DORA: Digital Operational Resilience Act

Even operationally-resilient and ISO 27001 compliant entities must meet new and significant analysis and reporting requirements, and soon, in order to meet DORA's very prescriptive requirements.

DECISION FOCUS

2024 REGTECH 100

www.RegTech100.com

Don’t Underestimate DORA

As of January 17 2025, financial institutions will need to demonstrate compliance with DORA - obligations that underpin the Digital Operational Resilience Act drive for greater stability, security and consumer confidence throughout the European Union financial sector.

While in the main, DORA’s requirements are consistent with existing regulations and best practice, there’s no room for complacency. Even operationally-resilient and IS0 27001 compliant entities may be surprised by the depth of DORA’s specific and often very prescriptive requirements – **two of which in particular, oblige you to make major changes.**

Decode DORA requirements with Decision Focus

The DORA framework – spanning five areas, often referred to as the 'five pillars' - sets out criteria, templates and instructions that will shape how financial organisations operating in the EU manage ICT and cyber risks, and withstand, respond to and recover from the impact of ICT incidents.

Aimed at ensuring continuity of critical functions and minimising disruption for customers, the new legislation also applies to non-EU firms that have trading branches in the EU.

With consistency, transparency and demonstrability front of mind, the regulators are placing considerable emphasis on reporting, communication and ongoing assessments facilitated by standardised formats.

DORA is by no means a regulatory curveball for those with robust operational resilience practices, but the layers of technical detail within the Regulatory Technical Standards (RTS) should not be underestimated.

New rules for the impact assessment, classification and reporting of ICT incidents and the introduction of a very detailed 'Register of Information' for third parties demand require new processes to be established. These will require constant maintenance.

They may sound innocuous but it's important for organisations not to undervalue or misjudge what these will entail for DORA compliance.

DORA – Five Pillars

1 ICT RISK MANAGEMENT FRAMEWORK

- Embed ICT risk management within overarching framework
- ICT specific risk assessment & remediation
- Specific reporting for ICT/DORA stakeholders

2 ICT INCIDENT MANAGEMENT

- Establish robust incident detection and logging
- Undertake both cause & impact analysis
- Implement RTS 1 complaint materiality assessment + reporting
- Incident lifecycle management: detection - remediation – closure

3 DIGITAL OPERATIONAL RESILIENCE TESTING

- Identity critical products and services
- Develop scenario test library & ensure sufficient test coverage
- Schedule and execute tests
- Remediate test findings
- Periodic effectiveness reviews

4 ICT THIRD-PARTY RISK MANAGEMENT

- Establish ICT Third-Party register
- Include DORA criteria inselection, in onboarding and monitoring
- Apply contractual security clauses
- Concentration risk assessment and remediation

5 THREAT AND INTELLIGENCE SHARING

- Collect and share intelligence on Cyber Threat Intelligence
- Collaborate with industry peers to enhance resilience
- Reporting & compliance

One cohesive compliance platform - covering all DORA demands

Decision Focus modern cloud-based GRC software helps organisations meet all the complex process and reporting requirements of DORA.

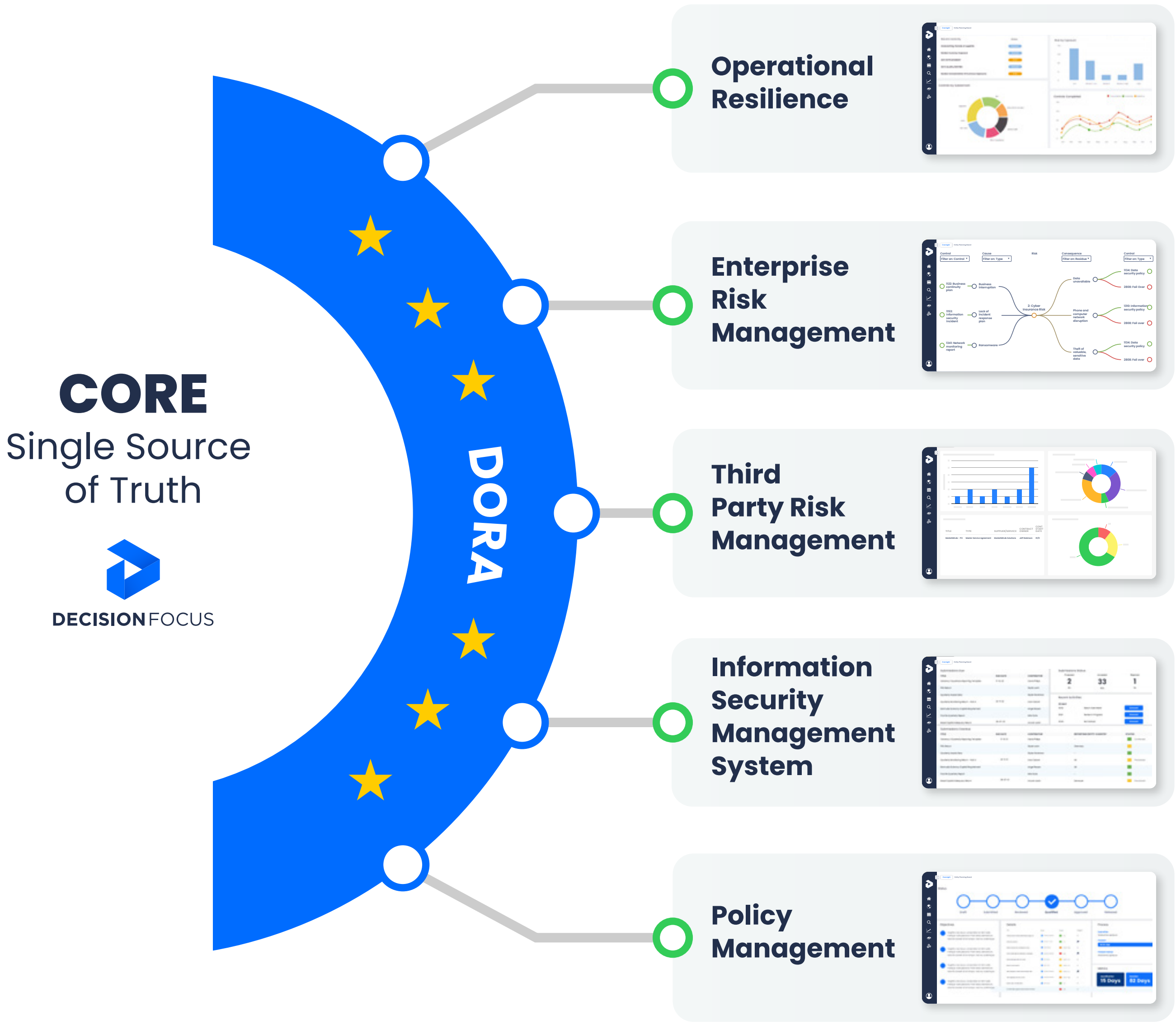
Our solution provides DORA project teams with a central repository of required DORA data for real-time performance monitoring, exception reporting and streamlined auditing.

Multi-discipline, multi-stakeholder, integrated assurance

Five modules collectively cover every aspect of your new DORA obligations: Enterprise Risk Management, Operational Resilience, Third Party Risk Management, Information Security Management and Policy Management.

Since all modules operate on the same integrated assurance platform using a single, shared repository, we provide an holistic DORA solution that serves all stakeholders simultaneously.

This helps to remove barriers between departments whilst facilitating data sharing. Because Decision Focus provides a no code, SaaS solution, it places no burden on your organisation's IT resources and means you can implement our DORA solution within a matter of weeks, not months.



CORE

Single Source of Truth

DECISION FOCUS

DORA

Operational Resilience

Enterprise Risk Management

Third Party Risk Management

Information Security Management System

Policy Management

DORA: Digital Operational Resilience Act

Enterprise Risk Management

Decision Focus Enterprise Risk Management (ERM) module provides the understanding and oversight you need for more effective ICT risk-taking, mitigation and the ability to act on opportunities.

Working from one single repository – a single source of truth – provides a seamless, integrated experience for risk and control owners. Intuitive dashboards bring 'all the right things together' to help drive thought processes. Data analysis is streamlined and reporting structured, with critical data trends, tables and charts at your fingertips. Real-time performance metrics and exception reporting provide certainty and assurance to both your risk committee and stakeholders.

Addresses these DORA requirements

Pillar 1 (ICT Risk Management Framework) and Pillar 2 (ICT Incident Management)

SIGNIFICANT OBLIGATION

Our ERM module provides a centralised capability for incident logging, analysis and reporting. DORA has introduced a very specific method for analysing the impact of incidents and we have upgraded the ERM module to cater for these.

Operational Resilience

Our Operational Resilience module is designed to help you establish and continually validate your organisation's capability to operate during periods of disruption.

Use our module to rank and validate products and services and measure the business impact of disruption to these products and services to determine Important Business Services ("IBS"). Our module allows you to determine which processes and resources support the IBSs, conduct tolerance analysis, dependency mapping, recovery strategies and resilience testing.

Addresses these DORA requirements

Pillar 2 (ICT Incident Management) and Pillar 3 (Digital Operational Resilience Testing)

Operational Resilience focuses on the resilience of your company's products and services to disruption by internal and external factors. Fundamental to understanding this, is scheduling and executing scenario testing that considers severe, but plausible disruption scenarios, alongside the key processes and resources required to maintain the services within approved impact tolerances.

In the unfortunate event that a critical situation materialises, incident management provides an effective means for identifying, analysing and managing the response to a disruptive event.

Third Party Risk Management

Decision Focus Third Party Risk Management (TPRM) module is a central repository of third parties and associated third party risk.

The module manages the entire lifecycle of third parties including due diligence, contract management and SLA oversight. It streamlines the gathering of critical data from third parties via a secure portal. The module allows you to reduce onboarding time for third parties and achieve faster completion of the due diligence process.

Addresses these DORA requirements

RECORD OF INFORMATION

SIGNIFICANT OBLIGATION

The record of information is the second area which places particularly onerous new obligations upon organisations falling within the legislation.

DORA defines the extensive information that you are obliged to record about your third party suppliers/vendors. You must be able to demonstrate that the correct information is held and how the data affects risk ranking.

DECISION FOCUS

Information Security Management

Decision Focus Information Security Management System (ISMS) enables you to define and manage the controls your organisation needs to protect the confidentiality, availability and integrity of assets from threats and vulnerabilities.

The ISMS is designed to achieve and maintain compliance with ISO27001 or provide a framework for embedding the best practice described within the framework for organisations who do not seek compliance. With both DORA and increasingly complex requirements, which differ across geographies e.g., ISO, NIST, PIPL, NIS, many organisations need to comply with multiple requirements and understand where there is overlap. Data privacy often is connected within the same department but is a separate offering.

Addresses these DORA requirements

Pillar 4
(ICT Third-Party Risk Management)

DORA requires organisations to recognise the risks inherent with third-party ICT providers. It sets guidelines for financial institutions to rigorously oversee and manage these risks. This pillar demands a thorough vetting and managing process for third-party vendors. Institutions must ensure their partners adhere to DORA's security standards and have robust risk management practices in place to maintain their operational resilience.

*ISMS In conjunction with our TPRM module above, cover both third-party and other ICT risks.

Policy Management

Our Policy Management module helps the governance of board policies and employee attestations to these policies.

You can create multiple readership groups to ensure the relevant population receives policies for review and view dashboards to provide oversight of end-user attestation. You have the capability to connect policies to controls and manage policy approvals, updates, version control and change history.

Addresses these DORA requirements

All Pillars

While we have highlighted the two key enhancements in rigor with DORA, a number of other areas require you to demonstrate compliance without specific reporting. This is where the Policy Management module comes in. The ability to clearly document your policies, show adherence to these by your employees and even policy change management is critical to full DORA compliance.

An award-winning solution - built by risk experts, for risk professionals

Built by GRC experts, for GRC professionals and with no code configuration, Decision Focus offers a **cohesive enterprise-wide solution** that **beyond a point solution for DORA or Infosec risk,** provides a complete, consolidated solution for managing all governance, risk and compliance across the organisation.

A centralised, 'single source of truth' for all DORA and ERM data means a seamless, integrated experience

Elevate discussions with regulators – build stakeholder confidence allowing you to focus on more strategic discussions

Ready to go modules and deep domain knowledge make implementation fast, seamless and stress-free

Agility and resilience, through a flexible, no code platform that you can even adjust yourself

Fast and easy adoption across three lines of defence – easy to use, modern intuitive software that users love (no training required)

Award-winning GRC software, trusted by world-class brands and recognised by industry analysts

Raises the profile of risk and compliance across the business, engaging stakeholders, embedding risk culture and informing risk-based decision making

DECISION FOCUS

Embedding innovation through agile GRC

See how Decision Focus can support your DORA compliance journey and ongoing GRC maturity.

Please get in touch to book a demo.

DECISION FOCUS

DORA RGB V1 23.08.2024

decisionfocus.com