

Indonesia Regulatory Hub

Country-specific obligations, regulatory sources and product workflow mappings.

IDN Regulatory Hub

Region: APAC

Practical governance across financial supervision, technology and privacy

Indonesia's financial-services regime combines OJK risk-management and governance requirements with technology controls and national personal-data protection. Firms need connected evidence for board accountability, internal controls, audit coverage, digital incidents and remediation.

IDN

APAC governance, risk and compliance intelligence

OJK

Financial Services Authority

Industries Regulated

Banking and lending, Regulated financial services

BI

Bank Indonesia

Industries Regulated

Banking and lending

BSSN

National Cyber and Crypto Agency

Industries Regulated

Government and critical infrastructure

Komdigi

Ministry of Communication and Digital Affairs

Industries Regulated

Cross-sector data controllers and processors

Supervisory Priorities

What Regulated Organisations Need to Operationalise.

The applicable perimeter depends on entity type, licence and sector. These priorities provide a practical starting point for programme design and evidence management.

01

Bank Risk Management

02

Corporate Governance

03

Technology and Cyber Resilience

04

Personal-Data Controls

Regulatory Alignment

Indonesia Regulation and Product Map

Each row translates an official regulatory source into an operational GRC focus, then identifies only the platforms with a defensible workflow or evidence role.

Research Review

Official-source and product-fit review completed 1 September 2026.

Primary Fit

The platform directly manages a central process or evidence set described in the requirement.

Supporting Fit

The platform contributes linked evidence, oversight or follow-up but is not the main system for the requirement.

Not Shown

A weak or unsubstantiated product relationship is intentionally omitted.

Indonesia Regulation And Product Map

OJK Risk Management Requirements for Commercial Banks OJK

Applies To: Commercial banks and banking groups within scope

Operational Focus: Risk governance, appetite and limits, control functions, monitoring, risk reporting and independent review.

Platform Fit and Workflow Support: Primary fit Risk-based assurance, control design and effectiveness testing, evidence, findings and action follow-up. Primary fit Risk and control registers, assessments, appetite or limits, KRIs, treatments, approvals and board reporting. Boundary Workflow and evidence support only. Applicability and legal interpretation remain with the organisation and its advisers.

Source: Source

<https://ojk.go.id/en/regulasi/otoritas-jasa-keuangan/peraturan-ojk/default.aspx>

OJK Governance Requirements for Commercial Banks OJK

Applies To: Commercial banks operating in Indonesia

Operational Focus: Board and committee governance, internal controls, compliance, internal audit, conflicts and corrective follow-up.

Platform Fit and Workflow Support: Primary fit Audit universe, risk-based planning, RCM-linked testing, working papers, evidence, findings and follow-up. Supporting fit Risk and control registers, assessments, appetite or limits, KRIs, treatments, approvals and board reporting. Boundary Workflow and evidence support only. Applicability and legal interpretation remain with the organisation and its advisers.

Source: Source

<https://ojk.go.id/en/regulasi/otoritas-jasa-keuangan/peraturan-ojk/default.aspx>

POJK 34/2025 on Information Technology Implementation OJK

Applies To: Rural banks and Sharia rural banks within the regulation's scope

Operational Focus: IT governance, digital security, incident response, third-party services, business continuity, control testing and assurance.

Platform Fit and Workflow Support: Primary fit Third-party risks, controls, assessments, treatments, approvals, KRIs and oversight reporting. Primary fit Risk-based assurance, control testing, evidence, findings, approvals and remediation follow-up. Primary fit Cyber-event intake, escalation, investigation, root cause, corrective action, recovery tracking and audit trail. Boundary Workflow and evidence support only. Applicability and legal interpretation remain with the organisation and its advisers.

Source: Source

<https://ojk.go.id/en/berita-dan-kegiatan/siaran-pers/Pages/OJK-Issues-Regulation-On-Information-Technology-Implementation-For-BPR-And-BPRS-Digital-Security.aspx>

POJK 3/2024 on Financial-Sector Technology Innovation OJK

Applies To: Financial-sector technology innovation providers within scope

Operational Focus: Risk management, governance, consumer data, incident handling, supervisory reporting and service-provider controls.

Platform Fit and Workflow Support: Primary fit Third-party risks, controls, assessments, treatments, approvals, KRIs and oversight reporting. Primary fit Cyber-event intake, escalation, investigation, root cause, corrective action, recovery tracking and audit trail. Boundary Notification workflow and evidence can be configured. Submission to an authority requires an approved process or integration.

Source: Source

<https://ojk.go.id/en/fungsi-utama/itsk/informasi-iakd/publikasi-dan-kajian/default.aspx>

Personal Data Protection Law No. 27 of 2022 Komdigi

Applies To: Personal-data controllers and processors within scope

Operational Focus: Data governance, impact assessment, security, breach notification, processor oversight and accountability records.

Platform Fit and Workflow Support: Primary fit Incident intake, assessment, investigation, notification workflow, corrective action, escalation and closure evidence. Supporting fit Privacy risks, controls, assessments, treatment actions, ownership, approvals and management reporting. Boundary Notification workflow and evidence can be configured. Submission to an authority requires an approved process or integration.

Source: Source

<https://peraturan.bpk.go.id/Details/229798/uu-no-27-tahun-2022>

This mapping is an implementation aid, not legal advice. It describes configurable workflow and evidence support, not automatic compliance. Always validate applicability, current versions, implementation dates and supervisory expectations with qualified advisers and the relevant authority.

Product Mapping Grounded in the 2026 Solution Briefs.

The mapping uses the capabilities documented in the current brochures. It does not extend the platforms beyond their stated functional scope.

Risk and Control Intelligence

Best suited to enterprise risk ownership, risk and control registers, assessments, appetite and tolerances, KRIs, treatments, approvals, dashboards and board reporting.

Central risk and control register

KRI threshold alerts

Treatment action tracking

AI-assisted drafting and classification

Independent Assurance

Best suited to the audit universe, risk-based planning, engagement execution, RCM-linked design and effectiveness testing, evidence, findings, approvals and follow-up.

Risk-based audit planning

ToD and ToE test procedures

Working papers and evidence

GIAS 2024 observation drafting

Incident Response and Closure

Best suited to incident intake, triage, investigation, root-cause analysis, escalation, notifications, corrective and preventive actions, closure and lessons learned.

Central incident register

Investigation and root cause

Escalation and notifications

Corrective-action tracking

Scope boundary

The platforms support governance workflows, accountability, evidence and reporting. They do not calculate regulatory capital or liquidity, replace technical cybersecurity monitoring, provide legal interpretation, issue external-audit opinions or automatically file statutory notifications unless an approved integration and process are configured.

Connected Operating Model

From Obligation to Board-Ready Evidence.

Use one traceable workflow to translate requirements, manage execution and demonstrate oversight.

01

Catalogue Obligations

Structure local requirements by entity, licence, authority and accountable owner.

02

Connect Operational Evidence

Link obligations to risks, controls, incidents, tests, findings and remediation.

03

Monitor and Assure

Track KRIs, control status, audit coverage, incidents and action closure continuously.

Risk intelligence

Independent assurance

Incident response

TransVare APAC | Indonesia

Build a Connected GRC Operating Model for Indonesia

See how TransVare can support local regulatory readiness while preserving regional visibility and board oversight.