

Poland Regulatory Hub

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

POL Regulatory Hub

Region: Europe

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.

POL

Europe governance, risk and compliance intelligence

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

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

Supervised-Entity Corporate Governance

02

Operational and ICT Risk

03

Digital Operational Resilience

04

Cyber Incident Reporting

05

Personal-Data Breach Notification

Regulatory Alignment

Poland 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.

Poland Regulation And Product Map

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.

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

Source: Source

https://www.knf.gov.pl/en/MARKET/Regulations_and_practice/Practice

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.

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://www.knf.gov.pl/en/MARKET/Regulations_and_practice/Practice/banking_sector/Recommendations_of_the_PFSa?articleId=44256&p_id=19

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.

Platform Fit and Workflow Support: Primary fit Third-party risks, controls, assessments, treatments, approvals, KRIs and oversight reporting. Primary fit Disruption reporting, escalation, investigation, corrective action, recovery tracking and closure evidence. Boundary Workflow and evidence support only. Applicability and legal interpretation remain with the organisation and its advisers.

Source: Source

<https://eur-lex.europa.eu/eli/reg/2022/2554/oj/eng>

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.

Platform Fit and Workflow Support: Primary fit Cyber-event intake, escalation, investigation, root cause, corrective action, recovery tracking and audit trail. Supporting fit Risk and control registers, assessments, appetite or limits, KRIs, treatments, approvals and board reporting. Boundary GRC workflow and evidence support only. The platforms do not replace technical security monitoring, detection or protection tools.

Source: Source

<https://www.gov.pl/web/cyfryzacja/nowelizacja-ustawy-o-krajowym-systemie-cyberbezpieczenstwa-ksc---obowiazki-podmiotow-kluczowych-i-waznych>

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.

Platform Fit and Workflow Support: Primary fit Incident intake, assessment, investigation, notification workflow, corrective action, escalation and closure evidence. Primary 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://uodo.gov.pl/en/672/1410>

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 Europe | Poland

Build a Connected GRC Operating Model for Poland

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