ACC EUROPE ANNUAL CONFERENCE

3-5 June 2026
Copenhagen, Denmark

ACC Association of Corporate Counsel
EUROPE

This session is held under the

Chatham House Rules

SHOOSMITHS

DORA in the Dock: One Year On — Progress, Pitfalls, and What's Next

Anton Maslakov
Global Regulatory Legal Coordinator in MEE
SAP

Bryce Clarke
Senior Manager, Senior Corporate Counsel
Amazon Web Services

Nick Holland
Partner
Shoosmiths LLP

Moderator:

Aurelie Jespers
Associate General Counsel
WTW

SHOOSMITHS

DORA in the Dock: One Year On — Progress, Pitfalls, and What's Next

Anton Maslakov
Global Regulatory Legal Coordinator in MEE
SAP

Bryce Clarke
Senior Manager, Senior Corporate Counsel
Amazon Web Services

Nick Holland
Partner
Shoosmiths LLP

Moderator:

Aurelie Jespers
Associate General Counsel
WTW

Overview of NIS 2

- **Network and Information Systems 2 Directive (EU) 2022/2555 ('Cybersecurity Directive' or 'NIS 2')**
  - This EU law contains cybersecurity management and reporting obligations for critical infrastructure, replacing the current EU Cybersecurity Directive ("NIS 1", or 2016/1148) of May 2018 and came into effect on 17 January 2023.
  - EU Member states had until until 17 October 2024 to put provisions into national law, but as at May 2026 only 22 countries have fully implemented the Directive into national law and that law is in force, although the position remains uneven and continues to evolve across Member States.
  - Applies to the following two types of sectors (High Criticality and Critical) which are broadly interpreted: High Criticality Sectors are Energy, Transport, Banking, Financial Markets, Health, Drinking Water, Waste Water, Digital Infrastructure, ICT services, public administration, space and Critical Sectors are postal/courier, waste management, management and distribution of chemicals, production/processing and distribution of food, manufacturing, digital providers and research
  - NIS 2 will apply to certain public entities, as well as private organisations which provide their services or carry out their activities in the EU, in the regulated sectors set out below, with: (i) an annual turnover over €10m; and (ii) more than 50 employees, unless caught under the High Critical sector
  - Essential vs Important Entities- Essential entities will be subject to additional regulatory measures, which may include (among other measures):
    - Random on-site inspections
    - Regular security audits
    - Ad hoc audits
    - Designation of a monitoring officer
  - By contrast, important entities will be subject only to regulatory action where the regulator receives evidence or indication of, or information about, some non-compliance by the organisation in question. This action can include ex post on-site inspections, targeted audits, security scans and requests for access to data, documentation and evidence of implementation of policies.

Overview of Requirements

- Go beyond what is required under ISO 27001 or SOC 11
- Risk analysis and infosec policies;
  - Incident handling and business continuity procedures;
  - Cybersecurity training;
  - Procedures for security in network and information systems acquisition, development and maintenance, including vulnerability handling and disclosure;
  - Cryptography policies and procedures;
  - Human resources security, access control policies and asset management; and
  - Use of multi-factor/continuous authentication solutions and secured communications and backup communications systems (where appropriate)
- Breach Reporting: Under NIS 2, a significant incident is one that: (i) causes, or is capable of causing, severe operational disruption of the services or financial loss to the organisation concerned; and/or (ii) affects, or is capable of affecting, other persons by causing considerable material or non-material damage.
- Organisations must submit an 'early warning' report within 24 hours of discovery of a significant incident, followed by an 'incident notification' containing an initial assessment of the incident, within 72 hours. A final report should be submitted no later than one month after the incident notification. EU member states are expected to assist organisations by providing single entry points and automated systems for reporting purposes.
- Unlike GDPR, this reporting deals with incidents relating to data and not just personal data as prescribed by GDPR (and most other privacy regimes around the world)
- Registration requirements
- Supply chain requirements
- Customer flow down requirements
- Create and update RoPAs

Penalties

- Financial penalties up to of up to €10 million or 2% of the company's total worldwide turnover (whichever is higher) for essential entities and up to €7 million or 1.4% of the company's total worldwide turnover (whichever is higher) for important entities;
- The exact amount of fines may vary, but they are designed to be proportionate to the severity of the violation and the size of the entity;
- Enforcement action against entities including inspections, audits and requests for information;
- **Personal and criminal liability for directors and senior officers along with management bans in some but not all EU member states**

Overview of DORA

- Digital Operational Resilience Act ("**DORA**") came into effect on 17 January 2023 but became enforceable on 17 January 2025-it is an Act and not a Directive and thus applies automatically.
- DORA applies to:
  - 'Union financial entities' operating within the EU; and
  - ICT third parties providing ICT services to 'Union financial entities.'
- A 'Union financial entity' means a financial entity authorised to conduct activities in the EU, and in the absence of an authorization, DORA will not apply.
- Examples include credit institutions; payment institutions; account information service providers; electronic money institutions; investment firms; crypto-asset service providers as authorised under a Regulation of the European Parliament and of the Council on markets in crypto-assets and issuers of asset-referenced tokens; central securities depositories; central counterparties; trading venues; trade repositories; managers of alternative investment funds; management companies; data reporting service providers; insurance and reinsurance undertakings; insurance intermediaries, reinsurance intermediaries and ancillary insurance intermediaries; institutions for occupational retirement provision; credit rating agencies; administrators of critical benchmarks; crowdfunding service providers and securitisation repositories
- In addition to regulating 'Union financial entities,' an ICT provider may also be directly regulated by DORA where it provides services to 'Union financial entities' (i.e., a "**Critical Third-Party Provider**" or "**CTPP**").
- CTPPs are directly subject to DORA – and its oversight mechanisms – but must be "designated" as such by a Supervisory Authority – i.e., this is not a self-regulatory determination.
- To determine if you are a CTTP, you must assess to see if you are likely to pass any of the 'four tests of applicability':
  - Test A – "systemic impact"
  - Test B – "systemic character or importance"
  - Test C – "criticality or importance of functions" or
  - Test D – "substitutability"
- DORA is considered lex specialis to the NIS 2. This means that, where an organisation is regulated by both NIS 2 and DORA, the compliance requirements of DORA will prevail over those required by NIS 2 (at least in respect of those activities which fall within the scope of DORA).

Incident Timelines

- **Initial Notification:** Major incidents must be reported to the relevant competent authorities (eg the national financial regulator like the DFSA in Denmark) and potentially the European Central Bank (ECB) or national supervisors. This often must happen within a matter of hours (e.g., initial warning within 4 hours, or a finalized initial report within 24 hours).

- **Intermediate Report:** Within 72 hours of the initial notification, an updated report detailing the status, initial assessment, and indicators of compromise must be submitted.

- **Final Report:** A comprehensive report must be provided upon resolution of the incident, usually within a month, detailing the root cause and actions taken to mitigate the event.

- **Threat Sharing:** Organizations are also obligated to voluntarily share cyber threat intelligence and information with other financial entities to build collective resilience

Overview of Requirements

- EU Supervisory Authorities have now largely finalised and adopted technical standards and operative provisions required under DORA, including:
  - Risk Management Controls: granular information security controls required for a financial entity's risk management framework.
  - Testing and assurance: details around which advanced testing tools financial entities must utilize when assessing the resiliency of their cybersecurity controls.
  - Incident Classification: criteria and materiality thresholds for security incidents and, particularly when the threshold for major incidents is triggered, standard forms for incident notification.
  - Outsourcing: further details on the contractual arrangements financial entities must implement with Third Party Providers or CTPPs, including standard form reporting criteria for maintaining the annual register of outsourced providers.
  - Oversight and Sanctions: producing harmonise conditions relating to the oversight of CTPPs, including available sanctions for non-compliance.
  - A small number of measures and guidance continuing to evolve as firms progress through implementation.

Penalties

DORA establishes rigorous financial penalties for violations of its requirements with entities (including CTPPs):

- DORA requires Member States to implement effective, proportionate and dissuasive administrative penalties for breaches of its requirements.
- Specific penalties are determined at national level and they may include significant financial sanctions, public reprimands and measures against senior management

For Financial Entities:

- **Fines:** Up to 2% of total annual worldwide turnover, or 1% of average daily turnover, depending on the severity of the violation.
- **Individual/Executive Fines:** Board members and senior executives can face personal fines up to €1,000,000 for gross negligence.
- **Operational Restrictions:** Regulators can enforce public disclosure of the violation, issue temporary bans on senior management, and temporarily suspend operational licenses.

For CTPPs:

- **Periodic Penalty Payments:** Daily fines accumulating up to 1% of the average daily worldwide turnover in the preceding business year until compliance is restored, lasting up to six months.
- **Statutory Fines:** Fines can reach up to €5,000,000 for organizations and €500,000 for individuals.

DORA top ten tips

- **Focus on operational resilience,** not just compliance.
- Understand that, even where services are outsourced**, regulatory responsibility remains with FS entities**, not suppliers.
- **Align contracts and supplier management** with DORA expectations.
- **Be prepared for engagement with regulators** to be ongoing and iterative, not occasional or reactive.
- Develop **clear internal escalation and reporting** processes.
- **Map and control the full supply chain**
- **C-Suite** ongoing engagement critical
- **Training** and **Tabletop** exercises essential
- **Governance and ongoing maintenance**
- Above all **be prepared**