POINT OF VIEW - SEPTEMBER 2026

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

Connected prudential controls, digital resilience and breach governance

Spain combines Banco de España prudential supervision, CNMV governance expectations, European digital resilience and AEPD privacy enforcement. Institutions need aligned risk appetite, control testing, internal audit, incident escalation and board reporting.

**REGION**
Europe

**REGULATORY HUB**
ESP

Spain

**Country in Brief**

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

# 01 Spain Regulatory Landscape

Spain combines Banco de España prudential supervision, CNMV governance expectations, European digital resilience and AEPD privacy enforcement. Institutions need aligned risk appetite, control testing, internal audit, incident escalation and board reporting.

### BdE

Banco de España

**Industries Regulated**

Banking and lending

### CNMV

National Securities Market Commission

**Industries Regulated**

Capital markets and listed companies

### AEPD

Spanish Data Protection Agency

**Industries Regulated**

Cross-sector data controllers and processors

### INCIBE

National Cybersecurity Institute of Spain

**Industries Regulated**

Capital markets and listed companies, Government and critical infrastructure

## 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 **Prudential governance and controls**
- 02 **Corporate-governance oversight**
- 03 **ICT operational resilience**
- 04 **Third-party risk**
- 05 **Incident and breach notification**

## 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 Spain 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.

## Law 10/2014 and Royal Decree 84/2015 on Credit Institutions

**Spanish Government and BdE**

| | |
|---|---|
| **Applies To** | Credit institutions operating within the Spanish prudential regime |
| **Operational Focus** | Governance, risk management, internal controls, remuneration, supervisory reporting, recovery and accountable management. |
| ERMCare **Primary Fit** | Risk and control registers, assessments, appetite or limits, KRIs, treatments, approvals and board reporting. |
| 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** |

## Circular 2/2016 on Supervision and Solvency

**BdE**

| | |
|---|---|
| **Applies To** | Credit institutions within the circular's scope |
| **Operational Focus** | Risk governance, capital and liquidity controls, internal processes, reporting, supervisory review and remediation evidence. |
| ERMCare **Primary Fit** | Risk and control registers, assessments, appetite or limits, KRIs, treatments, approvals and board reporting. |
| AuditCare **Supporting Fit** | Risk-based assurance, control design and effectiveness testing, evidence, findings and action follow-up. |
| **Scope Boundary** | Workflow, control and evidence support only. The platforms do not calculate regulatory capital, liquidity or prudential ratios. |
| **Official Source** | **Open Official Source** |

## Good Governance Code of Listed Companies

**CNMV**

| | |
|---|---|
| **Applies To** | Spanish listed companies on a comply-or-explain basis |
| **Operational Focus** | Board risk oversight, control functions, audit committees, internal audit, reporting and governance accountability. |
| 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 Spanish financial supervisors**

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

## GDPR Personal Data Breach Notification

**AEPD**

| | |
|---|---|
| **Applies To** | Controllers and processors handling personal data within the GDPR's scope |
| **Operational Focus** | Incident documentation, risk assessment, 72-hour notification where required, affected-person communication and corrective actions. |
| IncidentCare® **Primary Fit** | Incident intake, assessment, investigation, notification workflow, corrective action, escalation and closure evidence. |
| ERMCare® **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 | **Law 10/2014 and Royal Decree 84/2015 on Credit Institutions**<br>Spanish Government and BdE | **Official Source** |
| 02 | **Circular 2/2016 on Supervision and Solvency**<br>BdE | **Official Source** |
| 03 | **Good Governance Code of Listed Companies**<br>CNMV | **Official Source** |
| 04 | **Digital Operational Resilience Act**<br>European Union and Spanish financial supervisors | **Official Source** |
| 05 | **GDPR Personal Data Breach Notification**<br>AEPD | **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 Spain.

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