Panorays

A Practical Approach to Complying with Third-Party Related Aspects of DORA

April 2024

Compliance and Third-Party Risk

Classification

DORA: Register of Information

Assessment

GDPR: Compliance with privacy controls, data subject rights

Monitoring

Many regulations: Incident reporting

Panorays

DORA - Huge Focus on Third-Party Risk

Financial entities (FEs), as part of their ICT risk management framework, should “**maintain and update…a register of information in relation to all contractual arrangements** on the use of ICT services provided by ICT third-party service providers.”

JC 2023 85 - 10 01 2024 Final Report - On Draft Implementing Technical Standards - Article 28(3)

“Financial entities shall **define, establish and implement an ICT-related incident management process** to detect, manage and notify ICT-related incidents.”

DORA Regulation

“The financial entity must **fully monitor the ICT subcontracting chain** and must document it.”

JC 2023 67 27 November 2023 Consultation Paper on Draft Regulatory Technical Standards

Panorays

DORA Compliance: Third Party ICT Risk

1

Information Communication Technologies (ICT)-risk management framework

2

Strategy for managing third-party ICT risk

3

Register of information

4

Exit strategy

5

Contractual provisions

6

Incident reporting

12/2023 Draft Regulatory Technical Standards

DORA: Adopt a Framework

DORA Regulation	In practical terms
Adopt and implement an Information Communication Technologies (ICT)-risk management framework	■ Adopt an ISMS (Information Security Management System), which is a security control framework, like ISO 27001/2 ■ DORA may reference the NIS2 Directive, likely to be an evolution of IS0 27001/2

Panorays

DORA: Implement a Strategy

DORA Regulation	In practical terms
Design and implement a strategy for managing third-party ICT risk	Create a framework and process to: ■ Designate third-party ICT services that support critical functions ■ Determine the criticality and “sensitiveness” of the data shared ■ Identify the ICT service in the terms DORA requires ■ Assess the ICT’s, leveraging questionnaires and doc requests ■ Identify 3rd, 4th and 5th parties which may represent potential concentration risk

Panorays

DORA: Register of Information

DORA Regulation	In practical terms
Register of information	■ Provide reports to the "Supervisory Authority", for categorizing 3P ICT relationships supporting "critical and important functions" (CIFA) ■ Know and report 4th and 5th parties, regarding "concentration risk"

Panorays

DORA: Exit Strategy

DORA Regulation	In practical terms
Exit strategy	Plan how to end a 3P ICT relationship, ensuring the “resiliency” of your business, regardless of the success or failure of any supplier relationship

Panorays

DORA: Contractual Provisions

DORA Regulation	In practical terms
Contractual provisions	Contractual terms in your contract with a 3P ICT enforcing the implementation and operation of the security controls required by DORA

DORA: Incident Reporting

DORA Regulation	In practical terms
Incident reporting	Reporting on a breach or other cyber incident to the supervisory authority (“SA”) in your country

Panorays

Addressing the Pillars with a TPCRM Platform

1

Information Communication Technologies (ICT)-risk management framework

2

Strategy for managing third-party ICT risk

3

Register of information

4

Exit strategy

5

Contractual provisions

6

Incident reporting

Panorays

12/2023 Draft Regulatory Technical Standards

DORA: How Panorays Helps

Strategy for managing third-party ICT Risk

DORA-specific inherent risk questionnaire:

- Identify the provider: contractual agreement, reference number
- Select the relevant one or more of 19 ICT-related services
- Rank the provider: direct ICT service provider, subcontractor, or supplier to a subcontractor
- Where are services provided?
- Governing law of agreement?
- Annual expense of contract
- Location of data stored and location of data processed?
- Do the services purchased support critical or important functions ("CIFA")?
- Sensitiveness of the data
- Level of reliance on ICT provider

Panorays

DORA: How Panorays Helps

Strategy for managing third-party ICT Risk

DORA-specific questionnaire content (Shared Assessments SIG)

- Shared Assessments is mapping and validating content against DORA
- SIG 2025 will support DORA

DORA: How Panorays Helps

Register of information

Report categorizing third-party ICT's according to:

- "Sensitiveness" of data shared
- Level of reliance on the ICT service supporting the critical or important function
- Identification of subcontractors and subcontractors' suppliers (*Concentration Risk*)

DORA: How Panorays Helps

Incident reporting

- Risk Insights map events to digital supply chain
- Inherent risk-driven alerts of events affecting critical and important functions (CIFA’s)
- Alert FE’s as early as possible, so they can report to SA’s

Thank you

Panorays