May 10, 2024

The Brussels Effect (Again): Compliance Strategies for the EU's New Digital and Cyber Laws

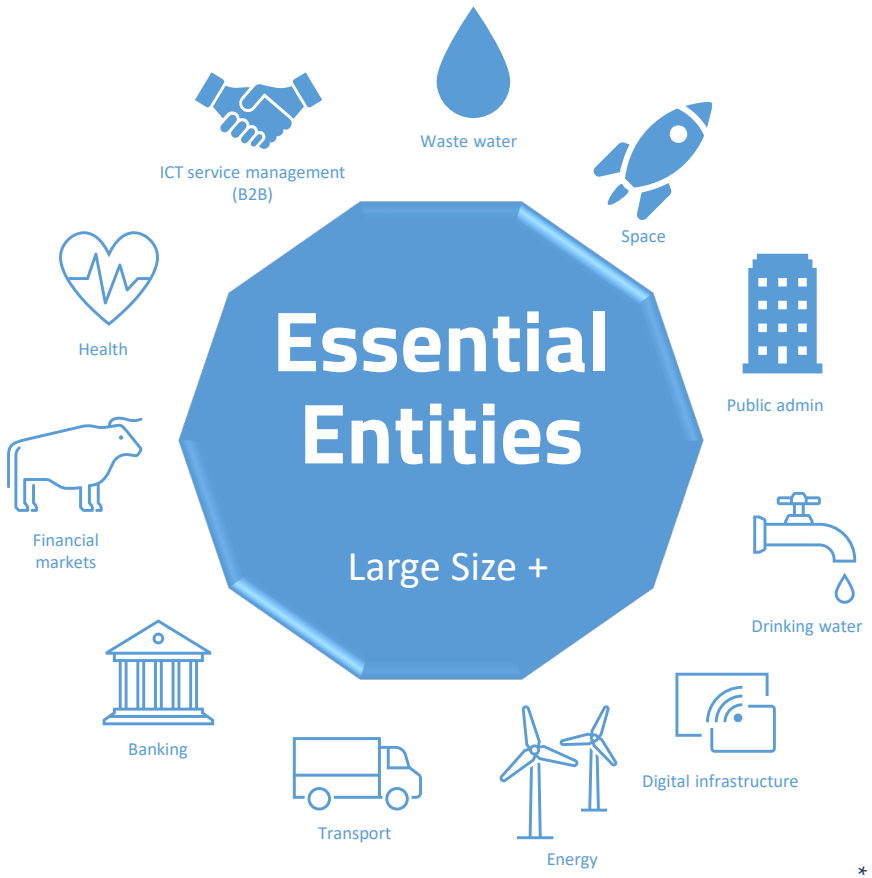
Privacy+ Security Forum

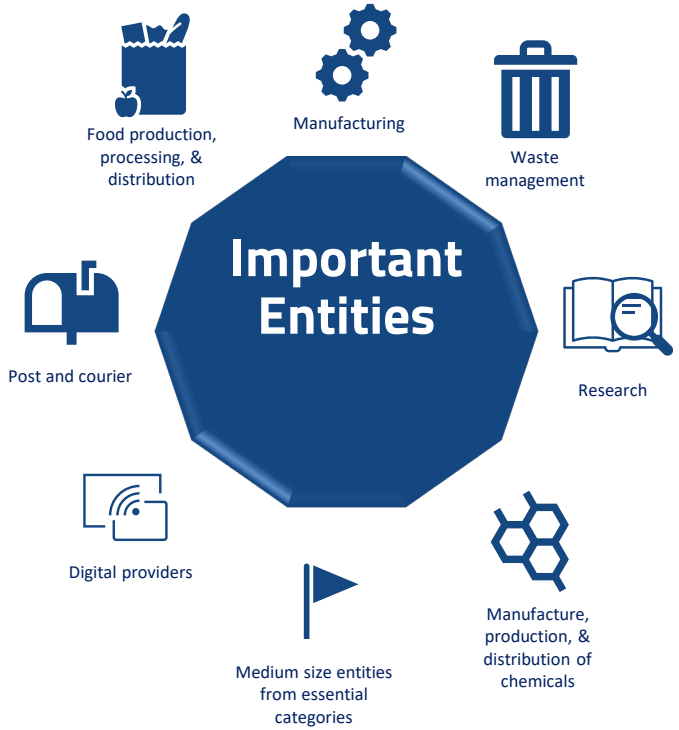
Compliance Strategies for NIS2

Jennifer Everett
Jones Day (Washington, D.C.)

Privacy+ Security Forum

Scope of NIS2





* Direct suppliers or service providers are not in scope but will be subject to due diligence from in-scope NIS2 organizations.

Location

provide services or carry out activities in any country of the EU

Medium Size

50+ employees or more than €10 million in revenue

Large Size

250+ employees or more than €50 million in revenue

Industry

operate in any of 18 critical sectors

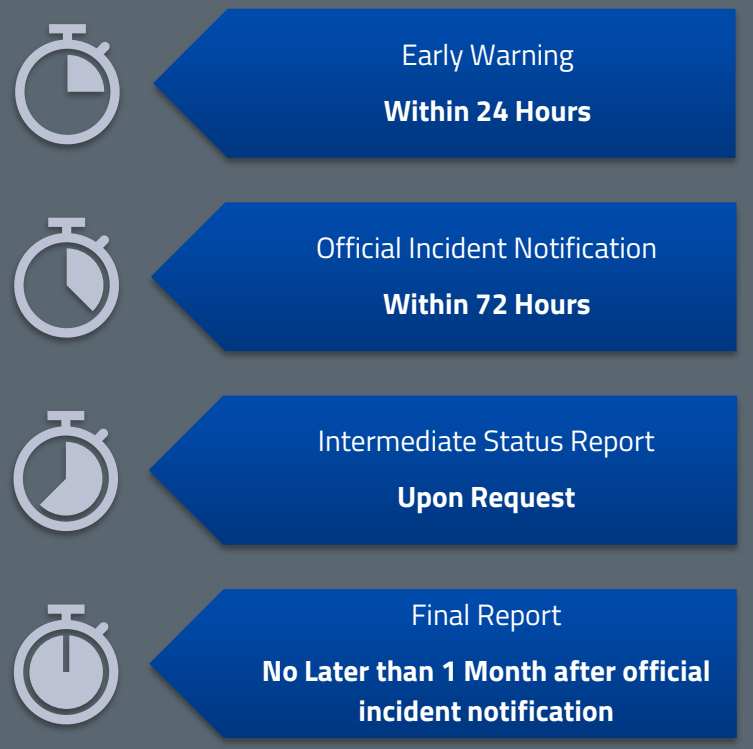
How to Comply with NIS2

Privacy+ Security Forum

Governance

- Approve the adequacy of cybersecurity risk measures taken by the entity.
- Supervise implementation of risk management measures.
- Follow training to gain sufficient knowledge and skills to identify risks.
- Offer similar training to employees on a regular basis.
- Be accountable for non-compliance.

Incident Reporting



Cyber Risk Management

1. Risk analysis & information system security
2. Incident handling
3. Business continuity measures
4. Supply chain security
5. Security in system acquisition, development and maintenance
6. Policies and procedures to assess effectiveness of cybersecurity risk management measures
7. Computer hygiene and cybersecurity trainings
8. Policies on appropriate use of cryptography and encryption
9. Human resources security, access control policies and asset management
10. Use of MFA and secured voice/video/text communication

How to Comply with NIS2 (continued)

Privacy+ Security Forum

- Determine whether NIS2 applies, directly or indirectly
- Engage, involve and train senior management early
- Perform cybersecurity risk assessment and vendor due diligence
- Execute corrective action as needed
- Develop roadmap for implementation of additional compliance measures
- Monitor for Member State adoption of NIS2 by October 17, 2024

Enforcement and Penalties

Privacy+ Security Forum

Supervision and Enforcement Orders

Supervision:

- On-site inspections;
- Security audits;
- Security scans;
- Requests for data, information, and evidence to assess cybersecurity risk management measures and policies; and
- Requests for evidence of implementation of cybersecurity policies.

Enforcement Orders:

- Stricter enforcement powers than present in NIS1.

Administrative Fines

Important

Up to 7 million euro or 1.4% annual turnover

Essential

Up to 10 million euro or 2% annual turnover

- Fines may be assessed in addition to warnings and orders.
- Periodic penalty payments may be assessed to compel entities to cease an infringement of the directive.