POINT OF VIEW - SEPTEMBER 2026

Poland: From Regulatory Obligation to Board-Ready Evidence.

Financial governance, ICT resilience and accountable incident management

Poland combines PFSA governance and technology expectations, European digital operational resilience, national cybersecurity duties and GDPR supervision. Regulated organisations need coordinated risk, controls, internal audit, incident reporting and senior-management oversight.

REGION
Europe

REGULATORY HUB
POL

Poland

Country in Brief

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

01 Poland Regulatory Landscape

Poland combines PFSA governance and technology expectations, European digital operational resilience, national cybersecurity duties and GDPR supervision. Regulated organisations need coordinated risk, controls, internal audit, incident reporting and senior-management oversight.

KNF

Polish Financial Supervision Authority

Industries Regulated

Banking and lending, Regulated financial services

NBP

National Bank of Poland

Industries Regulated

Banking and lending

UODO

Personal Data Protection Office

Industries Regulated

Cross-sector data controllers and processors

CSIRT NASK

Computer Security Incident Response Team operated by NASK

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 Supervised-entity corporate governance	02 Operational and ICT risk
03 Digital operational resilience	04 Cyber incident reporting
05 Personal-data breach notification	

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 Poland 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.

Principles of Corporate Governance for Supervised Institutions

KNF

Applies To	Financial institutions supervised by KNF within the principles' scope
Operational Focus	Management and supervisory-board responsibilities, risk governance, internal controls, compliance, internal audit and transparent reporting.
ERMVare® **Primary Fit**	Risk and control registers, assessments, appetite or limits, KRIs, treatments, approvals and board reporting.
AuditVare® **Primary Fit**	Audit universe, risk-based planning, RCM-linked testing, working papers, evidence, findings and 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**

Recommendation D on Information Technology and ICT Environment Security

KNF

Applies To	Banks operating within the recommendation's scope
Operational Focus	ICT strategy, security governance, risk assessment, outsourcing, continuity, incident response, monitoring and independent assurance.
ERMVare® **Primary Fit**	Third-party risks, controls, assessments, treatments, approvals, KRIs and oversight reporting.
AuditVare® **Primary Fit**	Risk-based assurance, control testing, evidence, findings, approvals and remediation follow-up.
InciVare® **Primary Fit**	Cyber-event intake, escalation, investigation, root cause, corrective action, recovery tracking and audit trail.
Scope Boundary	Workflow and evidence support only. Applicability and legal interpretation remain with the organisation and its advisers.
Official Source	**Open Official Source**

Digital Operational Resilience Act

European Union and KNF

Applies To	Financial entities and ICT third-party providers within DORA's scope
Operational Focus	ICT risk governance, major incident reporting, resilience testing, third-party registers, recovery and management-body accountability.
ERMVare® **Primary Fit**	Third-party risks, controls, assessments, treatments, approvals, KRIs and oversight reporting.
InciVare® **Primary Fit**	Disruption reporting, escalation, investigation, corrective action, recovery tracking and closure evidence.
Scope Boundary	Workflow and evidence support only. Applicability and legal interpretation remain with the organisation and its advisers.
Official Source	**Open Official Source**

National Cybersecurity System Act, 2026 Amendment

Ministry of Digital Affairs and national CSIRTs

Applies To	Essential and important entities within the amended national regime
Operational Focus	Information-security management, incident reporting to CSIRTs, accountable contacts, cybersecurity audits and documented remediation.
InciVare® **Primary Fit**	Cyber-event intake, escalation, investigation, root cause, corrective action, recovery tracking and audit trail.
ERMVare® **Supporting Fit**	Risk and control registers, assessments, appetite or limits, KRIs, treatments, approvals and board reporting.
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**

GDPR Personal Data Breach Notification

UODO

Applies To	Controllers and processors handling personal data within the GDPR's scope
Operational Focus	Breach logging, risk assessment, notification without undue delay, affected-person communication, root-cause analysis and corrective action.
InciVare® **Primary Fit**	Incident intake, assessment, investigation, notification workflow, corrective action, escalation and closure evidence.
ERMVare® **Primary Fit**	Privacy risks, controls, assessments, treatment actions, ownership, approvals and management 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	**Principles of Corporate Governance for Supervised Institutions** KNF	**Official Source**
02	**Recommendation D on Information Technology and ICT Environment Security** KNF	**Official Source**
03	**Digital Operational Resilience Act** European Union and KNF	**Official Source**
04	**National Cybersecurity System Act, 2026 Amendment** Ministry of Digital Affairs and national CSIRTs	**Official Source**
05	**GDPR Personal Data Breach Notification** UODO	**Official Source**

THE NEXT STEP

Build a Connected GRC Operating Model for Poland.

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