ETSI Doc. CYBER(23)033009r1, 17 Feb 2023

Center for Internet Security®

Deconstruction and Implementation of the Digital Operational Resilience Act (DORA)

Tony.Rutkowski@CISecurity.org

EU Digital Operational Resilience Act

DORA basics

- Formally known as *Regulation (EU) 2022/2554 of the European Parliament and of the Council of 14 December 2022 on digital operational resilience for the financial sector and amending Regulations (EC) No 1060/2009, (EU) No 648/2012, (EU) No 600/2014, (EU) No 909/2014 and (EU) 2016/1011*, ELI: https://eur-lex.europa.eu/eli/reg/2022/2554/oj
- Exists as a companion to the NIS2 Directive and Critical Entities Resilience (CRE) Directive
- Tabled by the European Commission on 24 September 2020, as part of a package which also includes stability, consumer protection, and EU Cybersecurity Strategy
- Focuses on ICT risk and sets rules on risk-management, incident reporting, operational resilience testing and third-party risk monitoring for a broad array of EU financial and insurance entities with significant penalties for non-complience
- Published 27 Dec 2022; came into initial force 17 Jan 2023, applying measures by 17 Jan 2025
- ESAs required to submit draft regulatory standards by 17 Jan 2024 and 17 Jul 2024
- Creates a “Lead Overseer”

DORA key objectives

- **Uniform requirements for the security of network and information systems supporting the business processes of financial entities to achieve a high common level of digital operational resilience**
  - information and communication technology (ICT) risk management
  - reporting of major ICT-related incidents and notifying, on a voluntary basis, significant cyber threats to the competent authorities
  - reporting of major operational or security payment-related incidents to the competent authorities by credit, payment, and electronic money institutions, and account information service providers
  - digital operational resilience testing
  - information and intelligence sharing in relation to cyber threats and vulnerabilities
  - measures for the sound management of ICT third-party risk
- **contractual arrangement requirements between ICT third-party service providers and financial entities**
- **establishment and conduct of the Oversight Framework for critical ICT third-party service providers when providing services to financial entities**
- **cooperation among competent authorities, and rules on supervision and enforcement by competent authorities of DORA**
- **a sector-specific implementation of the NIS2 Directive**

What is under the DORA regime (Art. 2)

- ICT third-party service providers
- account information service providers
- administrators of critical benchmarks
- central counterparties
- central securities depositories
- credit institutions
- credit rating agencies
- crowdfunding service providers
- crypto-asset service providers and issuers of asset-referenced tokens
- data reporting service providers
- electronic money institutions
- institutions for occupational retirement provision
- insurance and reinsurance undertakings
- insurance intermediaries, reinsurance intermediaries & ancillary insurance intermediaries
- investment firms
- management companies
- managers of alternative investment funds
- payment institutions
- securitisation repositories
- trade repositories
- trading venues

DORA Structure

Chap. I	General provisions
Art. 1	Subject matter
Art. 2	Scope
Art. 3	Definitions
Art. 4	Proportionality principle
Chap. II	ICT risk management
Art. 5	Governance and organisation
Art. 6	ICT risk management framework
Art. 7	ICT systems, protocols and tools
Art. 8	Identification
Art. 9	Protection and prevention
Art. 10	Detection
Art. 11	Response and recovery
Art. 12	Backup policies and procedures, restoration and recovery procedures and methods
Art. 13	Learning and evolving
Art. 14	Communication
Art. 15	Further harmonisation of ICT risk management tools, methods, processes and policies
Art. 16	Simplified ICT risk management framework
Art. 17	ICT-related incident management process
Art. 18	Classification of ICT-related incidents and cyber threats
Art. 19	Reporting of major ICT-related incidents and voluntary notification of significant cyber threats
Art. 20	Harmonisation of reporting content and templates
Art. 21	Centralisation of reporting of major ICT-related incidents
Art. 22	Supervisory feedback
Art. 23	Operational or security payment-related incidents concerning credit institutions, payment institutions, account information service providers, & electronic money institutions
Chap. IV	Digital operational resilience testing
Art. 24	General requirements for the performance of digital operational resilience testing
Art. 25	Testing of ICT tools and systems
Art. 26	Advanced testing of ICT tools, systems and processes based on TLPT
Art. 27	Requirements for testers for the carrying out of TLPT
Chap. V	Managing of ICT third-party risk
Sec. I	Key principles for a sound management of ICT third-party risk
Art. 28	General principles
Art. 29	Preliminary assessment of ICT concentration risk at entity level
Art. 30	Key contractual provisions
Sec. II	Oversight Framework of critical ICT third-party service providers
Art. 31	Designation of critical ICT third-party service providers
Art. 32	Structure of the Oversight Framework
Art. 33	Tasks of the Lead Overseer
Art. 34	Operational coordination between Lead Overseers
Art. 35	Powers of the Lead Overseer
Art. 36	Exercise of the powers of the Lead Overseer outside the Union
Art. 37	Request for information
Art. 38	General investigations
Art. 39	Inspections
Art. 40	Ongoing oversight
Art. 41	Harmonisation of conditions enabling the conduct of the oversight activities
Art. 42	Follow-up by competent authorities
Art. 43	Oversight fees
Art. 44	International cooperation
Chap. VI	Information-sharing arrangements
Art. 45	Information-sharing arrangements on cyber threat information and intelligence
Chap. VII	Competent authorities
Art. 46	Competent authorities
Art. 47	Cooperation with structures and authorities established by Directive (EU) 2022/2555
Art. 48	Cooperation between authorities
Art. 49	Financial cross-sector exercises, communication and cooperation
Art. 50	Administrative penalties and remedial measures
Art. 51	Exercise of the power to impose administrative penalties and remedial measures
Art. 52	Criminal penalties
Art. 53	Notification duties
Art. 54	Publication of administrative penalties
Art. 55	Professional secrecy
Art. 56	Data Protection
Chap. VIII	Delegated acts
Art. 57	Exercise of the delegation
Chap. IX	Transitional and final provisions
Art. 58	Review clause
Art. 59	Amendments to Regulation (EC) No 1060/2009
Art. 60	Amendments to Regulation (EU) No 648/2012
Art. 61	Amendments to Regulation (EU) No 909/2014
Art. 62	Amendments to Regulation (EU) No 600/2014
Art. 63	Amendment to Regulation (EU) 2016/1011
Art. 64	Entry into force and application

DORA treatment of standards

- **Art. 5 (Governance and organisation) calls for the financial entity management body to put in place policies that aim to ensure the maintenance of high standards of availability, authenticity, integrity and confidentiality, of data**
- **Art. 9 (Protection and prevention) requires "financial entities design, procure and implement ICT security policies, procedures, protocols and tools that aim to ensure the resilience, continuity and availability of ICT systems, in particular for those supporting critical or important functions, and to maintain high standards of availability, authenticity, integrity and confidentiality of data, whether at rest, in use or in transit"**
- **Art. 15 (Further harmonisation of ICT risk management tools, methods, processes and policies)**
  - The ESAs shall, through the Joint Committee, in consultation with the European Union Agency on Cybersecurity (ENISA), develop common draft regulatory technical standards
  - When developing those draft regulatory technical standards, the ESAs shall take into account the size and the overall risk profile of the financial entity, and the nature, scale and complexity of its services, activities and operations, while duly taking into consideration any specific feature arising from the distinct nature of activities across different financial services sectors.
  - The ESAs shall submit those draft regulatory technical standards to the Commission by 17 January 2024.
- **Art. 16 (Simplified ICT risk management framework)**
  - The ESAs shall, through the Joint Committee, in consultation with the ENISA, develop common draft regulatory technical standards…
  - The ESAs shall submit those draft regulatory technical standards to the Commission by 17 January 2024
- **Art. 18 (Classification of ICT-related incidents and cyber threats)**
  - The ESAs shall, through the Joint Committee and in consultation with the ECB and ENISA, develop common draft regulatory technical standards…
  - The ESAs shall submit those draft regulatory technical standards to the Commission by 17 January 2024
- **Art. 20 (Harmonisation of reporting content and templates)**
  - The ESAs, through the Joint Committee, and in consultation with ENISA and the ECB, shall develop: (a) common draft regulatory technical standards…
  - The ESAs shall submit the common draft regulatory technical standards …by 17 July 2024.
- **Art. 26 (Advanced testing of ICT tools, systems and processes based on TLPT [threat-led penetration testing)**
  - The ESAs shall, in agreement with the ECB, develop joint draft regulatory technical standards…
  - The ESAs shall submit those draft regulatory technical standards to the Commission by 17 July 2024.
- **Art. 28 (General Principles [for a sound management of ICT third-party risk]}**
  - The ESAs shall, through the Joint Committee, develop draft implementing technical standards to establish the standard templates for the purposes of the register of information…, including information that is common to all contractual arrangements on the use of ICT services. The ESAs shall submit those draft implementing technical standards to the Commission by 17 January 2024.
  - The ESAs shall, through the Joint Committee, develop draft regulatory technical standards to further specify the detailed content of the policy….in relation to the contractual arrangements on the use of ICT services supporting critical or important functions provided by ICT third-party service providers.
  - When developing those draft regulatory technical standards, the ESAs shall take into account the size and the overall risk profile of the financial entity, and the nature, scale and complexity of its services, activities and operations. The ESAs shall submit those draft regulatory technical standards to the Commission by 17 January 2024.
- **Art. 30 (Key contractual provisions)**
  - The ESAs shall, through the Joint Committee, develop draft regulatory technical standards to specify further the elements…which a financial entity needs to determine and assess when subcontracting ICT services supporting critical or important functions.
  - When developing those draft regulatory technical standards, the ESAs shall take into consideration the size and overall risk profile of the financial entity, and the nature, scale and complexity of its services, activities and operations.
  - The ESAs shall submit those draft regulatory technical standards to the Commission by 17 July 2024.
- **Art. 33 (Tasks of the Lead Overseer)**
  - …assessment…shall cover…the use of relevant national and international standards applicable to the provision of its ICT services to the financial entities
- **Art. 41 (Harmonisation of conditions enabling the conduct of the oversight activities)**
  - The ESAs shall, through the Joint Committee, develop draft regulatory technical standards…
  - The ESAs shall submit those draft regulatory technical standards to the Commission by 17 July 2024.

DORA TC CYBER work

- **Implementation guidance and collaboration**
- **Regulatory standards deliverables**

17 Jan 2024	Art. 15	Further harmonisation of ICT risk management tools, methods, processes and policies
	Art. 16	Simplified ICT risk management framework
	Art. 18	Classification of ICT-related incidents and cyber threat
	Art. 28	General Principles for a sound management of ICT third-party risk
17 Jul 2024	Art. 10	Harmonisation of reporting content and templates
	Art. 26	Advanced testing of ICT tools, systems and processes based on threat-led penetration testing
	Art. 30	Key contractual provisions
	Art. 41	Harmonisation of conditions enabling the conduct of the oversight activities

Special issue: encryption

- **Art. 9 4 requires financial entities**
  - implement policies and protocols for strong authentication mechanisms, based on relevant standards and dedicated control systems, and protection measures of cryptographic keys whereby data is encrypted based on results of approved data classification and ICT risk assessment processes
- **Art. 35 1(d)(i) empowers the Lead Overseer to "issue recommendations…concerning**
  - the use of specific ICT security and quality requirements or processes, in particular in relation to the roll-out of patches, updates, encryption and other security measures which the Lead Overseer deems relevant for ensuring the ICT security of services provided to financial entities
- ***Council Resolution on Encryption* adopted on 14 Dec 2020 notes that certain types of end-to-end encryption pose fundamental challenges**
  - For Member States protecting essential security interests
  - For network service providers in meeting an array of compliance obligations, including cybersecurity risk management
  - Calls for cooperation on solutions for meeting these requirements
- **ETSI ISG ETI work and CYBER Middlebox Security Protocols are especially relevant**