POINT OF VIEW - SEPTEMBER 2026

Italy: From Regulatory Obligation to Board-Ready Evidence.

Prudential governance, ICT resilience and accountable incident response

Italy's framework combines Bank of Italy prudential requirements, CONSOB market supervision, listed-company governance, European digital resilience and national privacy and cybersecurity oversight. Institutions need connected controls, assurance, incident management and board reporting.

REGION	REGULATORY HUB	
Europe	ITA	 Italy

Country in Brief

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

01 Italy Regulatory Landscape

Italy's framework combines Bank of Italy prudential requirements, CONSOB market supervision, listed-company governance, European digital resilience and national privacy and cybersecurity oversight. Institutions need connected controls, assurance, incident management and board reporting.

BdI

Bank of Italy

Industries Regulated

Banking and lending, Payments and fintech

CONSOB

National Commission for Companies and the Stock Exchange

Industries Regulated

Capital markets and listed companies

ACN

National Cybersecurity Agency

Industries Regulated

Capital markets and listed companies, Government and critical infrastructure

Garante

Italian Data Protection Authority

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	**Bank governance and internal controls**
02	**ICT risk and continuity**
03	**Independent assurance**
04	**Third-party resilience**
05	**Cyber and privacy incident 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 Italy 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.

Supervisory Provisions for Banks, Circular 285

BdI

Applies To	Banks and banking groups within the circular's scope
Operational Focus	Corporate governance, risk appetite, internal controls, risk management, internal audit, information systems, continuity and supervisory reporting.
ERMCare® **Primary Fit**	Operational-risk registers, critical-service assessments, controls, KRIs, treatments and leadership reporting.
AuditCare® **Primary Fit**	Audit universe, risk-based planning, RCM-linked testing, working papers, evidence, findings and 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**

Cybersecurity and Operational-Resilience Regulatory Framework

BdI

Applies To	Banks, payment institutions and other supervised entities within applicable provisions
Operational Focus	ICT governance, continuity, cyber incidents, regulatory reporting, resilience testing, outsourcing and audit evidence.
InciCare® **Primary Fit**	Cyber-event intake, escalation, investigation, root cause, corrective action, recovery tracking and audit trail.
ERMCare® **Primary Fit**	Third-party risks, controls, assessments, treatments, approvals, KRIs and oversight reporting.
AuditCare® **Primary Fit**	Risk-based assurance, control testing, evidence, findings, approvals and remediation follow-up.
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**

Digital Operational Resilience Act

European Union, BdI and CONSOB

Applies To	Financial entities and ICT third-party providers within DORA's scope
Operational Focus	ICT risk governance, incident reporting, testing, third-party risk, recovery and management-body accountability.
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**

Italian Corporate Governance Code

Corporate Governance Committee and Borsa Italiana

Applies To	Italian listed companies adopting the Code
Operational Focus	Board oversight, internal-control and risk-management systems, audit committee functions, internal audit and governance disclosure.
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	Notification workflow and evidence can be configured. Submission to an authority requires an approved process or integration.
Official Source	**Open Official Source**

GDPR and Personal Data Protection Code

Garante

Applies To	Controllers and processors handling personal data within the Italian regime
Operational Focus	Data governance, security, processor oversight, breach assessment, regulatory notification, response and corrective action.
InciVare® **Primary Fit**	Incident intake, assessment, investigation, notification workflow, corrective action, escalation and closure evidence.
ERMVare® **Supporting 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	**Supervisory Provisions for Banks, Circular 285** BdI	**Official Source**
02	**Cybersecurity and Operational-Resilience Regulatory Framework** BdI	**Official Source**
03	**Digital Operational Resilience Act** European Union, BdI and CONSOB	**Official Source**
04	**Italian Corporate Governance Code** Corporate Governance Committee and Borsa Italiana	**Official Source**
05	**GDPR and Personal Data Protection Code** Garante	**Official Source**

THE NEXT STEP

Build a Connected GRC Operating Model for Italy.

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