memastikan kontrol keamanan (teknis dan prosedural) berjalan efektif.
   d) Mengelola tim keamanan siber, termasuk SOC dan Incident Response.
   e) Melaporkan risiko dan insiden siber secara berkala kepada Direksi dan Dewan Pengawas, serta melaporkan kepada regulator sesuai ketentuan.
   f) Menjaga independensi fungsi keamanan siber dari pengembangan dan operasional TI.

3. **Unit Keamanan Siber / Cybersecurity Division**

   Unit ini bertanggung jawab menjalankan fungsi-fungsi teknis dan nonteknis keamanan, termasuk:
   a) Security Operations Center (SOC)
   b) Threat hunting & monitoring
   c) Identity & access management
   d) Vulnerability management
   e) Cloud & infrastructure security
   f) Incident response
   g) Cyber resilience & recovery

h) Governance, risk & compliance (GRC)

4. **Tim Tanggap Insiden Siber (Computer Security Incident Response Team – CSIRT)**

   CSIRT bertanggung jawab untuk:
   a) melakukan deteksi, analisis, isolasi, eradikasi, dan pemulihan insiden,
   b) melakukan triage dan eskalasi insiden,
   c) melakukan forensik terhadap insiden yang berdampak material,
   d) memberikan laporan insiden kepada manajemen dan regulator,
   e) menyusun lessons learned pasca insiden.
   Anggota CSIRT berasal dari berbagai fungsi seperti keamanan siber, infrastruktur TI, legal, komunikasi, dan manajemen risiko.

5. **Fungsi Audit Internal (Internal Audit)**

   Audit internal harus:
   a) independen dari unit TI dan unit keamanan siber,
   b) melakukan pemeriksaan berkala terhadap efektivitas kontrol keamanan,
   c) memverifikasi kepatuhan terhadap regulasi maupun standar bisnis yang berlaku termasuk namun tidak terbatas pada: OJK, BI, BSSN, UU PDP, dan pedoman AFTECH,
   d) melakukan audit insiden besar atau material.

6. **Komite Risiko / Komite Teknologi**

   Jika organisasi memiliki komite.
   Fungsi komite:
   a) mengevaluasi risiko siber,
   b) menilai efektivitas kontrol dan mitigasi,
   c) memberikan rekomendasi strategis kepada Direksi mengenai investasi keamanan, arsitektur TI, dan risiko pihak ketiga.

2.3 Kebijakan Keamanan Siber (Cybersecurity Policy Framework)

Kebijakan keamanan siber merupakan dokumen formal yang menjadi landasan seluruh penerapan keamanan.

Setiap anggota AFTECH minimal harus memiliki kebijakan berikut:

1. **Kebijakan Keamanan Siber Utama (Information & Cybersecurity Policy)**
   Berisi prinsip umum kontrol keamanan, struktur tata kelola, dan mandat CISO.
2. **Kebijakan Pengelolaan Akses (IAM Policy)**
   Meliputi RBAC/ABAC, MFA, manajemen identitas, privileged access, dan zero trust.
3. **Kebijakan Pengembangan Aplikasi (Secure SDLC Policy)**

Mewajibkan:
a) code review,
b) static/dynamic application security testing,
c) secure coding standard,
d) DevSecOps pipeline.

4. **Kebijakan Keamanan Data (Data Security & Privacy Policy)**
   Mencakup:
   a) klasifikasi data,
   b) enkripsi,
   c) data masking,
   d) pemusnahan data,
   e) data retention,
   f) perlindungan data pribadi sesuai UU PDP.

5. **Kebijakan Infrastruktur atau Cloud Security**
   Meliputi:
   a) konfigurasi cloud atau virtual machine,
   b) manajemen akses,
   c) shared responsibility model,
   d) audit secara berkala.

6. **Kebijakan Keamanan Jaringan**
   Termasuk firewall, IPS/IDS, segmentation, endpoint security, dan hardening.

7. **Kebijakan Manajemen Kerentanan dan Patching**
   Mencakup VA, pentesting, patch SLA, dan mekanisme prioritisasi.

8. **Kebijakan Manajemen Insiden (Incident Response Policy)**
   Harus mencakup indikator insiden material, alur pelaporan internal, eskalasi ke regulator, dan kolaborasi dengan AFTECH CSIRT.

9. **Kebijakan Keamanan Pihak Ketiga (Third Party Security Policy)**
   Mencakup:
   a) due diligence,
   b) SLA keamanan,
   c) pengawasan berkala,
   d) exit plan.

10. **Kebijakan Keamanan Khusus Produk Fintech**
    Opsional berdasarkan model bisnis, misalnya:
    a) kebijakan anti-fraud,
    b) anti-money laundering (AML),
    c) payment security,
    d) API security untuk open finance/open data.

e) Transfer dana (BI Fast, RTGS, SWIFT)

Semua kebijakan direview minimal setahun sekali atau ketika terjadi perubahan signifikan.

2.4 Strategi Keamanan Siber

Organisasi memiliki strategi keamanan siber jangka menengah (1–3 tahun) yang mencakup:

1. **Arah Strategis Keamanan Siber**
   a) penyelarasan keamanan dengan tujuan bisnis,
   b) prioritas kontrol berdasarkan risiko,
   c) target peningkatan maturitas keamanan.
   d) penyelarasan kebijakan keamanan dengan kebijakan internal lain yang terkait

2. **Peta Jalan (Roadmap) Keamanan Siber**
   Meliputi:
   a) penguatan tata kelola,
   b) implementasi teknologi keamanan,
   c) peningkatan SDM dan keamanan SDM;
   d) peningkatan monitoring & deteksi,
   e) peningkatan ketahanan operasional,
   f) penguatan program audit.

3. **Sumber Daya**
   a) anggaran tahunan keamanan,
   b) kebutuhan SDM,
   c) investasi teknologi keamanan (SIEM, IAM, SOAR, Phishing Simulator, dsb).

4. **KPI dan Indikator Keberhasilan**
   Contoh:
   a) waktu deteksi insiden (MTTD),
   b) waktu pemulihan insiden (MTTR),
   c) tingkat kepatuhan manajemen kerentanan,
   d) tingkat keberhasilan simulasi phishing dan/atau pengujian dengan skenario lain,
   e) peningkatan skor maturitas;
   f) peningkatan nilai Human Cybersecurity Awareness Index.

2.5 Budaya Keamanan Siber (Cybersecurity Culture)

Penerapan teknologi saja tidak cukup untuk mencapai ketahanan siber; diperlukan budaya organisasi yang menjunjung tinggi perilaku aman, etika digital, dan kesadaran risiko.

Sasaran Budaya keamanan siber/informasi adalah SDM dalam kendali organisasi/perusahaan menyadari dan memahami kebijakan dan standar keamanan yang diterapkan organisasi, kontribusi masing-masing terhadap efektifitas keamanan informasi, manfaat meningkatnya keamanan informasi, serta implikasi terhadap ketidakpatuhan terhadap kebijakan, standar, dan sistem keamanan informasi.

Program budaya keamanan siber meliputi:

1. Pelatihan dan Sertifikasi Pegawai

Wajib untuk seluruh karyawan:

- pelatihan keamanan siber berkala yang diintegrasikan ke dalam program pemeliharaan dan peningkatan wajib SDM,
- pelatihan anti-phishing,
- pelatihan spesifik untuk developer, engineer, dan analis.
- setiap karyawan yang bertanggung jawab pada (non)bidang IT sekurang-kurangnya memiliki sertifikasi CSCU (Certified Secure Computer User) (?)

Sertifikasi untuk personel teknis disarankan:
CEH, OSCP, CISSP, CISM, Security+, ISO 27001 LI dan/atau LA, ISO 27701 LI dan/atau LA, dsb.

2. Kampanye Awareness

a) security bulletin,
b) poster digital,
c) video edukasi,
d) kuis keamanan.

3. Simulasi dan Eksperimen Perilaku

a) phishing simulation,
b) social engineering test,
c) cybersecurity drill exercise,
d) table-top exercise.

4. Tata Kelola Whistleblowing

- Menyediakan jalur aman untuk pelaporan kelemahan keamanan atau potensi kebocoran internal.
- Memberikan apresiasi secara tertutup kepada para pelapor kelemahan keamanan atau potensi kebocoran internal

5. Evaluasi Kepatuhan Individu

Bagian dari KPI karyawan:

a) kepatuhan kebijakan,
b) hasil simulasi phishing (dapat berupa Human Cybersecurity Risk Index),
c) perilaku penggunaan perangkat pribadi (BYOD).

2.6 Pelaporan dan Eskalasi

Agar tata kelola berjalan efektif, penyelenggara Fintech wajib menerapkan mekanisme pelaporan, yaitu:

1. Laporan Berkala kepada Manajemen

Minimal setiap bulan atau kuartal:

a) metrik keamanan,
b) status risiko siber,
c) *Human Cybersecurity Risk Index*,
d) hasil monitoring dan audit,
e) laporan insiden dan remedi.

2. Laporan Insiden Material

Insiden signifikan harus dilaporkan sesuai regulasi yang berlaku, sebagai contoh namun tidak terbatas kepada:

a) OJK (jika Penyelenggara ITSK)
b) Bank Indonesia (untuk PJP/PIP)
c) BSSN
d) Aparat penegak hukum (jika menyangkut kriminal siber)
e) AFTECH-CSIRT untuk kolaborasi industri (opsional, namun direkomendasikan).

2.7 Evaluasi dan Audit Tata Kelola

Organisasi wajib melakukan audit tata kelola untuk memverifikasi efektivitas penerapan kebijakan, kontrol, dan struktur keamanan.

Audit mencakup:

a) audit kebijakan dan kepatuhan,
b) audit konfigurasi teknis,
c) audit pihak ketiga,
d) audit manajemen risiko,
e) audit insiden siber.

Audit dilakukan oleh:

a) tim internal audit, dan/atau
b) auditor eksternal independen.

Frekuensi audit minimum: setahun sekali atau sesuai regulasi yang berlaku.

BAB 3
MANAJEMEN RISIKO SIBER

Manajemen Risiko Siber merupakan proses sistematis untuk mengidentifikasi, menganalisis, menilai, memitigasi, dan memantau risiko siber yang dapat berdampak pada kelangsungan layanan, perlindungan data pengguna, dan stabilitas ekosistem Fintech. Pendekatan berbasis risiko (risk-based approach) adalah landasan penting bagi anggota AFTECH untuk menerapkan kontrol keamanan yang tepat, efektif, dan proporsional sesuai model bisnis masing-masing.

Bab ini memuat kerangka manajemen risiko siber yang sebaiknya diterapkan oleh setiap anggota AFTECH.

3.1 Prinsip Manajemen Risiko Siber

Penerapan manajemen risiko siber mengacu pada prinsip-prinsip berikut:

1. **Relevan dengan Bisnis**
   Proses penilaian risiko harus mencerminkan karakteristik produk, model bisnis, teknologi, data, dan konsumen yang dilayani.
2. **Risiko sebagai Dasar Kontrol**
   Setiap kontrol keamanan ditentukan berdasarkan tingkat risiko, bukan sekadar daftar pemeriksaan formal.
3. **Proporsional & Adaptif**
   Risiko harus dikelola dengan skala yang sesuai dengan ukuran organisasi, kompleksitas sistem, serta pertumbuhan teknologi.
4. **Berkesinambungan**
   Risiko harus dievaluasi dan diperbaharui secara berkala, mengikuti perubahan ancaman, teknologi, dan regulasi.
5. **Akuntabilitas**
   Manajemen puncak bertanggung jawab atas keputusan pengelolaan risiko dan alokasi sumber daya untuk mitigasi.

3.2 Kerangka Manajemen Risiko Siber (Cyber Risk Management Framework)

Kerangka manajemen risiko ini terdiri atas lima tahapan utama:

1. Identifikasi Aset dan Lingkungan Teknologi
2. Identifikasi Ancaman dan Kerentanan
3. Penilaian dan Pengukuran Risiko
4. Perlakuan Risiko (Risk Treatment)
5. Pemantauan dan Review Risiko

Kerangka ini selaras dengan ISO 27005 dan NIST Risk Management Framework (RMF).

3.3 Identifikasi Aset (Asset Identification)

Penyelenggara Fintech direkomendasikan memiliki inventaris lengkap yang selalu diupdate terhadap seluruh aset informasi, yang meliputi:

1. Aset Data

Seluruh data operasional yang dikelola Fintech, dengan metadata berikut:

a) Lokasi: database, object storage, backup, atau archive
b) Pemilik data: data owner per domain (misal: Head of Product, Head of Operations)
c) Klasifikasi: confidential / restricted / internal / public
d) Format data: structured (DB), semi-structured (JSON), unstructured (file)
e) Retensi: masa simpan & kebijakan pemusnahan

Contoh jenis aset data:

a) Data pribadi pengguna
b) Data transaksi
c) Data sensitif perusahaan
d) API data dan metadata

2. Aset Sistem dan Aplikasi

Setiap sistem memiliki metadata berikut:

a) Lokasi deployment: on-prem, cloud, container, kubernetes, dll
b) Pemilik layanan (service owner): individu atau tim yang bertanggung jawab
c) Environment: production / staging / development
d) Versi aplikasi & build ID
e) Klasifikasi: internal / confidential / internal / public
f) Hak akses: admin, operator, read-only
g) Integrasi: aplikasi terkait atau dependency yang digunakan

Contoh jenis aset:

a) Mobile apps
b) Backend services
c) APIs
d) Core Fintech system
e) Third-party modules

3. Infrastruktur TI

Setiap aset infrastruktur dicatat dengan metadata:

a) Lokasi fisik atau region cloud
b) Jenis resource: compute, storage, database, load balancer, dll
c) Kapasitas & spesifikasi teknis
d) Klasifikasi sensitivitas
e) Status operasional: aktif, tidak aktif, deprecated
f) Pemilik infrastruktur: tim DevOps / Infra
g) Criticality level: critical / important / supporting

Contoh jenis aset:

a) Server on-premise
b) Cloud infrastructures (IaaS/PaaS/SaaS)
c) Container & Kubernetes
d) Database
e) Storage

4. Aset Jaringan

Setiap aset jaringan memiliki metadata:

a) Lokasi jaringan / segmentasi: DMZ, internal, restricted
b) Pemilik jaringan: Network/Security team
c) Klasifikasi: internal / restricted
d) Rule set / konfigurasi dasar
e) Endpoint atau akses publik
f) Status & versi konfigurasi

Contoh jenis aset:

a) VPN
b) Firewall
c) Load balancer
d) IDS/IPS
e) CDN

5. Aset Manusia

Aset manusia direkam berdasarkan peran dan hak akses, dengan metadata:

a) Role pengguna: admin, developer, operator, CS, vendor
b) Privileged access: ada / tidak
c) Sistem yang dapat diakses
d) Status akses: aktif, suspend, offboard
e) Kontrak & masa berlaku (untuk vendor/contractor)
f) Departemen pemilik user

Contoh jenis aset:

a) Administrator
b) Developer
c) CS/operation
d) Vendor
e) Contractor

6. Aset Proses

Setiap proses dicatat dengan metadata berikut:

a) Pemilik proses (process owner)
b) Lokasi dokumen (nama file, path, atau URL)
c) Tanggal pembuatan dan revisi terakhir
d) Status validasi: aktif / perlu review
e) Klasifikasi: internal / confidential
f) Ruang lingkup & keterkaitan proses lain

Contoh jenis aset:

a) SOP operasional
b) SOP fraud
c) SOP insiden
d) SOP keamanan data

Setiap aset harus diklasifikasikan berdasarkan nilai dan tingkat sensitivitas.

3.4 Identifikasi Ancaman dan Kerentanan

1. Ancaman Siber (Threats)

Meliputi:

a) Ransomware, malware, trojan
b) Phishing & social engineering
c) Eksploitasi API dan aplikasi
d) Kebocoran data (data breach)
e) Insider threat
f) Supply chain attack
g) Credential stuffing
h) Serangan DDoS
i) Zero-day exploit
j) Fraud berbasis digital

2. Kerentanan (Vulnerabilities)

Meliputi:

a) Konfigurasi salah (misconfiguration)
b) Weak authentication
c) Dependencies rentan
d) Kode tidak aman
e) Infrastruktur cloud tidak terproteksi
f) Patch tidak diperbarui
g) Akses berlebih
h) Kontrol jaringan lemah
i) Eksposur data yang tidak terenkripsi

Setiap kerentanan harus dipadankan dengan aset terkait menggunakan metode mapping asset → vulnerability → threat.

3.5 Penilaian Risiko (Risk Assessment)

Setiap risiko dihitung dengan mempertimbangkan dua faktor:

1. Dampak (Impact)

Menilai akibat jika serangan terjadi. Dampak bisa berupa:

a) kerugian finansial,
b) gangguan operasional,
c) kerusakan infrastruktur,
d) pelanggaran data pribadi,

e) kerusakan reputasi,
f) pelanggaran regulasi.

Kategori dampak: rendah, sedang, tinggi, kritis.

2. Kemungkinan (Likelihood)

Seberapa besar risiko tersebut dapat terjadi, berdasarkan:

a) sejarah insiden,
b) eksposur aset,
c) kerentanan yang belum ditutup,
d) kecanggihan pelaku ancaman.

Kategori kemungkinan: jarang, cukup sering, sering, sangat sering.

3. Tingkat Risiko (Risk Level)

Dihitung dengan formula:

Risk Level = Impact × Likelihood

Hasilnya dikategorikan menjadi:

a) Low
b) Medium
c) High
d) Critical

Rekomendasi: Risiko High dan Critical wajib segera dimitigasi.

3.6 Perlakuan Risiko (Risk Treatment)

Setiap risiko memiliki empat opsi utama:

1. Mitigasi (Mitigate)

Menurunkan risiko dengan menerapkan kontrol teknis, administratif, atau fisik.
Contoh:

a) enkripsi data,
b) MFA,
c) WAF,
d) patching cepat,
e) API authentication.

2. Penghindaran (Avoid)

Menghapus proses atau fitur yang menciptakan risiko terlalu besar.
Contoh:

a) menonaktifkan API publik yang tidak diperlukan,
b) menghindari penyimpanan data sensitif tertentu.

3. Transfer (Transfer)

Memindahkan sebagian risiko kepada pihak lain.
Contoh:

a) cyber insurance,
b) outsourcing layanan keamanan,
c) cloud shared responsibility.

4. Penerimaan (Accept)

Risiko diterima jika:

a) tingkatnya rendah,
b) mitigasi terlalu mahal dibanding nilai aset,
c) tidak berdampak pada kepatuhan atau data pribadi.

Rekomendasi: Setiap keputusan harus disetujui oleh manajemen puncak dan didokumentasikan dalam Risk Register.

3.7 Kontrol Keamanan untuk Mitigasi Risiko

Kontrol mitigasi risiko mencakup area berikut:

1. Kontrol Teknologi

a) firewall, IDS/IPS, WAF
b) endpoint protection
c) SIEM & SOC monitoring
d) vulnerability scanner
e) API gateway
f) IAM dan PAM
g) enkripsi data

2. Kontrol Proses

a) SOP insiden
b) SOP change management
c) SOP backup dan restore
d) SOP cloud security
e) pengelolaan logging dan monitoring
f) prosedur pengendalian akses

3. Kontrol Sumber Daya Manusia

a) pelatihan keamanan
b) kebijakan penggunaan perangkat
c) prosedur rekrutmen dan offboarding
d) role-based access control

4. Kontrol Pihak Ketiga

a) vendor due diligence
b) SLA keamanan
c) kontrol integrasi API

d) audit pihak ketiga
e) exit plan

3.8 Pemantauan Risiko (Risk Monitoring)

Organisasi direkomendasikan untuk memantau risiko secara berkala melalui:

1. Monitoring Harian dan Real-Time

a) alert SOC (Security Operation Center)
b) anomali trafik API
c) deteksi fraud
d) pemantauan cloud misconfiguration

2. Review Mingguan/Bulanan

a) vulnerability backlog
b) status patching
c) perubahan infrastruktur
d) status pengendalian akses

3. Pemutakhiran Penilaian Risiko

Dilakukan:

a) minimal setiap tahun, atau
b) saat terjadi perubahan besar (fitur baru, migrasi cloud, integrasi API).

4. Dashboard Risiko Siber

Berisi:

a) tingkat risiko per aset
b) risiko terbuka (open risk)
c) risiko kritikal
d) tren insiden
e) rekomendasi mitigasi
f) status kepatuhan

Dashboard dilaporkan kepada Direksi atau Komite Risiko.

3.9 Pelaporan Risiko Siber

Pelaporan internal dan eksternal mencakup:

1. Laporan Internal ke Manajemen

Minimal setiap kuartal:

a) top 10 risiko utama,
b) risiko kritikal yang belum dimitigasi,
c) rekomendasi,
d) insiden signifikan,
e) perubahan eksposur ancaman.

2. Laporan Kepada Regulator

Sesuai dengan regulator yang menaungi masing - masing bisnis:

a) OJK
b) BI
c) Komdigi
d) BSSN (kategori insiden nasional),
e) AFTECH Cyber Coordination (opsional tetapi direkomendasikan).

3.10 Risk Register dan Dokumentasi

Setiap organisasi direkomendasikan mempunyai dan melakukan update secara berkala dokumentasi sebagai berikut:

1. Aset Register
2. Threat & Vulnerability Mapping
3. Risk Assessment Document
4. Risk Treatment Plan
5. Risk Acceptance Form
6. Risk Register (Master)
7. Incident Log & Evidence
8. Third-Party Risk File

Dokumentasi harus dijaga akurasinya dan siap diperiksa oleh auditor internal/eksternal.

3.11 Integrasi Risiko Siber dengan Enterprise Risk Management (ERM)

Risiko siber harus menjadi bagian integral dari ERM perusahaan, meliputi:

a) risiko operasional,
b) risiko teknologi,
c) risiko kepatuhan,
d) risiko reputasi,
e) risiko strategis.

Penyampaian risiko siber dalam rapat komite risiko wajib menggunakan bahasa bisnis yang dipahami manajemen agar keputusan mitigasi dapat dilakukan lebih cepat dan efektif.

3.12 Tingkat Maturitas Manajemen Risiko Siber

Organisasi harus menilai maturitas manajemen risikonya berdasarkan:

1. Basic —> risk register sederhana, belum terintegrasi.
2. Defined —> proses formal dan terdokumentasi.
3. Managed —> telah berjalan konsisten.
4. Integrated —> risiko siber terhubung dengan ERM.
5. Optimized —> risk-informed decision making & automation.

BAB 4
PELINDUNGAN DATA & KEAMANAN INFORMASI

Pelindungan Data & Keamanan Informasi, ditulis lengkap, formal, sistematis, dan selaras dengan:

1. UU PDP,
2. POJK/SEOJK Keamanan Siber,
3. PBI 2/2024 tentang Keamanan Sistem Informasi & Ketahanan Siber,
4. ISO 27001, ISO 27701,
5. NIST Cybersecurity Framework,
6. praktik terbaik global (OWASP, CIS Controls).

Pelindungan data dan keamanan informasi merupakan fondasi utama dalam menjaga kepercayaan konsumen, kelangsungan bisnis, serta peran Fintech dalam ekosistem keuangan digital nasional. Setiap anggota AFTECH direkomendasikan menerapkan perlindungan data menyeluruh yang mencakup kebijakan, proses, kontrol teknis, serta mekanisme pemantauan dan audit yang sejalan dengan ketentuan perundang-undangan dan standar global.

Bab ini menetapkan prinsip, mekanisme, dan kontrol wajib terkait pelindungan data dan keamanan informasi pada penyelenggara Fintech.

4.1 Prinsip Pelindungan Data dan Keamanan Informasi

Setiap penyelenggara wajib menerapkan prinsip berikut:

1. **Confidentiality (Kerahasiaan)**
   Data hanya dapat diakses oleh pihak yang berwenang dengan mekanisme autentikasi dan otorisasi yang kuat.
2. **Integrity (Integritas)**
   Data harus terlindungi dari perubahan yang tidak sah dan tetap konsisten selama siklus hidupnya.
3. **Availability (Ketersediaan)**
   Data dan sistem harus dapat diakses sesuai kebutuhan operasional tanpa gangguan yang tidak semestinya.
4. **Privacy by Design & Privacy by Default**
   Setiap fitur, produk, dan arsitektur sistem wajib memasukkan pengamanan privasi sejak tahap perancangan.
5. **Minimal Data Principle**
   Hanya data yang diperlukan untuk layanan yang boleh dikumpulkan, disimpan, dan diproses.
6. **Zero Trust Architecture**
   Tidak ada entitas—internal atau eksternal—yang otomatis dipercaya tanpa verifikasi berlapis.

7. **End-to-End Security**
   Data harus terlindungi dalam seluruh siklus hidup: pengumpulan, penyimpanan, pemrosesan, transfer, dan pemusnahan.

4.2 Klasifikasi Data dan Sistem Informasi

Setiap anggota AFTECH direkomendasikan untuk memetakan dan mengklasifikasikan data berdasarkan tingkat sensitivitas:

1. **Data Sangat Sensitif**
   a) Data pribadi spesifik (biometrik, identitas unik)
   b) Data finansial, nomor rekening
   c) Authentication secrets (OTP, token kriptografi)
2. **Data Sensitif**
   a) Identitas pribadi dasar
   b) Data transaksi
   c) Informasi pengguna yang dapat menimbulkan risiko fraud
3. **Data Internal**
   a) Dokumentasi teknis
   b) SOP
   c) Data operasional non-pribadi
4. **Data Publik**
   Informasi yang dapat diakses publik secara legal

Setiap kategori memiliki kontrol minimum yang berbeda, termasuk:

a) tingkat enkripsi,
b) akses,
c) retensi,
d) durasi penyimpanan,
e) persetujuan pengguna, dan
f) persyaratan audit.

4.3 Pengamanan Data (Data Protection Controls)

Untuk menjaga keamanan data, organisasi dapat menerapkan kontrol berikut:

1. **Enkripsi**
   a) Data at-rest harus dienkripsi minimal menggunakan AES-256.
   b) Data in-transit wajib dienkripsi menggunakan TLS 1.2/1.3.
   c) Kunci enkripsi dikelola melalui KMS (Key Management System).

2. **Data Masking & Tokenization**
   Untuk data sensitif, harus dilakukan:
   a) Masking untuk tampilan antarmuka,
   b) Tokenization untuk penyimpanan atau pemrosesan di pihak ketiga.

3. **Data Loss Prevention (DLP)**
   Mencegah kebocoran internal/eksternal yang selaras dengan klasifikasi informasi dan daftar aktivitas pemrosesan data pribadi pada sistem, jaringan, maupun perangkat lain yang mengolah, menyimpan, ataupun mentransmisikan informasi sensitif/rahasia, melalui:
   a) inspeksi email,
   b) pemantauan transfer data,
   c) pemblokiran akses tidak sah.

4. **Secure Data Storage**
   a) Tidak menyimpan data kredensial dalam clear text,
   b) Backup terenkripsi,
   c) Isolasi database per lingkungan.

4.4 Pengamanan Aplikasi (Application Security)

Keamanan aplikasi diwajibkan mengikuti prinsip Secure SDLC.

1. **Secure Development Lifecycle (SDLC)**
   Meliputi:
   a) threat modeling,
   b) secure coding guideline (OWASP),
   c) code review,
   d) SAST & DAST,
   e) DevSecOps automation.

2. **API Security**
   a) autentikasi API wajib menggunakan OAuth 2.0/OpenID Connect,
   b) rate limiting,
   c) input validation,
   d) API gateway sebagai kontrol utama,
   e) hanya membuka endpoint yang diperlukan.

3. **Proteksi dari Kerentanan dengan referensi kerangka kerja keamanan siber seperti OWASP Top 10**
   Mampu mengatasi risiko seperti:
   a) injection,
   b) broken authentication,
   c) broken access control,
   d) insecure deserialization,
   e) SSRF, dan lainnya.

4.5 Keamanan Infrastruktur dan Jaringan

Setiap anggota AFTECH direkomendasikan menjaga keamanan infrastruktur dengan kontrol berikut:

1. **Network Segmentation**

a) Memisahkan lingkungan production, staging, dan development.
b) Memisahkan database network dari jaringan aplikasi dan user.
c) Menggunakan admin/management network khusus dengan akses terbatas.
d) Menerapkan access control list (ACL) dan aturan isolasi antar-segmen.
e) Menggunakan bastion host untuk seluruh akses administratif.
f) Mengaktifkan logging dan monitoring di seluruh jalur antar-segmen.

2. Firewall & IDS/IPS

a) Menggunakan firewall berlapis (edge, internal, WAF).
b) Menerapkan kebijakan deny-by-default dan membuka port secara selektif.
c) Menggunakan IDS/IPS untuk mendeteksi anomali dan serangan jaringan.
d) Mengaktifkan blocking otomatis terhadap aktivitas mencurigakan berulang.
e) Melakukan review berkala terhadap konfigurasi firewall dan rule set.
f) Mengintegrasikan log firewall/IDS/IPS ke dalam SIEM.

3. Zero Trust Network Access (ZTNA)

a) Tidak ada segmen jaringan yang otomatis dipercaya.
b) Setiap akses divalidasi dengan MFA dan kebijakan berbasis identitas.
c) Menerapkan prinsip least privilege untuk semua user dan sistem.
d) Menggunakan ZTNA atau VPN dengan enkripsi end-to-end untuk akses remote.
e) Memverifikasi kondisi perangkat sebelum memberikan akses (device compliance).
f) Melakukan continuous verification terhadap sesi yang sedang aktif.

4. Endpoint Security

a) Menggunakan EDR/XDR untuk deteksi dan respons ancaman pada perangkat.
b) Mengaktifkan anti-malware dan proteksi anti-ransomware.
c) Melakukan device integrity check (root/jailbreak, OS patch level).
d) Menerapkan full-disk encryption pada perangkat yang memiliki akses sensitif.
e) Melakukan patching secara berkala dari sumber yang dipercaya untuk OS dan aplikasi.
f) Membatasi penggunaan USB/removable media pada perangkat operasional.

4.6 Keamanan Cloud (Cloud Security)

Apabila menggunakan cloud computing, direkomendasikan untuk melakukan pengamanan dengan standar sebagai berikut:

1. Konfigurasi Keamanan Cloud

- least privilege IAM,
- disable public bucket,
- logging wajib aktif,
- deteksi misconfiguration otomatis melalui CSPM.

2. **Shared Responsibility Model**
   Penyelenggara wajib memahami perbedaan tanggung jawab antara:
   - cloud provider,
   - aplikasi internal,
   - admin organisasi.

3. **Keamanan Container & Kubernetes**
   - image scanning,
   - secrets management,
   - pod security policies,
   - RBAC Kubernetes.

4. **Keamanan Konfigurasi & patching**
   - pemeliharaan dan pengujian konfigurasi
   - pemeliharaan dan pengujian patching termasuk penilaian dampaknya terhadap operasional sistem/aplikasi/layanan

5. **Klausul exit atau pemberhentian penggunaan layanan cloud**
   - memiliki perjanjian untuk menetapkan, memonitor, mengevaluasi, dan memberhentikan penggunaan layanan cloud (jika diijinkan regulasi)

4.7 Manajemen Akses dan Identitas (IAM)

Pengamanan identitas yang direkomendasikan adalah sebagai berikut:

1. **Multi-Factor Authentication**
   Untuk diterapkan kepada:
   - admin,
   - developer,
   - akses portal produksi,
   - akses cloud,
   - pengguna dengan aset sensitif.

2. **Principle of Least Privilege**
   Akses hanya diberikan sesuai tugas dari individu dan dievaluasi berkala.

3. **Privileged Access Management (PAM)**
   Untuk akses super-admin atau root:
   - approval workflow,
   - session recording,

- password rotation otomatis.

4. **Lifecycle Management**
   Diimplementasikan untuk proses:
   - onboarding,
   - role transfer,
   - offboarding cepat (dalam <24 jam).

4.8 Pengelolaan Data Pribadi (Privacy Management)
Seluruh anggota wajib mematuhi UU Perlindungan Data Pribadi (UU PDP).
Kontrol minimum:

1. **Dasar Pemrosesan Data**
   - persetujuan,
   - perjanjian,
   - kewajiban hukum,
   - kepentingan sah.

2. **Hak Subjek Data**
   Termasuk:
   - hak akses,
   - hak perbaikan,
   - hak penghapusan,
   - hak pembatasan pemrosesan.

3. **Data Processing Record**
   Direkomendasikan untuk mencatat:
   - kategori data,
   - tujuan pemrosesan,
   - pihak ketiga penerima data,
   - durasi penyimpanan.

4. **Pelaporan Pelanggaran Data**
   Insiden kebocoran data harus dilaporkan kepada:
   - pemilik data,
   - regulator (OJK/BI/BSSN sesuai yurisdiksi), dalam batas waktu sesuai ketentuan.

4.9 Retensi dan Pemusnahan Data
Setiap organisasi direkomendasikan memiliki kebijakan retensi data yang mencakup:

1. **Retensi Berdasarkan Regulasi**
   Contoh:
   - Data transaksi biasanya wajib disimpan 5 tahun atau sesuai dengan peraturan yang berlaku
   - Data pribadi tidak boleh disimpan melebihi tujuan pemrosesan.

2. **Pemusnahan Data**
   Dilakukan secara aman melalui:
   - secure wipe,
   - cryptographic erasure,
   - prosedur audit trail.

3. **Backup & Recovery**
   Backup dilakukan secara:
   - terenkripsi,
   - diuji recovery secara berkala,
   - disimpan di lokasi berbeda (offsite/DR center).

4.10 Logging, Monitoring, dan Audit Keamanan

Organisasi wajib memastikan seluruh aktivitas yang berdampak pada keamanan terekam dan dianalisis.

1. **Logging**
   Mencatat:
   - login/logoff,
   - perubahan konfigurasi,
   - akses ke data sensitif,
   - anomali trafik API.

2. **Monitoring**
   - SOC harus memonitor real-time,
   - SIEM wajib mengkonsolidasi log,
   - alert anomali ditindak cepat.

3. **Audit Trail**
   Perlakuan terhadap log:
   - tidak boleh dimodifikasi,
   - disimpan dalam durasi yang ditentukan,
   - harus dapat diaudit oleh otoritas terkait.

4.11 Keamanan dalam Siklus Hidup Data (Data Lifecycle Security)

Keamanan data harus dijaga dari awal hingga akhir dengan ruang lingkup:

1. **Pengumpulan Data**
   - minimasi data (collect only necessary data),
   - transparansi kepada pengguna.

2. **Penyimpanan & Pemrosesan**
   - enkripsi,
   - akses terbatas,
   - pemantauan.

3. **Distribusi/Transfer**
    - gunakan kanal terenkripsi,
    - batasi akses berdasarkan kebutuhan.

4. **Pemusnahan**
    - prosedur pemusnahan formal,
    - audit bukti pemusnahan.

4.12 Pengamanan Terhadap Regulasi dan Audit Eksternal

Organisasi wajib memastikan kesiapan audit untuk terhadap regulasi yang berlaku. Sebagai contoh:

- OJK (ITSK, inovasi keuangan digital),
- Bank Indonesia (PJP/PIP),
- BSSN (insiden siber),
- KPI UU PDP (jika berlaku),
- Pengguna jasa internal audit, eksternal audit, dan independent assessor.

Dokumen dan bukti teknis harus siap sewaktu-waktu.

BAB 5
TANGGAP INSIDEN SIBER
(INCIDENT RESPONSE & CSIRT)

TANGGAP INSIDEN SIBER (INCIDENT RESPONSE & CSIRT) secara penuh, komprehensif, dan siap implementasi, selaras dengan:

- SEOJK 29/2022 – Ketahanan Siber,
- OJK ITSK,
- PBI 2/2024 (KKS BI),
- Standar NIST SP 800-61 (Computer Security Incident Handling Guide),
- ISO 27035 (Incident Management),
- BSSN Panduan IR Nasional (Peraturan BSSN Nomor 1 Tahun 2024 tentang Pengelolaan Insiden Siber).

Tanggap Insiden Siber (Incident Response - IR) adalah proses sistematis untuk mendeteksi, menganalisis, mengendalikan, memitigasi, dan memulihkan insiden siber yang dapat mengganggu layanan Fintech, menyebabkan kebocoran data, atau menimbulkan risiko sistemik terhadap ekosistem keuangan digital nasional.

Setiap anggota AFTECH sangat direkomendasikan mengimplementasikan mekanisme tanggap insiden yang efektif, terdokumentasi, dan diaudit secara berkala.

5.1 Tujuan dan Prinsip Tanggap Insiden Siber

Tujuan

1. Meminimalkan dampak operasional, finansial, hukum, dan reputasi.
2. Mengembalikan layanan secepat mungkin.
3. Mencegah perluasan insiden dan serangan berulang.
4. Mematuhi kewajiban pelaporan regulator dan UU PDP.
5. Menghasilkan bukti yang valid untuk investigasi hukum.
6. Mendukung kolaborasi industri dan AFTECH-CSIRT.

Prinsip

- Cepat dan Tepat – deteksi dini dan respon awal sangat menentukan.
- Terdokumentasi – seluruh langkah harus memiliki audit trail.
- Terkoordinasi – multi-unit (IT, keamanan, legal, PR, manajemen).
- Berdasarkan Risiko – prioritas sesuai dampak bisnis dan data.
- Forensik dan Bukti Digital – menjaga chain of custody.
- Continuous Improvement – lessons learned wajib dilakukan.

5.2 Struktur Tim Tanggap Insiden Siber (CSIRT)

Setiap anggota AFTECH direkomendasikan membentuk CSIRT internal atau menunjuk pihak ketiga yang kompeten dengan SLA tertentu.

Komposisi CSIRT direkomendasikan namun tidak terbatas pada:

- **Incident Commander (IC)**
  - Biasanya CISO atau pejabat keamanan senior.
  - Bertanggung jawab pada keseluruhan manajemen insiden.
- **Security Operations (SOC Team)**
  - Melakukan deteksi, analisis, dan triase.
- **Forensic & Malware Analyst**
  - Melakukan investigasi digital, bukti, dan identifikasi akar masalah.
- **Infrastructure/DevOps Responder**
  - Menangani isolasi sistem, patching, rollback, backup.
- **Application Security & Developer**
  - Memperbaiki kerentanan aplikasi/API.
- **Legal & Compliance Officer**
  - Menilai kewajiban pelaporan ke regulator.
- **Communication & PR Officer**
  - Menangani komunikasi internal–publik.
- **Management Representative**
  - Memberi otorisasi keputusan strategis (shutdown, cut-off, dll).

5.3 Klasifikasi Insiden Siber

Untuk memastikan respons yang efektif, insiden diklasifikasikan sebagai berikut:

Level 1 — Minor

- Malware low-risk, tanpa dampak operasional.
- Upaya phishing tanpa kompromi akun.
- Anomali trafik yang tidak berdampak.

Level 2 — Moderate

- Akun pegawai dikompromi.
- Serangan DDoS dengan dampak sementara.
- Kerentanan kritis ditemukan pada sistem produksi.

Level 3 — Major

- Gangguan layanan signifikan (> 30 menit).
- Fraud digital yang berdampak finansial.
- Eksposur data pengguna berskala terbatas.

Level 4 — Critical / Material Breach

- Kebocoran data pribadi dalam jumlah besar.
- Serangan ransomware yang mengganggu layanan.
- Compromise sistem pembayaran atau API kritikal.

- Gangguan operasional besar dengan potensi risiko sistemik.

Kategori Level 4 - Critical / Material Breach dilaporkan ke regulator (OJK/BI/BSSN) dalam waktu tertentu sesuai dengan peraturan yang berlaku.

5.4 Tahapan Tanggap Insiden (Incident Response Lifecycle)

Mengikuti standar NIST SP 800-61 dan ISO 27035, proses IR terdiri dari enam tahap:

1. **Preparasi (Preparation)**

   Organisasi wajib memiliki:
   - Kebijakan IR,
   - SOP insiden,
   - Playbook khusus (ransomware, phishing, fraud, API breach),
   - Kontak darurat,
   - Tools IR: SIEM, EDR, SOAR, log server, forensic tools,
   - Latihan berkala: tabletop exercise, simulation drill, blue vs red team.

2. **Deteksi & Identifikasi (Detection & Identification**

   Sumber deteksi:
   - SOC alerts,
   - SIEM logs,
   - EDR/XDR,
   - User reports,
   - Third-party notifications,
   - Darkweb monitoring.

   Verifikasi awal dilakukan dengan:
   - Analisis log,
   - Korelasi event,
   - Penelusuran IOC (Indicators of Compromise).

   Output tahap ini:
   - Kode insiden,
   - Level insiden,
   - Scope awal (sistem, data, pengguna yang terdampak).

3. **Isolasi & Kontainmen (Containment)**

   Tindakan cepat untuk mencegah eskalasi:
   - blokir akun,
   - isolasi server,
   - putuskan koneksi jaringan tertentu,
   - shutdown layanan tertentu,
   - menerapkan rule firewall/WAF baru,
   - memblokir token API/credential yang bocor.

Harus mempertimbangkan:

- continuity business,
- risiko hilangnya bukti forensik.

4. **Eradikasi (Eradication)**
   Tujuan: membersihkan ancaman dari lingkungan produksi.
   Contoh tindakan:
   - menghapus malware/backdoor,
   - patching kerentanan zero-day,
   - menghapus file jahat,
   - perbaikan konfigurasi cloud/jaringan,
   - reset password dan token sensitif.

5. **Pemulihan (Recovery)**
   Mengembalikan layanan ke kondisi normal dengan aman:
   - restore dari backup yang bersih,
   - monitoring intensif pasca recovery,
   - re-enable layanan secara bertahap,
   - pemulihan data transaksional,
   - validasi integritas sistem,
   - post-publish testing untuk aplikasi.

   Catatan: Sistem hanya boleh kembali aktif setelah mendapat persetujuan Incident Commander.

6. **Lessons Learned & Reporting**
   Dilakukan dalam waktu maksimal 7–14 hari setelah insiden selesai.
   Hasilnya:
   - laporan kronologi lengkap,
   - akar penyebab (root cause analysis),
   - daftar perbaikan jangka pendek/panjang,
   - update kebijakan dan SOP,
   - rekomendasi untuk CSIRT dan SOC.

   Ini menjadi dasar peningkatan kebijakan dan penguatan sistem.

5.5 Playbook Insiden Wajib (Mandatory Incident Playbooks)

Setiap anggota AFTECH direkomendasikan memiliki playbook minimal untuk:

1. **Phishing dan Social Engineering Attack**
   - deteksi cepat,
   - blokir domain/email,
   - edukasi pengguna.

2. **Ransomware Attack**
    - isolasi total,
    - identifikasi strain,
    - dekripsi (jika tersedia),
    - keputusan business cut-off.

3. **Fraud Digital dan Akun Kompromi**
    - freeze akun,
    - rollback transaksi (jika memungkinkan),
    - investigasi anomaly.

4. **API/Data Breach**
    - isolate endpoint,
    - audit log,
    - notifikasi regulator dan pengguna.

5. **DDoS Attack**
    - aktivasi mitigasi,
    - CDN/WAF rerouting,
    - kerja sama ISP.

6. **Cloud Misconfiguration**
    - memperbaiki konfigurasi IAM,
    - menutup akses publik,
    - rotate keys.

5.6 Mekanisme Pelaporan Insiden Kepada Regulator

Kewajiban pelaporan mengikuti kerangka sesuai ketentuan berlaku. Sebagai contoh:

- OJK ITSK (jika Fintech terdaftar/berizin),
- SEOJK 29/2022 (kategori insiden material),
- PBI KKS BI (PJP, PIP, PUVA),
- UU PDP (pelanggaran data pribadi),
- BSSN (insiden terkait infrastruktur nasional).

Isi Minimum Laporan Insiden

1. Waktu awal terdeteksi
2. Jenis insiden
3. Level insiden
4. Sistem terdampak
5. Estimasi data pengguna terdampak
6. Dampak operasional
7. Tindakan mitigasi sementara
8. Rencana pemulihan
9. Status pemulihan

10. Langkah preventif jangka panjang

Waktu Pelaporan (secara umum)

- Insiden kritikal → ≤ 24 jam
- Kebocoran data pribadi → sesuai UU PDP
- Insiden material → mengikuti SEOJK dan PBI

5.7 Kolaborasi Industri: AFTECH-CSIRT Coordination Hub

Untuk memperkuat ekosistem Fintech nasional, AFTECH dapat membangun ataupun bekerjasama dengan pihak terkait seperti BSSN untuk Cyber Coordination Hub yang berfungsi:

1. Threat Intelligence Sharing

- IOC, pattern attack, IP jahat, domain phishing, dsb.

2. Early Warning System

Memberikan peringatan kepada anggota jika ada:

- kerentanan kritis,
- serangan aktif,
- kampanye penipuan.

3. Incident Collaboration

Bantuan lintas organisasi ketika:

- serangan terjadi secara masif,
- berdampak sistemik.

4. Standard Response Framework

Menjaga keselarasan respons industri.

5.8 Persyaratan Audit & Evaluasi IR

Setiap organisasi direkomendasikan untuk:

1. **Mengevaluasi efektivitas IR minimal setahun sekali**
   Melalui:
   - audit kebijakan,
   - audit forensik,
   - inspeksi kesiapan SOC,
   - uji insiden (tabletop & simulation).

2. **Melakukan Penetration Test Terkait IR**
   Untuk menguji:
   - respon tim,
   - kecepatan isolasi,
   - ketahanan sistem.

3. **Melakukan Review Kesiapan CSIRT**
   Mencakup:
   - personel,
   - tools,

- SLA IR,
- kompetensi.

5.9 Indikator Kinerja (IR KPI & Metrics)

Untuk memastikan IR berjalan efektif, berikut metrik yang direkomendasikan namun tidak terbatas kepada:

1. **MTTD — Mean Time to Detect**
   Waktu rata-rata dari serangan terjadi hingga terdeteksi.

2. **MTTA — Mean Time to Acknowledge**
   Waktu respon CSIRT terhadap alert.

3. **MTTR — Mean Time to Respond/Recover**
   Waktu pemulihan insiden.

4. **Number of Incidents by Severity**
   Tren peningkatan atau penurunan.

5. **Repeat Attack Ratio**
   Apakah mitigasi sebelumnya efektif?

BAB 6
KETAHANAN LAYANAN DAN KONTINUITAS BISNIS (CYBER RESILIENCE, BCP & DRP)

KETAHANAN LAYANAN & CONTINUITY (BCP/DRP) secara lengkap, formal, dan siap implementasi, dapat mengacu namun tidak terbatas pada:

- PBI 2/2024 – Keamanan Sistem Informasi & Ketahanan Siber,
- SEOJK 29/2022,
- OJK-ITSK,
- ISO 22301 (Business Continuity Management System),
- NIST SP 800-34 (Contingency Planning),
- praktik terbaik global industri keuangan.

Bab ini merupakan standar minimum yang wajib dimiliki oleh penyelenggara Fintech agar dapat bertahan dan pulih dari insiden siber, gangguan operasional, maupun bencana.

Ketahanan layanan (cyber resilience) adalah kemampuan organisasi untuk mempertahankan operasional kritikal selama terjadi insiden dan memastikan pemulihan cepat dengan dampak minimal terhadap konsumen dan ekosistem keuangan nasional.
Bab ini mengatur persyaratan bagi anggota AFTECH dalam menyusun, menerapkan, menguji, dan mengevaluasi Business Continuity Plan (BCP) dan Disaster Recovery Plan (DRP).

6.1 Tujuan Ketahanan Layanan

BCP/DRP disusun untuk:

1. Menjamin kelangsungan layanan kritikal Fintech.
2. Mengurangi gangguan operasional dan kerugian finansial.
3. Melindungi data pengguna dan integritas transaksi.
4. Memenuhi ketentuan regulator untuk menjaga stabilitas sektor keuangan.
5. Memastikan organisasi mampu pulih cepat dari insiden besar.
6. Mendukung kepercayaan publik dan reputasi perusahaan.

6.2 Prinsip Dasar Ketahanan Layanan

1. **Resilience by Design**
   Arsitektur layanan harus dirancang untuk tetap beroperasi meski sebagian fungsi terganggu.

2. **Redundancy & High Availability**
   Tidak boleh ada single point of failure pada layanan kritikal.

3. **Proaktif dan Preventif**
   Pencegahan lebih utama dibanding pemulihan.

4. **Risk-Based Planning**
   BCP/DRP harus selaras dengan profil risiko perusahaan.

5. **Evidence-Based & Tested**
   Perencanaan harus didukung data dan diuji secara berkala.

6. **Recovery-Oriented**
   Pemulihan harus terukur waktu dan prioritasnya.

6.3 Identifikasi Layanan dan Proses Bisnis Kritis

Setiap organisasi direkomendasikan untuk mengidentifikasi proses kritikal yang harus tetap berjalan meski terjadi insiden.

Contoh layanan kritikal Fintech:

- autentikasi pengguna,
- transaksi pembayaran,
- penyaluran pinjaman,
- core system backend,
- API yang terhubung ke bank atau merchant,
- manajemen saldo dan ledger,
- fraud detection system.

Dokumen wajib:

- daftar proses bisnis kritikal,
- RACI matrix,
- pemilik proses (process owner),
- dependensi sistem/teknologi.

6.4 Business Impact Analysis (BIA)

BIA adalah dasar utama penyusunan BCP/DRP.

Komponen BIA:

1. **Dampak Gangguan**
   - keuangan,
   - reputasi,
   - kepatuhan,
   - operasional,
   - pengalaman pelanggan.

2. **Maximum Tolerable Downtime (MTD)**
   Waktu maksimum layanan boleh berhenti sebelum dampak menjadi serius.

3. **Recovery Time Objective (RTO)**
   Target waktu pemulihan layanan setelah terjadi gangguan.

4. **Recovery Point Objective (RPO)**
   Jumlah data maksimum yang boleh hilang.

5. **Ketergantungan Sistem**
   - API internal & eksternal,
   - cloud provider,
   - database,
   - third party integrations,
   - network infrastructure.

   Contoh standar industri yang dapat menjadi rujukan:
   - RTO 15–60 menit untuk layanan kritikal.
   - RPO 0–15 menit (melalui incremental/real-time backup).

6.5 Business Continuity Plan (BCP)

BCP adalah dokumen operasional yang berisi langkah-langkah untuk menjaga kelangsungan bisnis saat terjadi gangguan.

Secara minimum, BCP mencakup:

1. Skema aktivasi BCP
   - peran dan tanggung jawab,
   - kriteria aktivasi (threshold),
   - otorisasi.
2. Rencana kontinuitas layanan
   - redundansi aplikasi,
   - strategi cadangan personel (backup roles),
   - skenario WFH massal.
3. Komunikasi krisis
   - ke karyawan,
   - ke regulator,
   - ke pengguna,
   - ke media (PR).
4. Strategi alternatif operasi
   - fallback server,
   - manual process (jika applicable),
   - bypass terhadap fungsi non-kritikal.
5. Dokumentasi pendukung
   - flowchart proses bisnis kritikal,

- kontak darurat,
- vendor dependency chart,
- SOP aktivasi BCP.

6.6 Disaster Recovery Plan (DRP)

DRP fokus pada pemulihan infrastruktur IT setelah gangguan teknis besar, insiden siber berat, atau bencana fisik.

Komponen DRP:

1. **Arsitektur Pemulihan**
   - data center primer & sekunder,
   - hot/warm/cold site,
   - multi-region cloud deployment,
   - database replication (sync/async).

2. **Rencana Pemulihan Sistem**

   Untuk setiap sistem kritikal:
   - urutan pemulihan,
   - langkah teknis,
   - checklist kesehatan sistem,
   - verifikasi integritas data.

3. **Prosedur Backup**
   - jadwal backup (harian, incremental, real-time),
   - enkripsi backup,
   - penyimpanan offsite,
   - cyber-resilient backup (immutable storage).

4. **Prosedur Restore**
   - validasi sumber backup,
   - prosedur restore otomatis/manual,
   - tes integritas data (checksum, hash verify).

5. **Dokumentasi Infrastruktur**
   - network diagram,
   - cloud template (IaC),
   - inventory server,
   - daftar credential khusus DRP.

6.7 Strategi Teknologi untuk Ketahanan Layanan

1. **High Availability**
   - load balancing,
   - automatic failover,
   - cluster redundancy.

2. **Cloud Resilience**
    - multi-zone, multi-region,
    - auto-scaling,
    - failback capability.

3. **Data Resilience**
    - versioning,
    - immutable backup,
    - point-in-time recovery.

4. **Network Resilience**
    - redundant ISP,
    - DDOS protection,
    - separation of concerns.

5. **Application Resilience**
    - circuit breaker pattern,
    - graceful degradation,
    - blue-green deployment,
    - canary release.

6.8 Uji Coba BCP/DRP

Testing dilakukan minimal 2 kali setahun, mencakup:

1. **Tabletop Exercise**
   Simulasi skenario insiden untuk menguji peran setiap tim.

2. **Technical DR Simulation**
   Pemulihan penuh/parsial dari backup:
    - restore database,
    - failover cloud region,
    - pemulihan API gateway.

3. **Unannounced Drill**
   Tes nyata tanpa pemberitahuan sebelumnya.

4. **External Dependency Test**
    - API ke bank/mitra,
    - payment gateway,
    - cloud provider.

Hasil uji coba dicatat dan diremediasi.

6.9 Komunikasi Krisis (Crisis Communication Plan)

Setiap organisasi direkomendasikan memiliki rencana komunikasi krisis yang mencakup:

1. **Kanal komunikasi internal**
    - WhatsApp emergency group,
    - email broadcast,
    - hotline internal,
    - war-room virtual.

2. **Komunikasi ke publik**
   Harus:
    - jujur,
    - ringkas,
    - tidak mengungkap detail teknis sensitif.

3. **Komunikasi ke regulator**
   Mengikuti kewajiban pelaporan sesuai dengan ketentuan yang berlaku:
    - OJK,
    - BI,
    - BSSN,
    - Kementerian/institusi lain terkait.

4. **Komunikasi ke pengguna**
   Jika layanan terganggu:
    - status dashboard,
    - push notification,
    - update berkala.

6.10 Ketahanan Personel (Human Continuity)

BCP juga mencakup rencana keberlanjutan sumber daya manusia:

- backup roles (minimal dua orang per fungsi kritikal),
- dokumentasi SOP dan transfer knowledge,
- cross-training,
- prosedur pergantian shift saat insiden panjang,
- perlindungan keselamatan personel saat bencana fisik.

6.11 Integrasi Ketahanan Layanan dengan Incident Response (IR)

BCP/DRP terintegrasi dengan CSIRT:

- IR menangani insiden (fase taktis),
- BCP menjaga operasional (fase operasional),
- DRP memulihkan infrastruktur (fase teknis).

Ketiga dokumen harus sinkron melalui:

- alur eskalasi yang sama,

- komunikasi krisis yang padu,
- integrasi dashboard risiko.

6.12 Review dan Audit Berkala

Organisasi wajib melakukan:

1. **Review tahunan**
   Terhadap:
   - BIA,
   - BCP,
   - DRP,
   - arsitektur TI.

2. **Audit eksternal**
   Minimal setahun sekali atau sesuai permintaan regulator.

3. **Continuous Improvement**
   Masukan dari:
   - hasil drill,
   - hasil audit,
   - perubahan regulasi,
   - perubahan infrastruktur,
   - insiden aktual.

BAB 7
PENGELOLAAN PIHAK KETIGA
DAN RISIKO SUPPLY CHAIN

PENGELOLAAN PIHAK KETIGA & SUPPLY CHAIN RISK yang sangat detail, komprehensif, dan implementable, setara standar pedoman tingkat regulator (OJK–BI–BSSN) dan mengikuti:

- SEOJK 29/2022
- POJK ITSK 4/POJK.03/2021
- PBI 2/2024 KKS BI
- ISO 27036 (Supplier Relationship Security)
- NIST SP 800-161 (Supply Chain Risk Management)
- OWASP Secure Procurement
- CIS Control 15

Bab ini dirancang agar langsung dapat digunakan oleh tim GRC, Legal, Procurement, dan Security di anggota AFTECH.

Pengelolaan keamanan pihak ketiga adalah komponen kritikal dalam ekosistem Fintech. Layanan Fintech sangat bergantung pada penyedia cloud, payment processor, API partner, vendor IT, integrator, data provider, outsourcing operasional, hingga penyedia layanan AI, sehingga risiko keamanan tidak hanya bersumber dari internal, tetapi juga dari seluruh rantai pasok digital.

Kesalahan pengelolaan vendor dapat menyebabkan:

- kebocoran data,
- fraud,
- downtime operasional,
- kompromi API,
- serangan supply chain,
- pelanggaran regulasi (termasuk UU PDP).

Oleh karena itu, seluruh anggota AFTECH direkomendasikan memiliki kerangka risiko pihak ketiga yang sistematis.

7.1 Tujuan dan Ruang Lingkup

Tujuan Pengelolaan Third Party Risk

1. Memastikan pihak ketiga tidak menjadi titik masuk serangan.
2. Menjamin kontrol keamanan vendor memenuhi standar industri.
3. Melindungi data pengguna yang diproses oleh vendor.
4. Menjaga stabilitas operasional layanan Fintech.
5. Mengelola risiko rantai pasok secara menyeluruh.
6. Memenuhi kewajiban regulator (OJK, BI, BSSN, UU PDP).

Ruang Lingkup Vendor

Pihak ketiga mencakup:

- penyedia cloud (AWS, GCP, Azure, Alibaba, dll),
- payment gateway/processor,
- penyedia API keuangan,
- penyedia layanan biometrik,
- vendor software development,
- outsourced customer service,
- SaaS provider (CRM, email, analytic),
- penyedia AI/LLM atau model scoring,
- penyedia fraud detection services,
- pihak outsource data center,
- konsultan keamanan,
- penyedia penetration testing,
- penyedia email/SMS OTP.

7.2 Prinsip Dasar Pengelolaan Pihak Ketiga

1. Risk-Based Approach – tingkat kontrol mengikuti tingkat risiko vendor.
2. Zero Trust Vendor – setiap akses vendor diverifikasi dan dibatasi.
3. Defense in Depth – kontrol keamanan berlapis.
4. Shared Responsibility Model – jelas batas kewajiban vendor–perusahaan.
5. Least Privilege & Need-to-Know – vendor hanya boleh mengakses yang dibutuhkan.
6. Continuous Monitoring – pengawasan tidak berhenti setelah kontrak ditandatangani.
7. Compliance Alignment – vendor harus sejalan dengan UU PDP dan regulasi keuangan.

7.3 Klasifikasi Vendor Berdasarkan Risiko

Vendor diklasifikasikan dalam 4 kategori:

1. **Vendor Risiko Sangat Tinggi (Tier 1)**

   Memiliki akses ke:

   - data pribadi pengguna tingkat tinggi,
   - data finansial,
   - sistem core,
   - jaringan produksi.

   Contoh: cloud provider, KYC provider, payment API, fraud detection engine.

2. **Vendor Risiko Tinggi (Tier 2)**

   Mengelola:

   - data internal penting,
   - akses API non-kritikal,

- modul/komponen aplikasi.

3. **Vendor Risiko Sedang (Tier 3)**
   Menyediakan layanan pendukung:
   - HR tools,
   - CRM,
   - analytics,
   - marketing platforms.

4. **Vendor Risiko Rendah (Tier 4)**
   Tidak mengakses data:
   - kantor,
   - cleaning service,
   - vendor supply umum.

   Kontrol keamanan berbeda per level vendor.

7.4 Siklus Pengelolaan Pihak Ketiga (Third Party Management Lifecycle)
Siklus ini dijalankan pada tahap:

1. Identification
2. Screening & Due Diligence
3. Risk Assessment
4. Contracting
5. Onboarding
6. Monitoring & Review
7. Termination & Exit Plan

Berikut detail langkah-langkahnya.

7.4 Tahap 1 – Identifikasi Vendor
Dokumentasikan:
- nama vendor,
- jenis layanan,
- data yang diakses/diproses,
- integrasi teknis,
- kategori risiko.

Gunakan template Vendor Inventory Register.

7.4 Tahap 2 – Due Diligence Keamanan
Untuk vendor Tier 1 & 2.

Checklist due diligence minimum:

A. Dokumen Kepatuhan

- ISO 27001 certificate,
- SOC 2 Type II,
- PCI DSS (jika memproses kartu),
- laporan audit internal,
- kebijakan keamanan dan privasi.

B. Legal & Regulatory

- Kepatuhan UU PDP,
- sub-processing disclosure,
- bukti penunjukan DPO (jika wajib).

C. Technical Security Controls

- enkripsi (AES-256 / TLS 1.3),
- IAM & least privilege,
- MFA untuk staf vendor,
- vulnerability management,
- penetration test report (max 12 bulan),
- anti-DDOS,
- keamanan cloud (CSPM).

D. Operational Security

- Disaster Recovery Plan,
- SLA uptime,
- incident response procedure,
- SOC availability (24/7 monitoring).

E. Data Handling & Privacy

- retensi data,
- mekanisme akses data,
- lokasi penyimpanan data (data residency),
- prosedur data deletion.

7.4 Tahap 3 – Penilaian Risiko Vendor

Risiko vendor dinilai berdasarkan:

1. Data sensitivity
2. System dependency level
3. Access privileges
4. Likelihood of compromise
5. Vendor maturity
6. Compliance gaps

Output berupa:

- Vendor Risk Score,
- rekomendasi: approve, conditional, atau reject.

7.4 Tahap 4 – Perjanjian Kontrak (Contracting)

Kontrak vendor wajib memuat klausul keamanan berikut:

A. Data Protection & Confidentiality

- vendor tunduk pada UU PDP,
- batasan pemrosesan data (purpose limitation),
- larangan transfer data tanpa izin.

B. Security Controls

- standar minimal (ISO 27001/NIST),
- enkripsi wajib,
- akses terbatas.

C. Incident Notification

Vendor wajib melaporkan insiden dalam:

- ≤ 12 jam untuk Tier 1,
- ≤ 24 jam untuk Tier 2.

D. Audit Rights

AFTECH/anggota memiliki hak:

- audit remote,
- review keamanan tahunan,
- permintaan bukti kontrol.

E. Sub-processor Management

Vendor harus:

- mengungkap pihak ke-4 (fourth-party),
- melarang penggunaan vendor tidak resmi.

F. Termination & Data Return

Saat kontrak berakhir:

- data harus dimusnahkan secara aman,
- ada certificate of destruction.

G. Cyber Insurance (opsional wajib untuk Tier 1)

7.4 Tahap 5 – Onboarding Vendor

Sebelum vendor aktif:

A. Akses Teknis

- buat akun khusus vendor (tidak sharing),
- aktifkan MFA,

- gunakan least privilege,
- siapkan expiring access token.

B. Integrasi Keamanan

- logging & monitoring API,
- traffic isolation,
- rate limiting,
- firewall rules.

C. Awareness Training

Vendor harus mengikuti pelatihan:

- keamanan data,
- phishing avoidance,
- privacy compliance.

7.4 Tahap 6 – Monitoring & Review Berkala

1. Monitoring Harian

- anomali API,
- trafik tidak biasa,
- tanda penyalahgunaan akses vendor.

2. Review Triwulanan

Vendor Tier 1 wajib:

- update laporan patching,
- laporan SOC,
- penetration test summary.

3. Audit Tahunan Vendor

Meliputi:

- audit dokumentasi keamanan,
- walkthrough arsitektur,
- review kebijakan privasi,
- random log inspection.

4. Performance & SLA Review

Memonitor:

- downtime,
- breach history,
- komitmen perbaikan.

7.4 Tahap 7 – Termination, Offboarding & Exit Plan

Jika kerja sama berakhir:

1. Cabut Seluruh Akses Vendor

- akun,
- token API,
- credential cloud.

2. Hapus atau Kembalikan Data

Vendor wajib:

- menghapus seluruh data,
- memberikan Certificate of Destruction.

3. Risiko Vendor Replacement

Mitigasi:

- parallel run,
- rollback plan.

4. Dokumentasi Offboarding

Harus dicatat sebagai bagian audit.

7.5 Keamanan Fourth-Party (Sub-Vendor)

Untuk mengelola risiko besar berasal dari pihak yang tidak kita lihat:

- meminta daftar sub-processor vendor,
- meminta bukti keamanan mereka,
- mewajibkan vendor mengaudit pihak ke-4,
- memantau reputasi vendor di publik/darkweb.

7.6 Automasi dan Tools yang Direkomendasikan

1. Vendor Risk Management Platforms

- OneTrust,
- SecurityScorecard,
- Bitsight,
- UpGuard.

2. Cloud Security Monitoring

- Prisma Cloud,
- Wiz,
- Lacework.

3. SIEM/SOC Tools

- Splunk,
- Elastic SIEM,
- Wazuh (open source).

4. Document & Workflow Automation

- Jira
- Notion Security Hub
- Confluence playbook

7.14 Indikator Kinerja Pengelolaan Vendor (KPI)

1. Vendor Approval Time (≤ 7 hari)
2. Vendor Assessment Completion Rate (> 95%)
3. Vendor SLA Compliance (> 99.5%)
4. Jumlah Insiden yang Bersumber dari Vendor (harus turun)
5. Patch SLA Vendor (critical ≤ 72 jam)
6. Quarterly vendor review compliance (> 90%)

7.7 Matriks Kontrol Minimum Berdasarkan Risiko Vendor

Tier 1 – Risiko Sangat Tinggi

- audit on-site,
- pen-test wajib,
- SLA insiden ≤ 12 jam,
- continuous monitoring,
- cyber insurance wajib.

Tier 2 – Risiko Tinggi

- annual audit,
- laporan keamanan tahunan,
- SLA insiden ≤ 24 jam.

Tier 3 – Risiko Sedang

- self-assessment questionnaire,
- dokumen keamanan standar.

Tier 4 – Risiko Rendah

- NDAs,
- perjanjian privasi standar.

BAB 8
PENGUJIAN KEAMANAN
(SECURITY TESTING, VA/PT, RED TEAMING & SDLC)

PENGUJIAN KEAMANAN (SECURITY TESTING) yang sangat lengkap, komprehensif, dan implementable, disusun setara pedoman regulator dan standar global:

- SEOJK 29/2022 – Ketahanan Siber
- POJK ITSK
- PBI 2/2024
- ISO 27001/27017/27034
- NIST SP 800-115 (Technical Guide to Security Testing)
- OWASP Testing Guide v5
- MITRE ATT&CK, Red Team Framework

Bab ini menjadi pedoman wajib bagi anggota AFTECH agar proses pengujian keamanan dilakukan terstruktur, terjadwal, terdokumentasi, dapat diaudit, dan menghasilkan peningkatan nyata terhadap keamanan layanan Fintech.

Pengujian keamanan merupakan elemen utama dalam manajemen risiko siber untuk memastikan bahwa kerentanan, kesalahan konfigurasi, dan celah arsitektur dapat ditemukan dan diperbaiki sebelum dimanfaatkan oleh penyerang.
Setiap anggota AFTECH wajib melaksanakan pengujian keamanan secara berkala pada seluruh lapisan: aplikasi, API, infrastruktur, mobile apps, jaringan, cloud, serta proses SDLC.

8.1 Tujuan Security Testing

1. Mengidentifikasi kerentanan teknis dan kesalahan implementasi.
2. Menilai efektivitas kontrol keamanan yang telah diterapkan.
3. Mencegah kebocoran data dan fraud pada layanan Fintech.
4. Menjamin keamanan integrasi API dan open finance.
5. Menguji kesiapan respons insiden dan ketahanan operasional.
6. Memenuhi standar regulator (OJK, BI, UU PDP) dan industri.

8.2 Ruang Lingkup Security Testing

Security testing wajib mencakup:

A. Aplikasi

- aplikasi web,
- aplikasi mobile (Android/iOS),
- backend services,
- microservices.

B. API dan Integrasi

- open API,
- internal API,
- partner API.

C. Infrastruktur

- server, OS, container, Kubernetes, CI/CD pipeline,
- cloud infrastructure (IAM, storage, networking),
- database.

D. Jaringan

- firewall, VPN, WAF, load balancer,
- network segmentation.

E. Teknologi Identitas

- SSO, IAM, MFA, OAuth/OIDC.

F. Proses dan SDLC

- code review,
- dependency scanning,
- secret scanning,
- infrastructure-as-code scanning.

8.3 Jenis Pengujian Keamanan

Terdapat empat kategori utama:

1. Vulnerability Assessment (VA)

Tujuan: mengidentifikasi kerentanan yang diketahui (known vulnerabilities).
Metode:

- automated scanner,
- cloud posture scanning (CSPM),
- dependency/library scanning.

Output:

- daftar CVE, prioritas remediation, patching plan.

VA dilakukan setiap bulan atau saat ada major update.

2. Penetration Testing (PT)

Tujuan: mengeksploitasi kerentanan untuk memastikan dampaknya nyata.
Jenis:

1. Black box – tanpa akses informasi.
2. Grey box – akses terbatas (paling umum).
3. White box – akses penuh (source code, credential).

Teknik:

- OWASP Web Testing Guide,
- OWASP Mobile Testing Guide,
- SANS Top 25 attack.

Frekuensi:

- minimal 2x setahun,
- wajib setelah major release.

Wajib dilakukan oleh:

- internal team bersertifikasi, atau
- lab eksternal yang kompeten (CREST, OSCP, CEH, GIAC, dll).

3. Red Team Exercise

Tujuan: meniru serangan agresif dunia nyata untuk menguji:

- deteksi SOC (SIEM, XDR),
- respon CSIRT,
- kesiapsiagaan pengguna,
- pertahanan jaringan,
- integritas sistem kritikal.

Lingkup:

- phishing,
- social engineering,
- privilege escalation,
- lateral movement,
- cloud misconfiguration exploitation,
- data exfiltration test.

Frekuensi:

- setahun sekali untuk perusahaan Tier 1 & 2.

Standar:

- MITRE ATT&CK Framework,
- Red Team maturity model.

4. Bug Bounty Program (Opsional)

Mengundang komunitas keamanan untuk mencari bug secara legal.
Model:

- private bounty (undangan terbatas),
- public bounty (opsional untuk perusahaan besar).

Platform:

- HackerOne, Bugcrowd, YesWeHack.

8.4 Pengujian Keamanan dalam SDLC (Secure SDLC Testing)

Pengujian keamanan dilakukan pada setiap tahap SDLC.

8.4.1 Tahap Desain

- threat modeling (STRIDE, PASTA),
- peninjauan arsitektur keamanan,
- security requirements list.

8.4.2 Tahap Pengembangan

Rutin:

- static application security testing (SAST),
- secret/token scanning,
- code review.

Tools:

- SonarQube,
- GitHub Advanced Security,
- Semgrep,
- Trivy.

8.4.3 Tahap Build & Integration

- dependency scanning (SCA),
- container scanning,
- IaC scanning (Terraform, Helm).

8.4.4 Tahap Pre-Production

- DAST (Dynamic testing),
- fuzzing,
- API/GraphQL testing,
- environment security validation.

8.4.5 Tahap Release

- penetration test,
- security sign-off,
- code freeze approval by CISO.

8.4.6 Tahap Operasional

- continuous monitoring,
- anomaly detection,
- privilege audit.

8.5 Pengujian Keamanan untuk API & Open Finance

Pengujian terhadap API wajib meliputi:

- authorization bypass test,
- token manipulation,
- rate limit bypass,
- mass assignment attack,
- SSRF,
- injection,
- replay attack,
- BOLA (Broken Object Level Authorization),
- enumeration.

Tools:

- Postman Security,
- BurpSuite Pro,
- OWASP ZAP,
- APIsec,
- StackHawk.

8.6 Pengujian Keamanan Mobile Apps

Dapat mengacu kepada OWASP Mobile Top 10:

Ruang Lingkup:

- rooting/jailbreak detection,
- certificate pinning,
- obfuscation & anti-tampering,
- insecure data storage,
- leaked sensitive tokens,
- reverse engineering resistance.

Tools:

- MobSF,
- Frida,
- Objection,
- jadx.

8.7 Pengujian Keamanan Cloud & Infrastruktur

Cloud Security Testing mencakup:

- IAM misconfig,
- overly permissive roles,
- storage bucket exposure,
- network misconfiguration,
- secrets exposed,
- overly permissive firewall rules,
- duplicate keys,

- weak encryption.

Tools:

- ScoutSuite,
- Prowler,
- Prisma Cloud,
- Lacework,
- Wiz.

8.8 Dokumentasi & Pelaporan Pengujian

Setiap pengujian wajib menghasilkan:

1. Technical Report

- vulnerability evidence,
- exploitation steps,
- environment detail.

2. Business Risk Summary

- dampak,
- likelihood,
- criticality.

3. Remediation Plan

- timeline patching,
- person-in-charge,
- mitigation steps.

4. Retest Report

Validasi bahwa kerentanan telah diperbaiki.

8.9 Frekuensi Minimal Pengujian

Jenis Pengujian	Frekuensi yang disarankan
Vulnerability Assessment	Bulanan
Web Pen-Test	2x per tahun
Mobile Pen-Test	1x per tahun
API Pen-Test	2x per tahun
Cloud Posture Scan	Mingguan
Red Team Exercise	Tahunan
Secure Code Review	Setiap release
SAST/SCA	Continuous Integration
DR/BCP Simulation	Tahunan

8.10 Key Metrics (KPI) untuk Security Testing

1. VA/PT Findings Trend

2. Mean Time to Remediate (MTTR)
3. % Critical findings closed < 72 jam
4. Pen-Test Remediation Compliance
5. Coverage testing (prosentase modul/sistem yang diuji)
6. False Positive Ratio
7. Security Testing SLA Compliance

8.11 Integrasi dengan CSIRT & Risk Management

Pengujian keamanan terhubung ke:

- CSIRT (insiden yang ditemukan saat pentest),
- ITSM (ticketing),
- GRC (risk register),
- DevSecOps pipeline.

Kerentanan kritikal harus langsung masuk:

- IR escalation,
- BCP scenario activation (jika berdampak besar),
- mandatory patch cycle.

8.12 Pengujian untuk Kepatuhan Regulator

Pengujian untuk kepatuhan regulator, wajib untuk mematuhi ketentuan yang berlaku seperti:

- Penetration Testing (Uji Penetrasi) oleh pihak independen,
- laporan hasil PT disampaikan ke regulator saat diminta,
- mandatory root cause analysis untuk insiden kritikal,
- mandatory re-test untuk memastikan bahwa remediasi telah selesai.

BAB 9
MANAJEMEN RISIKO SIBER TINGKAT LANJUT

MANAJEMEN RISIKO SIBER TINGKAT LANJUT yang sangat komprehensif, detail, dan implementable, mengacu pada:

- NIST Cybersecurity Framework (CSF) 2.0
- ISO 27005 (Information Security Risk Management)
- ISO 31000 (Risk Management)
- MITRE ATT&CK Risk Mapping
- OJK ITSK
- PBI 2/2024 KKS BI
- BSSN – Penilaian Risiko Siber Nasional

Bab ini dirancang agar dapat langsung dijadikan framework risk management bagi seluruh anggota AFTECH, terutama yang mengelola data sensitif, transaksi keuangan, dan infrastruktur digital kritikal.

Manajemen risiko siber merupakan proses sistematis untuk mengidentifikasi, menilai, memonitor, dan mengendalikan risiko-risiko yang dapat berdampak terhadap keberlangsungan bisnis, keamanan data, dan stabilitas ekosistem Fintech nasional.

Pada Bab ini, standar risiko dasar diperluas menjadi pendekatan modern, terukur, terotomasi, dan berbasis intelijen ancaman.

9.1 Tujuan Manajemen Risiko Siber Tingkat Lanjut

1. Mengidentifikasi risiko dengan metode kuantitatif maupun kualitatif.
2. Menjamin kontrol keamanan selalu sesuai tingkat ancaman terbaru.
3. Memastikan seluruh keputusan bisnis memperhitungkan risiko siber.
4. Menghubungkan risiko teknis dengan dampak finansial dan regulasi.
5. Melindungi data pengguna sesuai UU PDP dan standar industri.
6. Menciptakan transparansi risiko lintas unit dan lintas pengambil keputusan.
7. Memperkuat ketahanan ekosistem Fintech melalui intelijen ancaman.

9.2 Lingkup Risiko Siber

Manajemen risiko mencakup seluruh area berikut:

1. Risiko Teknologi

- kerentanan sistem,
- cloud misconfiguration,
- zero-day vulnerabilities,
- kegagalan arsitektur.

2. Risiko Data

- kebocoran data,
- penyalahgunaan data,
- pelanggaran UU PDP,
- ransomware.

3. Risiko Operasional

- kelalaian SDM,
- kegagalan proses,
- kesalahan konfigurasi sistem.

4. Risiko Pihak Ketiga

- supply chain attacks,
- sub-processor compromise,
- integrasi API berisiko.

5. Risiko Fraud & Financial Crime

- account takeover (ATO),
- synthetic identity fraud,
- API abuse,
- bot attack.

6. Risiko Regulasi & Kepatuhan

- non-compliance terhadap OJK/BI/BSSN,
- sanksi UU PDP.

7. Risiko Reputasi

- pemberitaan negatif,
- penyebaran opini negatif di media sosial (ulasan, komentar, dll)
- kehilangan kepercayaan pengguna.

8. Risiko Geopolitik & Ancaman Negara

- APT groups,
- serangan terhadap sektor keuangan,
- serangan terhadap cloud regional.

9.3 Framework Manajemen Risiko Siber

Framework dapat mengacu pada berikut:

1. ISO 27005 Risk Management Lifecycle

- Context establishment
- Risk assessment
- Risk treatment
- Risk acceptance
- Risk communication

- Risk monitoring

2. NIST CSF 2.0

- Identify
- Protect
- Detect
- Respond
- Recover
- Govern (komponen baru)

3. Risk Scoring Model (AFTECH Standardized Model)

Risiko dihitung berdasarkan:

- Likelihood (kemungkinan),
- Impact (dampak),
- Exposure (paparan),
- Detectability (kemampuan mendeteksi).

9.4 Identifikasi Risiko (Risk Identification)

Organisasi wajib:

- memetakan sistem kritikal,
- memetakan data sensitif,
- mengidentifikasi aset digital (CMDB),
- mengidentifikasi threat actor: APT, cyber criminals, hacktivists, insider threat,
- memetakan risiko sektor Fintech: KYC, payment, API, loan, investment.

Sumber identifikasi risiko:

- vulnerability assessment,
- hasil pen-test,
- temuan audit,
- insiden historis,
- threat intelligence (AFTECH-CSIRT),
- darkweb monitoring,
- regulatory review.

9.5 Penilaian Risiko (Risk Assessment)

Penilaian risiko dilakukan dengan setidaknya dua pendekatan:

A. Penilaian Kualitatif

- Tinggi, Sedang, Rendah
- Dampak: Finansial, Operasional, Reputasi, Kepatuhan
- Likelihood: High/Medium/Low

Matriks Risiko 3×3 atau 5×5 digunakan untuk evaluasi awal.

B. Penilaian Kuantitatif (Pendekatan Lanjutan)
Menggunakan metode:
1. FAIR Model (Factor Analysis of Information Risk)
Menentukan:

- Loss Event Frequency
- Loss Magnitude

2. Monte Carlo Simulation
Untuk menentukan:

- potensi kerugian tahunan (ALE),
- skenario kerugian ekstrem.

3. MITRE ATT&CK Threat Maturity Scoring
Risiko dihitung berdasarkan:

- prevalensi teknik serangan,
- kemampuan pendeteksian saat ini,
- kemampuan mitigasi.

Output:

- Cyber Risk Exposure Index,
- Prioritas mitigasi,
- Justifikasi anggaran keamanan.

9.6 Penanganan Risiko (Risk Treatment)
Terdapat empat opsi:
1. Mitigate (Mengurangi)

- patching,
- WAF,
- DDoS mitigation,
- encryption enforcement,
- privilege reduction.

2. Transfer

- cyber insurance,
- outsourcing ke vendor bersertifikasi.

3. Accept

- hanya untuk risiko rendah,
- harus disetujui oleh CISO dan manajemen.

4. Avoid

- menolak integrasi API berisiko,

- menghentikan fitur tertentu.

9.7 Risk Register (Katalog Risiko Siber)

Risk Register wajib berisi:

- risiko,
- root cause,
- aset terdampak,
- owner,
- likelihood & impact,
- score & rating,
- kontrol eksisting,
- rekomendasi mitigasi,
- target waktu perbaikan (SLA),
- status remediation.

9.8 Risk Appetite & Risk Tolerance

Setiap organisasi wajib menetapkan:

1. Risk Appetite

Tingkat risiko yang masih dapat diterima organisasi dalam konteks bisnis.
Contoh:

- downtime < 15 menit/bulan,
- tidak boleh ada data pribadi bocor,
- MTTR insiden kritikal ≤ 2 jam.

2. Risk Tolerance

Variasi risiko yang bisa diterima dalam operasional harian.

3. Risk Capacity

Batas maksimum sebelum risiko mengancam keberlangsungan perusahaan.

9.9 Continuous Risk Monitoring

Pemantauan risiko dilakukan melalui:

1. SOC Monitoring

- SIEM, EDR, XDR.

2. Threat Intelligence,

- CERT,
- vendor TI global.

3. Patch & Vulnerability Trends

- Sebagai contoh SLA perbaikan:
  - critical ≤ 72 jam,
  - high ≤ 7 hari,
  - medium ≤ 30 hari.

4. Attack Surface Management

- scanning domain,
- port exposure,
- expired certificates.

5. Cloud Security Posture Management (CSPM)

- IAM misconfig monitoring,
- storage exposure detection.

9.10 Pengelolaan Risiko Data dan UU PDP

Setiap risiko yang memengaruhi data pribadi wajib mematuhi:

- prinsip transparansi
- prinsip keabsahan pemrosesan data,
- prinsip minimalisasi data,
- kontrol akses ketat,
- audit log data access,
- mekanisme breach notification,
- Data Protection Impact Assessment (DPIA).

DPIA wajib untuk:

- penggunaan AI,
- biometrik,
- pemrosesan data anak,
- profiling otomatis,
- transfer data lintas negara.

9.11 Integrasi Risiko Siber dengan Risiko Enterprise (ERM)

Risiko siber tidak boleh berdiri sendiri.

Harus terhubung dengan:

- risiko operasional,
- risiko TI,
- risiko kepatuhan,
- risiko fraud,
- risiko reputasi.

Setiap perubahan skor risiko harus dilaporkan pada:

- Dewan Pengawas,
- Komite Risiko,
- Manajemen Senior.

9.12 Dashboard Risiko Siber (Cyber Risk Dashboard)

Dashboard real-time minimal memuat:

1. Risk Score Keseluruhan

2. Risiko per Divisi / Sistem
3. Trends Temuan Keamanan
4. Peringatan Risiko dari Threat Intel
5. SLA Patching
6. Attack Vectors terbanyak
7. Status remidiasi risiko kritikal
8. Peringkat vendor risiko tinggi
9. Heatmap Risiko (5×5)

Contoh platform yang dapat digunakan:

- PowerBI,
- Kibana,
- Grafana,
- Splunk,
- Looker.

9.13 Penilaian Risiko Eksternal & Ancaman Sistemik

AFTECH mendorong penilaian risiko eksternal pada beberapa domain berikut:

1. Ekosistem Pembayaran

- koneksi ke bank,
- PJP/PIP/PUVA.

2. Open Finance & API Economy

- risiko partner API,
- risiko aggregator data.

3. Ancaman Siber Nasional

- APT Asia,
- ransomware gang,
- geopolitik cloud region.

4. Infrastruktur Publik

- ISP outage,
- cloud region down,
- kegagalan SMS OTP gateway.

9.14 Pengukuran Risiko Siber Kuantitatif (Opsional Tingkat Lanjut)

Metode lanjutan untuk perusahaan besar:

1. Value-at-Risk for Cyber (Cyber VaR)

Menentukan nilai kerugian maksimum pada tingkat probabilitas tertentu.

2. Annualized Loss Expectancy (ALE)

$$ALE = SLE \times ARO$$

(SLE = single loss event, ARO = annual rate of occurrence)

3. Scenario-Based Stress Testing

Contoh skenario:

- ransomware yang mematikan seluruh produksi,
- kebocoran data > 1 juta akun,
- compromise API ke partner bank.

9.15 Rekomendasi Governance untuk Risiko Siber

1. Komite Risiko Siber tingkat direksi.
2. Pembahasan risiko siber minimal per kuartal.
3. Pelaporan risiko kritikal harus real-time.
4. Evaluasi risk appetite setahun sekali.
5. Integrasi risiko dengan strategi bisnis.

BAB 10
AUDIT & PENGAWASAN KEAMANAN SIBER

AUDIT & PENGAWASAN KEAMANAN SIBER, disusun sangat detail, komprehensif, implementatif, dan selaras dengan:

- SEOJK 29/2022 – Ketahanan Siber
- POJK ITSK (4/POJK.03/2021)
- PBI 2/2024 – Keamanan Sistem Pembayaran
- ISO 27001/27002/27007/19011
- NIST CSF 2.0
- NIST 800-53 & 800-55 (Security Metrics & Assessment)
- COBIT 2019

Bab ini akan menjadi standar audit untuk anggota AFTECH, agar setiap perusahaan Fintech memiliki tata kelola audit keamanan yang terstruktur, dapat diverifikasi, dan menghasilkan peningkatan nyata terhadap keamanan sistem.

Audit dan pengawasan keamanan siber adalah proses penilaian independen terhadap efektivitas kontrol, kebijakan, proses, dan teknologi yang digunakan untuk melindungi data dan sistem elektronik. Audit berfungsi memastikan bahwa seluruh anggota AFTECH:

1. Mematuhi regulasi nasional;
2. Menjalankan standar keamanan tinggi;
3. Mengurangi risiko siber;
4. Menjaga kepercayaan publik terhadap ekosistem Fintech.

10.1 Tujuan Audit Keamanan Siber

1. Menilai efektivitas pengendalian keamanan (technical & non-technical).
2. Menilai kepatuhan terhadap kebijakan internal dan regulasi.
3. Mengidentifikasi celah keamanan atau kesalahan implementasi.
4. Memberikan rekomendasi peningkatan secara berkelanjutan.
5. Mendukung tata kelola (governance) dan manajemen risiko siber.
6. Menjadi dasar keputusan strategis manajemen dan regulator.

10.2 Ruang Lingkup Audit Siber

Audit mencakup seluruh domain berikut:

1. Tata Kelola Keamanan Siber

- kebijakan & SOP,
- roles & responsibilities,
- struktur CISO & fungsi keamanan,
- risk governance.

2. Manajemen Aset & Data

- data classification,
- CMDB,
- data lifecycle,
- kepatuhan UU PDP.

3. Infrastruktur & Jaringan

- firewall rules,
- segmentation,
- cloud security configuration,
- server hardening.

4. Aplikasi & API

- secure coding,
- pen-test findings,
- API authorization.

5. Identitas & Akses

- IAM,
- MFA,
- privileged access review,
- zero trust controls.

6. Manajemen Kerentanan

- patch management,
- baseline compliance,
- vulnerability trends.

7. Monitoring & Incident Response

- SIEM, SOC, EDR logs,
- IR readiness & playbook maturity.

8. Ketahanan Layanan (BCP/DRP)

- failover tests,
- DR drills,
- backup integrity.

9. Pihak Ketiga

- vendor risk management,
- contract compliance.

10. DevSecOps & SDLC Security

- SAST, SCA, DAST,
- secret scanning,

- IaC security.

10.3 Jenis Audit yang Wajib Dilakukan

Terdapat tiga level audit yang dapat diimplementasikan seluruh anggota AFTECH.

1. Audit Internal Keamanan Siber

Dilakukan oleh:

- internal audit team,
- unit GRC/IT Audit.

Frekuensi:

- minimal 1 kali per tahun.

Tujuan:

- mengevaluasi kepatuhan kebijakan internal,
- memverifikasi SOP yang dijalankan,
- mencari gap governance.

2. Audit Eksternal / Independen

Dilakukan oleh:

- auditor eksternal bersertifikasi,
- perusahaan konsultan keamanan yang berkompeten.

Frekuensi:

- minimal 1 kali per tahun,
- sesuai kewajiban SEOJK 29/2022 atau regulasi yang berlaku

Lingkup:

- keamanan aplikasi,
- cloud security,
- kepatuhan ITSK/UU PDP,
- penilaian maturity.

3. Audit Regulator (OJK/BI/BSSN)

Audit formal dilakukan oleh regulator jika:

- terjadi insiden material,
- ada peningkatan risiko sistemik,
- ada permintaan informasi atau pemeriksaan tematik,
- saat proses perizinan/registrasi Fintech baru.

Perusahaan wajib mempersiapkan:

- dokumentasi lengkap,
- evidences,
- rekaman perubahan,
- laporan insiden.

10.4 Metodologi Audit Siber

Audit direkomendasikan untuk mengikuti kerangka formal, antara lain:

1. ISO 19011 – Audit Guidelines

- planning,
- scope definition,
- sampling method,
- evidence gathering,
- reporting.

2. ISO 27007 – ISMS Auditing Framework

- menilai kontrol ISO 27001 Annex A,
- verifikasi implementasi kontrol operasional.

3. NIST 800-53A

- technical control testing,
- management & operational control testing.

4. COBIT 2019

- governance,
- maturity.

5. OWASP ASVS

- audit keamanan aplikasi (web/API/mobile).

10.5 Proses Audit Siber (Audit Lifecycle)

1. Perencanaan (Planning)

- tentukan ruang lingkup,
- tentukan aset yang diaudit,
- siapkan dokumen: kebijakan, SOP, konfigurasi, arsitektur.

2. Pengumpulan Bukti (Evidence Collection)

Metode:

- wawancara,
- pemeriksaan dokumen,
- review konfigurasi,
- log review,
- observasi proses operasional,
- audit trail,
- vulnerability scanning & PT report.

3. Validasi & Verifikasi

- sampel diuji kebenarannya,
- perbandingan dengan standar,

- cross-check log & konfigurasi.

4. Penilaian (Assessment)

- risk scoring,
- maturity scoring,
- compliance scoring.

5. Pelaporan (Audit Report)

Isi laporan:

- temuan (findings),
- risiko terkait,
- root cause,
- rekomendasi,
- prioritas perbaikan.

6. Pemantauan (Follow-Up)

- memverifikasi perbaikan,
- tracking remediation SLA.

10.6 Maturity Level Penilaian Keamanan Siber

AFTECH menetapkan 5 tingkat kematangan:

Tingkat	Deskripsi
0 — Non-existent	Tidak ada kontrol.
1 — Initial/Ad-hoc	Ada kebijakan, tidak konsisten.
2 — Repeatable	Proses berjalan, belum terukur.
3 — Defined	SOP terdokumentasi, kontrol stabil.
4 — Managed	Monitoring & KPI berjalan, perbaikan berkelanjutan.
5 — Optimized	Otomasi penuh, best practice global, threat-driven.

Setiap komponen keamanan dapat diberi nilai maturity.

10.7 Pengawasan Keamanan Siber Berbasis Risiko

Pengawasan menggunakan pendekatan risk-based supervision:

Parameter yang dipantau:

1. tingkat kerentanan (jumlah CVE),
2. patching SLA compliance,
3. hasil pen-test,
4. hasil red team,
5. insiden siber yang terjadi,
6. fraud metrics,
7. perubahan arsitektur signifikan,
8. ketergantungan vendor kritikal.

Kategori Pengawasan

- Intensif (untuk high-risk Fintech),
- Moderate,
- Light Touch (untuk low-risk Fintech).

AFTECH dapat membuat dashboard pengawasan untuk seluruh anggota.

10.8 Pengawasan Berkelanjutan (Continuous Monitoring)

Organisasi diharapkan menerapkan monitoring 24/7 melalui:

Technical Monitoring

- SIEM, EDR, XDR,
- cloud security posture (CSPM),
- API abuse monitoring,
- fraud monitoring engine.

Governance Monitoring

- status audit finding,
- maturity trends,
- risk register updates.

Tools:

- Jira, Confluence, Notion GRC,
- PowerBI/Grafana dashboards.

10.9 Audit terhadap Pihak Ketiga

Bagian ini terkait dengan Bab 7 (vendor management), namun audit wajib mencakup:

1. Kepatuhan kontrak vendor

- SLA keamanan,
- insiden vendor,
- laporan patching,
- laporan pen-test.

2. Audit keamanan API partner

- autentikasi,
- enkripsi,
- rate limiting.

3. Audit sub-processor (fourth party)

- daftar sub-vendor,
- kontrol keamanan mereka,
- kebijakan data handling.

10.10 Key Metrics (KPI & KRI) untuk Audit Keamanan Siber

Beberapa Key Performance Indicator (KPI) yang dapat digunakan:

1. % audit findings resolved on time (target > 90%)
2. Rata-rata waktu penyelesaian temuan (MTTR)
3. % proses yang diaudit sesuai jadwal
4. Peningkatan maturity tiap tahun
5. Jumlah temuan berulang (harus turun)

Beberapa Key Risk Indicator (KR) yang dapat digunakan:

1. jumlah temuan kritikal per kuartal
2. patching compliance < 70%
3. jumlah high-risk vendor
4. peningkatan insiden siber
5. privilege escalation risk score

10.11 Audit Trail & Bukti Kepatuhan

Setiap organisasi direkomendasikan untuk menyimpan setidaknya:

- konfigurasi sistem,
- bukti patching,
- bukti akses log,
- perubahan arsitektur (change management),
- laporan IR,
- backup log minimal 1–3 tahun (sesuai regulasi yang berlaku).

Audit trail harus:

- lengkap,
- tidak dapat dimodifikasi,
- tersedia untuk pemeriksaan regulator.

10.12 Peran CISO, Internal Audit, & Dewan Pengawas

CISO

- bertanggung jawab atas kesiapan audit,
- menyampaikan laporan bulanan/kuartal.

Internal Audit

- menguji pengendalian internal,
- melakukan review independen.

Dewan Pengawas/Komite Risiko

- menerima laporan audit kritikal,
- memutuskan prioritas perbaikan.

10.13 Program Audit Tahunan (Annual Cyber Audit Plan)

Dokumen ini berisi:

1. daftar area audit,
2. risiko utama,
3. auditor yang ditunjuk,
4. jadwal audit,
5. ruang lingkup,
6. metode,
7. deliverables,
8. mekanisme follow-up.

10.14 Penilaian Kepatuhan terhadap Regulasi

Setiap anggota AFTECH wajib memastikan kepatuhan terhadap:

- POJK ITSK (ITSK/OJK digital financial innovation),
- SEOJK 29/2022 – Ketahanan Siber,
- PBI 2/2024 – Keamanan Sistem Pembayaran,
- UU PDP (Data Protection),
- Standar BSSN.

Audit kepatuhan mencakup:

- mengukur gap compliance,
- membuat improvement roadmap,
- melakukan verifikasi perbaikan.

10.15 Tindak Lanjut dan Evaluasi Temuan

Setiap temuan dapat dikelompokkan berdasarkan:

Severity Level

- Critical
- High
- Medium
- Low

Target Remediasi

Sebagai contoh:

- Critical: ≤ 7 hari
- High: ≤ 14 hari
- Medium: ≤ 30 hari
- Low: ≤ 90 hari

Temuan harus dimasukkan ke:

- risk register,
- remediation tracker,
- dashboard keamanan.

BAB 11
EDUKASI, PELATIHAN & KESADARAN SIBER

EDUKASI, PELATIHAN & KESADARAN SIBER, disusun komprehensif, implementable, dan sesuai standar global, mengacu pada:

- OJK ITSK & SEOJK 29/2022
- PBI 2/2024
- ISO 27001 Annex A.7 (Human Resource Security)
- NIST SP 800-50 (Awareness & Training Program)
- NIST NICE Cybersecurity Workforce Framework
- SANS Security Awareness Maturity Model

Bab ini dirancang untuk dapat langsung digunakan sebagai pedoman nasional edukasi siber bagi seluruh anggota AFTECH.

Sumber daya manusia adalah vektor risiko terbesar sekaligus lini pertahanan pertama organisasi. Lebih dari 80% insiden siber berasal dari human error, termasuk phishing, salah konfigurasi, atau kelalaian dalam menjaga data.

Karena itu, edukasi, pelatihan, dan kesadaran siber yang kuat menjadi komponen wajib dalam keamanan Fintech, memastikan seluruh pegawai memahami ancaman, kebijakan, dan peran mereka dalam menjaga keamanan data.

11.1 Tujuan Program Pelatihan & Kesadaran Siber

1. Meningkatkan kemampuan pegawai mengenali dan merespons ancaman siber.
2. Memastikan seluruh karyawan memahami kebijakan keamanan perusahaan.
3. Mengurangi risiko human error dalam insiden siber & fraud digital.
4. Menciptakan budaya keamanan (security culture) yang berkelanjutan.
5. Memastikan kesiapan pegawai dalam menghadapi insiden kritikal.
6. Memenuhi persyaratan regulasi.

11.2 Ruang Lingkup Program Edukasi & Awareness

Program ini direkomendasikan untuk mencakup seluruh lapisan organisasi:

1. Seluruh Pegawai (General Awareness)

- keamanan data,
- kebijakan perusahaan,
- phishing,
- hygiene digital.

2. Tim Teknis (Technical Security Training)

- SAST/DAST,
- secure coding,

- cloud security,
- network defense.

3. Eksekutif & Manajemen (Executive Cyber Literacy)

- risiko siber,
- cyber resilience,
- risk appetite,
- governance & decision making.

4. Pihak Ketiga (Vendor & Mitra API)

- kepatuhan kebijakan data,
- kewajiban keamanan integrasi.

5. CSIRT, SOC, & Tim Keamanan (Advanced Training)

- digital forensics,
- incident response,
- red teaming,
- threat intelligence,
- MITRE ATT&CK.

11.3 Struktur Program Awareness (Lifecycle)

Dapat mengacu pada NIST SP 800-50, program awareness terdiri dari 5 fase:

1. **Initiate** – menetapkan tujuan & kebijakan.
2. **Develop** – membuat modul, kurikulum, materi.
3. **Implement** – pelaksanaan pelatihan, simulasi.
4. **Measure** – evaluasi efektivitas.
5. **Improve** – perbaikan berkelanjutan.

11.4 Kurikulum Pelatihan Wajib (Mandatory Training Curriculum)

Berikut kurikulum minimum yang direkomendasikan untuk dimiliki anggota AFTECH:

1. Untuk Semua Pegawai (Basic Cyber Awareness)

Durasi: 1–2 jam setiap kuartal

Materi yang direkomendasikan berupa:

- pengenalan ancaman siber,
- phishing & social engineering,
- keamanan kata sandi & MFA,
- keamanan data pribadi (UU PDP),
- kebijakan penggunaan perangkat,
- cara melaporkan insiden,
- keamanan bekerja dari rumah (WFH),
- keamanan mobile & cloud apps,
- ancaman malware dan ransomware.

Metode:

- video learning,
- quiz online,
- poster,
- simulasi phishing.
- Learning management system (LMS)
- AI Chatbot

2. Untuk Developer & DevOps (Secure Coding & DevSecOps
Durasi: 2–8 jam per kuartal
Materi:

- OWASP Top 10 (web/mobile/API),
- secure SDLC,
- threat modeling,
- secrets management,
- secure CI/CD,
- API security best practices,
- dependency scanning (SCA),
- container/Kubernetes security,
- infrastructure-as-code security.

Metode:

- workshop hands-on,
- live coding secure fix,
- capture the flag (CTF).

3. Untuk SOC/CSIRT (Advanced Technical Training)
Durasi: 8–40 jam per tahun
Materi:

- digital forensics,
- malware analysis,
- security operations,
- incident handling,
- blue team analysis,
- MITRE ATT&CK,
- anomaly detection,
- log correlation,
- SIEM rule tuning,
- threat hunting.

Tools:

- Splunk,
- Elastic,
- Wazuh,
- Suricata,

- Sysmon.

4. Untuk Manajemen Eksekutif & Board (Cyber Leadership Training)

Durasi: 2–4 jam per semester

Materi:

- cyber governance,
- risk appetite & tolerance,
- business impact of cyber incidents,
- cyber crisis communication,
- decision-making in cyber incidents,
- overview regulasi OJK/BI/BSSN/UU PDP,
- reputational risk.

Metode:

- executive briefing,
- tabletop exercise,
- scenario-based simulation.

5. Untuk Vendor & Third Party

Durasi: 1–2 jam x 2 kali/ tahun

Materi:

- UU PDP (prosesor data)
- kebijakan keamanan vendor,
- standar akses & integrasi API,
- enkripsi & data handling,
- security obligations in contract,
- breach notification.

11.5 Program Simulasi & Latihan Praktis

Untuk membangun ketahanan nyata, setiap organisasi dapat melaksanakan:

1. Simulasi Phishing Berkala (Phishing Drill)

- minimal 1 kali per bulan;
- tingkat kesuksesan < 5% dianggap baik;
- metrik risiko data breach > 60%
- security awareness score > 60%
- harus mencakup media komunikasi yang digunakan perusahaan sepert: email, WhatsApp, SMS, chat.

2. Tabletop Exercise (TTX)

Simulasi insiden untuk manajemen:

- data breach,
- ransomware,
- fraud besar,

- API compromise.
- Minimal: 2 kali per tahun.

3. Cyber Range Training / Blue Team Drill
Simulasi teknis untuk SOC:
- reverse engineering malware,
- log review,
- incident containment.

4. Red Team vs Blue Team Exercise
Untuk perusahaan maturity tinggi.

5. BCP/DRP Simulation
- failover test;
- backup restore test;
- cloud region failover.

11.6 Mekanisme Evaluasi & Pengukuran Efektivitas
Untuk memastikan program awareness efektif, organisasi direkomendasikan untuk memonitor:

1. Phishing Reporting Rate
Target: meningkat setiap kuartal.

2. Phishing Compromise Rate
Target: < 2%.

3. Pelatihan Wajib Selesai (Completion Rate)
Target: > 95% pegawai.

4. Post-training Test Score
Target: minimum 80%.

5. Incident Response Awareness Score
Bertujuan untuk memastikan setiap pegawai tahu dan paham dalam melaporkan insiden siber

6. Audit Hasil Awareness Program
Verifikasi melalui audit tahunan.

7. Reduction in Human-induced Incidents
Misalnya:
- salah kirim data,
- credential leak,
- misconfiguration.

11.7 Konten Edukasi yang Harus Diperbarui Berkala

Minimal tiap 6 bulan, seluruh materi harus dievaluasi berdasarkan:

- perkembangan ancaman terbaru,
- kampanye phishing yang sedang marak,
- temuan audit & pentest,
- insiden nasional & global.

Materi harus menyertakan:

- contoh nyata insiden di Indonesia,
- modul interaktif,
- studi kasus sektor keuangan.

11.8 Metode Penyampaian Edukasi

Berikut metode pelatihan yang direkomendasikan:

- e-learning platform internal,
- webinar & workshop,
- micro-learning 5 menit,
- poster awareness,
- chatbot edukasi,
- Slack/Teams reminder bot,
- gamification & CTF.

11.9 Peran Masing-Masing Bagian Organisasi

1. CISO / Cybersecurity Division

- mendesain kurikulum,
- memastikan keselarasan kebijakan,
- melakukan monitoring efektivitas.

2. HRD

- memasukkan pelatihan dalam onboarding,
- tracking completion rate.

3. Internal Audit

- menilai efektivitas program,
- memeriksa dokumentasi.

4. Manajemen Senior

- memberikan arahan strategis,
- mengaktifkan budaya keamanan.

5. Pegawai

- mengikuti pelatihan,
- berperan aktif melaporkan insiden.

11.10 Awareness untuk Pengguna (Customer Education)

Anggota AFTECH didorong untuk melaksanakan edukasi publik mengenai:

- penipuan online,
- phishing/whishing/smishing,
- cara mengenali aplikasi palsu,
- keamanan OTP,
- keamanan mobile banking/Fintech,
- social engineering,
- investasi bodong,
- keamanan akun & password.
- current issue tentang kejahatan di bidang Fintech

Metode:

- media sosial,
- email edukasi,
- halaman “Keamanan” di website,
- video,
- poster.

11.11 Standar Kepatuhan untuk Awareness Program

Agar auditable, program awareness direkomendasikan untuk menyimpan:

- daftar peserta pelatihan,
- jadwal training,
- materi pelatihan,
- hasil ujian/quiz,
- hasil phishing drill,
- laporan evaluasi efektivitas.

Durasi penyimpanan:

- minimal 3 tahun atau mengikuti standar ketentuan yang berlaku.

BAB 12
TATA KELOLA AI & KEAMANAN AI
(AI GOVERNANCE & AI SECURITY)

TATA KELOLA AI & KEAMANAN AI (AI GOVERNANCE & AI SECURITY) yang sangat lengkap, komprehensif, dan implementable, mengacu pada:

- OECD AI Principles
- EU AI Act
- NIST AI Risk Management Framework (NIST AI RMF, 2023)
- ISO/IEC 42001 (AI Management System)
- ISO/IEC 23894 (AI Risk Management)
- Singapore Model AI Governance Framework
- UU PDP Indonesia (Data Protection)
- Strategi Nasional AI 2020-2045 dan/atau Peta Jalan AI
- Pedoman Etik AFTECH untuk Inovasi Keuangan Digital

Bab ini sangat relevan untuk AFTECH karena penggunaan AI semakin masif:
KYC biometrik, fraud detection, credit scoring, behavioral analytics, chatbots, underwriting otomatis, hingga agentic AI.

Artificial Intelligence (AI) menghadirkan peluang besar bagi sektor Fintech, namun juga risiko signifikan terkait keamanan, privasi, bias algoritmik, manipulasi data, dan kerentanan teknis.

Karena itu, setiap anggota AFTECH direkomendasikan untuk menerapkan kerangka tata kelola dan keamanan AI agar penggunaan AI tetap:

- aman,
- dapat dipercaya,
- etis,
- akuntabel, dan
- sesuai regulasi.

Bab ini mengatur standar minimum untuk pengembangan, implementasi, integrasi, dan pengawasan AI dalam layanan Fintech.

12.1 Tujuan Tata Kelola & Keamanan AI

1. Menjamin penggunaan AI yang aman, transparan dan dapat dipertanggungjawabkan.
2. Mengelola risiko bias, diskriminasi, dan unfair treatment.
3. Melindungi data pribadi sesuai UU PDP & standar global.
4. Mencegah penyalahgunaan AI oleh pihak internal maupun eksternal.
5. Menjamin integritas model, data, dan output AI.
6. Memastikan AI tidak menciptakan risiko sistemik di sektor Fintech.

7. Mendukung inovasi yang bertanggung jawab dalam ekosistem digital Indonesia.

12.2 Ruang Lingkup AI dalam Sektor Fintech

Ruang lingkup ini berlaku bagi seluruh bentuk AI yang digunakan anggota AFTECH:

1. Machine Learning & Deep Learning

- credit scoring,
- anti-fraud,
- underwriting otomatis.

2. Biometric AI

- facial recognition,
- liveness detection,
- voice authentication.

3. NLP & Chatbots

- customer support,
- virtual assistants,
- sentiment analysis.

4. Generative AI

- document automation,
- code generation,
- content generation.

5. Agentic AI

- autonomous decision-making,
- automation with minimal human supervision.

6. Third-party AI (OpenAI API, AWS AI, Google Vertex AI, dll)

- Wajib masuk ke dalam vendor risk management (Bab 7).

12.3 Prinsip Dasar Tata Kelola AI

10 prinsip tata kelola AI:

1. Aman (Safety)
2. Akurat (Accuracy)
3. Aditif (Fairness/No Bias)
4. Transparan (Transparency)
5. Akuntabel (Accountability)
6. Privasi Terlindungi (Privacy by Design)
7. Beralasan (Explainability)
8. Bertanggung jawab (Responsible Use)
9. Dapat Diaudit (Auditability)
10. Human-in-the-loop (HiTL) untuk keputusan besar

Prinsip ini wajib diterapkan pada seluruh modul AI kritikal.

12.4 Klasifikasi Risiko AI (AI Risk Level)

AI diklasifikasikan berdasarkan level risiko (mengacu EU AI Act):

1. Minimal Risk

- chatbot non-keuangan,
- rekomendasi konten.

2. Limited Risk

- scoring ringan,
- automasi internal,
- NLP analytics.

3. High Risk (Wajib Pengawasan Ketat)

- credit scoring,
- fraud detection,
- biometrik,
- AML screening,
- risk assessment models.

4. Unacceptable Risk (Dilarang)

- manipulasi perilaku pengguna,
- penggunaan AI untuk diskriminasi,
- surveillance tanpa dasar hukum,
- prediksi kriminalitas berbasis ras/etnis.

12.5 AI Lifecycle & Governance Framework

Manajemen AI direkomendasikan untuk mengikuti siklus resmi:

1. Planning
2. Data Collection & Preparation
3. Model Development
4. Model Validation
5. Deployment
6. Monitoring & Maintenance
7. Retirement & Deletion

Setiap fase memiliki kontrol keamanan yang wajib dipatuhi.

12.6 Manajemen Risiko AI (AI Risk Management)

Mengacu NIST AI RMF & ISO 23894:

Risiko yang harus dikendalikan:

- bias algoritmik,

- data poisoning,
- model inversion,
- model extraction,
- adversarial attack,
- hallucination pada generative AI,
- risiko hukum (UU PDP),
- risiko reputasi.

Risk Scoring AI:

- impact: low–critical
- likelihood: low–high
- detectability: low–high
- exposure: narrow–wide

Output:

- AI risk score,
- mitigating actions,
- model approval status.

12.7 Keamanan Data untuk AI (AI Data Security)

Standar minimum:

1. Data Minimization – hanya gunakan data diperlukan.
2. Data Labeling Governance – labeling harus berkualitas dan audit-able.
3. Dataset Privacy
    - anonymization,
    - pseudonymization,
    - masking.
4. Data Provenance – asal data harus jelas.
5. Compliance with UU PDP – legal basis pemrosesan data.
6. Access Control – dataset AI hanya boleh diakses per kebutuhan.
7. Dataset Versioning – untuk akurasi dan audit jejak model.

12.8 Keamanan Model AI (AI Model Security Controls)

Sangat direkomendasikan untuk menerapkan:

1. Model Hardening

- Adversarial training,
- Feature squeezing,
- Gradient masking (opsional).

2. Confidence Scoring

Model harus memberikan tingkat keyakinan (confidence threshold).

3. Model Explainability

Untuk high-risk AI:

- SHAP, LIME, Explainable Boosting Machine.

4. Anti-Model Extraction

- API rate limiting,
- dynamic model watermarking,
- request filtering.

5. Anti-Data Poisoning

- input validation,
- anomaly detection during training.

6. Anti-Model Inversion Attack

- noise injection,
- output bounding.

7. Logging Wajib

- model input (non-sensitive),
- output,
- confidence,
- decision time.

12.9 Validasi Model AI (Model Validation & Testing)

Pengujian dilakukan secara:

1. Pre-deployment

- accuracy test,
- bias test (gender, usia, wilayah),
- fairness scoring,
- adversarial robustness test,
- stress testing.

2. Post-deployment

- monitoring drift (data/model drift),
- degradation detection,
- fairness re-evaluation per 3–6 bulan,
- retraining policy.

3. Third-party Validation

Untuk high-risk AI:

- external audit,
- peer review,
- regulator review jika diperlukan.

12.10 Pengawasan & Audit AI

Audit AI mencakup:

A. Audit Dokumentasi

- dataset,
- model card,
- bias test report,
- security test,
- explainability report.

B. Audit Kepatuhan

Mengacu:

- UU PDP,
- AI ethics,
- AFTECH AI policy.

C. Audit Teknis

- adversarial testing,
- robustness testing,
- model extraction simulation.

Audit dilakukan minimal 1 kali per tahun untuk high-risk AI.

12.11 AI Incident Response & Model Monitoring

Organisasi wajib membuat AI Incident Response Playbook khusus:

Kategori AI Incident

- kesalahan keputusan model,
- bias signifikan (unfair output),
- model drift,
- data leak dalam training set,
- model extraction,
- hallucination berbahaya (untuk generative AI),
- abuse oleh pihak ketiga.

Monitoring Real-time

- anomaly scores,
- drift detection,
- performance degradation alerts.

12.12 Penggunaan AI Generatif (Generative AI Policy)

Generative AI (ChatGPT, Gemini, Claude, Llama) digunakan untuk:

- summarization,
- productivity tools,
- drafting internal docs,
- code generation,

- customer interaction (opsional).

Larangan

- memasukkan data pribadi,
- memasukkan data rahasia pelanggan,
- memasukkan source code kritikal,
- melakukan keputusan otomatis tanpa human-in-the-loop.

Wajib

- red-teaming internal LLM,
- prompt injection testing,
- hallucination filtering.

12.13 Tata Kelola Agentic AI (Advanced Autonomous AI)

Jika anggota AFTECH menggunakan autonomous agent AI:

Wajib menerapkan:

1. Human approval untuk keputusan berisiko tinggi
2. Safety limits
3. Behavior constraints
4. Autonomy Risk Register
5. Model chaining auditability
6. Rollback & kill switch
7. Execution sandboxing

Ini penting untuk perusahaan yang memakai autonomous fraud engine atau auto-decision scoring.

12.14 Struktur Tata Kelola AI dalam Perusahaan

Direkomendasikan memiliki struktur:

1. AI Governance Council

- Komite lintas divisi (CISO, CTO, Legal, Risk, Data Science).

2. AI Risk Officer

- bertanggung jawab terhadap risiko & kepatuhan.

3. Data Science Team

- model development & MLOps.

4. AI Ethics Team

- fairness, transparency, bias governance.

5. IT Security & CISO

- AI security & model protection.

12.15 Dokumentasi AI yang Wajib Dibuat Perusahaan

Dokumen setidaknya mencakup:

1. AI Policy – kebijakan umum.
2. Model Cards – dokumentasi teknis tiap model.
3. Data Sheets for Datasets – asal, kualitas, risiko dataset.
4. AI Risk Assessment Report.
5. Explainability Report.
6. Bias Testing Report.
7. AI Incident Report (jika terjadi).
8. Model Lifecycle Logbook.
9. Third-party AI Contract & SLA.

BAB 13
FRAUD DETECTION &
FRAUD RISK MANAGEMENT FRAMEWORK

FRAUD DETECTION & FRAUD RISK MANAGEMENT FRAMEWORK, disusun sangat komprehensif, implementable, dan sesuai standar regulator serta best practice global:

- POJK ITSK & SEOJK 29/2022
- PBI 22/2024 (Sistem Pembayaran & Ketahanan Siber BI)
- UU ITE & UU PDP
- NIST Fraud Framework
- ACFE Fraud Framework
- FFIEC (Anti-Fraud Guidance)
- Basel Committee – Operational Risk & Fraud
- MITRE ATT&CK for Fraud
- FIDO & OpenID Security Standard

Bab ini sangat penting karena fraud digital adalah risiko terbesar di sektor Fintech, terutama yang menggunakan:

- e-wallet & pembayaran,
- P2P lending,
- buy-now-pay-later (BNPL),
- digital banking,
- neobank,
- aggregator API,
- e-KYC, dan
- kanal digital lainnya.

Fraud digital semakin canggih dan memanfaatkan kombinasi teknik sosial, kelemahan platform, serangan bot, rekayasa identitas, manipulasi API, serta penyalahgunaan data.

Karena itu, diperlukan kerangka yang sistematis untuk mencegah, mendeteksi, merespons, dan memulihkan fraud dalam layanan Fintech.

13.1 Tujuan Framework Fraud Management

1. Mengurangi kerugian finansial perusahaan dan konsumen.
2. Melindungi pengguna dari tindak kejahatan digital.
3. Meningkatkan integritas dan kepercayaan publik pada Fintech.
4. Memenuhi kewajiban regulasi (OJK/BI/UU PDP).
5. Membangun deteksi fraud yang proaktif & real-time.
6. Mendukung investigasi hukum dan audit.

13.2 Klasifikasi Fraud pada Sektor Fintech

Fraud pada Fintech dibagi menjadi 6 domain besar:

1. Account-Based Fraud

- Account Takeover (ATO),
- credential stuffing,
- SIM swap,
- phishing,
- OTP interception,
- device hijacking.

2. Identity Fraud

- stolen identity,
- synthetic identity,
- fake KYC documents,
- AI-generated identity (deepfake KYC).

3. Transactional Fraud

- unauthorized transfer,
- merchant fraud,
- payment reversal fraud,
- refund abuse,
- chargeback fraud.

4. Loan & Credit Fraud

- multiple account loan,
- fake employer data,
- manipulated credit score,
- loan stacking,
- first-payment default (fraudulent borrowers).

5. Insider Fraud

- privilege abuse,
- data leak,
- unauthorized system access,
- collusion fraud.

6. Infrastructure & API Fraud

- bot-driven fraud,
- API abuse,
- MITM attack,
- fraud via compromised vendor systems.

13.3 Fraud Risk Governance Structure

Setiap anggota AFTECH direkomendasikan untuk memiliki:

1. Fraud Risk Committee

- CFO, CISO, Chief Risk Officer, Chief Compliance Officer, CTO.
- Mengawasi risiko fraud dan memutuskan mitigasi strategis.

2. Fraud Management Unit (FMU) / Fraud Operations Team

- bertanggung jawab monitoring harian & investigasi.

3. Fraud Data Science Team

- model detection, ML scoring, graph analytics.

4. Internal Audit

- memastikan efektivitas kontrol anti-fraud.

5. CSIRT / Cybersecurity Team

- bekerja sama dalam kasus fraud berbasis siber.

13.4 Fraud Risk Assessment (ID, Analyse & Score)

Risiko fraud dicatat dalam Fraud Risk Register dan dievaluasi berdasarkan:

- probability (likelihood),
- impact (severity),
- fraud vector (human/tech/bot),
- detectability,
- fraud maturity pattern.

Gunakan matriks risiko 5×5 untuk prioritas mitigasi.

Metode yang digunakan:

- ACFE Fraud Tree,
- MITRE Fraud Techniques,
- ML anomaly-based scoring,
- behavioral profiling,
- attack surface mapping.

13.5 Pencegahan Fraud (Fraud Prevention Controls)

Pencegahan adalah lapisan pertama.

1. Identity & Access Protection

- e-KYC with liveness detection & anti-spoofing,
- biometric multi-factor,
- risk-based authentication (RBA),
- device binding (device fingerprinting),
- geolocation profiling.

2. Credential Security

- auto-blocking on failed login attempts,
- passwordless login (opt.),
- mandatory MFA for high-risk users.

3. Transaction Protection

- dynamic fraud scoring,
- transaction velocity rules,
- risk-based step-up authentication (OTP/biometric),
- challenge-response for abnormal transactions.

4. API Protection

- OAuth2/OIDC strict implementation,
- anti-replay tokens,
- dynamic rate limiting.

5. Behavioral Biometrics

Analisis:

- kecepatan mengetik,
- pola swipe,
- pola navigasi,
- gyroscope.

6. Anti-Bot Technology

- CAPTCHA v3,
- bot detection engine,
- device telemetry analysis.

13.6 Deteksi Fraud (Detection Controls)

Deteksi harus berjalan real-time.

1. Rule-Based Detection

Contoh rule:

- login dari IP sangat berbeda dari biasanya,
- device baru + nominal besar,
- transaksi cepat berulang.

2. Machine Learning Models

Jenis model:

- anomaly detection (unsupervised),
- supervised fraud classifier,
- graph neural network (GNN)
  → sangat efektif untuk mendeteksi syndicate fraud.

3. Graph Analytic

Untuk mendeteksi:

- kolusi,
- sindikat multi-akun,
- pinjaman berulang,
- merchant fraud.

Tools:

- Neo4j,
- TigerGraph,
- Graphistry.

4. Threat Intelligence

Dari:

- AFTECH-CSIRT,
- BSSN,
- BI,
- darkweb monitoring,
- telco intel (SIM swap).

5. Fraud Monitoring Center (24/7)

Menggunakan:

- SIEM,
- fraud engine,
- anti-bot platform,
- custom dashboards.

13.7 Response & Investigation (Fraud Response Lifecycle)

Ketika fraud terdeteksi:

1. Containment

- freeze rekening,
- suspend akun,
- blokir device,
- disable API keys.

2. Investigation

- analisis log,
- trace transaksi,
- device fingerprinting,
- mapping ke sindikat,
- korelasi dengan fraud intelligence.

3. Customer Notification

Jika saldo/akun berisiko.

4. Law Enforcement Coordination
Melibatkan:

- kepolisian (cybercrime unit),
- penyidik OJK/BI.

5. Recovery

- reversal transaksi (jika memungkinkan),
- pemulihan akun,
- reset credential.

6. Root Cause Analysis
Mandatory setelah insiden fraud besar.

13.8 Fraud Monitoring Tools & Architecture

Arsitektur detection minimum:

1. Data Ingestion Layer
    - logs, transaksi, device data, biometrik.
2. Real-time Stream Processing
    - Kafka, Flink, Spark.
3. Machine Learning Engine
    - fraud scoring, anomaly detection.
4. Rules Engine
    - risk scoring thresholds.
5. Decision Engine
    - approve, challenge, or block.
6. Case Management System
    - investigasi, workflow, evidences.
7. Dashboard Monitoring
    - alerting, metrics, heatmaps.

13.9 Fraud Metrics, KPI & KRI

Key Performance Indicators (KPI)

1. Fraud detection rate (> 90%)
2. Fraud false positive rate (target < 2–5%)
3. Mean Time to Detect Fraud (MTTD)
4. Mean Time to Respond (MTTR)
5. % fraud cases resolved in SLA
6. Customer impact score

Key Risk Indicators (KRI)

1. Lonjakan transaksi abnormal

2. Tingginya login gagal
3. Kenaikan blocking rate
4. Kenaikan account takeover attempt
5. Fraud financial losses

13.10 Perlindungan Data untuk Anti-Fraud (UU PDP)

Karena fraud detection memakai data sensitif:

Wajib:

1. legal basis pemrosesan data,
2. data minimization,
3. encryption,
4. strict access control,
5. retention limit,
6. DPIA untuk fraud AI.

Tidak boleh:

- memprofilkan pengguna untuk tujuan diskriminatif,
- menggunakan data tanpa izin pengguna,
- mengirim data ke pihak ketiga yang tidak sesuai kontrak.

13.11 Kolaborasi Industri Anti-Fraud (AFTECH Fraud Network)

AFTECH dapat bekerjasama dengan pihak terkait seperti BSSN untuk membentuk:

1. Fraud Information Sharing Group

Berbagi:

- nomor rekening penipu,
- nomor HP fraud,
- domain phishing,
- modus mengemuka.

2. Fraud Early Warning System

Memberikan alert ke seluruh anggota.

3. Koordinasi Dengan Regulator

OJK, BI, BSSN, Kemenkominfo, dan perbankan.

4. Darkweb & Threat Intel Hub

Untuk memonitor:

- jual beli data,
- sindikat siber lokal,
- malware/ phishing kits.

13.12 Fraud Prevention for Customers (Customer Education)

Selain sistem internal, edukasi publik sangat penting.

Isi edukasi:

- jangan bagikan OTP,
- hindari phishing & social engineering,
- cara cek aplikasi asli,
- keamanan PIN,
- waspada rekayasa psikologis.

Media:

- email blast,
- in-app notification,
- media sosial,
- video pendek,
- blog security.

13.13 Regulasi dan Kepatuhan Anti-Fraud

Anggota AFTECH wajib mematuhi:

- POJK ITSK,
- SE OJK terkait fraud,
- PBI anti-fraud & siber,
- UU ITE,
- UU PDP,
- standar pelaporan insiden.

Penggunaan data untuk fraud detection harus proporsional dan sesuai hukum dan peraturan yang berlaku.

BAB 14
CYBER THREAT INTELLIGENCE (CTI) & EARLY WARNING SYSTEM

CYBER THREAT INTELLIGENCE (CTI) & EARLY WARNING SYSTEM, disusun sangat komprehensif, operasional, dan siap diterapkan oleh seluruh anggota AFTECH.
Bab ini mengikuti standar global:

- NIST SP 800-150 – Cyber Threat Intelligence Guide
- MITRE ATT&CK, D3FEND, CAPEC
- ISO 27002 & ISO 27035
- FIRST, ENISA Threat Intel Framework
- Financial Sector ISAC (FS-ISAC)
- BSSN National Cyber Threat Intelligence Standard

Karena sektor Fintech adalah salah satu target utama penjahat siber, CTI dan sistem peringatan dini (EWS) menjadi komponen strategis yang tidak bisa diabaikan.

Cyber Threat Intelligence (CTI) adalah proses pengumpulan, analisis, dan distribusi informasi ancaman siber secara terstruktur untuk mendukung deteksi, pencegahan, dan pengambilan keputusan strategis.

Dalam ekosistem Fintech, CTI berfungsi sebagai radar pertahanan, mendeteksi ancaman jauh sebelum menimbulkan dampak operasional atau kebocoran data.

14.1 Tujuan dan Manfaat CTI bagi Fintech

1. Mengidentifikasi ancaman sebelum menjadi serangan.
2. Meningkatkan deteksi SOC melalui IOC & TTP terbaru.
3. Mengurangi risiko fraud dan ATO melalui threat intel real-time.
4. Mengamankan API dan integrasi open finance.
5. Mendukung investigasi insiden dan attributing attackers.
6. Membantu kepatuhan terhadap regulator dan standar keamanan.
7. Menguatkan kolaborasi lintas industri untuk menghadapi serangan masif.

14.2 Ruang Lingkup CTI dalam Konteks Fintech

CTI mencakup:

1. Strategic Intelligence

- tren ancaman jangka panjang,
- lanskap adversaries,
- mapping geopolitik digital.

2. Operational Intelligence

- malware campaign,
- phishing operation,
- botnet assignment,
- darkweb discussions.

3. Tactical Intelligence

- Indicators of Compromise (IOC),
- signatures,
- malicious IP/domain hashes,
- TTP adversaries (MITRE ATT&CK).

4. Technical Intelligence

- exploit PoC,
- vulnerability details,
- zero-day trends,
- botnet C2 information.

14.3 Kategori Ancaman Utama pada Fintech

1. Financially Motivated Cybercriminals

- pemerasan,
- ransomware,
- ATO,
- money mule.

2. Fraud Syndicates

- synthetic identity,
- SIM swap fraud,
- phishing & social engineering.

3. APT Groups (Advanced Persistent Threat)

- serangan menuju infrastruktur keuangan,
- serangan pada API bank/Fintech.

4. Hacktivists

- DDoS,
- defacement,
- data breach publik.

5. Insider Threat

- pegawai nakal,
- vendor compromise.

14.4 Cyber Threat Intelligence Lifecycle

Mengacu kepada NIST:

1. Planning & Direction
2. Collection
3. Processing & Normalization
4. Analysis & Correlation
5. Production (Intelligence Output)
6. Dissemination & Sharing
7. Feedback & Refinement

Setiap organisasi Fintech sangat direkomendasikan memiliki siklus ini meski dalam skala sederhana.

14.5 Sumber CTI yang Wajib Digunakan Fintech

1. Internal Sources

- SIEM logs,
- EDR/XDR alerts,
- fraud system alerts,
- honeypots,
- abuse reports.

2. External Sources

- AFTECH-CSIRT early warning system,
- BSSN National CTI,
- BI & OJK advisories,
- FS-ISAC,
- Open-source CTI (OSINT),
- Threat intel vendors (Recorded Future, CrowdStrike, Palo Alto Unit 42, dll).

3. Darkweb & Deepweb Monitoring

- jual beli kredensial Fintech,
- database bocor,
- malware kits,
- phishing-as-a-service.

4. Malware & Phishing Repositories

- VirusTotal,
- PhishTank,
- Malpedia.

14.6 Analisis CTI Menggunakan MITRE ATT&CK

MITRE ATT&CK adalah standar analisis ancaman berbasis TTP (tactics, techniques, and procedures).

Setiap intel harus di-mapping ke:

- Initial Access

- Privilege Escalation
- Lateral Movement
- Credential Access
- Exfiltration
- Impact

Fintech wajib memanfaatkan:
- MITRE ATT&CK Navigator untuk heatmap ancaman,
- D3FEND untuk kontrol teknis mitigasi.

14.7 Early Warning System (EWS) untuk Fintech

AFTECH mengusulkan model EWS nasional untuk Fintech, berfungsi seperti radar ancaman dengan komponen:

1. Threat Feed Aggregator
- IOC/IP/domain berbahaya real-time.
- integrasi API dengan anggota AFTECH.

2. Fraud Threat Feed
- nomor rekening penipu,
- nomor HP fraud,
- device ID mencurigakan.

3. Darkweb Alert
- data Fintech dijual,
- campaign phishing baru,
- skema fraud emerging.

4. Vulnerability Alert
- zero-day (misalnya RCE, supply chain),
- critical CVE,
- patch advisories.

5. DDoS Early Warning
- deteksi traffic abnormal antar Fintech,
- indikator botnet.

6. API Threat Warning
- attack signatures terhadap Open Finance API.

14.8 Arsitektur CTI & EWS yang Direkomendasikan

Sistem CTI minimum terdiri dari:

1. Collection Layer
- threat feeds, logs, honeypots, darkweb scrapers.

2. Data Processing Layer

- normalisasi IOC,
- de-duplication,
- correlation engine.

3. Analysis Layer

- scoring,
- threat clustering,
- MITRE mapping.

4. Storage Layer

- threat intel database,
- IOC repository.

5. Dissemination Layer

- API ke SIEM Fintech,
- dashboard intel,
- automated alerts.

6. Integration Layer

- fraud engines,
- SOC playbooks,
- IR playbooks.

14.9 Threat Scoring Model

Mengacu ENISA + NIST:

Parameter:

1. Threat Credibility
2. Threat Capability
3. Attack Complexity
4. Motivation
5. Historical Attacks
6. Exposure to Fintech
7. Severity & Potential Damage

Output:

- Threat Score (1–10)
- Prioritas mitigasi otomatis

14.10 CTI Use Cases untuk Fintech

1. Prevention

- blocklist IP/domain botnet,
- patch priority via vulnerability intel.

2. Detection

- correlate IOC dengan log internal,
- anomali akses API.

3. Response

- IR playbook otomatis ketika TTP tertentu terdeteksi.

4. Fraud Protection

- blacklist device/sindikasi penipu,
- informasikan pattern fraud antar Fintech.

5. Risk Management

- penyesuaian risk appetite berdasarkan ancaman terbaru.

6. Third-Party Security

- cek vendor di darkweb,
- supply chain risk scoring.

14.11 CTI Sharing Model di AFTECH

Untuk memperkuat ekosistem, AFTECH membangun:

1. AFTECH Cyber Threat Intelligence Hub

Berisi:

- IOC repository,
- taktik cybercrime,
- darkweb findings,
- fraud network intel.

2. Fintech-to-Fintech Sharing Group

Anggota dapat membagikan:

- domain phishing baru,
- nomor rekening penipu,
- pola bot attack,
- modus fraud terkini.

3. Automated IoC Sharing (STIX/TAXII)

Protokol standar untuk berbagi:

- hash malware,
- IP berbahaya,
- domain berbahaya,
- malware family.

4. Joint Cyber Drill

Simulasi ancaman besar antar Fintech untuk:

- meningkatkan readiness,

- menguji IR lintas industri.

14.12 Integrasi CTI dengan SOC, CSIRT, dan Fraud Unit

CTI menghasilkan:

- IOC
- TTP
- Threat score
- Emerging threats

SOC:

- mengkorelasikan intel dengan SIEM.

CSIRT:

- menggunakan intel untuk IR decision-making.

Fraud Unit:

- menganalisis pergerakan sindikat,
- menemukan relasi antar kasus.

Integrasi ini direkomendasikan untuk dilakukan secara otomatisasi semaksimal mungkin.

14.13 Peran & Struktur Tim CTI

Untuk anggota AFTECH menengah-besar:

1. Threat Intelligence Analyst
Menganalisis data ancaman.

2. CTI Engineer
Integrasi API, automation, ingestion.

3. Threat Hunter (Opsional)
Proaktif mencari ancaman.

4. Malware Analyst (Opsional)
Untuk analisis file berbahaya.

5. CTI Lead / Manager
Mengatur produksi intel.

14.14 KPI & KRI CTI

KPI

- jumlah intel relevan yang diproduksi,
- IOC-to-detection conversion rate,
- response time dari intel → action,

- darkweb detection rate.

KRI

- peningkatan serangan pada sektor Fintech,
- jumlah IOC meningkat drastis,
- new malware strains targeting Fintech,
- abnormal botnet traffic.

14.15 Kepatuhan & Regulasi CTI

CTI harus mematuhi:

- UU PDP (data pribadi tidak boleh diekspos),
- UU ITE,
- regulasi OJK/BI terkait pelaporan insiden,
- larangan mengumpulkan data ilegal.

BAB 15
MANAJEMEN IDENTITAS & AKSES (IAM) & ZERO TRUST ARCHITECTURE

MANAJEMEN IDENTITAS & AKSES (IAM) BERBASIS ZERO TRUST, disusun sangat komprehensif, operasional, dan implementable, menjadi fondasi keamanan bagi organisasi Fintech anggota AFTECH.
Referensi standar global:

- NIST SP 800-63 (Digital Identity Guidelines)
- NIST SP 800-207 (Zero Trust Architecture)
- ISO 27001 Annex A – Access Control
- FIDO2 / WebAuthn Standards
- OAuth 2.0 / OIDC Security Best Practices
- CSA Cloud Controls Matrix (CCM)
- PCI DSS Access Control Requirements

IAM adalah tulang punggung keamanan Fintech; kesalahan konfigurasi akses merupakan penyebab lebih dari 40% insiden keamanan. Karena itu, framework IAM harus ketat, konsisten, dan diaudit secara berkala.

IAM mengatur siapa yang dapat mengakses apa, kapan, dan bagaimana, secara aman dan terkontrol.

Arsitektur Zero Trust memastikan bahwa akses tidak otomatis dipercaya, meskipun berasal dari jaringan internal.

15.1 Tujuan IAM & Zero Trust

1. Melindungi sistem perusahaan dari akses tidak sah.
2. Memastikan setiap identitas (manusia atau mesin) tervalidasi secara kuat.
3. Menerapkan prinsip least privilege dan need-to-know.
4. Mencegah insiden insider threat dan penyalahgunaan akses.
5. Mengamankan API dan layanan open finance.
6. Memperkuat deteksi penyusupan dan anomali akses.
7. Memenuhi regulasi keamanan siber OJK–BI–UU PDP.

15.2 Lingkup IAM dalam Sektor Fintech

IAM mencakup:

1. Human Identity

- pegawai,
- vendor/outsourcing,
- regulator (akses audit),
- mitra integrasi.

2. Machine Identity

- API keys,
- service accounts,
- cloud IAM roles,
- microservices identity.

3. Customer Identity

- user authentication,
- device binding,
- behavioral biometrics.

4. API & Application Identity

- OAuth tokens,
- JWT,
- workload identity.

15.3 Prinsip Zero Trust untuk Fintech

Zero Trust berdasarkan 7 prinsip inti:

1. Never Trust, Always Verify
2. Continuous Authentication & Authorization
3. Least Privilege Access
4. Micro-Segmentation
5. Device Posture Validation
6. Contextual & Risk-Based Access
7. Encrypt Everywhere

Setiap akses harus melalui risk assessment berdasarkan:

- lokasi,
- device posture,
- time of access,
- role,
- behavioral pattern.

15.4 Kerangka IAM untuk Fintech

IAM dibagi menjadi 4 pilar:

1. Identity Governance & Administration (IGA)

Mengatur lifecycle identitas.

2. Access Management

Autentikasi & otorisasi.

3. Privileged Access Management (PAM)

Kontrol akses level tinggi.

4. Machine Identity & API Access Control
Mengamankan workload, API, dan sistem otomatis.

15.5 Identity Lifecycle Management (IAM Lifecycle)

IAM diharapkan untuk mencakup siklus penuh:

1. Identity Creation

- onboarding otomatis lewat HRIS,
- verifikasi identitas pegawai/vendor.

2. Provisioning

- access diberikan berdasarkan role,
- auto-provision untuk aplikasi standar.

3. Access Review & Certification

- dilakukan minimal setiap 3 bulan,
- memastikan tidak ada access creep.

4. Rotation & Audit

- password, key, token harus diratakan periodik,
- semua akses dicatat dan dapat diverifikasi.

5. Deprovisioning
Harus otomatis dalam ≤ 24 jam saat pegawai:

- keluar,
- cuti panjang,
- pindah proyek,
- kontrak vendor berakhir.

15.6 Mekanisme Autentikasi (Authentication Requirements)

Multi-Factor Authentication (MFA) diwajibkan Untuk:

- akses admin,
- akses cloud,
- akses VPN,
- akses production systems,
- akses API management.

Jenis MFA yang direkomendasikan:

- FIDO2/WebAuthn,
- TOTP-based authenticator,
- push authentication (Okta, Duo),
- biometrik untuk mobile.

OTP via SMS tidak direkomendasikan untuk sistem internal.

Risk-Based Authentication (RBA)
Setiap login harus memiliki skor risiko berdasarkan:

- device kepercayaan,
- lokasi IP (geo-risk),
- waktu akses,
- velocity login,
- pola perilaku pengguna.

Jika skor risiko tinggi → trigger step-up authentication.

15.7 Mekanisme Otorisasi (Authorization Requirements)

1. Role-Based Access Control (RBAC)

- role harus didefinisikan jelas,
- role standar untuk pegawai baru.

2. Attribute-Based Access Control (ABAC)
Akses berdasarkan:

- divisi,
- lokasi,
- project assignment.

3. Policy-Based Access Control (PBAC)
Untuk sistem kompleks, misalnya:

- open finance API,
- cloud IAM.

4. Just-In-Time (JIT) Access
Akses admin diberikan hanya saat dibutuhkan, dengan timer.

15.8 Privileged Access Management (PAM)
Akses privileged adalah risiko yang tinggi dalam pengelolaan teknologi.
Kontrol yang wajib:

1. Password vaulting (contoh: cyberark, thycotic).
2. Session recording untuk seluruh akses admin.
3. Just-in-time PAM (temporary elevation).
4. Command restriction untuk super admin.
5. Approval workflow untuk akses sensitif.
6. Segregation of duties (SoD):
    - developer tidak boleh akses produksi,
    - devops tidak boleh akses data pelanggan,
    - fraud team tidak boleh mengubah rules tanpa pengawasan.

15.9 Zero Trust Network Security

1. Micro-Segmentation

Memisahkan:

- production vs development,
- API gateway,
- database,
- fraud engine,
- internal tools.

2. East-West Traffic Inspection

Setiap komunikasi antar layanan diperiksa.

3. Mutual TLS (mTLS)

Wajib untuk microservices.

4. Device Posture Checking

Sebelum login, device harus:

- terenkripsi,
- memiliki endpoint protection,
- tidak di-root/jailbreak.

15.10 Machine Identity & API Keys Management

Karena Fintech mengandalkan API dan automation, machine identity harus diamankan.

Sangat direkomendasikan untuk:

1. tidak menyimpan API key di source code,
2. gunakan secrets manager (AWS Secrets Manager, HashiCorp Vault),
3. key rotation minimal setiap 90 hari,
4. least privilege untuk API keys,
5. audit log untuk semua penggunaan API.

15.11 Customer Identity & Access Management (CIAM)

Untuk end-user:

1. Pengamanan Identitas Pengguna

- device binding,
- behavioral biometrics,
- enforce strong password policy,
- passwordless login (opsional).

2. Fraud & ATO Prevention

- velocity rules,
- impossible travel detection,
- user risk scoring.

3. Data Minimization

- hanya mengumpulkan data yang diperlukan,
- proteksi sesuai UU PDP.

15.12 Logging, Monitoring, & Analytics untuk IAM

Setiap akses (human/machine/API) direkomendasikan untuk dicatat setidaknya:

- login success/failure,
- privilege escalation,
- role change,
- non-compliant devices,
- expired tokens.

Gunakan:

- SIEM,
- UEBA (User & Entity Behavior Analytics),
- anomaly detection.

15.13 Audit & Review IAM (Quarterly & Annual)

Audit mencakup:

- kelebihan akses (access creep),
- inactive accounts,
- shadow admin,
- API keys tidak terpakai,
- expired certificates.

Review dilakukan:

- Quarterly – akses pegawai.
- Annual – desain IAM & kebijakan.
- Ad-hoc – saat insiden.

15.14 Metrik Keberhasilan IAM

KPI:

1. akses privileged yang diaudit (target 100%).
2. completion rate MFA (> 99%).
3. inactive accounts removed (< 24 jam).
4. API key rotation compliance (> 98%).
5. anomalous login detection rate.

KRI:

1. lonjakan login gagal,
2. perangkat tidak compliant,
3. meningkatnya permintaan elevation access,
4. shadow admin terdeteksi.

15.15 Kepatuhan & Regulasi IAM

IAM setidaknya memenuhi kepatuhan yang berlaku, sebagai contoh:

- UU PDP (akses berbasis need-to-know),
- POJK ITSK/SEOJK 29/2022,
- PBI 22/2024,
- PCI DSS (jika memproses kartu),
- BSSN Security Framework,
- standar audit TI OJK/BI.

BAB 16
CONTINUITY PLANNING, BCP/DRP & CYBER CRISIS MANAGEMENT

CONTINUITY PLANNING, BUSINESS CONTINUITY PLAN (BCP), DISASTER RECOVERY PLAN (DRP), & CYBER CRISIS MANAGEMENT, disusun sangat komprehensif, operasional, dan siap diimplementasikan oleh seluruh anggota AFTECH.

Bab ini mengikuti standar global:

- ISO 22301 – Business Continuity Management System (BCMS)
- ISO 27031 – ICT Readiness for Business Continuity
- NIST SP 800-34 – Contingency Planning Guide for IT
- FFIEC Business Continuity Guidelines
- ENISA Business Continuity for Critical Digital Services
- Regulasi OJK–BI terkait ketahanan operasional & insiden siber

BCP/DRP sangat krusial karena Fintech termasuk Critical Digital Infrastructure, dan kegagalan layanan bisa mengakibatkan:

- kerugian finansial,
- gangguan sistemik,
- reputational damage,
- hilangnya kepercayaan publik.

16.1 Tujuan Continuity Planning

1. Menjamin layanan Fintech tetap beroperasi dalam kondisi gangguan.
2. Memastikan pemulihan cepat setelah insiden siber, bencana alam, atau kegagalan sistem.
3. Melindungi data dan transaksi pengguna dari kehilangan atau korupsi.
4. Menghindari risiko sistemik pada ekosistem keuangan digital.
5. Memenuhi kewajiban regulasi dari OJK–BI.
6. Mengurangi risiko kerugian finansial dan reputasi.
7. Meningkatkan ketahanan operasional digital (Digital Operational Resilience).

16.2 Ruang Lingkup BCP/DRP

Penerapan continuity mencakup:

- infrastruktur TI (cloud/on-prem),
- aplikasi inti,
- API open finance,
- pembayaran digital,
- core lending/ewallet system,
- data center & cloud region,
- SDM kritikal,
- vendor & third-party services,

- customer communication,
- cyber incident response & recovery.

16.3 Business Impact Analysis (BIA)

BIA adalah fondasi BCP.
Setiap anggota AFTECH wajib melakukan BIA minimal 1x per tahun.
Output BIA:

1. Critical Business Functions (CBF)
2. Dampak gangguan (keuangan, operasional, legal, reputasi)
3. Maximum Tolerable Downtime (MTD)
4. Recovery Time Objective (RTO)
5. Recovery Point Objective (RPO)
6. Prioritas pemulihan sistem

Contoh kategori RTO standar Fintech:

Sistem	RTO	RPO
Payment API	15 menit	0–5 menit
Core lending	1 jam	< 15 menit
KYC system	4 jam	< 30 menit
Reporting system	24 jam	< 24 jam

16.4 Risk Assessment untuk Continuity

Analisis risiko meliputi:

1. Risiko Teknologi

- cloud outage,
- data corruption,
- hardware failure.

2. Risiko Siber

- ransomware,
- DDoS,
- data breach,
- insider sabotage.

3. Risiko Operasional

- human error,
- SOP failure.

4. Risiko Fisik

- bencana alam,
- banjir,
- kebakaran,
- gempa.

5. Risiko Vendor

- kegagalan API partner,
- cloud malfunction,
- telco outage.

16.5 Business Continuity Plan (BCP) – Struktur Dokumen

BCP setidaknya memiliki komponen berikut:

1. Pendahuluan & tujuan
2. BCP governance structure
3. Critical Business Functions (CBF)
4. RTO & RPO per sistem
5. Continuity strategy & mitigation
6. Communication plan
7. Emergency response procedure
8. Workforce continuity (remote, backup, rotation)
9. Vendor contingency plan
10. Evacuation plan (opsional)
11. Panduan pemulihan layanan
12. Checklist BCP
13. Appendix kontak darurat & peta risiko

16.6 Disaster Recovery Plan (DRP) – Komponen Inti

DRP adalah prosedur teknis pemulihan layanan TI.

DRP setidaknya mencakup:

1. Sistem Prioritas

- aplikasi core,
- API gateway,
- database,
- payment switch,
- fraud engine.

2. Backup Strategy

- incremental + full backup,
- 3-2-1 backup rule:
  - 3 copies
  - 2 media
  - 1 offsite/immutable storage (WORM)

3. Data Replication

- multi-region replication,
- synchronous/asynchronous replication.

4. Failover Strategy

- pilot light,
- warm standby,
- active-active (untuk Fintech besar).

5. Recovery Procedures

- restore database,
- start application stack,
- validate API connectivity,
- health check services.

6. DR Runbook

- langkah-langkah pemulihan detail,
- screenshot/CLI commands,
- siapa melakukan apa (role-based).

7. Testing & Verification

- UAT pasca pemulihan,
- rollback readiness.

16.7 Cloud Disaster Recovery Requirements

Jika perusahaan menggunakan cloud computing, sangat direkomendasikan untuk memenuhi:

1. Multi-AZ (Availability Zone)
2. Multi-region redundancy (opsional tapi direkomendasikan)
3. Automated failover (RDS, Redis, Kubernetes)
4. Infrastructure-as-Code (IaC) DR
5. Automated backup validation
6. DR drills minimal 2x per tahun

16.8 Crisis Management Structure

Saat terjadi insiden besar, struktur crisis management harus aktif.

1. Cyber Crisis Management Team (CCMT)

- CEO (ketua),
- CISO,
- CTO,
- COO,
- Chief Risk Officer,
- Head of Communications.

2. Peran CCMT

- membuat keputusan strategis,
- menentukan layanan yang dipulihkan dulu,
- berkoordinasi dengan regulator,

- mengatur komunikasi publik.

3. Activation Criteria

Crisis mode aktif jika terjadi:

- ransomware,
- downtime sistem > RTO,
- kebocoran data besar,
- serangan DDoS yang menyebabkan layanan berhenti,
- kegagalan cloud region.

16.9 Cyber Crisis Playbook

Playbook dapat mencakup skenario sebagai berikut:

1. Ransomware

- isolate servers,
- backup restore,
- verify no reinfection,
- regulator notification.

2. DDoS Large Attack

- traffic rerouting,
- CDN protection,
- upstream filtering.

3. Cloud Region Outage

- failover ke region lain,
- DNS switching,
- traffic rerouting.

4. Payment/Transfer Service Outage

- fallback manual process,
- partial service recovery.

5. Multi-API Partner Down

- API prioritization,
- transaction queue mechanisms.

16.10 Crisis Communication Plan

Harus disiapkan untuk:

1. Regulator

- laporan ke OJK, BI, BSSN (≤ 1×24 jam).
- format sesuai SE regulator.

2. Pengguna

- notifikasi jelas namun tidak membuat panik,

- edukasi langkah yang harus dilakukan.

3. Media

- press statement,
- designated spokesperson.

4. Internal Staff

- pembaruan rutin via WhatsApp/Slack/email.

Semua komunikasi harus:

- faktual,
- tidak spekulatif,
- menjaga kepercayaan publik.

16.11 Testing BCP/DRP (Wajib Tahunan)

Jenis pengujian:

1. Tabletop Exercise

Simulasi non-teknis → diskusi alur pemulihan.

2. Simulation Exercise

Simulasi teknis tanpa mematikan layanan (partial test).

3. Full Disaster Recovery Drill

Failover dan pemulihan nyata.

4. Communication Drill

Menguji kesiapan tim & kecepatan respons.

Output:

- laporan hasil tes,
- gaps & vulnerabilities,
- corrective actions.

16.12 Dokumentasi & Audit BCP/DRP

Dokumen yang perlu disimpan:

- BCP logbook,
- DRP runbook,
- hasil testing,
- evidence failover,
- catatan perubahan,
- daftar kontak darurat.

Audit:

- internal audit setiap tahun,

- external audit (opsional),
- audit regulator (OJK/BI).

16.13 Metrik Keberhasilan Continuity Planning

KPI:

1. RTO dipenuhi 100% pada sistem kritikal.
2. RPO dipenuhi sesuai SLA.
3. Kecepatan failover.
4. Kelulusan DR test (≥ 95%).
5. Tidak ada kehilangan data.

KRI:

1. Backup gagal.
2. API latency meningkat.
3. Gagal failover otomatis.
4. Tingginya alert cloud disk penuh.

16.14 Integrasi BCP/DRP dengan Cybersecurity & Risk Management

BCP tidak boleh berdiri sendiri. Setidaknya terhubung langsung dengan:

- Incident Response Plan (IRP)
- CTI & Early Warning System (Bab 14)
- Fraud Response (Bab 13)
- Vendor Risk Management (Bab 7)
- AI Risk (Bab 12)
- IAM Zero Trust (Bab 15)

Ketahanan operasional hanya tercapai jika seluruh komponen saling terintegrasi.

BAB 17
CLOUD SECURITY ARCHITECTURE & GOVERNANCE

CLOUD SECURITY ARCHITECTURE & GOVERNANCE, disusun sangat komprehensif, teknis, dan implementable, agar seluruh anggota AFTECH dapat menerapkan keamanan cloud yang setara standar dunia.
Referensi global yang digunakan:

- NIST SP 800-144 (Guidelines on Security and Privacy in Public Cloud)
- NIST CSF 2.0
- ISO/IEC 27017 (Cloud Security Controls)
- ISO/IEC 27018 (Cloud PII Protection)
- CSA Cloud Controls Matrix (CCM v4)
- CIS Benchmarks (AWS/Azure/GCP)
- OWASP Cloud-Native Security Guidelines
- PBI 22/2024 Sistem Pembayaran & Ketahanan Siber
- SEOJK 29/2022 TI & Risiko Siber

Bab ini memastikan layanan cloud Fintech:
AMAN, resilient, compliant, scalable, cost-effective, dan auditable.

Cloud menjadi fondasi operasional Fintech modern. Namun cloud juga membawa risiko unik: misconfiguration, exposed buckets, API compromise, IAM weakness, insecure containers, supply chain attack, kehilangan kendali data. Karena itu, diperlukan standar keamanan cloud yang ketat dan auditable, agar ekosistem digital Indonesia dapat beroperasi secara aman.

17.1 Tujuan Cloud Security Framework

1. Melindungi data pelanggan & transaksi di cloud.
2. Menjamin ketersediaan layanan 24/7.
3. Mencegah kesalahan konfigurasi (root cause 70% insiden cloud).
4. Mengatur akses & identitas cloud secara aman.
5. Mengontrol API & data movement antar sistem.
6. Memenuhi regulasi OJK–BI–UU PDP terkait keamanan & privasi data.
7. Menyediakan arsitektur cloud yang dapat diaudit.

17.2 Model Layanan Cloud yang Diatur

Framework ini berlaku untuk:

1. IaaS

- compute
- storage
- networking,

- firewalls.

2. PaaS

- RDS, BigQuery, CosmosDB,
- serverless (Lambda, Cloud Functions),
- managed Kubernetes.

3. SaaS

- email/office,
- CRM,
- analytics platform.

4. Container & Kubernetes Environment

- EKS/AKS/GKE,
- private container engines.

5. Hybrid Cloud

- on-prem & cloud integration.

6. Multi-cloud

Sebagi contoh:

- AWS + GCP
- AWS + Azure
- Alibaba Cloud + AWS

17.3 Prinsip Arsitektur Cloud Aman untuk perusahaan

Beberapa contoh prinsip arsitektur keamanan cloud

1. Zero Trust Cloud-native
2. Defense-in-depth
3. Least Privilege Access (IAM)
4. Encryption Everywhere
5. Segregation of Duties
6. Immutable Infrastructure
7. Automated Security Controls
8. Observability by Design
9. Secure-by-default configuration
10. Compliance continuous monitoring

17.4 Cloud Governance Structure

1. Cloud Governance Board

Dapat terdiri dari CTO, CISO, Architect Lead, Compliance Lead.

2. Cloud Security Team

Bertanggung jawab untuk mengatur kontrol teknis & monitoring.

3. DevSecOps Team
Bertugas untuk memastikan integrasi keamanan dalam pipeline CI/CD.

4. Cloud Infrastructure Team
Melakukan implementasi dan menerapkan standar arsitektur & automasi.

5. Internal Audit
Bertanggung jawab untuk memastikan kepatuhan cloud security.

17.5 Cloud Shared Responsibility Model

Fintech harus memahami batas tanggung jawab:

Layer	Cloud Provider	Perusahaan (Customer)
Infrastruktur Fisik	✔	✘
Virtualization Layer	✔	✘
OS & Middleware	✘	✔
Data & Access	✘	✔
Application Config	✘	✔
Network Config	✘	✔
Encryption Management	✘ / ✔	✔

Kegagalan memahami model ini adalah salah satu penyebab kebocoran data terbesar.

17.6 Keamanan Identitas Cloud (Cloud IAM)

IAM cloud adalah risiko terbesar. Oleh karena itu, sangat direkomendasikan untuk menerapkan:

1. SSO + MFA untuk semua akun cloud
Admin menggunakan MFA berbasis aplikasi. Penggunaan MFA dengan SMS direkomendasikan untuk dihindari.

2. IAM Role-based Access Control
Tidak boleh ada hard coded credential.

3. No Root Account Usage
Akun root harus:

- dikunci,
- dikenali,
- hanya dipakai untuk emergency.

4. Service Accounts Rotation
API keys, tokens, dan secrets diputar setiap 90 hari.

5. Just-in-time Access
Akses admin diberikan sementara, bukan permanen.

17.7 Keamanan Jaringan Cloud

1. Zero Trust Network Segmentation
Bertujuan untuk memisahkan:

- production,
- testing,
- dev,
- fraud systems,
- payment core.

2. Private Subnet for Critical Systems
Database tidak boleh punya public IP.

3. WAF + API Gateway Security
Untuk seluruh endpoint Fintech.

4. DNS Security

- DNSSEC,
- anti DNS hijacking.

5. mTLS untuk Microservices
Layanan saling verifikasi identitas.

17.8 Data Security & Encryption

1. Encryption-at-rest (Wajib)

- KMS/CloudHSM,
- key rotation otomatis.

2. Encryption-in-transit
TLS 1.2/1.3 wajib.

3. DLP (Data Loss Prevention)
Sensor kebocoran data:

- nomor kartu,
- NIK,
- data sensitif lainnya.

4. Logging Data Access
Siapa mengakses data apa, kapan, dari mana.

5. Data Residency & Sovereignty

Sesuai regulasi Indonesia:

- data tertentu wajib berada di wilayah hukum Indonesia,
- referensi PBI + SEOJK.

17.9 Cloud Workload Security

1. Hardening Compute Instance

- gunakan CIS Benchmark,
- disable unused services.

2. Serverless Security

- set resource-based permissions,
- monitor invocation anomalies.

3. Kubernetes Security

- RBAC strict,
- avoid privileged containers,
- enable network policies,
- use admission controllers,
- scan container images (Trivy/Anchore).

17.10 Storage Security

1. No Public Buckets

Cloud storage bucket cloud direkomendasikan untuk:

- public-blocked,
- encrypted,
- versioning on.

2. Object Lock (WORM)

Untuk mencegah ransomware.

3. Lifecycle Management

Untuk efisiensi & keamanan data.

17.11 API Security di Cloud

Mengingat penggunaan API adalah komponen penting dalam teknologi Fintech, sangat direkomendasikan untuk:

1. API gateway dengan auth & rate limit,
2. OAuth2/OIDC,
3. JWT dengan signature dan expiry pendek,
4. Anti replay/token binding,
5. Schema validation,
6. API anomaly detection.

17.12 DevSecOps & CI/CD Security

1. Mandatory Code Scanning

- SAST,
- DAST,
- SCA (dependency scanning).

2. Secrets Scanning

Tidak boleh ada credentials di repo Git.

3. Signed Artifacts

- container image signing,
- provenance tracking (SLSA > LEVEL 2 direkomendasikan).

4. IaC Security

Terraform/CloudFormation harus:

- di-scan (Checkov, Tfsec),
- mengikuti modul standar AFTECH.

17.13 Monitoring & Logging Cloud

1. Centralized Log Management

Gunakan:

- CloudWatch,
- Stackdriver,
- Sentinel,
- ELK.

2. SIEM Integration

Untuk korelasi ancaman real-time.

3. UEBA (User & Entity Behavior Analytics)

Mendeteksi anomali akses admin.

4. Cloud Security Posture Management (CSPM)

Sangat direkomendasikan untuk perusahaan yang menggunakan cloud computing:

- Prisma Cloud,
- Wiz,
- Lacework,
- AWS Security Hub.

5. Vulnerability Scanning

- Direkomendasikan untuk dijalankan berkala untuk semua aset.
- Frekuensi yang optimal adalah setidaknya 1 minggu sekali

17.14 Backup, DR & High Availability di Cloud

Backup

- 3-2-1 rule,
- cross-region backup (terenkripsi),
- automated backup validation.

Disaster Recovery

- multi-AZ (wajib),
- multi-region (opsional untuk Fintech kecil, wajib untuk Fintech besar).

High Availability

- load balancing,
- auto-scaling,
- health check otomatis.

17.15 Vendor Cloud Risk Management

Jika menggunakan:

- AWS,
- GCP,
- Azure,
- Alibaba Cloud,
- atau cloud lokal.

Wajib dilakukan:

1. cloud vendor due diligence,
2. penilaian keamanan,
3. SLA review termasuk uptime & incident response,
4. audit bukti kepatuhan (ISO, SOC 2).

17.16 Cloud Threat Modeling

Gunakan:

- STRIDE,
- PASTA,
- MITRE ATT&CK Cloud Matrix.

Analisis ancaman:

- exposed buckets,
- API compromise,
- credential abuse,
- container breakout,
- supply chain attack,
- misconfiguration.

17.17 Cloud Security Testing

Jenis pengujian:

1. Cloud-focused Penetration Test
2. Kubernetes PenTest
3. API PenTest
4. Serverless Penetration Test
5. Configuration Audit (CIS Benchmark)
6. Red Teaming Cloud (untuk Fintech besar)

17.18 Compliance & Audit Cloud

Audit wajib dilakukan:

- setidaknya 1 kali setiap tahun,
- perubahan besar,
- insiden siber kritikal.

Audit meliputi:

- IAM,
- storage security,
- network rules,
- logging,
- API,
- container security.

17.19 Cloud Security Metrics & KPI

KPI:

1. zero public buckets (100%).
2. MFA untuk semua akun cloud.
3. vulnerability remediation SLA.
4. IAM misconfiguration → 0.
5. secrets exposed → 0.

KRI:

1. open ports tiba-tiba muncul.
2. privilege escalation permission.
3. CSPM critical alerts.
4. IAM anomalies.
5. excessive data transfer out.

BAB 18
MOBILE SECURITY & API SECURITY FRAMEWORK

MOBILE SECURITY & API SECURITY FRAMEWORK, disusun sangat komprehensif, teknis, dan langsung dapat diimplementasikan oleh seluruh anggota AFTECH.

Bab ini berlandaskan standar global:

Untuk Mobile Security

- OWASP Mobile Security Testing Guide (MSTG)
- OWASP Mobile Application Security Verification Standard (MASVS)
- Google/Apple Mobile Security Best Practices
- NIST Mobile Security Guidelines

Untuk API Security

- OWASP API Security Top 10 (2023)
- OAuth 2.0 Security BCP
- OpenID Connect Security
- API Gateway Best Practices (Cloud-native)
- NIST Zero Trust API Architecture
- FAPI (Financial-grade API Standard)

Bab ini sangat krusial karena 90% layanan Fintech berbasis mobile app & API, dan kedua komponen ini menjadi sasaran utama kelompok penipu dan pelaku kejahatan siber.

Fintech modern bertumpu pada dua hal:

1. Mobile apps sebagai front-end utama pengguna, dan
2. API sebagai fondasi integrasi & transaksi.

Karena itu, keamanan mobile dan API harus dirancang sekelas standar perbankan internasional.

18.1 Tujuan Framework Mobile & API Security

1. Mencegah manipulasi aplikasi mobile dan kebocoran data.
2. Mencegah penyalahgunaan API oleh pelaku fraud, bot, dan attacker.
3. Melindungi transaksi pengguna & komunikasi antar sistem.
4. Menjamin integritas identitas digital (device binding, biometrics).
5. Mencegah reverse engineering, tampering, dan malware injection.
6. Mengurangi risiko fraud seperti ATO, phishing, dan credential stuffing.
7. Memenuhi regulasi OJK–BI–UU PDP.

18.2 Lingkup Mobile & API Security

Framework ini mengatur:

A. Mobile Security

- Android & iOS apps
- biometric & device binding
- mobile network security
- local storage encryption
- app integrity & anti-tampering
- mobile malware protection
- secure session management

B. API Security

- Open Finance API
- internal microservices API
- partner/vendor API
- OAuth2/OIDC authentication
- API gateway controls
- fraud API detection
- API rate limiting & anomaly detection

18.3 Mobile Security Architecture (High-Level)

Mobile app harus dirancang dengan:

- Secure App Layer
    1. encrypted storage
    2. secure keystore
    3. code obfuscation
    4. anti-tamper & anti-root
- Secure Communication Layer
    1. TLS pinning
    2. mutual TLS (optional)
    3. encrypted API traffic
- Secure Backend Layer
    1. API gateway
    2. JWT/OAuth authentication
    3. device fingerprinting
- Secure Identity Layer
    1. biometric authentication
    2. secure session management

18.4 Mobile Threat Model untuk Fintech

Ancaman mobile meliputi:

1. Reverse Engineering

APK decompilation → akses ke logic & credential.

2. Tampering & Repackaging
Aplikasi dipasang malware, dipasang iklan fraud, atau diubah fungsinya.

3. Credential Stealing
Melalui phishing atau overlay app malware.

4. Device Compromise
Root/jailbreak → keamanan runtuh.

5. Malware Injection
Banking trojan, screen overlay, keylogger.

6. Unsafe Data Storage
Data sensitif disimpan di local storage tanpa enkripsi.

7. Network Attacks
MITM, SSL stripping, rogue WiFi.

8. Weak Session Management
Session hijack & replay attack.

18.5 Mobile Security Controls (Based on MASVS)

Framework ini mengadopsi kontrol MASVS Level 2 (high-security apps).

A. Security Controls untuk App Layer

1. Code Obfuscation (Wajib)

- ProGuard, DexGuard, atau tool sejenis.
- Melindungi dari reverse engineering.

2. Anti-Tampering

- integrity check (checksum),
- certificate check,
- debugging detection,
- hook detection (Frida/Xposed).

3. Anti-Root/Jailbreak Detection
Jika aplikasi mendeteksi root/jailbreak → batasi fungsi.

4. Secure Storage
Gunakan:

- Android Keystore,
- iOS Keychain.

5. Tidak boleh menyimpan:

- PIN,
- access token,
- password,
- key rahasia.

6. No Hardcoded Keys
Tidak boleh ada API keys dalam code.

B. Network Security Controls

1. TLS 1.2/1.3 Only
Semua koneksi harus terenkripsi.

2. Certificate/SSL Pinning
Prevent MITM dan interception.

3. No Use of HTTP
Semua endpoint harus HTTPS.

4. Replay Attack Protection
Gunakan:
- nonce,
- timestamp,
- signature.

C. Identity Controls & Authentication

1. Secure Biometric Authentication
- gunakan fitur OS (FaceID, TouchID, BiometricPrompt),
- jangan membuat biometric engine sendiri.

2. Device Binding
Mengikat akun → device tertentu menggunakan:
- device fingerprinting,
- hardware ID,
- keystore binding.

3. Session Management
- token harus short-lived,
- auto logout on risk event,
- refresh token rules strict.

D. Malware & Fraud Protection

1. Detect Overlay Attacks
Jika sistem mendeteksi screen overlay → blokir transaksi.

2. Detect Keylogger Behavior
Gunakan behavioral analytics.

3. Device Risk Scoring
Setiap login → skor risiko device:

- secure OS?
- rooted?
- sideloaded apps?
- risky permissions?

Jika risk tinggi → challenge MFA.

18.6 Mobile Penetration (Pentest) Testing Requirements

Mobile app Fintech wajib menjalani pentest sesuai dengan regulasi yang berlaku:

1. sebelum launching,
2. minimal 1x per tahun,
3. jika ada fitur kritikal baru.

Mengikuti:

- OWASP MSTG
- MASVS
- SANS Mobile Checklist

Test mencakup:

- static analysis (SAST),
- dynamic analysis (DAST),
- network MITM testing,
- API fuzzing,
- root/jailbreak bypass attempts.

18.7 API Security Architecture

API Fintech adalah target utama penyerang karena:

- menjadi pintu masuk transaksi,
- mengandung data sensitif,
- terhubung ke banyak pihak (bank, partner, vendor).

Arsitektur API wajib mengikuti standar:

Layer 1 – API Gateway

- auth enforcement,
- rate limiting,
- threat filtering,
- logging.

Layer 2 – Identity Layer

- OAuth2 / OIDC,
- token management.

Layer 3 – Security Layer

- schema validation,
- signature,
- anomaly detection.

Layer 4 – Observability Layer

- API logs,
- API abuse detection,
- fraud correlation.

18.8 API Authentication & Authorization

(Mengikuti Financial-grade API — FAPI)

1. OAuth 2.0 (Mandatory)

- authorization code flow with PKCE.

2. OIDC for User Identity

Untuk login & SSO layanan Fintech.

3. JWT Requirements

- short-lived (≤ 15 menit),
- signed (RS256/ES256),
- no sensitive data inside token,
- audience claim & issuer check.

4. Token Binding

Mencegah replay attack.

5. Service-to-Service Auth

Gunakan:

- mTLS,
- workload identity (AWS IAM roles, GCP IAM),
- SPIFFE/SPIRE (opsional).

18.9 API Security Controls (Based on OWASP API Top 10)

1. Input Validation & Schema Enforcement

Gunakan strict JSON schema validation.

2. Rate Limiting

Per:

- IP,
- device,
- API key,
- account.

3. Anti-Bot & Abuse Protection
Integrasi SIM swap detection & behavioral analytics.

4. API Firewall / Web Application Firewall
Untuk mendeteksi:

- injection,
- brute force,
- DDoS API attacks.

5. RBAC/ABAC untuk API
Hanya role tertentu yang boleh akses endpoint tertentu.

6. Handling Sensitive Data

- masking,
- encryption,
- tokenization.

18.10 API Lifecycle Security

Security harus ada di setiap tahap:

1. Design

- threat modeling (STRIDE),
- schema definition.

2. Build

- code scanning,
- secrets scanning.

3. Deploy

- infra scanning (CSPM),
- secure container image.

4. Monitor

- API anomaly detection,
- AI-based fraud detection.

5. Retire

- remove deprecated endpoints,
- revoke old tokens.

18.11 API Threat Detection & Fraud Correlation

API menjadi entry point fraud. Oleh karena itu, setidaknya mempunyai fraud detection berdasarkan:

1. Anomaly-based detection

- login unusual,
- device baru,
- kecepatan transaksi abnormal.

2. Behavioral biometrics

- geolocation pattern,
- timing analysis.

3. IP Intelligence

- Tor exit nodes,
- VPN suspicious IP.

4. Threat Intelligence Integration

- block domains/IPs botnet secara otomatis.

18.12 API Penetration Testing Requirements

API Wajib melalui:

1. API security testing sebelum produksi,
2. pen-test tahunan,
3. continuous fuzzing untuk endpoint kritikal,
4. third-party security audit untuk open finance API.

18.13 API Logging & Monitoring

API harus mencatat:

- caller identity,
- endpoint accessed,
- request size & pattern,
- errors (401, 403, 429),
- risk score.

Log direkomendasikan terintegrasi dengan:

- SIEM,
- Threat Intelligence (Bab 14),
- Fraud Engine (Bab 13).

18.14 Mobile & API Governance

Governance mengatur:

1. secure coding standards,

2. versioning & release policy,
3. vulnerability disclosure program (VDP),
4. bug bounty program,
5. perubahan API harus melalui CAB (Change Advisory Board).

18.15 Kepatuhan & Regulasi

Mobile & API security harus mematuhi aturan yang berlaku namun tidak terbatas pada:

- UU PDP,
- SEOJK 29/2022,
- PBI 22/2024,
- Open API Payment Standards,
- PCI DSS (jika menyimpan data kartu),
- BSSN CSF.

18.16 KPI & KRI Mobile/API Security

Beberapa contoh metrik KPI yang dapat digunakan:

1. mobile app MASVS compliance,
2. 0 tampering/clone app incidents,
3. TLS pinning adoption rate,
4. API false positive < 2%,
5. deprecated API removal rate.

Beberapa contoh metrik KRI yang dapat digunakan:

1. lonjakan 401/403 API,
2. meningkatnya root/jailbreak detection,
3. API usage anomaly,
4. bot traffic spike,
5. suspicious APK clones detected.

BAB 19
SECURITY LOGGING, MONITORING, SIEM, SOC & INCIDENT DETECTION

SECURITY LOGGING, MONITORING, SIEM, SOC & INCIDENT DETECTION, disusun sangat komprehensif, teknis, operasional, dan langsung dapat diimplementasikan oleh seluruh anggota AFTECH.
Bab ini mengacu pada standar global:

- NIST SP 800-92 (Guide to Log Management)
- NIST SP 800-137 (Continuous Monitoring)
- ISO/IEC 27002 – Annex A.12 Logging & Monitoring
- MITRE ATT&CK Detection Framework
- SOC Maturity Model (SIM3)
- CERT Incident Management Maturity Model (IMMM)
- FFIEC Cybersecurity Assessment Tool

Sektor Fintech menjadi salah satu target paling intensif untuk serangan: bot attack, ATO, API abuse, DDoS, credential stuffing, ransomware, fraud, hingga breach skala besar. Maka logging dan SOC harus dirancang sekelas standar perbankan internasional.

19.1 Tujuan Logging & Monitoring

1. Mendeteksi serangan sebelum berdampak besar.
2. Memberikan bukti forensik saat insiden terjadi.
3. Menyediakan data threat intelligence untuk Bab 14.
4. Mengaktifkan alert otomatis atas aktivitas mencurigakan.
5. Memenuhi kepatuhan OJK–BI–UU PDP.
6. Meningkatkan respon cepat terhadap insiden siber.
7. Mendukung operasi fraud detection & behavioral analytics.

19.2 Ruang Lingkup Logging & Monitoring

Framework ini mencakup:

1. Infrastruktur

- server, VM, cloud instance, containers, Kubernetes.

2. Aplikasi & API

- authentication logs,
- authorization logs,
- API request/response logs,
- application errors.

3. Database Layer

- query logs,

- access logs,
- replication logs.

4. Network & Security Devices

- firewall,
- WAF,
- IDS/IPS,
- API gateway,
- load balancer.

5. User Activity

- admin activity,
- privileged access,
- developer console usage.

6. Endpoint & Device

- EDR/XDR logs,
- malware detection.

7. Cloud Platform

- cloud audit logs,
- IAM events,
- network ACL changes.

19.3 Jenis Log yang Wajib Dikumpulkan

A. Authentication Logs

- login success/failure
- MFA status
- risk-based auth scoring
- brute-force detection

B. Access Logs

- privilege escalation
- role changes
- sensitive data access
- admin access

C. API Logs

- endpoint calls
- request validation failures
- 401/403/429 patterns
- anomaly traffic
- token misuse

D. System Logs

- OS events
- services started/stopped
- kernel events

E. Application Logs

- exceptions & errors
- business logic failures

F. Cloud Audit Logs

- IAM changes
- storage bucket policy changes
- network rule changes
- creation/deletion of resources

G. Network Logs

- firewall allow/deny
- IDS/IPS signatures
- DDoS events

H. Endpoint Logs

- malware alerts
- suspicious file creation
- DLL injection attempts

19.4 Centralized Logging Architecture

Logging harus terpusat menggunakan arsitektur:

1. Log Collection Layer

- agent-based (Fluentd, Beats, CloudWatch Agent)
- agentless (API ingestion, syslog)

2. Log Transport Layer

- Kafka
- Pub/Sub
- Kinesis
- EventHub

3. Log Storage Layer

- Elasticsearch
- Splunk
- Cloud-native log storage

4. SIEM Correlation Layer

- rules engine,

- signature-based,
- anomaly-based,
- ML-based detection.

5. Visualization & Alerting Layer

- Kibana,
- Grafana,
- Splunk Dashboard,
- Sentinel,
- Elastic Security.

19.5 Security Information and Event Management (SIEM)

SIEM berfungsi:

1. mengumpulkan log,
2. mengkorelasikan event,
3. memberikan alert secara real-time.

Fungsi SIEM Wajib:

- log normalization,
- correlation rules,
- threat intel integration,
- MITRE ATT&CK mapping,
- real-time alerting,
- case management integration,
- dashboard monitoring,
- reporting untuk audit.

Vendor yang direkomendasikan:

- Splunk
- Elastic Security
- Microsoft Sentinel
- IBM QRadar
- Sumo Logic
- Wazuh (open-source)

19.6 SOC (Security Operations Center) Maturity Levels

Mengacu pada SIM3 model:

SOC Level 1 – Basic Monitoring

- alerting dasar
- manual triage
- tidak ada threat hunting

SOC Level 2 – Intermediate

- 24/7 monitoring

- rule correlation
- forensic capability dasar

SOC Level 3 – Advanced

- threat intelligence operational
- threat hunting rutin
- malware analysis
- API abuse detection
- cloud-specific detection

SOC Level 4 – Fintech-grade

- fully automated correlation
- fraud + cyber integrated
- real-time anomaly detection
- ML-assisted detection
- red team vs blue team exercises

AFTECH menyarankan minimal SOC Level 2 untuk Fintech kecil,
SOC Level 3 atau 4 untuk Fintech besar.

19.7 Role & Struktur SOC

SOC terbagi menjadi:

1. L1 Analyst

- monitoring dashboard
- triage alert

2. L2 Analyst

- deep investigation
- threat hunting
- incident verification

3. L3 Analyst

- forensics,
- reverse engineering,
- malware analysis

4. SOC Manager

- koordinasi incident
- reporting
- KPI management

5. Automation Engineer

- SOAR automation
- playbook scripting

- integration

19.8 MITRE ATT&CK–Based Detection Framework

SOC wajib memetakan deteksi ke:

Tactics:

- Initial Access
- Execution
- Privilege Escalation
- Lateral Movement
- Exfiltration
- Impact

Examples of Detection Rules:

- abnormal API calls
- mass login failures
- new admin role creation
- suspicious outbound traffic
- credential dumping patterns
- data exfiltration > threshold
- impossible travel events

19.9 Endpoint Security (XDR/EDR)

Endpoint setidaknya menggunakan:

- CrowdStrike / SentinelOne / Microsoft Defender / ESET Enterprise
- malware prevention
- exploit mitigation
- process behavioral monitoring
- file integrity monitoring
- anti-ransomware
- malware sandbox submission

Endpoint logs harus otomatis masuk SIEM.

19.10 API Security Monitoring

API adalah target utama Fintech. API monitoring harus mencakup:

1. API Anomaly Detection

- spike traffic
- new user-agent
- abnormal geolocation
- API brute force
- API credential stuffing

2. Token Abuse Detection

- refresh token misuse

- expired token attempts
- invalid signature

3. Fraud API Correlation

- device fingerprint mismatch
- money mule patterns
- velocity transactions

19.11 Behavioral Analytics (UEBA)

UEBA digunakan untuk mendeteksi:

- insider threat
- suspicious admin activity
- abnormal session patterns
- privilege misuse
- data scraping

UEBA menggunakan ML untuk mendeteksi deviation dari baseline perilaku normal.

19.12 Threat Intelligence Integration (Bab 14)

SIEM harus terintegrasi dengan CTI:

- IOC ingestion otomatis (IP, domain, hash),
- TTP adversary mapping,
- darkweb indicators,
- phishing indicators,
- fraud syndicate indicators.

19.13 SOAR (Security Orchestration, Automation & Response)

SOAR digunakan untuk:

- mengotomasi alert triage
- mengotomasi response (block IP, disable account)
- mengurangi MTTR < 30 menit
- mematuhi SOP insiden OJK–BI

Contoh Automation:

- jika login failed > 20/min → auto-block 30 menit
- jika API abuse → rate-limit otomatis
- jika outbound data > threshold → isolate instance

19.14 Incident Detection & Escalation Process

Stages:

1. Alert generated
2. L1 triage
3. L2 validation
4. Incident classification (Low–High)

5. Escalation ke IR Team
6. Containment
7. Forensics
8. Recovery
9. Root Cause Analysis
10. Reporting (Regulator)

19.15 Log Retention Policy

Untuk kepatuhan regulator:

- log security: min 3 tahun
- log transaksi: mengikuti OJK/BI
- log access & audit: min 2 tahun
- backup log tersimpan offsite (cloud WORM)

19.16 Metrics, KPI & KRI Logging/SOC

KPI:

1. Mean Time to Detect (MTTD)
2. Mean Time to Respond (MTTR)
3. % false positive alerts
4. detection coverage vs MITRE matrix
5. SOC readiness score
6. automated response success

KRI:

1. spike API errors
2. abnormal IAM changes
3. large outbound data transfer
4. increase in malware detection
5. cloud configuration drift

19.17 Governance, Audit & Compliance

SOC harus memenuhi:

- SEOJK 29/2022
- PBI 22/2024
- ISO 27001/27002
- BSSN CSF
- audit internal tahunan
- audit eksternal opsional

Audit mencakup:

- log completeness
- rule effectiveness
- alert mapping
- incident response traceability

- SLA response
- SOAR automation logs

BAB 20
SECURITY TESTING, RED TEAMING, VULNERABILITY MANAGEMENT & BUG BOUNTY PROGRAM

SECURITY TESTING, RED TEAMING, VULNERABILITY MANAGEMENT & BUG BOUNTY PROGRAM, disusun sangat komprehensif, implementable, dan sesuai standar global untuk seluruh anggota AFTECH.
Framework ini mengikuti:

- OWASP Testing Guide
- NIST SP 800-115 (Technical Guide to Security Testing)
- MITRE Adversarial Tactics, Techniques & Common Knowledge (ATT&CK®)
- PTES (Penetration Testing Execution Standard)
- OSSTMM
- ISO 27001 Annex A.12 & A.14
- US DoD Vulnerability Disclosure Program Framework
- Bugcrowd & HackerOne Standards

Bab ini memastikan seluruh Fintech memiliki keamanan proaktif, bukan hanya reaktif, melalui testing rutin, red teaming, dan program perburuan bug.

20.1 Tujuan Security Testing & VM Framework

1. Mengidentifikasi kelemahan keamanan sebelum dimanfaatkan penyerang.
2. Menguji efektivitas kontrol keamanan pada aplikasi & infrastruktur.
3. Meningkatkan ketahanan terhadap ancaman nyata.
4. Mempercepat remediasi kerentanan kritis.
5. Memenuhi standar regulator dan audit keamanan.
6. Mendukung inovasi Fintech secara aman & terkendali.
7. Menjaga kepercayaan pengguna dan stakeholder.

20.2 Ruang Lingkup Security Testing

Testing berlaku untuk:

1. Application Security

- web apps
- mobile apps
- API
- backend services
- cloud-native microservices

2. Infrastructure Security

- cloud infrastructure
- databases
- network security

- Kubernetes/containers
- identity & access management

3. Third-Party & Vendor Testing

- open finance API
- payment API
- cloud vendors
- SaaS integrations

4. People Security (Social Engineering)

- phishing simulation
- vishing
- impersonation test

5. Red Teaming (Adversary Simulation)

- threat actor simulation
- endpoint & network testing
- phishing + lateral movement
- privilege escalation
- detection evasion

20.3 Jenis Security Testing Wajib Fintech

1. Vulnerability Assessment (VA)

Scanning otomatis untuk:

- missing patch,
- misconfiguration,
- dependency vulnerability.

Frekuensi: mingguan untuk sistem kritikal.

2. Penetration Testing (Pentest)

Mengacu PTES + OWASP.
Wajib dilakukan:

- sebelum release fitur besar,
- minimal 2x per tahun untuk apps kritikal.

Jenis pentest:

- Web Application Pentest
- Mobile Pentest
- API Pentest
- Cloud Pentest
- Network Pentest
- Kubernetes Pentest
- Thick client / desktop app pentest (jika ada)

3. Secure Code Review
Manual + automated:

- SAST (Static Application Security Testing)
- SCA (Software Composition Analysis)
- Secrets scanning

Frekuensi: setiap commit CI/CD.

4. Dynamic Application Security Testing (DAST)
Untuk scanning runtime:

- input validation,
- SQLi,
- XSS,
- logic flaws.

5. Cloud Security Testing
Menggunakan:

- CSPM (Security Posture Management),
- CIS Benchmarking,
- misconfiguration scanning.

Frekuensi: harian.

6. Infrastructure Testing

- port scanning
- firewall rule audit
- K8s security test (RBAC, network policy, container escape)
- OS hardening validation

7. Social Engineering Testing
Minimal 2x per tahun, meliputi:

- phishing email simulation
- WhatsApp phishing
- SMS smishing

8. Red Teaming (Adversary Simulation)
Simulasi serangan nyata berdasarkan MITRE ATT&CK.
Dilakukan:

- 1x per tahun untuk Fintech besar,
- opsional untuk Fintech kecil.

20.4 Red Teaming Framework

Red Team mensimulasikan Advanced Persistent Threat (APT) untuk menguji ketahanan security secara keseluruhan.

Tahapan Red Team Ops:

1. Reconnaissance

Open-source intel, fingerprinting.

2. Initial Access

Spear phishing, exploitation, credential stuffing.

3. Execution

Malware simulation, malicious payload.

4. Privilege Escalation

Exploiting misconfig, IAM misuse.

5. Lateral Movement

Internal pivoting melalui:

- RDP
- SSH
- API traversal
- CI/CD compromise

6. Data Access & Exfiltration

Simulasi pencurian data.

7. Covering Tracks

Evading SIEM logs.

8. Reporting

Heatmap + rekomendasi mitigasi.

20.5 Purple Teaming

Kolaborasi Red Team (attack) & Blue Team (defense) untuk meningkatkan deteksi & respons.

Output:

- peningkatan rule detection pada SIEM,
- perbaikan alert SOC,
- tuning SOAR automation.

20.6 Vulnerability Management Program (VM)

VM wajib mencakup:

Cycle of VM

1. Identification
   - VA scans
   - cloud misconfig scans
   - pentest results
   - bug bounty submissions

2. Analysis
   - CVSS scoring
   - exploitability
   - asset value
   - exposure level
3. Prioritization
   - Critical → fix < 72 jam
   - High → fix < 7 hari
   - Medium → fix < 30 hari
   - Low → fix < 90 hari

4. Remediation
   - patching
   - updating dependencies
   - config fix
   - code fix
   -
5. Validation
   - re-test
   - re-scan

6. Reporting
   - dashboard VM
   - monthly report to CISO

20.7 Vulnerability Scoring & Risk Prioritization

Kerentanan harus diukur menggunakan:

1. CVSS 3.1 Score

- base score
- exploitability
- impact metric

2. EPSS (Exploit Prediction Scoring System)

Menentukan seberapa besar peluang exploit dalam 30 hari.

3. Asset Value Classification

- kritikal (payment/transaction)
- sensitif (database)
- non-kritikal

4. Exposure

- internet-facing
- internal-only

5. Compliance Requirement

- PCI DSS
- OJK
- BI

20.8 Bug Bounty Program (BBP)

Bug bounty program membuka peluang bagi ethical hacker untuk menemukan bug sebelum attacker jahat menggunakannya.

Model BBP:

1. Private Bug Bounty
    - untuk Fintech kecil
    - hanya peneliti terpilih
2. Public Bug Bounty
    - untuk Fintech besar
    - via platform: HackerOne, Bugcrowd, Yogosha

Rewarding Model:

- Low: 50k – 500k
- Medium: 500k – 5 juta
- High: 5 juta – 50 juta
- Critical: hingga 100+ juta

Bug Categories:

- account takeover
- authentication bypass
- remote code execution
- IDOR
- SQL injection
- broken access control
- sensitive data exposure
- misconfig & cloud issues

20.9 Vulnerability Disclosure Program (VDP)

VDP harus memuat:

- scope aplikasi
- rules of engagement
- safe harbor policy
- non-persecution clause
- response SLA
- disclosure timeline

VDP Response SLA:

- acknowledge: < 72 jam
- triage: < 7 hari
- remediation plan: < 14 hari

20.10 Security Testing & Red Teaming KPIs

Beberapa KPIs yang bisa dipertimbangkan:

1. % kerentanan critical yang diperbaiki ≤ SLA
2. penurunan high severity findings YOY
3. false negative reduction
4. jumlah detection improvement hasil purple team
5. mendeteksi 80% TTP MITRE ATT&CK Red Team
6. response time terhadap temuan bug bounty

Beberapa KRIs yang dapat dipertimbangkan:

1. peningkatan open vulnerabilities
2. cloud misconfig ditemukan mingguan
3. expired/misaligned access rights
4. peningkatan API attack patterns
5. anomaly spikes di WAF/API Gateway

20.11 Governance & Compliance

Security testing dan VM harus mematuhi:

- SEOJK 29/2022
- PBI 22/2024
- ISO 27001 Annex A
- PCI DSS (jika ada kartu)
- BSSN CSF
- dokumentasi bukti remediasi
- hasil pentest & VM report disimpan min 3 tahun

BAB 21
DATA GOVERNANCE, DATA PROTECTION, PRIVACY ENGINEERING & UU PDP COMPLIANCE

DATA GOVERNANCE, DATA PROTECTION, PRIVACY ENGINEERING & COMPLIANCE DENGAN UU PELINDUNGAN DATA PRIBADI (UU PDP).
Bab ini disusun super komprehensif, operasional, siap audit, dan sesuai standar global, menjadi gold standard yang dapat langsung diterapkan oleh seluruh anggota AFTECH.
Framework ini mengacu pada:

- UU No. 27/2022 tentang Pelindungan Data Pribadi
- PP/SE turunan UU PDP (proses harmonisasi regulasi)
- SEOJK 29/2022 (TI & Risiko Siber)
- PBI 22/2024 (Sistem Pembayaran)
- ISO/IEC 27701 (Privacy Information Management System - PIMS)
- NIST Privacy Framework
- OECD Privacy Principles
- GDPR (European Union)
- Singapore PDPA
- FIPS & ISO 27001 Annex A.5 (Information Security Policies)

Bab ini memastikan bahwa tata kelola data anggota AFTECH:
LEGAL, AMAN, TERKENDALI, MINIM RISIKO, AUDITABLE, SESUAI STANDAR INTERNASIONAL

Digital finance adalah industri dengan volume data paling masif:
data pribadi, biometrik, lokasi, KYC, perilaku transaksi, perangkat, kontak, bahkan pola keuangan. Karena itu, diperlukan kerangka tata kelola yang kuat agar inovasi tetap berjalan tanpa mengorbankan privasi dan keamanan.

21.1 Tujuan Data Governance & Privacy Framework

1. Melindungi data pribadi pengguna sesuai UU PDP.
2. Menjamin integritas, kerahasiaan, dan ketersediaan data.
3. Mengatur lifecycle data dari pengumpulan hingga pemusnahan.
4. Mengurangi risiko kebocoran data dan penyalahgunaan.
5. Memastikan transparansi dan akuntabilitas pemrosesan data.
6. Menyediakan pedoman yang siap diaudit oleh regulator.
7. Mendukung inovasi AI, analitik, dan open finance secara aman.

21.2 Ruang Lingkup Pengelolaan Data

Framework ini mencakup seluruh bentuk data:

A. Data Pribadi Dasar

Nama, NIK, alamat, tanggal lahir.

B. Data Pribadi Spesifik/Sensitif
Biometrik, kesehatan, data finansial, lokasi, identitas elektronik.

C. Data Transaksi
Transfer, pembayaran, aktivitas rekening.

D. Data Perilaku
Device fingerprinting, geolocation, pola belanja.

E. Data Sistem & Log
Log akses, API logs, fraud logs.

F. Data Analitik & Machine Learning
Dataset training AI, feature store, vectorized data.

21.3 Struktur Tata Kelola Data (Data Governance Model)

1. Data Protection Officer (DPO)
– wajib untuk Fintech besar

- memastikan kepatuhan UU PDP
- kontak utama dengan regulator

2. Chief Data Officer (CDO)

- mengelola strategi data
- kualitas data & metadata

3. Privacy Team

- DPIA, risk assessment, kebijakan PDP

4. Data Steward

- penjaga kualitas & keamanan data

5. Security Team

- encryption, IAM, data security

6. Engineering Team

- privacy-by-design implementation

21.4 Klasifikasi Data & Labeling

Setiap data harus diberi label:

Kategori	Contoh	Perlindungan
Publik	info umum	proteksi minimal
Internal	SOP internal	akses terbatas
Rahasia	data transaksi	enkripsi wajib
Sangat Rahasia	biometrik, NIK, PIN	enkripsi + akses firewall + monitoring 24/7

Semua sistem wajib mendukung data tagging & access control by classification level.

21.5 Prinsip Pengolahan Data (UU PDP + GDPR Alignment)

1. Purpose Limitation — data hanya dipakai untuk tujuan tertentu.
2. Data Minimization — tidak boleh mengumpulkan data berlebihan.
3. Lawful Processing — ada dasar hukum pengolahan.
4. Storage Limitation — data tidak disimpan lebih lama dari yang diperlukan.
5. Integrity & Confidentiality — keamanan ketat.
6. Accountability — bukti pemenuhan kewajiban.
7. Transparency — pengguna mengetahui bagaimana data mereka dipakai.
8. Accuracy — data harus akurat & terupdate.

21.6 Dasar Hukum Pemrosesan Data (Legal Basis)

Sesuai UU PDP:

- Persetujuan (Explicit Consent)
- Kontrak/Kebutuhan Layanan
- Kewajiban hukum
- Kepentingan yang sah (Legitimate Interest, harus melalui uji kepatutan)
- Pelindungan vital subjek data
- Penghapusan dan pemusnahan berdasar masa retensi sesuai ketentuan yang berlaku atau permintaan

Tidak diperbolehkan menggunakan “persetujuan tersirat”.

21.7 Data Lifecycle Management (End-to-End)

1. Data Collection

- hanya data yang diperlukan
- consent harus jelas & terpisah

2. Data Processing

- sesuai tujuan
- audit trail

3. Data Storage

- enkripsi at-rest & backup
- akses terbatas

4. Data Access

- RBAC/ABAC
- logging penuh

5. Data Sharing

- DPIA wajib sebelum berbagi data
- perjanjian pemrosesan data

6. Data Retention

- masa simpan berdasarkan regulasi
- data tidak relevan → dihapus

7. Data Deletion/Destruction

- soft deletion
- secure deletion (wiping)
- cryptographic erasure

21.8 Privacy by Design & Privacy Engineering

Seluruh sistem Fintech wajib menerapkan:

A. Data Minimization Mechanisms

- selective data collection
- optional data turned off by default

B. Data Masking & Tokenization

- mask nomor kartu
- token untuk transaksi

C. Encryption by Default

- AES-256
- TLS 1.3
- key rotation

D. Differential Privacy (Opsional tingkat tinggi)

Untuk analitik & AI dataset.

E. Federated Learning (Opsional)

Untuk model AI tanpa memindahkan raw data.

F. Access Control Enforcement

- dynamic access

- time-based access
- just-in-time access

G. Secure Multi-Party Computation (Opsional)
Untuk analitik lintas organisasi.

21.9 Data Subject Rights (Hak Subjek Data)

Wajib memberi fitur untuk:

1. Right to Access
Pengguna bisa meminta data mereka.

2. Right to Correction
Mengoreksi data yang salah.

3. Right to Deletion/Erasure
Menghapus data (kecuali diwajibkan regulator).

4. Right to Object
Menolak pemrosesan tertentu.

5. Right to Data Portability
Data dipindahkan ke layanan lain.

6. Right to Withdraw Consent
Persetujuan dapat dicabut kapan saja.

Fitur ini wajib user-friendly dan tersedia di aplikasi/website.

21.10 DPIA — Data Protection Impact Assessment

DPIA wajib untuk:

- data biometrik,
- decision-making berbasis AI,
- profiling,
- high-risk processing,
- data cross-border,
- data anak,
- open finance API sharing.

Komponen DPIA:

1. Deskripsi pemrosesan data
2. Risiko pada hak subjek data
3. Risiko operasional & teknis
4. Dampak hukum
5. Mitigasi teknis & prosedural

6. Residual risk score

21.11 Data Breach Management (Sesuai UU PDP)

Jika terjadi kebocoran data, wajib:

1. **Notifikasi ke subjek data ≤ 3 x 24 jam**
2. **Notifikasi ke regulator (Kominfo) ≤ 72 jam**
3. **Forensik digital & RCA**
4. **Remediation plan**
5. **Public disclosure (bila signifikan)**

Data breach severity:

- Low (tidak sensitif)
- Medium (data akun)
- High (finansial)
- Critical (biometrik, PIN, password)

21.12 Third-Party Data Sharing Governance

Data tidak boleh keluar kecuali:

- melalui API aman,
- tokenized,
- encrypted,
- ada kontrak Data Processing Agreement,
- vendor memenuhi:
  - ISO 27001
  - SOC 2
  - audit risiko
  - DPIA khusus vendor

Jika vendor gagal, maka dibutuhkan tindakan sesuai dengan ketentuan dan perjanjian kerjasama yang berlaku

21.13 Data Residency & Sovereignty

Mengacu regulasi:

- data tertentu wajib disimpan di wilayah hukum Indonesia,
- replikasi lintas negara harus mengikuti standar privacy,
- enkripsi & key management tidak boleh diserahkan ke vendor asing sepenuhnya.

21.14 Data Retention & Destruction Policy

Retensi minimal mengikuti regulasi seperti:

- transaksi: 5–10 tahun
- log keamanan: 3 tahun
- data biometrik: sesingkat mungkin

- data analitik: sesuai kebutuhan sah

Metode pemusnahan:
- cryptographic erase
- secure wipe
- data token invalidation

21.15 Data Security Controls (ISO 27001/27701 Alignment)
Kontrol teknis meliputi:

A. Encryption
- at-rest
- in-transit
- key rotation

B. IAM Controls
- role-based policy
- attribute-based access
- JIT access

C. Monitoring
- DLP alerts
- anomaly detection
- access audit trail
- fraud correlation

D. Data Masking & Tokenization

E. Segregation of Duties
- developer tidak boleh akses data produksi
- analyst hanya boleh lihat data pseudonymized

21.16 Data Quality & Metadata Governance

Fintech wajib menjaga:
- akurasi
- integritas
- lineage (asal data)
- metadata katalog (data dictionary)

Tools:
- data catalog
- data lineage tool
- metadata repository

21.17 AI & Data Protection (Integrasi Bab 12)

AI harus mematuhi:

1. **Fairness & Bias Testing**
2. **Explainability**
3. **No automated decision making tanpa human oversight**
4. **Dataset anonymization**
5. **Consent untuk profiling**

21.18 Privacy Incident Detection & DLP

DLP (Data Loss Prevention) digunakan untuk mendeteksi:

- pengiriman data ke luar organisasi
- upload ke cloud storage pribadi
- scraping data
- unauthorized export

Saluran yang sebaiknya di monitor:

- email
- web
- API
- USB
- database
- cloud storage

21.19 Audit & Metrics for Data Governance

KPI:

1. completion DPIA
2. data access reduction
3. zero unauthorized access
4. time to fulfill data subject request
5. data retention compliance

KRI:

1. peningkatan permintaan perbaikan data
2. data over-retention
3. data minimization violations
4. frequent DLP alerts
5. data sharing tanpa DPA

BAB 22
PHYSICAL SECURITY, ENVIRONMENTAL CONTROLS & FACILITY PROTECTION

PHYSICAL SECURITY, ENVIRONMENTAL CONTROLS & FACILITY PROTECTION, disusun sangat komprehensif, operasional, dan langsung dapat diterapkan oleh seluruh anggota AFTECH.
Bab ini mengacu pada:

- ISO/IEC 27001 Annex A.11 — Physical & Environmental Security
- NIST SP 800-116 (Physical Access Control Systems)
- TIA-942 Data Center Standard
- NFPA Fire Protection Standards
- FISMA Physical Security Controls
- BSSN CSF – Physical Layer Controls

Tujuan bab ini adalah memastikan bahwa keamanan fisik layanan Fintech berada pada standar yang sama dengan sektor perbankan dan data center internasional.

Walaupun Fintech cenderung digital-first, serangan fisik tetap menjadi ancaman signifikan:

- pencurian perangkat server,
- espionase fisik,
- akses ilegal ke ruang server,
- sabotase perangkat jaringan,
- insider attack,
- kerusakan akibat kebakaran atau banjir.

Karena itu, keamanan fisik harus menjadi bagian inti dari Cybersecurity Framework AFTECH.

22.1 Tujuan Pengamanan Fisik & Lingkungan

1. Mencegah akses fisik tidak sah ke aset TI kritikal.
2. Mengamankan fasilitas yang menyimpan dan memproses data pribadi pengguna.
3. Melindungi perangkat, jaringan, dan data dari ancaman lingkungan.
4. Memastikan kontinuitas layanan (availability) terhadap bencana fisik.
5. Mendukung kepatuhan terhadap OJK–BI–UU PDP.
6. Mengurangi risiko insider threat.

22.2 Ruang Lingkup Physical & Environmental Security

Framework berlaku untuk:

A. Kantor Operasional

- ruang kerja, meeting room, storage room

B. Data Center / Server Room
Baik on-prem, co-location, maupun cloud edge.

C. Network & Communication Rooms
Rak jaringan, router, switch, UPS.

D. Disaster Recovery Center (DRC)
Lokasi cadangan operasional.

E. Backup Storage Facilities

F. Mobile & Remote Equipment
Laptop, smartphone kantor, USB, token.

22.3 Physical Security Layered Defense (5 Layers)

AFTECH mewajibkan model pertahanan fisik berlapis:

1. Outer Layer – Boundary Protection

- pagar
- CCTV perimeter
- security checkpoint
- akses tamu terbatas

2. Middle Layer – Building Access Control

- kartu akses RFID
- biometrik visitor log
- turnstile

3. Inner Layer – Controlled Office Area

- restricted zones
- secure workstation
- no tailgating

4. Core Layer – Server Room / Data Center

- biometric entry
- 24/7 CCTV
- anti-passback system
- separate HVAC

5. Vault Layer – High-Security Zone
Untuk:

- HSM (Hardware Security Module)
- cryptographic keys
- sensitive data backup

22.4 Akses Fisik & Kontrol Identitas

A. Physical Access Control System (PACS)

Wajib menggunakan minimal salah satu:

- RFID card
- biometric access (fingerprint/iris/face)
- PIN + multifactor physical access
- QR-based visitor management

akses log disimpan min 2 tahun.

B. Visitor Access Management

- tamu harus didaftarkan
- diberikan badge khusus
- akses hanya dengan pendamping
- tidak boleh membawa laptop tanpa izin

C. Employee Access Leveling

Akses dibatasi berdasarkan:

- jabatan
- fungsi
- kebutuhan operasional

Prinsip: “least privilege” + “need to access”.

D. Anti-Tailgating Mechanisms

- turnstile
- mantrap entry system
- security officer standby

22.5 Server Room / Data Center Security Standards

1. Physical Requirements

- pintu baja anti-forced entry
- kunci elektromagnetik
- dinding tahan api minimal 2 jam
- lantai raised floor

2. CCTV Monitoring

- resolusi HD
- 24/7 recording
- minimal 90 hari retensi
- area yang wajib dipantau:
    - pintu server room
    - rak server
    - panel listrik

- UPS & genset
- HSM cabinet

3. Rack Security

- kunci individual pada setiap rack
- sensor pembukaan rak
- rack-level access logs

4. Cable Management & Protection

- kabel jaringan berada di tray khusus
- jalur kabel terkunci
- pemisahan kabel listrik & data

22.6 Environmental Controls

A. Fire Detection & Suppression

Mengikuti standar NFPA:

1. Fire Detection
   - smoke detector
   - heat detector
   - aspirating smoke detector (VESDA)
2. Fire Suppression
   - gas-based: FM-200, Inergen, NOVEC 1230
   - tidak diperbolehkan sistem air sprinkler untuk area server

B. Temperature & Humidity Control

- suhu: 18–27°C
- kelembapan: 40–60%
- HVAC terpisah khusus server

C. Water & Flood Protection

- sensor kebocoran
- raised floor
- anti-flood barrier

D. Power Protection

- UPS N+1
- genset dengan kapasitas minimal 8 jam
- surge protector
- automatic transfer switch (ATS)

22.7 Asset Protection & Hardware Security

1. Asset Tagging

Setiap perangkat memiliki:

- ID unik
- QR code
- location tracking

2. Hardware Hardening

- disable unused ports
- BIOS password
- disk encryption (BitLocker/ FileVault)

3. Secure Laptop & Mobile Devices

- EDR mandatory
- encrypted
- remote wipe
- device inventory management (MDM)

4. Secure Storage

- safe cabinet untuk media backup
- HSM vault
- lockable storage room

22.8 Physical Access Logging & Monitoring

Sistem PACS wajib mencatat:

- siapa yang masuk
- jam masuk/keluar
- area yang diakses
- anomali (misal: percobaan akses gagal)

Semua akses harus diaudit secara berkala seperti 3 atau 6 bulan.

22.9 Desktop & Workstation Security

Wajib diterapkan:

1. screen auto-lock: ≤ 5 menit
2. clean desk policy
3. no paper print untuk data sensitif
4. tidak boleh mencolokkan USB unauthorized
5. MDM untuk seluruh laptop
6. VPN saat remote work

22.10 Secure Operational Procedures

1. Media Handling

- tidak boleh menyimpan data sensitif di USB

- enkripsi wajib untuk portable media
- secure wipe saat memusnahkan media

2. Shredding & Destruction

Semua media kertas dengan informasi sensitif harus:

- dihancurkan menggunakan shredder industri
- dicatat dalam disposal log

3. Secure Meeting Rooms

- anti-eavesdropping (opsional level tinggi)
- larangan membawa device pada rapat high-security

22.11 Protection Against Social Engineering (Physical)

Ancaman fisik sering terjadi melalui:

- piggybacking / tailgating
- impersonation sebagai teknisi
- penempatan USB malware
- shoulder surfing

Mekanisme perlindungan:

- security awareness training
- signage “No tailgating”
- patroli keamanan
- pemasangan dummy camera untuk deterrence
- prosedur verifikasi identitas teknisi vendor

22.12 Remote Work & Offsite Security Requirements

Fintech wajib memiliki kebijakan:

Laptop Work-from-Home Security

- full disk encryption
- VPN always-on
- MFA mandatory
- prohibition of printing sensitive data
- internet minimum security (no public WiFi)

Remote Meeting & Virtual Workspace

- monitoring screen sharing
- no unauthorized recording
- remote wipe capability

22.13 Disaster Recovery Facility Physical Requirements

DRC harus memiliki:

- lokasi geografis berbeda
- jalur listrik berbeda

- akses fisik ketat
- kontrol lingkungan sama seperti pusat data
- redundansi internet minimal 2 ISP
- link VPN dengan enkripsi kuat

22.14 Physical Security Audits & Testing
Audit harus dilakukan 2x per tahun mencakup:

- walkthrough inspeksi fisik
- fire system testing
- access control review
- CCTV log sampling
- asset inventory match
- badge testing
- visitor process testing

Termasuk red team physical intrusion test (opsional untuk Fintech besar).

22.15 KPI & KRI Keamanan Fisik
KPI yang bisa dijadikan rujukan:

1. tidak ada tailgating
2. waktu respon alarm < 5 menit
3. SLA HVAC 99.9%
4. 100% biometric log retention
5. audit temuan diperbaiki ≤ 30 hari

KRI yang bisa dijadikan rujukan:

1. gagal akses fisik meningkat
2. suhu server room > threshold
3. kelembapan abnormal
4. power outage > 15 menit
5. perangkat hilang/tidak ditemukan

22.16 Kepatuhan & Standar Referensi
Fintech wajib memenuhi setiap regulasi yang berlaku:

- UU PDP (perlindungan fisik data pribadi)
- SEOJK 29/2022
- PBI 22/2024
- ISO 27001 Annex A.11
- ISO 22301 (BCM)
- BSSN Keamanan Fisik
- TIA-942 (data center tiers)

BAB 23
BUSINESS CONTINUITY MANAGEMENT (BCM) & DISASTER RECOVERY (DR)

BUSINESS CONTINUITY MANAGEMENT (BCM) & DISASTER RECOVERY (DR).

Bab ini disusun sangat komprehensif, implementable, sesuai standar global, serta langsung dapat dipakai untuk audit OJK–BI, penilaian risiko, dan kesiapan operasional Fintech.

Standar rujukan:

- ISO 22301: Business Continuity Management System
- ISO 27031 (ICT Readiness for BCM)
- NIST SP 800-34 (Contingency Planning Guide)
- FFIEC Business Continuity Handbook
- SAS-70/SSAE SOC Controls
- OJK – Manajemen Risiko TI & Risiko Siber (SEOJK 29/2022)

Fintech adalah sektor dengan continuous operations, tidak boleh berhenti karena insiden teknis, serangan siber, kegagalan jaringan, atau bencana alam. BCM & DR memastikan layanan tetap berjalan, data tetap aman, dan pengguna tetap mendapatkan layanan meskipun terjadi gangguan besar.

23.1 Tujuan BCM & DR Framework

1. Menjamin kelangsungan layanan kritikal Fintech.
2. Mencegah kegagalan operasional akibat ancaman internal maupun eksternal.
3. Mengurangi dampak finansial, reputasi, dan hukum.
4. Menyediakan rencana respons organisasi pada situasi darurat.
5. Memenuhi standar regulator (BI/OJK), terutama pada area resiliensi operasional.
6. Menyediakan tata kelola untuk pemulihan data dan sistem TI.
7. Mendukung ketahanan ekosistem digital nasional.

23.2 Ruang Lingkup BCM & DR

Framework berlaku untuk:

A. Sistem Layanan Utama Fintech

- transaksi keuangan
- pembayaran & e-money
- kartu/OTP/credential system
- API business-critical
- user authentication & login

B. Infrastruktur & Teknologi

- server, cloud, database
- network, security devices
- CDN & API gateway

C. Sumber Daya Manusia

- pekerja kritikal
- struktur komando saat bencana

D. Lokasi Fisik

- kantor utama
- data center
- disaster recovery center (DRC)

E. Vendor & Third Party Critical Providers

- payment gateway
- cloud provider
- open finance partners

23.3 Governance & Struktur BCM

Struktur BCM harus jelas dan formal:

1. BCM Steering Committee

Ketua: Direktur Risiko/Operasional.

Tugas:

- menyetujui kebijakan
- mengesahkan dokumen BCM
- evaluasi tahunan

2. Business Continuity Manager

- merancang, mengupdate BCP
- memimpin latihan dan uji coba

3. DR Lead (IT Disaster Recovery Manager)

- mengelola rencana pemulihan TI
- memimpin aktivasi DRC

4. Crisis Management Team (CMT)

Komposisi:

- CEO/COO
- CISO
- CTO
- Legal
- HR
- komunikasi publik

5. Pemilik Proses (Process Owner)

- memastikan daftar proses yang harus dipulihkan

6. Tim Operasional Kritis

- keamanan TI
- helpdesk
- payment operation team
- fraud monitoring

23.4 Risiko yang Dicakup BCM

1. Gangguan Infrastruktur

- listrik padam
- jaringan down
- kerusakan server

2. Bencana Alam

- banjir
- gempa
- kebakaran

3. Insiden Keamanan Siber

- ransomware
- DDoS
- APT attack
- data breach

4. Kegagalan Vendor

- cloud outage
- payment processor gagal
- open API partner down

5. Gangguan Operasional

- kesalahan manusia
- kegagalan konfigurasi
- release gagal

6. Krisis SDM

- pandemi
- demo/bencana kota
- pemogokan massal

23.5 Business Impact Analysis (BIA)

BIA menentukan:

1. Proses Kritis

- pembayaran real-time
- settlement
- KYC & onboarding
- customer support
- fraud detection

2. Dampak Gangguan

- finansial
- operasional
- reputasi
- legal/regulator

3. MTD (Maximum Tolerable Downtime)

Waktu maksimal layanan boleh mati sebelum dampak fatal.

4. RTO (Recovery Time Objective)

Berapa lama sistem harus pulih setelah gangguan.

5. RPO (Recovery Point Objective)

Berapa banyak data maksimal boleh hilang (hitungan menit).

Contoh standar yang dapat diaplikasikan:

Sistem	RTO	RPO
Core payment	1 jam	0 menit (real-time replication)
Authentication	< 30 menit	< 5 menit
Reporting	24 jam	12 jam
Fraud engine	1 jam	5 menit

23.6 BCM Strategy Options

A. Redundancy & High Availability

- multi-region cloud
- load balancer
- auto-failover

B. Disaster Recovery Center (DRC)

DRC wajib:

- lokasi berbeda secara geografis
- konektivitas multi-ISP
- data ter-replikasi real-time

C. Cloud-based DR

Untuk Fintech kecil → lebih efektif:

- multi-region cloud backup

- auto-restore snapshots

D. Manual Workaround
Prosedur darurat untuk:
- transaksi backend
- pelaporan regulator
- komunikasi nasabah

E. Vendor Alternate Mode
Jika vendor gagal:
- failover ke vendor cadangan
- switch API provider

23.7 Disaster Recovery (DR) Strategy
DR dilakukan berdasarkan jenis pemulihan:

1. Hot Site
- sinkronisasi real-time
- aktif otomatis saat primary down
- RTO < 1 jam

2. Warm Site
- data backup real-time / near-real-time
- aktivasi manual
- RTO 4–8 jam

3. Cold Site
- infrastruktur sudah siap, data belum
- RTO 24–72 jam

4. Cloud Native DR
- multi-region replication
- cross-zone load balancing
- automated failover

23.8 Backup & Restore Strategy
Standar backup yang direkomendasikan untuk Fintech:
1. Daily full backup
2. Hourly incremental backup (untuk sistem kritikal)
3. Encrypted backup (AES-256)
4. Offsite backup (cloud atau DRC)
5. Backup integrity check mingguan
6. Backup retention min 3 tahun

Restore test wajib dilakukan setiap 3 bulan.

23.9 Crisis Management Procedures

Jika terjadi insiden besar:

1. Aktivasi CMT (Crisis Management Team)

dipicu oleh:

- serangan ransomware
- data breach
- data center down
- kegagalan layanan kritikal

2. Pengalihan Komunikasi

- hotline khusus
- grup war room
- dokumentasi terpusat

3. Komunikasi Eksternal

- nasabah
- regulator (BI, OJK, Kominfo)
- mitra usaha
- media (jika diperlukan)

4. Pemetaan Dampak

- jumlah pengguna terkena
- data yang terpengaruh
- sistem yang rusak

23.10 Incident Response vs Business Continuity vs Disaster Recovery

Aktivitas	Fokus	Kapan digunakan
Incident Response	Menghentikan serangan	saat insiden keamanan
Business Continuity	Memastikan bisnis tetap berjalan	saat gangguan operasional
Disaster Recovery	Memulihkan sistem TI	setelah insiden selesai

23.11 DR Activation Flow

1. Deteksi insiden
2. Eskalasi ke CMT
3. Deklarasi disaster
4. Failover ke DRC
5. Aktivasi backup & layanan minimum
6. Komunikasi ke regulator
7. Operasi manual jika perlu
8. Pemulihan ke sistem utama (failback)

9. RCA & dokumentasi

23.12 BCM Testing & Simulation

BCM wajib diuji minimal 2x per tahun:

Jenis Uji:

1. Tabletop Exercise
2. Functional Test
3. Technical DR Test (Failover test)
4. Unannounced DR Drill
5. Full Disaster Simulation
    - gempa
    - cyber attack
    - listrik padam massal

Evaluasi mencakup:

- gap analisis
- SLA pemulihan
- ketepatan aktivasi tim
- stabilitas layanan failover

23.13 Vendor & Third-Party BCM Requirements

Fintech harus memastikan vendor kritikal memiliki:

- BCP
- DRP
- RTO/RPO jelas
- lokasi DR
- bukti uji DR tahunan
- SLA pemulihan

Vendor yang tidak memiliki BCM → tidak boleh menangani data sensitif.

23.14 Metrics, KPI & KRI BCM

KPI

1. RTO dan RPO tercapai saat testing
2. tingkat keberhasilan failover > 95%
3. kepatuhan test BCM 100%
4. waktu aktivasi CMT < 30 menit
5. seluruh proses BIA lengkap

KRI

1. kegagalan DR test
2. ketergantungan vendor tunggal (single point of failure)
3. backup gagal diverifikasi
4. peningkatan downtime bulanan

5. tidak ada offsite backup

23.15 Kepatuhan BCM

BCM wajib mematuhi ketentuan berlaku seperti:

- SEOJK 29/2022
- PBI 22/2024
- ISO 22301
- ISO 27031
- UU PDP (perlindungan data selama bencana)
- persyaratan audit tahunan OJK/BI

BAB 24
OPERATIONAL RISK MANAGEMENT & FRAUD RISK GOVERNANCE

OPERATIONAL RISK MANAGEMENT & FRAUD RISK GOVERNANCE, disusun sangat komprehensif, teknis, implementable, dan sesuai standar global.

Bab ini menjadi kerangka wajib bagi seluruh penyelenggara Fintech anggota AFTECH untuk memastikan risiko operasional & risiko fraud dapat dicegah, dideteksi, dan ditangani secara sistematis.

Framework ini merujuk pada:

- ISO 31000 (Risk Management)
- Basel II/III – Operational Risk Framework
- COSO Enterprise Risk Management (ERM)
- FFIEC IT & Operational Risk Handbook
- NIST Cybersecurity Framework
- ACFE Fraud Risk Management Guide
- OECD Fraud Prevention Guideline
- OJK SEOJK 29/2022
- PBI & ketentuan SP terkait fraud & operasional

Fintech adalah industri dengan risiko operasional tinggi akibat teknologi, proses, dan interaksi pengguna yang intensif. Selain itu, fraud berkembang sangat cepat melalui social engineering, account takeover (ATO), money mule, dan transaksi digital.

Bab ini menetapkan standar nasional untuk tata kelola risiko operasional & fraud di ekosistem AFTECH.

24.1 Tujuan Framework Operasional & Fraud

1. Mengidentifikasi risiko operasional secara komprehensif.
2. Mengurangi kerugian akibat kegagalan proses, sistem, atau manusia.
3. Mendeteksi dan mencegah fraud internal maupun eksternal.
4. Menjamin keandalan layanan Fintech yang berkelanjutan.
5. Memenuhi persyaratan regulator (BI, OJK, Kominfo).
6. Membentuk budaya anti-fraud dan risk awareness dalam organisasi.
7. Mendukung keamanan siber dan keberlanjutan bisnis.

24.2 Ruang Lingkup Risiko Operasional

Mencakup seluruh area Fintech:

A. Risiko Teknologi

- kegagalan sistem
- API down
- cloud outage

- cyber attack
- bug aplikasi

B. Risiko Proses

- SOP tidak jelas
- tidak ada kontrol 4-eye
- error operasional
- ketidaksesuaian prosedur

C. Risiko SDM

- human error
- kelalaian
- insider threat
- kurang pelatihan

D. Risiko Vendor/Third Party

- kegagalan vendor
- SLA tidak dipenuhi
- keamanan vendor lemah

E. Risiko Fraud

- ATO
- social engineering
- carding
- synthetic identity
- collusion
- internal fraud

24.3 Struktur Tata Kelola Risiko Operasional & Fraud

1. Board of Directors (BoD)

- menetapkan risk appetite & tolerance
- menyetujui kebijakan risiko

2. Chief Risk Officer (CRO)

- mengawasi risk management framework

3. Operational Risk Committee

- meninjau risiko utama
- memutuskan mitigasi

4. Fraud Risk Committee

- analisis tren fraud
- menetapkan kebijakan pencegahan

5. Risk Management Unit

- melakukan identifikasi & asesmen risiko

6. Fraud Management Unit

- fraud investigation
- fraud analytics

7. Internal Audit

- menguji efektivitas kontrol
- memberikan assurance ke BoD

24.4 Penilaian Risiko Operasional (Risk Assessment)

Siklus penilaian risiko Fintech:

1. Identifikasi Risiko

- workshop risiko
- incident review
- historical loss data
- audit findings
- monitoring alert

2. Analisis Risiko

- likelihood (probabilitas)
- impact (finansial, reputasi, hukum)
- risk velocity (kecepatan dampak)

3. Pengukuran Risiko

Menggunakan:

- heatmap risiko
- scoring matrix
- KRIs (Key Risk Indicators)

4. Mitigasi Risiko

Jenis mitigasi:

- Avoid
- Reduce
- Transfer (asuransi)
- Accept

5. Monitoring Risiko

- dashboard risiko
- risk update bulanan
- alert threshold

24.5 Key Risk Indicators (KRI) untuk Fintech

KRI wajib mencakup:

A. Teknologi

- system downtime
- API timeout rate
- database replication delay
- increase in error code 5xx
- patching backlog

B. Proses

- gagal settlement
- gagal reconciliation
- lonjakan dispute/complaint

C. SDM

- pelanggaran SOP
- akses tidak sah
- ketidakhadiran tim kritikal

D. Vendor

- SLA breach
- vendor outage
- vendor security incident

E. Fraud

- spike login attempts
- anomaly device fingerprint
- velocity pattern abnormal
- suspicious IP
- chargeback/fraud ratio

24.6 Fraud Risk Management Framework (ACFE Standard)

Fraud di Fintech dapat berupa:

1. External Fraud

- phishing
- ATO (Account Takeover)
- social engineering
- money mule
- synthetic identity
- carding
- promo abuse

2. Internal Fraud

- collusion

- misuse of privilege
- data theft
- misappropriation

24.7 Fraud Risk Lifecycle Governance

Framework terdiri dari 6 pilar:

1. Fraud Prevention

Sebelum fraud terjadi.

A. Strong KYC/KYB

- face match
- liveness detection
- e-KTP verification
- AML screening

B. Identity Proofing

- device fingerprinting
- IP geolocation
- phone + SIM swap detection

C. Transaction Controls

- limit management
- 2FA/MFA
- risk-based authentication

D. Access Control

- RBAC
- Privileged Access Monitoring

E. Policy & SOP

- anti-fraud code of conduct
- separation of duties
- maker-checker approval

2. Fraud Detection

Menggunakan:

A. Rule-based Detection

- suspicious patterns
- velocity rules
- anomaly thresholds

B. Machine Learning Fraud Engine

Model yang harus tersedia:

- ATO model
- transaction fraud model

- behavioral analytics
- device reputation model

C. Real-time Monitoring

- API abuse detection
- risk scoring engine
- UEBA (User & Entity Behavior Analytics)

D. Threat Intelligence Integration

- darkweb dump monitoring
- compromised credential
- botnet IP sensor

3. Fraud Mitigation / Interception

Jika fraud terdeteksi:

- transaksi diblok
- account freeze
- MFA challenge
- session termination
- device blocklist

4. Fraud Investigation

Tim Fraud Investigator wajib:

- mengumpulkan bukti
- melakukan log analysis
- bekerjasama dengan bank & payment gateway
- mengidentifikasi pola fraud
- investigasi insider threat

Tools investigasi:

- log correlation
- OSINT tools
- payment traceability
- device analytics

5. Fraud Recovery

- reimburse sesuai kebijakan
- proses dispute
- kerja sama dengan penegak hukum
- pemulihan dana jika memungkinkan

6. Fraud Reporting

Laporan wajib meliputi:

- jumlah kasus

- pola fraud
- root cause
- rekomendasi mitigasi
- laporan ke regulator jika signifikan

24.8 Model Fraud Analytics & Scoring

Model ML wajib terdiri dari:

1. ATO Model

Faktor:

- new device
- location anomaly
- unusual login timing
- impossible travel
- behavioral deviation

2. Transaction Fraud Model

Faktor:

- average spend deviation
- merchant abnormality
- velocity anomaly
- multiple accounts → same device

3. Device Intelligence

- emulator detection
- rooted/jailbroken
- VPN/proxy detection

4. Social Engineering / Scam

- pattern dari link phishing
- victim behavioral signals

24.9 Anti-Money Laundering (AML) & Fraud Integration

Fraud engine harus terintegrasi AML:

- name screening
- suspicious transaction pattern
- mule account detection
- layering pattern detection

Link dengan PPATK apabila ada transaksi mencurigakan.

24.10 Vendor & Third-Party Fraud Controls

Fintech wajib mengawasi vendor kritikal:

Kontrol minimal:

- audit keamanan tahunan
- fraud-SLA
- E-KYC provider reliability
- API abuse detection
- vendor fraud incident reporting

24.11 Fraud Red Teaming (Advanced)

Simulasi fraud untuk menguji ketahanan:

- synthetic identity creation
- bypassing KYC
- ATO simulation
- multi-account abuse
- promo fraud simulation

Output red teaming: fraud-resistant design improvements.

24.12 Pengendalian Internal (Internal Controls)

Kontrol wajib:

- maker-checker approval
- 4-eye principle
- limit transaction authority
- monthly access review
- session recording untuk admin

24.13 Fraud Whistleblowing System

Wajib memiliki:

- kanal anonim
- perlindungan whistleblower
- investigasi independen
- pelaporan langsung ke BOD/komisaris

24.14 KPI & KRI Fraud & Operational Risk

KPI

1. fraud prevented value
2. detection rate
3. false positive < 5%
4. SLA investigation
5. downtime operasional

KRI

1. spike login gagal
2. lonjakan transaksi abnormal
3. serangan phishing meningkat
4. integritas data turun
5. jumlah akses admin tidak wajar

24.15 Kepatuhan & Regulasi

Framework ini mematuhi:

- SEOJK 29/2022
- POJK Perlindungan Konsumen
- PBI 22/2024
- UU PDP
- AML/KYC rules (APU-PPT)
- FATF Recommendation

BAB 25
COMPLIANCE MANAGEMENT, LEGAL GOVERNANCE & REGULATORY ALIGNMENT

COMPLIANCE MANAGEMENT, LEGAL GOVERNANCE & REGULATORY ALIGNMENT, disusun komprehensif, operasional, dan siap audit untuk seluruh anggota AFTECH.

Framework ini mengikuti standar internasional dan regulasi nasional:

- ISO 37301 (Compliance Management System)
- ISO 37000 (Governance of Organizations)
- OECD Corporate Governance Principles
- SOX Compliance Controls
- NIST Cybersecurity Framework Governance Function
- OJK SEOJK 29/2022 – Tata Kelola TI & Risiko Siber
- PBI 22/2024 – SP & Inovasi Keuangan Digital
- UU PDP & PP Turunannya
- UU ITE, PP PSTE, UU Perlindungan Konsumen
- Standar AML/CTF (APU-PPT PPATK)

Bab ini menjadi landasan tata kelola hukum dan kepatuhan untuk mendukung keamanan siber, resiliensi operasional, perlindungan konsumen, dan integritas ekosistem Fintech Indonesia.

25.1 Tujuan Compliance & Legal Governance Framework

1. Memastikan Fintech mematuhi seluruh kewajiban hukum dan regulasi yang berlaku.
2. Mengurangi risiko hukum, sanksi, penalti, dan gangguan layanan akibat ketidakpatuhan.
3. Menyediakan kerangka kerja kepatuhan yang sistematis, terukur, dan berkelanjutan.
4. Mendukung prinsip transparansi, akuntabilitas, dan tata kelola yang baik (good governance).
5. Menjaga kepercayaan pengguna, mitra, regulator, dan investor.
6. Mengintegrasikan kepatuhan dengan keamanan siber, privasi, dan manajemen risiko operasional.

25.2 Ruang Lingkup Compliance Management

Framework ini mencakup:

A. Kepatuhan Regulator

- OJK: risiko siber, perlindungan konsumen, governance
- BI: SP, AML/CTF, interkoneksi

- Kominfo: PDP, layanan digital
- PPATK: APU-PPT
- BSSN: keamanan siber

B. Kepatuhan Hukum
- kontrak & perjanjian
- data privacy
- peraturan tenaga kerja
- perlindungan konsumen

C. Kepatuhan Teknologi
- standar keamanan TI
- perlindungan data
- cloud compliance
- Fintech licensing

D. Kepatuhan Internal
- SOP
- kebijakan HR
- standar etik & integritas

25.3 Struktur Tata Kelola Kepatuhan

1. Board of Directors
- menetapkan kebijakan kepatuhan
- memastikan resourcing memadai

2. Chief Compliance Officer (CCO)
- posisi independen
- pelapor langsung ke BoD

3. Compliance Committee
- meninjau regulasi baru
- koordinasi lintas unit

4. Legal Team
- interpretasi hukum
- drafting kontrak
- dukungan litigasi

5. Regulatory Liaison
- penghubung formal dengan regulator (OJK/BI/Kominfo/PPATK/BSSN)

6. Second Line Assurance

- monitoring kepatuhan
- review kebijakan

7. Internal Audit (Third Line)
- memberikan assurance atas kepatuhan
- menilai efektivitas kontrol

25.4 Compliance Program Maturity Model (ISO 37301)

Level 1 — Ad hoc
- tidak ada kebijakan formal
- reaktif terhadap regulasi

Level 2 — Initial
- ada beberapa kebijakan
- belum terintegrasi

Level 3 — Defined
- CMS formal & terdokumentasi
- mekanisme monitoring berjalan

Level 4 — Managed
- compliance terotomasi sebagian
- governance aktif
- pelatihan rutin

Level 5 — Optimized
- fully integrated CMS
- risk-driven
- advance reporting & analytics

AFTECH mendorong Fintech menuju Level 4 atau 5.

25.5 Kewajiban Kepatuhan Regulator Utama

A. OJK (SEOJK 29/2022, POJK Perlindungan Konsumen)
- risk management TI
- risk siber
- insident reporting ≤ 1x24 jam
- keamanan data konsumen
- transparansi layanan & biaya

B. Bank Indonesia (PBI 22/2024, SP & IJKD)
- integritas transaksi

- konektivitas payment gateway
- availability layanan
- fraud monitoring
- consumer dispute handling

C. Kominfo (UU PDP, PP PSTE)

- legal basis pengolahan data
- DPIA
- notifikasi kebocoran data
- penghapusan data

D. PPATK (APU-PPT)

- screening AML
- STR dan CTR
- KYC & KYB compliance

E. BSSN

- standar keamanan siber
- ketahanan infrastruktur digital

25.6 Regulatory Mapping Matrix

Fintech wajib melakukan regulatory mapping mencakup:

Regulator	Kewajiban	Unit Penanggung Jawab	Kontrol
OJK	Risiko TI & Konsumen	Compliance / CISO	TI Controls, SLA
BI	Sistem Pembayaran	Ops / IT	Availability, Fraud
Kominfo	PDP	DPO	Privacy Controls
PPATK	AML	AML Officer	Screening, STR
BSSN	Cybersecurity	CISO	CSF Maturity

Mapping ini diperbarui minimal triwulan.

25.7 Regulatory Change Management (RCM)

Framework RCM memastikan Fintech selalu mengikuti regulasi terbaru.

Tahapannya:

1. Monitoring Regulasi
    - siaran regulator
    - media pemerintah
    - asosiasi (AFTECH)
2. Analisis Dampak (Impact Assessment)
    - sistem

    - SDM
    - kontrak
    - operasional
3. Update Kebijakan Internal
4. Implementasi Kontrol Baru
5. Pelatihan Karyawan
6. Audit Kepatuhan

25.8 Legal Governance & Contract Management

Legal governance mencakup:

A. Contract Lifecycle Management

- drafting
- review legal
- approval
- signing
- renewal

B. Perjanjian dengan Third Party

Wajib mencakup:

- SLA
- SLO
- kerahasiaan (NDA)
- data processing agreement (DPA)
- liability & indemnity
- security clause
- breach notification

C. Terms & Conditions / Privacy Policy

Wajib:

- mudah dipahami
- fully aligned dengan UU PDP
- menetapkan hak pengguna
- menjelaskan data apa saja yang dikumpulkan

25.9 Compliance Risk Management

Compliance risk adalah risiko:

- sanksi hukum
- penalti finansial
- pemutusan izin Fintech

- reputasi rusak

Risiko harus dinilai dengan:
- probability
- severity
- velocity
- regulatory exposure

Kontrol:
- SOP
- pelatihan
- audit rutin
- monitoring otomatis

25.10 Mandatory Policies & SOPs

Setiap Fintech wajib memiliki minimal:
1. Information Security Policy
2. Data Privacy Policy
3. Incident Response Policy
4. Vendor Management Policy
5. Fraud Risk Policy
6. Risk Management Framework
7. BCM/DR Policy
8. Code of Ethics & Anti-Fraud
9. HR Security Policy
10. Regulatory Reporting SOP
11. Complaints Handling SOP

25.11 Compliance Monitoring & Reporting

Bagian dari Compliance Management System (CMS):

1. Monitoring Rutin
- compliance checklist
- control testing
- dashboard kepatuhan

2. Reporting Internal
- bulanan ke manajemen
- triwulan ke Board

3. Reporting ke Regulator
- insiden siber (≤ 24 jam)

- STR/CTR ke PPATK
- laporan berkala OJK/BI
- pemberitahuan data breach

4. Compliance Scoring

Setiap unit mendapat:
- skor compliance
- rekomendasi perbaikan

25.12 Pelatihan & Awareness Compliance

Program wajib:
- onboarding compliance training
- mandatory training tahunan
- training PDP
- AML training
- incident reporting training
- tabletop compliance exercise

25.13 Audit Kepatuhan

Audit dilakukan oleh Internal Audit (dan eksternal bila perlu):

Audit mencakup:
- ketepatan SOP
- bukti compliance
- kontrol teknis berfungsi
- readiness terhadap pemeriksaan regulator

Audit minimal 1x per tahun.

25.14 Enforcement: Sanksi Internal

Untuk pelanggaran kepatuhan:
- teguran
- pengurangan akses
- pembekuan akun admin
- SP (surat peringatan)
- pemutusan hubungan kerja
- pelaporan kepada otoritas jika signifikan

25.15 KPI & KRI Compliance

KPI

1. 100% mandatory training completion
2. audit compliance score ≥ 85%
3. tidak ada insiden penalti regulator
4. SLA laporan regulator terpenuhi
5. dokumentasi compliance update tepat waktu

KRI

1. keterlambatan laporan regulator
2. pelanggaran SOP meningkat
3. revisi kebijakan tidak dilakukan tepat waktu
4. peningkatan keluhan konsumen
5. penyimpangan kontrak vendor

25.16 Integrasi Compliance dengan Cybersecurity & Data Governance

Compliance harus terhubung dengan:

- Data Protection (Bab 21)
- Risk Management (Bab 24)
- Incident Response (Bab 6 & 7)
- Vendor Management (Bab 10)
- Security Logging & Monitoring (Bab 19)
- Fraud Governance (Bab 24)

Compliance bukan hanya administrasi, tetapi fungsi strategis untuk ekosistem Fintech nasional.

BAB 26
HUMAN RESOURCE SECURITY, INSIDER THREAT PREVENTION & WORKFORCE CYBER READINESS

HUMAN RESOURCE SECURITY, INSIDER THREAT PREVENTION & WORKFORCE CYBER READINESS, disusun sangat komprehensif, operasional, dan siap implementasi sehingga dapat digunakan langsung oleh anggota AFTECH sebagai standar nasional untuk keamanan SDM Fintech.
Framework ini mengacu pada:

- ISO/IEC 27001 Annex A.7 (Human Resource Security)
- NIST SP 800-181 (Cyber Workforce Framework)
- NIST SP 800-53 (Insider Threat Controls)
- NIST SP 800-50 (Cybersecurity Awareness Training)
- CERT Insider Threat Program Management Guide
- FFIEC IT Management Handbook
- OJK SEOJK 29/2022 (Keamanan TI & Risiko Siber)
- UU PDP & UU Ketenagakerjaan

Bab ini menempatkan manusia sebagai faktor keamanan terpenting: kekuatan sekaligus kelemahan.

Dalam ekosistem Fintech, mayoritas insiden keamanan muncul akibat:

- Human error
- Kelalaian
- Social engineering
- Penyalahgunaan akses (insider misuse)
- Kurangnya pelatihan
- Tekanan operasional & fraud collusion
- Demotivasi

Maka keamanan SDM menjadi komponen yang wajib ada dalam Cybersecurity Framework AFTECH.

26.1 Tujuan Human Resource Security Framework

1. Memastikan bahwa setiap pegawai aman, kompeten, dan bertanggung jawab.
2. Mengurangi risiko insider threat (karyawan, vendor, kontraktor).
3. Mencegah penyalahgunaan akses ke sistem kritikal.
4. Mendukung budaya keamanan siber di seluruh level organisasi.
5. Mewujudkan workforce yang siap menghadapi ancaman digital.
6. Memenuhi standar regulator dan audit (BI, OJK, BSSN).

26.2 Ruang Lingkup

Framework ini mencakup seluruh:

- pegawai tetap
- pegawai kontrak
- vendor/outsourcing
- partner KYC/KYB
- outsourced developer
- pengurus perusahaan
- pihak ketiga dengan akses sistem

26.3 Pre-Employment Security (Pra-Rekrutmen)

Semua calon pegawai yang akan mengakses sistem Fintech harus menjalani:

1. Background Check (Wajib)

Paling sedikit mencakup:

- verifikasi KTP
- verifikasi pendidikan
- riwayat pekerjaan
- pemeriksaan catatan kriminal (SKCK)
- fraud/AML/blacklist screening
- adverse media screening

2. Screening Khusus (Untuk Posisi Sensitif)

Termasuk:

- CISO, DevOps, Backend, DBA
- Admin system
- Fraud analyst
- Payment operation

Tambahan pemeriksaan:

- cek financial integrity
- cyber hygiene test
- personality & integrity assessment

3. Kontrak Kerja khusus Security Clause

Harus mencakup:

- NDA (Non-Disclosure Agreement)
- larangan misuse data
- larangan membawa data keluar
- aturan kewajiban keamanan TI

26.4 Onboarding Security Requirements

Setiap pegawai baru wajib:

1. Menandatangani Perjanjian Keamanan

Berupa:
- NDA
- Acceptable Use Policy (AUP)
- Data Privacy Policy
- Code of Conduct & Anti-Fraud

2. Awareness Training

Minimal mencakup:
- phishing
- password security
- mobile security
- secure handling of customer data
- insider threat awareness
- anti-fraud
- AML basic

3. Account Provisioning

Menggunakan prinsip:
- least privilege
- role-based access control
- time-based access (opsional)

4. HR–IT Access Workflow

SOP wajib memiliki:
- HR → IT → Security approval chain
- tracking seluruh akses yang diberikan
- pencatatan audit trail

26.5 During Employment: Operational HR Security Controls

A. Access Control Monitoring
- access review bulanan untuk sistem kritikal
- real-time alert untuk privileged access
- logging seluruh aktivitas admin

B. Segregation of Duties (SoD)

Tidak boleh ada karyawan yang dapat:

- membuat transaksi + menyetujui
- membuat akun admin + mengesahkan
- mengubah konfigurasi + deploy ke production

C. Continuous Training

Training wajib:

1. Cybersecurity Awareness (quarterly)
2. Phishing Simulation (monthly)
3. Fraud Awareness
4. Data Privacy Training
5. Secure Coding (untuk developer)

D. Monitoring Perilaku (UEBA/HR Analytics)

Untuk mendeteksi:

- perubahan perilaku abnormal
- access pattern tidak wajar
- conflict-of-interest
- potensi insider collusion

E. Enforcement of Work Policies

- Clean desk policy
- No unauthorized USB
- No personal cloud storage
- VPN mandatory saat remote work

F. Rotasi Pekerjaan (Job Rotation)

Untuk mencegah fraud & collusion.

26.6 Insider Threat Prevention Framework

Insider threat merupakan risiko terbesar di Fintech.

Framework terdiri dari:

1. Technical Controls

- logging & monitoring (SIEM)
- DLP (Data Loss Prevention)
- restricted access

- zero-trust controls
- screenshot prevention (opsional)
- record privileged sessions
- USB blocking

2. Behavioral Controls
- HR analytics
- abnormal login pattern
- mood/performance monitoring (opsional)
- employee assistance program (EAP)

3. Policy Controls
- NDAs
- anti-fraud governance
- acceptable use policies
- progressive discipline

4. Organizational Controls
- strong ethical culture
- leadership monitoring
- conflict-of-interest declaration
- segregation of duties

5. Insider Threat Response Team (ITRT)

Anggotanya:
- HR
- CISO
- Legal
- Internal Audit
- Fraud
- Risk Management

Tugas:
- investigasi
- mitigasi
- action to terminate/discipline
- forensik

26.7 Vendor & Third-Party Personnel Security

Vendor yang memiliki akses harus diperlakukan seperti pegawai internal.

Kontrol wajib:

- screening vendor personnel
- NDA vendor
- access approval
- VPN + MFA
- monitoring aktivitas vendor
- logging ke SIEM
- revokasi akses setelah kontrak selesai

Vendor tanpa kontrol ini tidak boleh mengakses data produksi.

26.8 Remote Work & Hybrid Work Security

1. Device Requirements
- laptop terenkripsi
- EDR mandatory
- mobile device via MDM

2. Home Office Security
- jaringan aman
- tidak boleh menggunakan WiFi publik
- device tidak boleh dipakai keluarga

3. Secure Remote Access
- VPN + MFA
- access time restriction
- IP allowlist (opsional)

4. Monitoring
- remote session behavior
- abnormal remote login

26.9 HR Incident Handling Procedure

Untuk insiden terkait SDM:

1. HR–Security–Legal Joint Protocol

Menangani:
- penyalahgunaan data
- insider sabotage
- fraud internal
- sexual/ethical misconduct
- pelanggaran SOP

2. Investigation

- forensik digital
- interview
- evidence preservation
- access log review

3. Action

- suspension
- access revoke
- termination
- laporan ke regulator (jika melibatkan data pribadi atau keuangan)
- pelaporan ke penegak hukum

26.10 Termination Process (Offboarding Security)

Saat pegawai keluar:

A. Immediate Access Revocation

- semua sistem internal
- email
- VPN
- production access
- cloud consoles

B. Return of Assets

- laptop
- token
- ID card
- mobile devices

C. Exit Interview

Untuk mendeteksi:

- potensi konflik
- motive risk
- unresolved issues

D. Deactivation Workflow

Didokumentasikan lengkap dan diaudit setiap bulan.

26.11 Workforce Cyber Readiness & Capability Framework

1. Cyber Workforce Segmentation

- General Staff (awareness)
- Sensitive Access Staff
- Technical Staff (DevOps, Engineering)
- Security Staff (Tier 1–Tier 3)

2. Competency Framework (NIST 800-181)

Role-targeted skills:
- secure coding
- cloud security
- incident response
- threat intelligence
- fraud analytics
- privacy engineering

3. Certification Recommendations

Untuk setiap level:

General Staff
- Cyber Hygiene
- PDP awareness

Technical Staff
- CEH
- CompTIA Security+
- Cloud Security (AWS/GCP/Azure)

Security Team
- CISSP
- CCSP
- OSCP
- GIAC (blue team, forensics)

26.12 Human Risk KPI & KRI

KPI
1. phishing click rate < 5%
2. 100% completion pelatihan wajib
3. zero unauthorized access
4. waktu pencabutan akses ≤ 15 menit
5. audit akses bulanan 100%

KRI

1. peningkatan kesalahan manusia
2. meningkatnya alert DLP
3. suspicious behavior patterns
4. akses admin di luar jam kerja
5. missed access revocation

26.13 Kepatuhan Regulasi & Audit SDM

Wajib mematuhi:

- SEOJK 29/2022
- UU PDP
- UU Ketenagakerjaan
- ISO 27001 Annex A.7
- sertifikasi tenaga profesional SP/Fintech (BI/OJK)

Audit SDM minimal 1x per tahun.

BAB 27
SECURE SOFTWARE DEVELOPMENT LIFECYCLE (SSDLC), DEVSECOPS & CI/CD SECURITY

SECURE SOFTWARE DEVELOPMENT LIFECYCLE (SSDLC), DEVSECOPS & CI/CD SECURITY, disusun SANGAT KOMPREHENSIF, OPERASIONAL, dan SIAP IMPLEMENTASI untuk seluruh Fintech anggota AFTECH.

Framework ini mengacu pada:

- OWASP SAMM (Software Assurance Maturity Model)
- OWASP ASVS (Application Security Verification Standard)
- OWASP MASVS (Mobile Security)
- NIST SP 800-218 (Secure Software Development Framework / SSDF)
- ISO/IEC 27034 (Application Security)
- BSIMM (Building Security in Maturity Model)
- Cloud Native Security Controls (Kubernetes, Terraform, IaC)
- DevSecOps Foundation Practices (DASA, SANS Institute)

Bab ini memastikan seluruh aplikasi Fintech—baik web, mobile, API, microservices, cloud-native—dibangun dengan standar keamanan kelas dunia.

Fintech modern hidup dalam ekosistem:

- mobile apps,
- API-driven architecture,
- microservices,
- Kubernetes & cloud,
- serverless functions,
- AI/ML pipelines.

Karenanya, keamanan harus tertanam dalam seluruh siklus pengembangan software, bukan hanya di akhir proses.

27.1 Tujuan SSDLC & DevSecOps Framework

1. Mengintegrasikan keamanan pada setiap tahap pengembangan.
2. Mengurangi risiko kerentanan kritis pada aplikasi Fintech.
3. Menjamin keamanan API, web, mobile, cloud, dan microservices.
4. Mengurangi biaya remediasi bug keamanan (lebih murah 80% bila diperbaiki di tahap awal).
5. Memastikan compliance terhadap OJK, BI, SEOJK 29/2022, UU PDP.
6. Meningkatkan ketahanan aplikasi terhadap serangan real-world.

27.2 Prinsip Utama SSDLC Fintech

1. Security by Design
2. Security by Default
3. Least Privilege
4. Zero Trust
5. Secure Coding Standard Mandatory
6. Automated Security Testing
7. Continuous Monitoring
8. Shift Left Security
9. Immutable Infrastructure
10. Secure Deployment

27.3 Tahapan SSDLC (End-to-End)

SSDLC terdiri dari 8 tahap utama:

1. Requirements (Security Requirement Engineering)

Security requirements harus ditentukan sejak awal:

A. Regulatory Requirements

- SEOJK 29/2022
- PBI 22/2024
- UU PDP

B. Technical Requirements

- authentication (MFA, OAuth2, OIDC)
- authorization (RBAC/ABAC)
- encryption (TLS 1.3, AES-256)
- logging & audit trail
- API security requirements
- mobile protection (OWASP MASVS)

C. Privacy Requirements

- data minimization
- consent flow
- privacy by design

D. Architectural Requirements

- API gateway mandatory
- no open database exposure
- secure cloud storage

2. Design (High-Level & Low-Level Security Architecture)

A. Threat Modeling (Wajib untuk Fintech)

Framework:

- STRIDE
- DREAD
- PASTA

Modeling dilakukan untuk:

- web apps
- mobile apps
- API
- cloud diagrams
- data flow

B. Security Architecture Patterns

Wajib untuk Fintech:

- microservices zero trust
- token-based API auth
- rate limiting
- cloud IAM separation
- secure session management

C. Secure Data Flow Design

Data sensitif harus:

- dienkripsi
- diberi token
- dibatasi aksesnya

D. Design Review Checklist

- anti-CSRF
- anti-XSS
- secure cookie
- API input validation
- SQL parameterization

3. Development (Secure Coding)

A. Coding Standard

Mengacu pada:

- OWASP ASVS

- SEI CERT Secure Coding
- MISRA (jika aplikasi embedded)

B. Secure Practices
- parameterized queries
- output encoding
- secure password hashing (Argon2/BCrypt)
- no hardcoded secrets
- no plaintext credentials

C. Secrets Management

Menggunakan:
- HashiCorp Vault
- AWS Secrets Manager
- GCP Secret Manager
- Azure Key Vault

D. Dependency Security
- SCA (Software Composition Analysis)
- vulnerability scanning pada library pihak ketiga
- banned libraries list

4. Code Review (Manual & Automated)

A. Manual Secure Code Review

Untuk komponen:
- authentication
- session
- encryption
- payment logic

B. Automated Tools
- SAST (Static Application Security Testing)
- linting
- SCA scanning

C. 4-Eye Principle

Semua code yang menyentuh:
- uang
- data pribadi
- payment routing

harus direview minimal 2 orang.

5. Build & CI (Continuous Integration Security)

CI pipeline wajib mengandung security gates:

A. Build Pipeline Controls

- security linting
- SAST scan
- dependency check
- secrets scanning
- IaC scanning (Terraform/Kubernetes)

B. CI Pipeline Security

- signed artifacts
- private registries
- build isolation

C. Build Environment Hardening

- no shared runners
- no plaintext logs

6. Testing (Security Testing)

A. Automated Testing

- SAST
- DAST
- API fuzzing
- mobile instrumentation testing
- dependency scanning

B. Manual Testing

- penetration testing
- business logic testing
- authorization break testing
- abuse-case testing

C. API Security Testing

Mengacu OWASP API Top 10:

- IDOR
- broken auth
- excessive data exposure
- mass assignment

D. Mobile App Testing

- jailbreak detection
- code obfuscation
- certificate pinning
- anti reverse engineering

E. Cloud Security Testing

- IAM review
- storage misconfig
- network firewall test

7. Deployment (Secure Release & Cloud Hardening)

A. Secure CI/CD Release

- signed releases
- controlled merge
- automated unit + sec test mandatory

B. Infrastructure Hardening

- Kubernetes security (network policies, PSP)
- zero trust network
- firewall policies

C. Environment Segregation

- dev
- staging
- UAT
- production (tidak boleh diakses developer)

D. Change Management

- CAB approval
- rollback plan
- post-release monitoring

8. Operations (Runtime Security)

A. Continuous Monitoring

- SIEM
- API anomaly
- fraud detection
- serverless monitoring

B. Vulnerability Management

- weekly scanning
- patching SLA
- container/registry scanning

C. Runtime Application Self-Protection (RASP)

Opsional: untuk Fintech besar.

D. Cloud Monitoring
- misconfiguration alerts
- IAM drift detection
- data exfiltration alerts

27.4 DevSecOps Framework

DevSecOps adalah penggabungan DevOps dan Security.

Fintech harus menerapkan:

A. Shift Left Security

Keamanan mulai dari:
- desain → coding → pipeline → produksi

B. Automated Security Controls

Security masuk dalam:
- commit
- merge
- build
- test
- deploy

C. Developer Security Training
- secure coding
- threat modeling
- OWASP ASVS training

D. Security as Code

Semua kontrol keamanan ditulis dalam:
- IaC (Terraform/K8s YAML)
- pipeline config
- secrets policy

E. Collaboration Charter

DevOps + Security wajib:

- code bersama
- incident response bersama
- continuous feedback

27.5 CI/CD Security Controls

A. Build Pipeline

- isolate build environment
- integrity checking
- package signing
- SBOM (Software Bill of Materials)

B. Deployment Pipeline

- canary deployment
- blue/green deployment
- automated rollback

C. Access Security

- no shared account
- MFA wajib
- no production access for dev

D. Supply Chain Security (SSDF)

- source verification
- pipeline signing
- image signing (Cosign)
- dependency provenance

27.6 Secure Cloud & Container Development

1. Container Security

- image vulnerability scanning
- minimal base image
- no root container
- seccomp & AppArmor

2. Kubernetes Security

- RBAC minimal
- namespace isolation
- network policy

- pod security standards

3. Serverless Security
- least privilege IAM
- environment variable encryption

27.7 Minimum Security Requirements per Aplikasi

Web Application
- OWASP ASVS Level 2
- HTTPS-only
- anti-CSRF
- secure cookies

Mobile Application
- OWASP MASVS Level 2
- device binding
- code obfuscation
- jailbreak detection

API
- OWASP API Top 10
- OAuth2/OIDC
- rate limiting
- schema validation

Cloud Apps
- zero trust
- IAM least privilege
- no public bucket/backdoor

27.8 Secure Coding Checklist (Ringkasan)
1. Tidak ada hardcoded credentials
2. SQL parameterization
3. XSS-safe output encoding
4. CSRF protection
5. JWT dengan short expiry
6. Tidak menyimpan data sensitif di local storage
7. Encrypt all PII
8. Input validation ketat

Checklist lengkap → Lampiran.

27.9 Bug Fixing & Patch SLAs

Severity	SLA Fix
Critical	< 72 jam
High	< 7 hari
Medium	< 30 hari
Low	< 90 hari

Tidak boleh ada kerentanan critical di produksi.

27.10 Metrics, KPI & KRI SSDLC

KPI

1. vulnerability reduction rate
2. SAST/DAST coverage
3. build pipeline security coverage
4. mean-time-to-remediate (MTTR) vulnerabilities
5. secure code training completion

KRI

1. increase in security bugs
2. repeated vulnerabilities
3. long-lived secrets
4. IaC misconfiguration spikes
5. high CVSS vulnerabilities unresolved

27.11 Kepatuhan & Audit

Harus memenuhi:

- SEOJK 29/2022
- PBI 22/2024
- UU PDP
- Developer access audit
- Logging on all development environments
- Audit trail pada CI/CD pipeline

Asosiasi Fintech Indonesia

Eco-S Coworking & Office Space Sahid Sudirman Residence,
Jl. Jenderal Sudirman No.86 2nd floor,
Karet Tengsin, Tanah Abang, Jakarta Pusat, DKI Jakarta 10220

www.fintech.id fintech.id fintechid Asosiasi Fintech Indonesia