POINT OF VIEW - SEPTEMBER 2026

# Switzerland: From Regulatory Obligation to Board-Ready Evidence.

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.

**REGION**
Europe

**REGULATORY HUB**
CHE

Switzerland

**Country in Brief**

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

# 01 Switzerland Regulatory Landscape

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.

### 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

## 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 | Operational-risk governance |
| 02 | Critical-function resilience |
| 03 | Independent internal audit |
| 04 | Cyber incident notification |
| 05 | Data-security breach response |

## 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 Switzerland 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.

## 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. |
| ERMVare® **Primary Fit** | Third-party risks, controls, assessments, treatments, approvals, KRIs and oversight reporting. |
| InciVare® **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** |

## 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. |
| 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** |

## 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. |
| ERMVare® **Supporting Fit** | Risk and control registers, assessments, appetite or limits, KRIs, treatments, approvals and board reporting. |
| AuditVare® **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** |

## 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. |
| InciVare® **Primary Fit** | Cyber-event intake, escalation, investigation, root cause, corrective action, recovery tracking and audit trail. |
| ERMVare® **Supporting Fit** | Risk and control registers, assessments, appetite or limits, KRIs, treatments, approvals and board reporting. |
| **Scope Boundary** | GRC workflow and evidence support only. The platforms do not replace technical security monitoring, detection or protection tools. |
| **Official Source** | **Open Official Source** |

## 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. |
| InciVare® **Primary Fit** | Incident intake, assessment, investigation, notification workflow, corrective action, escalation and closure evidence. |
| ERMVare® **Primary Fit** | Privacy risks, controls, assessments, treatment actions, ownership, approvals and management reporting. |
| **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 | **FINMA Circular 2023/1 Operational Risks and Resilience**<br>FINMA | **Official Source** |
| 02 | **FINMA Corporate Governance Circulars**<br>FINMA | **Official Source** |
| 03 | **Directive on Information Relating to Corporate Governance**<br>SER | **Official Source** |
| 04 | **Mandatory Cyber-Incident Notification for Critical Infrastructure**<br>NCSC | **Official Source** |
| 05 | **Federal Act on Data Protection, Article 24 Breach Notification**<br>FDPIC | **Official Source** |

TransVare provides configurable technology to support governance, risk, audit and incident-management processes. Platform use does not, by itself, constitute or guarantee regulatory compliance. Applicability depends on entity type, licence, sector and current legal requirements. Obtain professional advice before relying on any regulatory mapping.

THE NEXT STEP

## Build a Connected GRC Operating Model for Switzerland.

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