POINT OF VIEW - SEPTEMBER 2026

Japan: From Regulatory Obligation to Board-Ready Evidence.

Resilient governance across financial supervision and data protection

Japan's financial-sector framework emphasises sound governance, customer protection, cybersecurity, IT resilience and independent assurance. Organisations need a practical evidence trail from risk identification and control design through incident escalation, recovery and board reporting.

REGION	REGULATORY HUB	
APAC	JPN	 Japan

Country in Brief

4	**5**	**4**	**3**
Regulatory authorities profiled	Official regulatory sources mapped	Supervisory priorities operationalised	Connected TransVare platforms

01 Japan Regulatory Landscape

Japan's financial-sector framework emphasises sound governance, customer protection, cybersecurity, IT resilience and independent assurance. Organisations need a practical evidence trail from risk identification and control design through incident escalation, recovery and board reporting.

JFSA

Japan Financial Services Agency

Industries Regulated

Banking and lending, Insurance, Regulated financial services

JPX

Japan Exchange Group

Industries Regulated

Capital markets and listed companies

PPC

Personal Information Protection Commission

Industries Regulated

Cross-sector data controllers and processors

NISC

National center of Incident readiness and Strategy for Cybersecurity

Industries Regulated

Capital markets and listed companies, Government and critical infrastructure

02 Supervisory Priorities

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

01	**Financial risk governance**
02	**Cybersecurity and IT resilience**
03	**Independent audit evidence**
04	**Personal-data incident response**

03 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.

04

Report to Leadership

Turn current operational evidence into traceable executive and board oversight.

04 Japan Regulation and Product Map

Each official requirement below is translated into an operational GRC focus. Only platforms with a defensible workflow or evidence role are shown as a primary or supporting fit.

Supervisory Guidelines and Financial Inspection Framework

JFSA

Applies To	Banks, insurers and financial businesses within the applicable supervisory perimeter
Operational Focus	Governance, enterprise risk management, internal controls, internal audit, outsourcing, incident reporting and supervisory remediation.
ERMVare® **Primary Fit**	Third-party risks, controls, assessments, treatments, approvals, KRIs and oversight reporting.
AuditVare® **Primary Fit**	Audit universe, risk-based planning, RCM-linked testing, working papers, evidence, findings and follow-up.
InciVare® **Primary Fit**	Incident reporting, triage, investigation, root cause, corrective action, escalation and closure.
Scope Boundary	Workflow and evidence support only. Applicability and legal interpretation remain with the organisation and its advisers.
Official Source	**Open Official Source**

Guidelines on Cybersecurity for the Financial Sector

JFSA

Applies To	Financial institutions and other entities within the guideline's scope
Operational Focus	Cyber governance, risk assessment, third-party oversight, monitoring, incident escalation, recovery and assurance.
ERMVare® **Primary Fit**	Third-party risks, controls, assessments, treatments, approvals, KRIs and oversight reporting.
InciVare® **Primary Fit**	Cyber-event intake, escalation, investigation, root cause, corrective action, recovery tracking and audit trail.
Scope Boundary	GRC workflow and evidence support only. The platforms do not replace technical security monitoring, detection or protection tools.
Official Source	**Open Official Source**

IT Resilience Discussion Report
JFSA

Applies To	Financial institutions managing important technology services
Operational Focus	Resilience of critical services, dependency mapping, testing, incident learning, recovery and senior-management oversight.
InciVare® **Primary Fit**	Disruption reporting, escalation, investigation, corrective action, recovery tracking and closure evidence.
ERMVare® **Supporting Fit**	Operational-risk registers, critical-service assessments, controls, KRIs, treatments and leadership reporting.
Scope Boundary	Workflow and evidence support only. Applicability and legal interpretation remain with the organisation and its advisers.
Official Source	**Open Official Source**

Corporate Governance Code
JPX

Applies To	Companies listed on the Tokyo Stock Exchange
Operational Focus	Board effectiveness, risk oversight, audit and supervisory functions, internal controls and transparent accountability.
ERMVare® **Primary Fit**	Risk and control registers, assessments, appetite or limits, KRIs, treatments, approvals and board reporting.
AuditVare® **Supporting Fit**	Risk-based assurance, control design and effectiveness testing, evidence, findings and action follow-up.
Scope Boundary	Workflow and evidence support only. Applicability and legal interpretation remain with the organisation and its advisers.
Official Source	**Open Official Source**

Act on the Protection of Personal Information

PPC

Applies To	Business operators handling personal information within scope
Operational Focus	Data governance, security measures, processor oversight, breach assessment, notifications and response records.
InciVare® **Primary Fit**	Incident intake, assessment, investigation, notification workflow, corrective action, escalation and closure evidence.
ERMVare® **Supporting Fit**	Risk and control registers, assessments, appetite or limits, KRIs, treatments, approvals and board reporting.
Scope Boundary	Notification workflow and evidence can be configured. Submission to an authority requires an approved process or integration.
Official Source	**Open Official Source**

Research Review	Primary Fit	Supporting Fit	Not Shown
Official-source and product-fit review completed 1 September 2026.	Directly manages a central process or evidence set.	Contributes linked evidence, oversight or follow-up.	Weak or unsubstantiated relationships are omitted.

05 Brochure-Validated Product Capability

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

ERMVare®

Risk and Control Intelligence

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

AuditVare®

Independent Assurance

Audit universe, risk-based planning, engagement execution, RCM-linked control testing, evidence, findings, approvals and follow-up.

Risk-based audit planning | ToD and ToE procedures | Working papers and evidence | GIAS 2024 observation drafting

InciVare®

Incident Response and Closure

Incident intake, triage, investigation, root-cause analysis, escalation, notifications, corrective action, 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.

06 Sources, Scope and Next Step

Official sources used in this report are linked directly from each regulation summary. The mapping is an implementation aid and not legal advice.

01	**Supervisory Guidelines and Financial Inspection Framework** JFSA	**Official Source**
02	**Guidelines on Cybersecurity for the Financial Sector** JFSA	**Official Source**
03	**IT Resilience Discussion Report** JFSA	**Official Source**
04	**Corporate Governance Code** JPX	**Official Source**
05	**Act on the Protection of Personal Information** PPC	**Official Source**

THE NEXT STEP

Build a Connected GRC Operating Model for Japan.

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

TransVare US: Delaware
8 The Green, Street R
Dover, Kent 19901, State of Delaware
United States of America

For Local Alliance Partner and Sales Contact:
Connect@TransVare.com
TransVare.com