

Germany Regulatory Hub

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

DEU Regulatory Hub

Region: Europe

Integrated risk governance and digital resilience for German enterprises

Germany combines BaFin prudential risk-management expectations, listed-company governance, European digital operational resilience and data-protection duties, and national cybersecurity requirements. Institutions need traceable risk decisions, independent assurance, incident escalation and board-level accountability.

DEU

Europe governance, risk and compliance intelligence

BaFin

Federal Financial Supervisory Authority

Industries Regulated

Banking, insurance, payments, capital markets and regulated financial services

Bundesbank

Deutsche Bundesbank

Industries Regulated

Banking and lending

BSI

Federal Office for Information Security

Industries Regulated

Capital markets and listed companies, Government and critical infrastructure, Public and private organisations

BfDI

Federal Commissioner for Data Protection and Freedom of Information

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

Risk Appetite and Internal Controls

02

Independent Internal Audit

03

Digital Operational Resilience

04

ICT Third-Party Governance

05

Cyber and Privacy Incident Reporting

Regulatory Alignment

Germany 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.

Germany Regulation And Product Map

Minimum Requirements for Risk Management, MaRisk, Circular 06/2024 BaFin

Applies To: Credit and financial-services institutions within the circular's scope

Operational Focus: Risk strategy, appetite, internal controls, risk controlling, compliance, internal audit, outsourcing, continuity and board reporting.

Platform Fit and Workflow Support: Primary fit Third-party risks, controls, assessments, treatments, approvals, KRIs and oversight 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.bafin.de/SharedDocs/Veroeffentlichungen/DE/Rundschreiben/2024/rs_06_2024_MaRisk_BA.html

German Corporate Governance Code Government Commission on the German Corporate Governance Code

Applies To: German listed companies on an apply-and-explain basis

Operational Focus: Management and supervisory-board oversight, internal controls, risk management, audit committee responsibilities 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.dcgk.de/en/code.html>

Digital Operational Resilience Act European Union and BaFin

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

Operational Focus: ICT risk governance, incident classification and reporting, resilience testing, third-party risk, recovery and management-body 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://eur-lex.europa.eu/eli/reg/2022/2554/oj/eng>

BSI Act and Critical-Infrastructure Incident Reporting BSI

Applies To: Critical-infrastructure operators and other regulated organisations within national cybersecurity law

Operational Focus: State-of-the-art security, significant-incident notification, response coordination, evidence retention and resilience improvement.

Platform Fit and Workflow Support: Primary fit Disruption reporting, escalation, investigation, corrective action, recovery tracking and closure evidence. 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.bsi.bund.de/EN/Das-BSI/Auftrag/Gesetze-und-Verordnungen/NIS-Richtlinie/nis-richtlinie_node.html

General Data Protection Regulation BfDI and German state data-protection authorities

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

Operational Focus: Accountability, security controls, processor oversight, breach assessment, 72-hour notification where required and corrective action.

Platform Fit and Workflow Support: Primary fit Incident intake, assessment, investigation, notification workflow, corrective action, escalation and closure evidence. 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://eur-lex.europa.eu/eli/reg/2016/679/oj/eng>

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 | Germany

Build a Connected GRC Operating Model for Germany

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