POINT OF VIEW - SEPTEMBER 2026

Germany: From Regulatory Obligation to Board-Ready Evidence.

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.

REGION
Europe

REGULATORY HUB
DEU

Germany

Country in Brief

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

01 Germany Regulatory Landscape

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.

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

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	Risk appetite and internal controls
02	Independent internal audit
03	Digital operational resilience
04	ICT third-party governance
05	Cyber and privacy incident reporting

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 Germany 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.

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.
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.
Scope Boundary	Workflow and evidence support only. Applicability and legal interpretation remain with the organisation and its advisers.
Official Source	**Open Official Source**

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.
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**

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.
ERMCare® **Primary Fit**	Third-party risks, controls, assessments, treatments, approvals, KRIs and oversight reporting.
InciCare® **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**

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.
InciCare® **Primary Fit**	Disruption reporting, escalation, investigation, corrective action, recovery tracking and closure evidence.
AuditCare® **Supporting Fit**	Risk-based assurance, control design and effectiveness testing, evidence, findings and action follow-up.
Scope Boundary	Notification workflow and evidence can be configured. Submission to an authority requires an approved process or integration.
Official Source	**Open Official Source**

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.
InciCare® **Primary Fit**	Incident intake, assessment, investigation, notification workflow, corrective action, escalation and closure evidence.
AuditCare® **Supporting Fit**	Risk-based assurance, control design and effectiveness testing, evidence, findings and action follow-up.
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	**Minimum Requirements for Risk Management, MaRisk, Circular 06/2024** BaFin	**Official Source**
02	**German Corporate Governance Code** Government Commission on the German Corporate Governance Code	**Official Source**
03	**Digital Operational Resilience Act** European Union and BaFin	**Official Source**
04	**BSI Act and Critical-Infrastructure Incident Reporting** BSI	**Official Source**
05	**General Data Protection Regulation** BfDI and German state data-protection authorities	**Official Source**

THE NEXT STEP

Build a Connected GRC Operating Model for Germany.

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