
PCi
Security
Standards Council
®

DORA: How the Next Wave of Requirements Is Hitting the Payment Card Industry

Christopher Kristes

QSA, 3DS Assessor, P2PE QSA, CISSP, CISA
Executive Board Member, Head of Security Audits & PCI

more security. usd

Dr. Christian Schwartz

CISM, CRISC, GSTRT
Head of Security in Finance

more security. usd

PCI Security Standards Council

DORA is Relevant for Financial Entities and their Service Providers and must be Implemented by January 2025.

Situation

- The Digital Operational Resilience Act (DORA) applies to financial entities.
- Their service providers will face new requirements from the financial entities.
- Implementation of DORA must be completed by January 2025.

Challenges

- Financial entities are still in progress of implementing DORA on a tight timeline.
- Service providers have not yet received the new requirements by their clients.
- Financial entities will expect compliance with new requirements as soon as possible.

After this talk, you will be able to

- identify if you‘re impacted by DORA
- work with the DORA requirements and identify synergies with existing PCI requirements and
- plan a roadmap to a regulatory or customer driven compliance.

PCI Security Standards Council

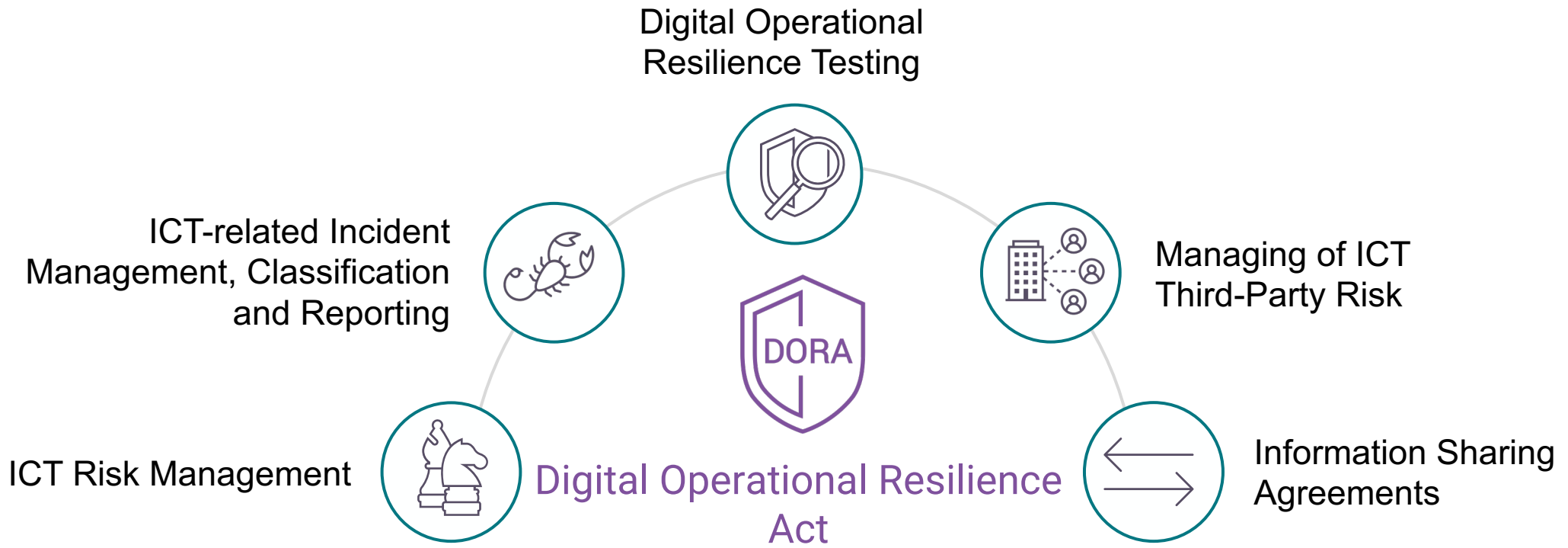
If and How an Enterprise is Impacted by DORA Depends on its Sector and Type of Relationship to Financial Entities.

Direct		Indirect	
Financial Entities	Critical ICT Service Providers	ICT Service Providers of Financial Entities	Sub-Contractors of ICT Service Providers
Directly regulated: 	**Directly regulated:** To be defined by the European Supervisory Authorities based on the contractual arrange-ments of the directly regulated financial entities.	**High impact:** If the provided services support critical or important functions of their client	
		Lower impact: If the provided services do not support critical or important functions of their client	

Distinction of impact by sector and relationship to financial entities

PCI Security Standards Council®

DORA Proportionally Addresses Resilience Risks by Enforcing Requirements across Multiple Information Security Domains.



Critical or Important Functions

DORA allows for proportionality by distinguishing between requirements for ICT assets or ICT third-party providers depending on whether or not they support critical or important functions.
A function is critical or important if[1)] (a) it would impact the soundness / continuity of its services or (b) is required for compliance with the requirements of its authorization.

1) Simplified definition. For full definition see REGULATION (EU) 2022/2554 (DORA), Article 3, Paragraph 22

DORA and PCI DSS Requirements are Complementary and Contain Potential to Exploit Synergies.

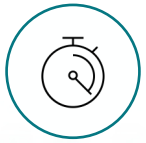
Deep Dive for Two Topics in DORA / PCI DSS

Reporting of ICT incidents

Digital operational resilience testing

PCI Security Standards Council

Deep Dive: Reporting of ICT-Incidents

PCI DSS		DORA
• For financial entities: PCI scope • For ICT third-parties: PCI-relevant service providers only	 Scope	• For financial entities: Whole enterprise • For ICT third-parties: All services provided to financial entities
• Types: No specific definitions, to be defined in the individual IRP • Thresholds: Not defined	 Criteria	• Types: Impacted clients, reputational impact, data loss, etc. • Thresholds: Unauthorized and malicious access or based on business metrics
• Initial notification: Immediately inform all relevant parties • Reporting: Defined by the individual payment brands	 Time frame	• Initial report: 4 hours after classification • Intermediate report: 72 hours after classification • Final report: 1 month after classification

PCI Security Standards Council

Deep Dive: Digital Operational Resilience Testing

	PCI DSS	DORA
 Scope	• Penetration testing: Simplified: PCI DSS scope with focus on CDE • Threat-led penetration testing (TLPT): Not required	• Normal testing: All ICT assets, risk based • Threat-led penetration testing (TLPT): Critical or important functions in live production environment
 Methods	• Normal testing: Pentests, Code Reviews, Vulnerability Scans, Wireless Tests • TLPT: N/A	• Normal testing: Pentests, Code Reviews, physical assessments, etc. • TLPT: Long-term red team engagement based on threat intelligence
 Results	• Normal testing: Risk-based remediation in vulnerability management program • TLPT: N/A	• Normal testing: Risk-based remediation in vulnerability management program • TLPT: Report to relevant authorities on findings and remediation plan

PCI Security Standards Council®

The Concrete Roadmap to DORA Compliance Depends on the Enterprise, but all Roadmaps Share Common Elements.

1 Identify Scope

- Identify impacted functions and dependencies
- Identify customers impacted by DORA
- Identify sub-contractors

2 Define Priorities

- Define critical or important functions
- Identify ICT third-parties/assets supporting critical or important functions

3 Define Actions

- Define new controls and processes
- Define new contractual requirements

4 Plan Roadmap

- Plan operational-ization of actions
- Schedule renegotiation for contract
- Inform stakeholders

5 Operationalize Controls

- Perform internal activities
- Control external activities
- Report progress to stakeholders

Relevant for Financial Entities

Relevant for ICT Service Providers

PCI Security Standards Council

THANK YOU

PCI Security Standards Council®


PCi
Security
Standards Council
®