

Netherlands Regulatory Hub

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

NLD Regulatory Hub

Region: Europe

Sound governance, information security and digital operational resilience

The Netherlands combines DNB prudential supervision, AFM conduct and governance oversight, European digital resilience and Dutch data-protection enforcement. Firms need clear governance, secure operations, controlled outsourcing, incident evidence and independent assurance.

NLD

Europe governance, risk and compliance intelligence

DNB

De Nederlandsche Bank

Industries Regulated

Banking and lending, Payments and fintech

AFM

Netherlands Authority for the Financial Markets

Industries Regulated

Banking and lending

AP

Dutch Data Protection Authority

Industries Regulated

Cross-sector data controllers and processors

NCSC-NL

National Cyber Security Centre Netherlands

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

Sound and Controlled Operations

02

Governance and Risk Oversight

03

Information Security

04

Outsourcing and Third-Party Resilience

05

Incident and Data-Breach Response

Regulatory Alignment

Netherlands 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.

Netherlands Regulation And Product Map

Financial Supervision Act Dutch Government, DNB and AFM

Applies To: Financial undertakings within the Act's applicable prudential and conduct provisions

Operational Focus: Sound governance, controlled business operations, risk management, internal controls, auditability and supervisory reporting.

Platform Fit and Workflow Support: Primary fit Risk and control registers, assessments, appetite or limits, KRIs, treatments, approvals and board reporting. Supporting fit Risk-based assurance, control design and effectiveness testing, evidence, findings and action follow-up. Boundary Notification workflow and evidence can be configured. Submission to an authority requires an approved process or integration.

Source: Source

<https://www.dnb.nl/en/sector-information/open-book-supervision/laws-and-eu-regulations/financial-supervision-act/>

Governance Requirements for Banks DNB

Applies To: Banks operating within DNB's supervisory perimeter

Operational Focus: Management-body effectiveness, risk culture, internal governance, control functions, internal audit and accountable decision-making.

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.dnb.nl/en/sector-information/open-book-supervision/open-book-supervision-sectors/banks/prudential-supervision/governance-banks/>

Digital Operational Resilience Act European Union and DNB

Applies To: Financial entities and ICT third-party providers within DORA's scope

Operational Focus: ICT risk, incident reporting, resilience testing, third-party registers, recovery, lessons learned and board oversight.

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://www.dnb.nl/en/sector-information/open-book-supervision/laws-and-eu-regulations/dora/>

Outsourcing Requirements DNB

Applies To: Banks, payment institutions and electronic-money institutions within scope

Operational Focus: Materiality, due diligence, contracting, monitoring, concentration risk, continuity, exit plans and audit access.

Platform Fit and Workflow Support: Primary fit Third-party risks, controls, assessments, treatments, approvals, KRIs and oversight reporting. Supporting fit Risk-based assurance, control design and effectiveness testing, evidence, findings and action follow-up. Boundary Workflow and evidence support only. Applicability and legal interpretation remain with the organisation and its advisers.

Source: Source

<https://www.dnb.nl/en/sector-information/open-book-supervision/open-book-supervision-themes/sector-information-supervision-stages-regular-supervision-prudential-supervision-governance-governance/outourcing-by-banks-payment-institutions-and-electronic-money-institutions/>

GDPR Data Breach Notification AP

Applies To: Controllers and processors handling personal data within the GDPR's scope

Operational Focus: Breach registers, risk assessment, regulatory notification, 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 Risk and control registers, assessments, appetite or limits, KRIs, treatments, approvals and board reporting. Boundary Notification workflow and evidence can be configured. Submission to an authority requires an approved process or integration.

Source: Source

<https://www.autoriteitpersoonsgegevens.nl/en/themes/security/data-breaches/this-is-how-you-report-a-data-breach>

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 | Netherlands

Build a Connected GRC Operating Model for the Netherlands

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