

# Russia Regulatory Hub

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

RUS Regulatory Hub

Region: Europe

## Integrated bank controls, operational-risk governance and incident accountability

Russia's framework combines Bank of Russia governance, internal-control and operational-risk requirements with public-company guidance and personal-data incident reporting. Regulated organisations need clear responsibility, complete event records, independent assurance and tracked remediation.

### RUS

Europe governance, risk and compliance intelligence

### CBR

Central Bank of the Russian Federation, Bank of Russia

Industries Regulated

Banking and lending, Capital markets and listed companies

### Roskomnadzor

Federal Service for Supervision of Communications, Information Technology and Mass Media

Industries Regulated

Telecommunications and digital services

### FSTEC

Federal Service for Technical and Export Control

Industries Regulated

Government, critical infrastructure and regulated information-security activities

### NCCCI

National Coordination Center for Computer Incidents

Industries Regulated

Government, critical infrastructure and cyber-incident response participants

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**

### **Bank Risk and Internal-Control Systems**

**02**

### **Operational-Risk Event Management**

**03**

### **Independent Internal Audit**

**04**

### **Public-Company Governance**

**05**

### **Personal-Data Incident Reporting**

Regulatory Alignment

### **Russia 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.

## Russia Regulation And Product Map

### Regulation 242-P on Internal Control in Credit Institutions CBR

Applies To: Credit institutions and banking groups within scope

Operational Focus: Internal-control systems, compliance, independent internal audit, control reporting, findings, escalation and corrective-action tracking.

Platform Fit and Workflow Support: Primary fit Audit universe, risk-based planning, RCM-linked testing, working papers, evidence, findings and follow-up. Primary fit Incident reporting, triage, investigation, root cause, corrective action, escalation and closure. Boundary Workflow and evidence support only. Applicability and legal interpretation remain with the organisation and its advisers.

Source: Source

[https://www.cbr.ru/faq\\_ufr/dbrnfaq/doc/forPrint/?id=423](https://www.cbr.ru/faq_ufr/dbrnfaq/doc/forPrint/?id=423)

### Ordinance 3624-U on Risk and Capital Management CBR

Applies To: Credit institutions and banking groups within scope

Operational Focus: Risk strategy, appetite, material-risk identification, limits, capital planning, monitoring, reporting and independent assessment.

Platform Fit and Workflow Support: Primary 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 Workflow and evidence support only. Applicability and legal interpretation remain with the organisation and its advisers.

Source: Source

[https://www.cbr.ru/faq\\_ufr/dbrnfaq/doc/forPrint/?id=423](https://www.cbr.ru/faq_ufr/dbrnfaq/doc/forPrint/?id=423)

### Regulation 716-P on Operational Risk Management CBR

Applies To: Credit institutions and banking groups within scope

Operational Focus: Operational-risk classification, event databases, assessment, controls, key indicators, scenario analysis, reporting and remediation.

Platform Fit and Workflow Support: Primary 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 Workflow and evidence support only. Applicability and legal interpretation remain with the organisation and its advisers.

Source: Source

[https://www.cbr.ru/faq\\_ufr/dbrnfaq/doc?number=716-%D0%9F](https://www.cbr.ru/faq_ufr/dbrnfaq/doc?number=716-%D0%9F)

## **Corporate Governance Code and Public-Company Recommendations CBR**

Applies To: Russian public joint-stock companies and other adopting issuers

Operational Focus: Board and committee oversight, risk management, internal controls, internal audit, governance evaluation and transparent reporting.

Platform Fit and Workflow Support: Primary fit Audit universe, risk-based planning, RCM-linked testing, working papers, evidence, findings and follow-up. Primary fit Risk and control registers, assessments, appetite or limits, KRIs, treatments, approvals and board reporting. Boundary Workflow and evidence support only. Applicability and legal interpretation remain with the organisation and its advisers.

Source: Source

[https://www.cbr.ru/issuers\\_corporate/](https://www.cbr.ru/issuers_corporate/)

## **Federal Law 152-FZ Personal Data Incident Reporting Roskomnadzor**

Applies To: Personal-data operators within the Law's scope

Operational Focus: Incident recording, initial regulatory notification, investigation updates, cause analysis, response measures and evidence retention.

Platform Fit and Workflow Support: Primary fit Incident intake, assessment, investigation, notification workflow, corrective action, escalation and closure evidence. Supporting 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://pd.rkn.gov.ru/incidents/>

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 | Russia

## **Build a Connected GRC Operating Model for Russia**

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