

Milestone I

Official launch

DORA in Control

Authors:

Sandeep Gangaram Panday – Schuberg Philis
Jeremy Oschmann – Schuberg Philis

06/11/2024

6 November

RiskEvent'24

Introducing a Practical Guide to Achieve Enhanced Digital Operational Resilience



Sandeep Gangaram Panday
Trust Officer – Co-author
Schuberg Philis



Jeremy Oschmann
IT Auditor – Co-author
Schuberg Philis

Overview of EU Legislations in the Digital Sector

- = Applicable law
- = In negotiation
- = Planned initiative

Research & Innovation	Industrial Policy	Connectivity	Data & Privacy	IPR	Cybersecurity	Law Enforcement	Trust & Safety	E-commerce & Consumer Protection	Competition	Media	Finance
Digital Europe Programme Regulation, E.U. 2020/1044	Recovery and Resilience Facility Regulation, E.U. 2020/1044	Frequency Bands Directive, E.U. 2017/1212	Efficiency Directive, E.U. 2018/1000	Database Directive, E.U. 96/90	Regulation for a Cybersecurity Act, E.U. 2019/881	Law Enforcement Directive, E.U. 2016/680	Product Liability Directive (PLD), E.U. 2024/1761	Unfair Contract Terms Directive (UCTD), E.U. 1993/13	EC Merger Regulation, E.U. 2004/1825	Smalls and Code Directive, E.U. 1990/269	Common WiFi system, E.U. 2024/1761
Horizon Europe Regulation, E.U. 2020/1345	Research and Innovation Programme Regulation, E.U. 2020/1345	Radio Spectrum Directive, E.U. 2002/1978	European Statistics, E.U. 2006/517	Community Design Directive, E.U. 2016/1738	Regulation on revision of European Cybersecurity Competence Centre, E.U. 2023/1861	Directive on combating fraud and counterfeiting of non-cash means of payment, E.U. 2018/1073	Tax Regulation, E.U. 2024/1761	Price Indication Directive, E.U. 1998/5	Technology Transfer Block Exemption Regulation, E.U. 2015/1033	Information Society Directive, E.U. 2002/95	Administrative cooperation in the field of taxation, E.U. 2015/118
Regulation on public access to research data, E.U. 2022/860	Connecting Europe Facility Regulation, E.U. 2020/1345	Open Internet Access Regulation, E.U. 2015/1188	General Data Protection Regulation (GDPR), E.U. 2016/679	Enforcement Directive (IP), E.U. 2016/1738	NIS 2 Directive, E.U. 2022/2554	Regulation on interoperability between EU information systems in the field of border control, E.U. 2019/1071	European Dimensionation Regulation (EMR), E.U. 2021/1008	E-commerce Directive, E.U. 2002/11	Company Law Directive, E.U. 2017/1132	Multi-stakeholder Service Directive (MANS), E.U. 2018/1818	Payment Services Directive 2 (PSD2), E.U. 2015/2376
Regulation on High Performance Computing Joint Undertaking, E.U. 2022/1112	European Electronic Communications Code Directive (EECC), E.U. 2018/1875	Regulation on the protection of trade secrets, E.U. 2016/943	Regulation on the free flow of non-personal data, E.U. 2018/1875	Directive on the protection of trade secrets, E.U. 2016/943	Cybersecurity Regulation, E.U. 2019/1907	Regulation on technical interconnection, E.U. 2019/1907	Radio Equipment Directive (RED), E.U. 2014/53	Unfair Commercial Practices Directive (UCPD), E.U. 2005/29	Market Surveys Regulation, E.U. 2018/1008	Liability Regulation, E.U. 2017/1445	Digital Operational Resilience Act (DORA) Regulation, E.U. 2023/2554
Regulation on Joint Undertaking under Horizon Europe, E.U. 2021/1046	As Top-level domain Regulation, E.U. 2018/1875	Regulation on the free flow of non-personal data, E.U. 2018/1875	Regulation on the free flow of non-personal data, E.U. 2018/1875	Regulation on the free flow of non-personal data, E.U. 2018/1875	Regulation on the free flow of non-personal data, E.U. 2018/1875	Regulation on the free flow of non-personal data, E.U. 2018/1875	Regulation on the free flow of non-personal data, E.U. 2018/1875	Regulation on the free flow of non-personal data, E.U. 2018/1875	Regulation on the free flow of non-personal data, E.U. 2018/1875	Regulation on the free flow of non-personal data, E.U. 2018/1875	Digital Operational Resilience Act (DORA) Regulation, E.U. 2023/2554
Decision on a plan to the Digital Decade, E.U. 2022/1981	Roaming Regulation, E.U. 2015/1188	Open Data Directive (ODD), E.U. 2017/1054	Open Data Directive (ODD), E.U. 2017/1054	Open Data Directive (ODD), E.U. 2017/1054	Open Data Directive (ODD), E.U. 2017/1054	Open Data Directive (ODD), E.U. 2017/1054	Open Data Directive (ODD), E.U. 2017/1054	Open Data Directive (ODD), E.U. 2017/1054	Open Data Directive (ODD), E.U. 2017/1054	Open Data Directive (ODD), E.U. 2017/1054	Open Data Directive (ODD), E.U. 2017/1054
European Digital Act Regulation, E.U. 2024/1761	Union Security Connectivity Programme, E.U. 2024/1761	Data Governance Act (DGA) Regulation, E.U. 2023/1678	Data Governance Act (DGA) Regulation, E.U. 2023/1678	Data Governance Act (DGA) Regulation, E.U. 2023/1678	Data Governance Act (DGA) Regulation, E.U. 2023/1678	Data Governance Act (DGA) Regulation, E.U. 2023/1678	Data Governance Act (DGA) Regulation, E.U. 2023/1678	Data Governance Act (DGA) Regulation, E.U. 2023/1678	Data Governance Act (DGA) Regulation, E.U. 2023/1678	Data Governance Act (DGA) Regulation, E.U. 2023/1678	Data Governance Act (DGA) Regulation, E.U. 2023/1678
Establishing the European Technology for Europe Platform (ETEP), E.U. 2024/1761	Digital Infrastructure Act, E.U. 2024/1761	European Data Act Regulation, E.U. 2023/1678	European Data Act Regulation, E.U. 2023/1678	European Data Act Regulation, E.U. 2023/1678	European Data Act Regulation, E.U. 2023/1678	European Data Act Regulation, E.U. 2023/1678	European Data Act Regulation, E.U. 2023/1678	European Data Act Regulation, E.U. 2023/1678	European Data Act Regulation, E.U. 2023/1678	European Data Act Regulation, E.U. 2023/1678	European Data Act Regulation, E.U. 2023/1678
European Digital Resilience Act Regulation, E.U. 2024/1761	European Digital Resilience Act Regulation, E.U. 2024/1761	European Digital Resilience Act Regulation, E.U. 2024/1761	European Digital Resilience Act Regulation, E.U. 2024/1761	European Digital Resilience Act Regulation, E.U. 2024/1761	European Digital Resilience Act Regulation, E.U. 2024/1761	European Digital Resilience Act Regulation, E.U. 2024/1761	European Digital Resilience Act Regulation, E.U. 2024/1761	European Digital Resilience Act Regulation, E.U. 2024/1761	European Digital Resilience Act Regulation, E.U. 2024/1761	European Digital Resilience Act Regulation, E.U. 2024/1761	European Digital Resilience Act Regulation, E.U. 2024/1761
Net Zero Industry Act, E.U. 2024/1761	Digital Networks Act, E.U. 2024/1761	Regulation on data collection for short-term rental, E.U. 2024/1761	Regulation on data collection for short-term rental, E.U. 2024/1761	Regulation on data collection for short-term rental, E.U. 2024/1761	Regulation on data collection for short-term rental, E.U. 2024/1761	Regulation on data collection for short-term rental, E.U. 2024/1761	Regulation on data collection for short-term rental, E.U. 2024/1761	Regulation on data collection for short-term rental, E.U. 2024/1761	Regulation on data collection for short-term rental, E.U. 2024/1761	Regulation on data collection for short-term rental, E.U. 2024/1761	Regulation on data collection for short-term rental, E.U. 2024/1761
EU Green Law		European Health Data Space Regulation, E.U. 2024/1761	European Health Data Space Regulation, E.U. 2024/1761	European Health Data Space Regulation, E.U. 2024/1761	European Health Data Space Regulation, E.U. 2024/1761	European Health Data Space Regulation, E.U. 2024/1761	European Health Data Space Regulation, E.U. 2024/1761	European Health Data Space Regulation, E.U. 2024/1761	European Health Data Space Regulation, E.U. 2024/1761	European Health Data Space Regulation, E.U. 2024/1761	European Health Data Space Regulation, E.U. 2024/1761
		Representation of GDPR Enforcement procedure, E.U. 2024/1761	Representation of GDPR Enforcement procedure, E.U. 2024/1761	Representation of GDPR Enforcement procedure, E.U. 2024/1761	Representation of GDPR Enforcement procedure, E.U. 2024/1761	Representation of GDPR Enforcement procedure, E.U. 2024/1761	Representation of GDPR Enforcement procedure, E.U. 2024/1761	Representation of GDPR Enforcement procedure, E.U. 2024/1761	Representation of GDPR Enforcement procedure, E.U. 2024/1761	Representation of GDPR Enforcement procedure, E.U. 2024/1761	Representation of GDPR Enforcement procedure, E.U. 2024/1761
		Access to research data, E.U. 2024/1761	Access to research data, E.U. 2024/1761	Access to research data, E.U. 2024/1761	Access to research data, E.U. 2024/1761	Access to research data, E.U. 2024/1761	Access to research data, E.U. 2024/1761	Access to research data, E.U. 2024/1761	Access to research data, E.U. 2024/1761	Access to research data, E.U. 2024/1761	Access to research data, E.U. 2024/1761
		Open Cultural	Open Cultural	Open Cultural	Open Cultural	Open Cultural	Open Cultural	Open Cultural	Open Cultural	Open Cultural	Open Cultural

Digital Operational Resilience Act (DORA)

17/01/2025

Old perspective

Focus on security

“Preserving of confidentiality, integrity, and availability of information.”

New perspective

Focus on resilience

“Anticipating, withstanding, **recovering from, and adapting to adverse conditions, stresses, attacks, or compromises”**

Digital Operational Resilience Act - DORA - (EU) 2022/2554



Aims to increase the **resilience** of the EU financial market



Enforceable from **17/01/2025**



Financial institutions and their (critical) **IT service providers**



Contains **detailed** requirements, spanning across 11 documents

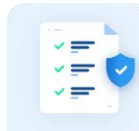
Network and Information Security Directive - NIS2 - (EU) 2022/2555



Aims to increase the **resilience** of the EU critical & important sectors



Enforceable from **17/10/2024**. In the Netherlands this is extended to be 2025



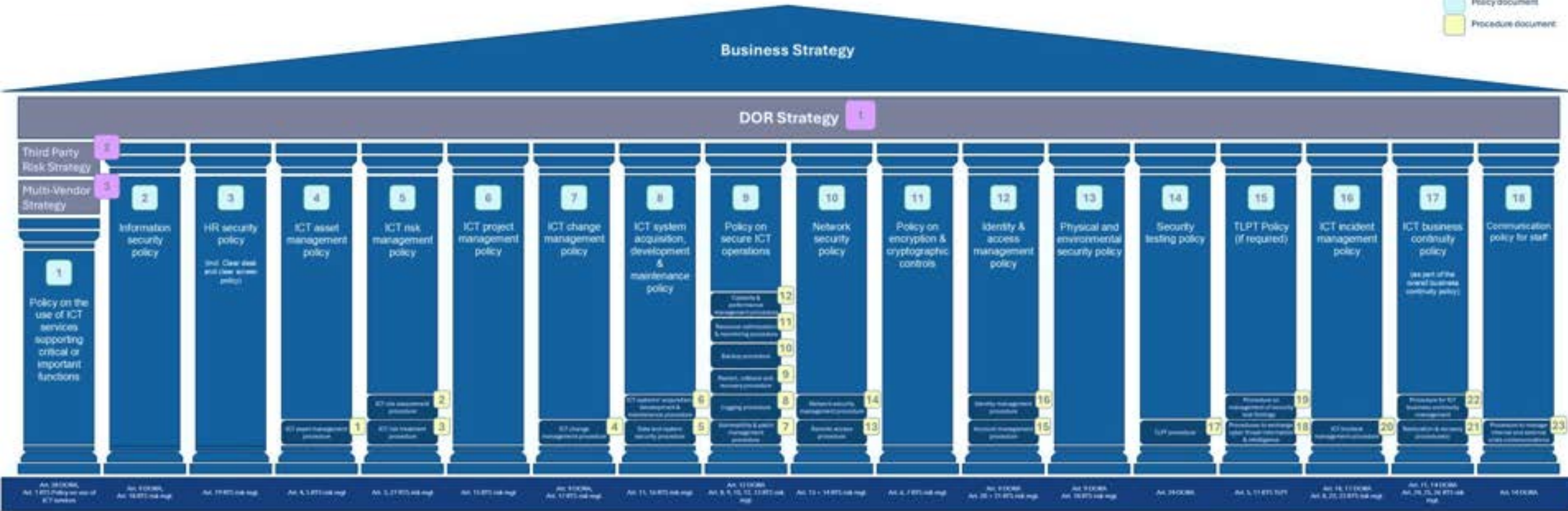
Operators of **critical infrastructure** and **essential/important services** in the EU



High level goals and requirements

Complexity


Overview of DORA policies and procedures





Article 4 'Proportionality principle'

Implement the rules laid down in accordance with the **principle of proportionality**, taking into account size and **overall risk profile**, and the nature, scale and **complexity** of services, activities and operations.



Article 7 (d) 'ICT systems, protocols and tools' & 12.3
'Restoration and Recovery'

Use and maintain updated ICT systems, protocols and tools that are **technologically resilient in order to adequately deal with additional information processing needs as required under **stressed market conditions** or other **adverse situations**. E.g., When **restoring**, use ICT systems that are **physically and logically segregated (12.3)**.**



Article 8.1 'Identification'

Identify, classify and adequately document all ICT supported business functions, roles and responsibilities, the information assets and ICT assets supporting those functions, and their roles and dependencies in relation to ICT risk.



Article 11.6 (a-b) 'Test Response and recovery'

Test the ICT business continuity plans and the ICT response and recovery plans in relation to ICT systems supporting all functions at least **yearly**, as well as in the event of any **substantive changes** to critical or important functions; And include **scenarios of cyber-attacks** and **switchovers** between the primary ICT infrastructure and the redundant capacity.



Article 28.3 'Register of information'

As part of their ICT risk management framework, financial entities shall maintain and update at entity level, and at sub-consolidated and consolidated levels, a [register of information](#) in relation to all contractual arrangements on the use of ICT services provided by ICT third-party service providers.



Challenges



Multifaceted interpretation



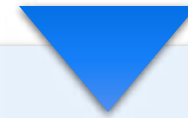
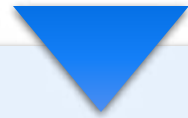
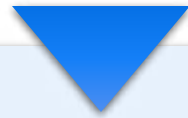
Translating requirements



Management engagement



Fragmented approach



Opportunities



Digital recoverability



Customer trust



Competitive advantage



Societal impact

1

Asset Inventory

Identify the ICT assets that
supports COI-functions

2

Risk Assessment

Establish a risk profile and
prioritize areas of attention

3

Gap Assessment

Identify DORA gaps and
highlight improvement areas

4

Roadmap

Develop a roadmap and build
towards DORA compliance

Engineering perspective

1

Asset Inventory

Identify the ICT assets that
supports COI-functions

2

Risk Assessment

Establish a risk profile and
prioritize areas of attention

3

Gap Assessment

Identify DORA gaps and
highlight improvement areas

4

Roadmap

Develop a roadmap and build
towards DORA compliance





DORA in Control

A Practical Guide to Achieve Enhanced Digital Operational Resilience

A study report by NOREA

Authors:

S. Gangaram Panday – Schuberg Philis

J. Oschmann – Schuberg Philis

©2024 NOREA, All rights reserved

PO box 242, 2130 AE Hoofddorp

Phone: +31 (0) 88 4960 380

The Netherlands

e-mail: norea@norea.nl



DORA in Control

A Practical Guide to Achieve Enhanced Digital Operational Resilience

A study report by NOREA

Authors:

S. Gangaram Panday – Schuberg Philis

J. Oschmann – Schuberg Philis

©2024 NOREA, All rights reserved

PO box 242, 2130 AE Hoofddorp

Phone: +31 (0) 88 4960 380

The Netherlands

e-mail: norea@norea.nl

DORA in Control

Key features



Accessible language



Actionable controls



DNB maturity model



Progress tracking



DNB58 mapping

DORA Simplified

Governance and Risk Management

1. Management responsibilities
2. Risk management framework
3. Risk assessments
4. (Internal) ICT audit

Operational Management

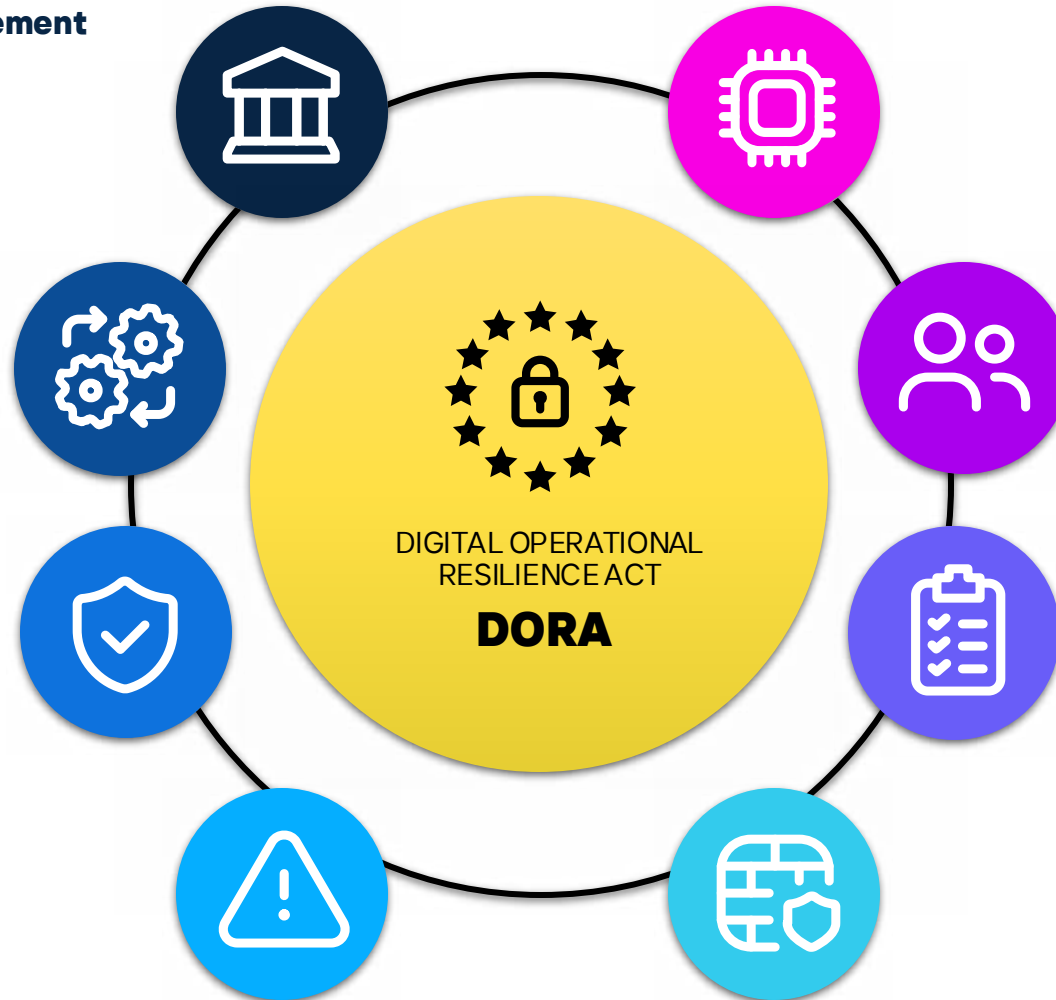
5. Asset management
6. Change management
7. ICT operations

Continuity Management

8. Backup management
9. Response & recovery

Incident Management

10. Incident classification
11. Incident management



Software and Systems Development

12. Acquisition, development, and maintenance
13. Project management

Third-party Risk Management

14. Third-party due diligence and selection
15. Third-party (standard) contract management
16. Third-party (critical) contract management
17. Third-party risk management
18. Subcontracting management

Resilience Testing

19. Digital operation resilience testing
20. Threat-led penetration testing

Security Management

21. Architectural and network security
22. Security monitoring & log management
23. Data and (legacy) system security
24. Encryption and cryptography
25. Identity and access management
26. Physical and environmental security
27. Security awareness
28. Vulnerability and patch management



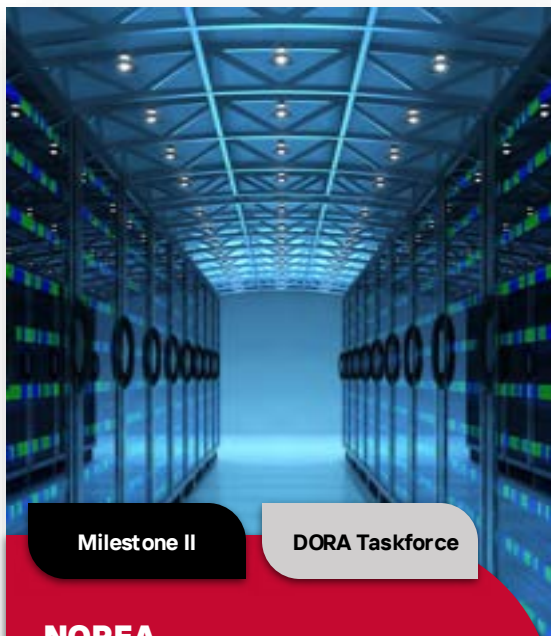
Progress Dashboard

DORA Domains	Code	Sub-domain ID	Sub-domain	Control ID	Control	Control description	DORA Level 1 and 2 Articles
Governance and Risk Management	BSM	1	Management Responsibilities	1.1	Overview of ICT risk	The Management body shall take ultimate responsibility for effectively managing all ICT risks of the financial entity. As such, the management body periodically (e.g. annually) reviews and approves: <ul style="list-style-type: none"> Policy related to the availability, authenticity, integrity, and confidentiality of data, including the policy on arrangements with ICT third-party service providers (see control 2.1). The roles, responsibilities and governance arrangements for ICT risk management (including those related to ICT third-party arrangements), including the continuous monitoring thereof. The policy on arrangements with ICT third-party service providers and those informed about third-party arrangements, services provided, planned material changes regarding third-party service providers, and understand the impact of these changes on critical and important functions of the entity (including risk assessment results). 	3.1 3.2 3.3 3.4 3.8 11.4 11.7
Governance and Risk Management	BSM	1	Management Responsibilities	1.2	Knowledge of the Management Body	The Management body shall ensure that it is kept up to date with sufficient knowledge and skills to understand and assess ICT risks and operations (e.g. through periodic training).	
Governance and Risk Management	BSM	1	Management Responsibilities	1.3	Digital Operational Resilience Strategy	The Management body shall set and approve the digital operational resilience strategy and periodically update when needed. <ul style="list-style-type: none"> The digital operational resilience strategy must: <ul style="list-style-type: none"> Set out how the risk management framework will be implemented. Elaborate on the alignment between the risk management framework and the business strategy and objectives. Establish the ICT risk tolerance level (based on risk appetite) and the impact tolerance level for ICT disruptions. Include clear security objectives, including Key Performance Indicators (KPIs) and risk metrics. Elaborate on the ICT reference architecture and any changes needed to reach specific business objectives. Outline the mechanisms in place to detect ICT-related incidents. Contain evidence to prove the current digital operational resilience situation (e.g. based on the number of major ICT-related incidents and the effectiveness of preventive measures). Contain how the digital operational resilience testing is implemented (see controls under 18 and 20). Outline the communication strategy in case of incidents (see 11.8). The Management body shall allocate and reuse the budget required for resources to fulfil the digital operational resilience needs of the entity. <ul style="list-style-type: none"> Secure monitoring is arranged on the effectiveness of the implementation of the digital operational resilience. 	
Governance and Risk Management	BSM	1	Management Responsibilities	1.4	Business Continuity Oversight	The Management body reviews and approves periodically (e.g. annually) the ICT business continuity policy and the ICT response and recovery plans.	
Governance and Risk Management	BSM	1	Management Responsibilities	1.5	Audit/Plan Approval and Review	The Management body reviews and approves periodically (e.g. annually) internal ICT audit plans, ICT audits, and material modifications to the audits.	

DORA in Control Framework

DORA in Control is endorsed by:



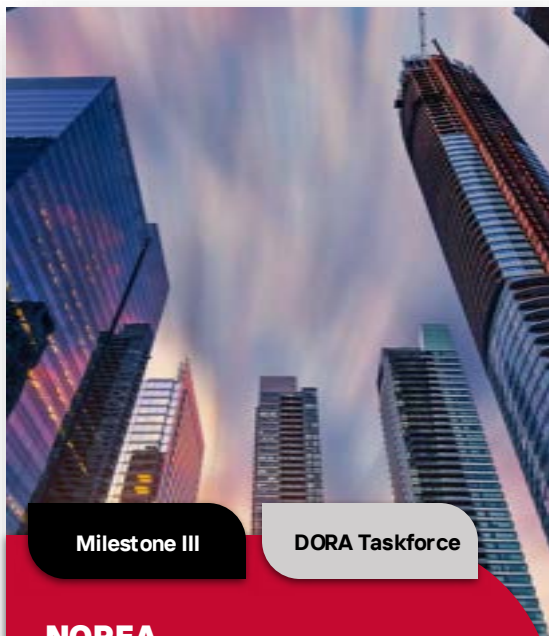


Milestone II

DORA Taskforce

NOREA Incident Reporting Tool

Release date:
28-10-2024



Milestone III

DORA Taskforce

NOREA Exit Plan Template

To be released:
~2024

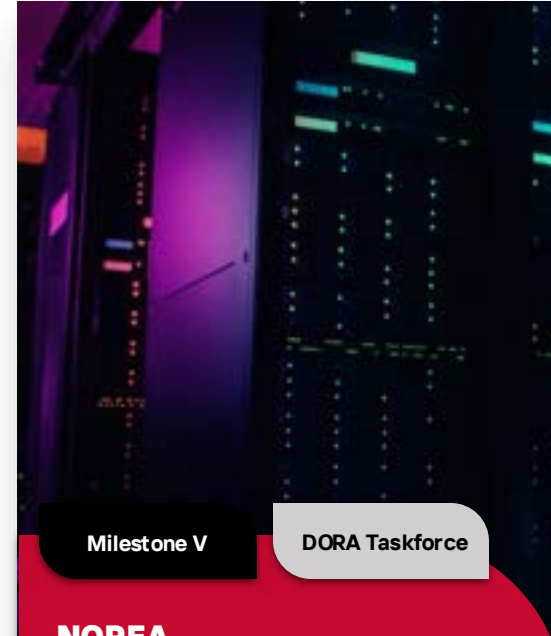


Milestone IV

DORA Taskforce

NOREA Boardroom Training Guidelines

To be released:
~2024



Milestone V

DORA Taskforce

NOREA Business Continuity Guidelines

To be released:
~2024



Download DORA in Control here:



www.norea.nl/dora