PROTECHT

EU DIGITAL OPERATIONAL RESILIENCE ACT (DORA)

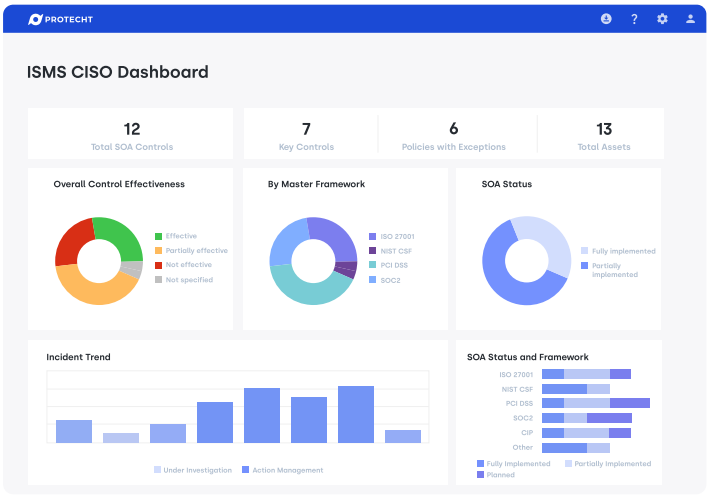
DORA compliance. Beyond the checkbox.

Protecht ERM is your comprehensive solution for achieving DORA compliance and operational resilience. Through integrated data and actionable insights, it enables financial entities to streamline compliance, minimise risks, and foster resilience beyond regulatory requirements.

Centralise and streamline ICT risk management.

Build a unified ICT risk framework with enhanced visibility, efficiency, and governance for true operational resilience.

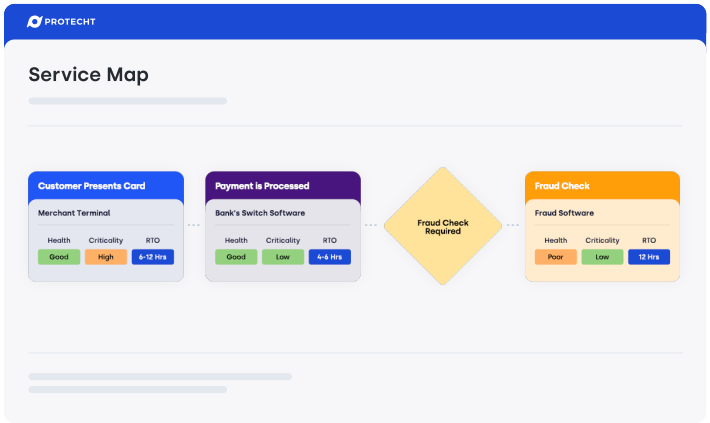
- **Tailored risk assessments:** Map risks, controls, and critical ICT functions for a holistic resilience strategy.
- **Role-based governance and workflow:** Ensure clear accountability and segregation of duties with role-based permissions.
- **Integrated dashboards:** Track key risk and resilience metrics and link them to critical business functions, countries or entities.
- **Pre-configured RTS libraries:** Embedded regulatory technical standards ensure compliance with detailed DORA requirements.



Optimise resilience testing and assurance.

Manage and monitor testing for ICT controls and critical business functions with Protecht's integrated tools.

- **Automated workflows:** Streamline control testing and validation with predefined templates and schedules which align to industry certifications such as ISO 27001, NIST, COBIT
- **Scenario-based assessments:** Identify and track vulnerabilities across systems and services with tailored resilience exercises.
- **Role segregation:** Ensure independent control testing with clear role distinctions across teams.
- **Best-practice metrics:** Track resilience KPIs and integrate results into your operational resilience plans.



PROTECHT

Strengthen ICT incident management and response.

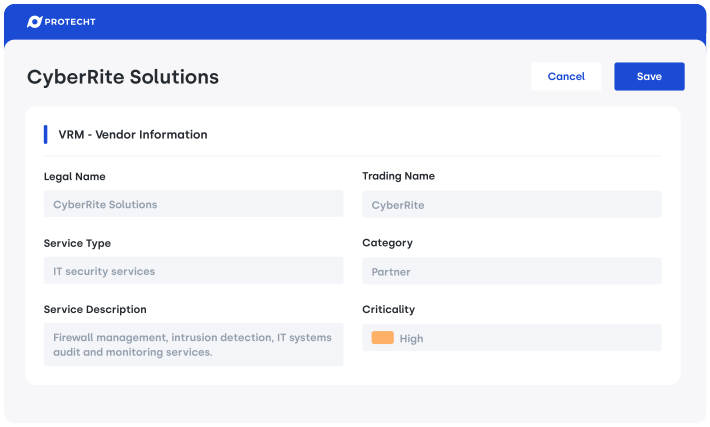
Simplify ICT incident management for efficient reporting, recovery, and alignment with regulatory obligations.

- **Centralised incident register:** Capture consistent data in a single system that is directly aligned to DORA's EBA RTS regulatory requirements
- **Automated workflows:** Trigger escalations and notify stakeholders in real time when incidents occur.
- **Root cause analysis tools:** Prevent recurring issues with bow tie analysis and action tracking.
- **Link to vendors and services:** Connect incidents to critical services and third-party providers to drive accountability.

Manage and actively monitor ICT third-party risk with ease.

Gain full visibility into third-party risks, dependencies, and compliance with DORA's ICT risk requirements.

- **Integrated vendor management:** Link third-party risks to operational resilience plans and critical functions.
- **Streamline vendor questionnaires** with our out-of-the-box DORA template, browse from the benchmark SIG libraries, or design your own. You can follow up with automated workflows.
- **Concentration risk reports:** Identify risks from key fourth parties and service dependencies.
- **End-to-end tracking:** Monitor contracts, performance, and risk levels across your third-party ecosystem.



Enable secure information sharing and collaboration.

Facilitate safe and compliant sharing of cyber threat intelligence under DORA's guidelines.

- **Configurable registers:** Track sharing arrangements and shared/received data securely and efficiently.
- **Real-time notifications:** Ensure timely updates and adherence to information-sharing policies.
- **Exportable records:** Export the register of information with a single click into the XBRL CSV files ready for direct upload into the EBA portal without further manipulation

Find out more about how Protecht ERM can solve your DORA compliance problems.

Website: www.protechtgroup.com
Email us: sales@protechtgroup.com
Call us: +44 20 3978 1360

DORA-EMEA-2025-10