

Switzerland Regulatory Hub

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

CHE Regulatory Hub

Region: Europe

Operational resilience, cyber reporting and accountable financial governance

Switzerland combines FINMA operational-risk and governance expectations, exchange disclosure rules, national cyber-incident reporting and a modern federal data-protection regime. Institutions need traceable risks, controls, incidents, assurance and management-body reporting.

CHE

Europe governance, risk and compliance intelligence

FINMA

Swiss Financial Market Supervisory Authority

Industries Regulated

Banking and lending, Insurance

SER

SIX Exchange Regulation

Industries Regulated

Capital markets and listed companies

NCSC

National Cyber Security Centre

Industries Regulated

Capital markets and listed companies, Government and critical infrastructure

FDPIC

Federal Data Protection and Information Commissioner

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

Operational-Risk Governance

02

Critical-Function Resilience

03

Independent Internal Audit

04

Cyber Incident Notification

05

Data-Security Breach Response

Regulatory Alignment

Switzerland 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.

Switzerland Regulation And Product Map

FINMA Circular 2023/1 Operational Risks and Resilience FINMA

Applies To: Banks and other supervised institutions within the circular's scope

Operational Focus: Operational-risk management, critical functions, resilience tolerances, business continuity, incident management, outsourcing and reporting.

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.finma.ch/en/documentation/circulars/>

FINMA Corporate Governance Circulars FINMA

Applies To: Banks and insurers within the relevant circulars' scope

Operational Focus: Board responsibilities, risk appetite, internal controls, compliance, internal audit independence and governance 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.finma.ch/en/documentation/circulars/>

Directive on Information Relating to Corporate Governance SER

Applies To: Issuers subject to SIX listing rules

Operational Focus: Transparent governance disclosure, board and committee structures, control mechanisms, audit information and accountability.

Platform Fit and Workflow Support: Supporting 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.ser-ag.com/en/resources/laws-regulations-determinations/corporate-governance.html>

Mandatory Cyber-Incident Notification for Critical Infrastructure NCSC

Applies To: Critical-infrastructure operators within the national notification regime

Operational Focus: Critical-incident assessment, timely reporting, response coordination, service recovery and documented follow-up.

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.report.ncsc.admin.ch/en/>

Federal Act on Data Protection, Article 24 Breach Notification FDPIC

Applies To: Controllers handling personal data within the FADP's scope

Operational Focus: High-risk breach assessment, regulatory notification, data-subject communication, response documentation 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://www.edoeb.admin.ch/en/guidelines-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 | Switzerland

Build a Connected GRC Operating Model for Switzerland

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