

Turkey Regulatory Hub

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

TUR Regulatory Hub

Region: Middle East / Europe

Integrated banking controls and breach evidence for Turkey

Turkey combines detailed banking internal-systems requirements with information-systems regulation, capital-market governance and a mature personal-data protection regime. Banks and enterprises need a defensible connection between risk governance, internal audit, technology incidents and time-bound breach notification.

TUR

Middle East / Europe governance, risk and compliance intelligence

BRSA

Banking Regulation and Supervision Agency

Industries Regulated

Banking and lending

CMB

Capital Markets Board

Industries Regulated

Capital markets and listed companies

KVKK

Personal Data Protection Authority

Industries Regulated

Cross-sector data controllers and processors

USOM

National Cyber Incidents Response Center

Industries Regulated

Government and critical infrastructure

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 Management and Internal Systems

02

Independent Internal Audit and Assurance

03

Information-Systems Governance

04

Cyber Incident and Breach Response

05

Third-Party Continuity and Resilience

06

Board and Capital-Market Reporting

Regulatory Alignment

Turkey 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.

Turkey Regulation And Product Map

Banking Law No. 5411 BRSA

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

Operational Focus: Internal control, risk management, internal audit systems, consolidated oversight and governance responsibilities.

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.bddk.org.tr/Mevzuat/DokumanGetir/961>

Regulation on Information Systems and Electronic Banking Services BRSA

Applies To: Banks operating in Turkey

Operational Focus: Information-systems governance, risk controls, continuity, third-party services, security events, monitoring and electronic-banking resilience.

Platform Fit and Workflow Support: Primary fit Third-party risks, controls, assessments, treatments, approvals, KRIs and oversight reporting. Primary fit Cyber-event intake, escalation, investigation, root cause, corrective action, recovery tracking and audit trail. Boundary Workflow and evidence support only. Applicability and legal interpretation remain with the organisation and its advisers.

Source: Source

<https://www.bddk.org.tr/Mevzuat/DokumanGetir/1063>

Communique on Corporate Governance II-17.1 CMB

Applies To: Publicly held companies within the Communique's applicable scope

Operational Focus: Board and committee governance, internal control and audit oversight, risk management, disclosure and accountable follow-up.

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 Notification workflow and evidence can be configured. Submission to an authority requires an approved process or integration.

Source: Source

<https://spk.gov.tr/kurumsal-yonetim-ilkeleri>

Personal Data Protection Law No. 6698 KVKK

Applies To: Data controllers and processors within scope

Operational Focus: Data-security measures, controller accountability, internal audits and notification when data is obtained unlawfully.

Platform Fit and Workflow Support: Primary fit Incident intake, assessment, investigation, notification workflow, corrective action, escalation and closure evidence. Primary fit Audit universe, risk-based planning, RCM-linked testing, working papers, evidence, findings and follow-up. Boundary Notification workflow and evidence can be configured. Submission to an authority requires an approved process or integration.

Source: Source

<https://www.kvkk.gov.tr/Icerik/6649/Personal-Data-Protection-Law>

Board Decision No. 2019/10 on Breach Notification KVKK

Applies To: Data controllers, including relevant overseas controllers

Operational Focus: 72-hour Board notification, affected-person communication, breach documentation, response plans and accountable ownership.

Platform Fit and Workflow Support: Primary fit Incident intake, assessment, investigation, notification workflow, corrective action, escalation and closure evidence. 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.kvkk.gov.tr/Icerik/6647/The-Board-Decision-No-2019-10-of-24-01-2019-about-Procedures-and-Principles-of-Personal-Data-Breach-Notification->

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 Middle East / Europe | Turkey

Build a Connected GRC Operating Model for Turkey.

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