Why is ISO 27001 Important for IT Companies in the Context of DORA and NIS2?

Presenter:
Dejan Kosutic

Hosted by
Perry Johnson Registrars, Inc.

Advisera

ISO 27001 will be very important for NIS2 and DORA

Where is ISO 27001 useful for NIS2/DORA, and where it is not

Suppliers for companies in NIS2 and DORA scope

ISO 27001 provides a solid framework for NIS2 and DORA compliance – both for organizations in scope and for their IT suppliers

Advisera

Agenda

- Mapping ISO 27001 with NIS 2
- Using ISO 27001 for critical infrastructure companies
- Using ISO 27001 for suppliers of critical infrastructure companies
- Mapping ISO 27001 with DORA
- Using ISO 27001 for financial organizations
- Using ISO 27001 for suppliers of financial organizations
- Q&A

Mapping ISO 27001 with NIS 2

- NIS 2 is not specific on how to implement cybersecurity
- It encourages the use of international standards
- ISO 27000 series is mentioned in the preamble
- ISO 27001 maps very well with:
  - Article 20 Governance
  - Article 21 Cybersecurity risk-management measures
- ISO 27001 does not provide guidance for Article 23 Reporting obligations

Using ISO 27001 for critical infrastructure companies

NIS2	ISO 27001
Article 20 – Governance	Clause 5 – Leadership
	Clause 9 – Performance evaluation
	Clauses 7.2 & 7.3 – Competence & Awareness
Article 21 – Cybersecurity risk management measures	Clause 6 – Planning
	Clause 10.2 – Nonconformity and corrective action
	Annex A – Security controls
Article 23 – Reporting obligations	Incident management controls from Annex A?

Using ISO 27001 for suppliers of critical infrastructure

- Suppliers that provide services to companies in NIS 2 scope do not need to comply with NIS 2
- Certification – EU Commission and EU countries:
  - European cybersecurity certification schemes
  - International cybersecurity standards (ISO 27001)
- Assessment of suppliers:
  - Vulnerabilities of each supplier
  - Overall quality of products and services
  - Secure development procedures

Mapping ISO 27001 with DORA

- DORA and its CDRs are much more prescriptive than NIS2
- In most articles, DORA has more detailed requirements than ISO 27001
- DORA does not mention ISO 27001 as an obligation for financial organizations

Using ISO 27001 for financial organizations

PDCA cycle	ISO 27001 clauses	DORA
Plan	Clause 4 – Context Clause 5 – Leadership Clause 6 – Planning Clause 7 – Support	Article 5 – Governance Article 6 – ICT risk management framework Article 8 – Identification
Do	Clause 8 – Operation Annex A security controls	Articles 9 to 12; 14 Chapter 3 – ICT-related incident management, classification and reporting Chapter 4 – Digital operational resilience testing Chapter 5 – Managing of ICT third-party risk
Check & Act	Clause 9 – Performance evaluation Clause 10 – Improvement	Article 13 – Learning and evolving

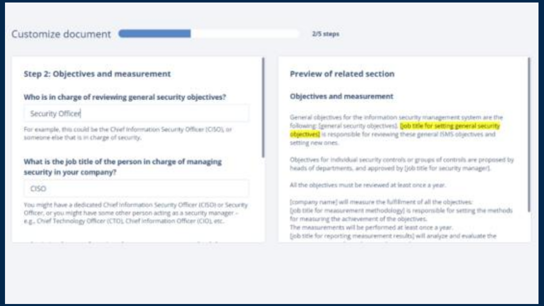
Using ISO 27001 for suppliers of financial org.

- ICT third-party service provider = any company providing digital or data services to financial entities
- ICT providers need to comply with several DORA articles
- Article 28 – all ICT providers must “comply with appropriate information security standards”
- Critical ICT service providers – additional (very strict) requirements

Conclusion

ISO 27001 is already established, NIS2 and DORA are not

NIS2 and ISO 27001 solutions



Customize document 2/5 steps

Step 2: Objectives and measurement

Who is in charge of reviewing general security objectives?

Security Officer

For example, this could be the Chief Information Security Officer (CISO), or someone else that is in charge of security.

What is the job title of the person in charge of managing security in your company?

CISO

You might have a dedicated Chief Information Security Officer (CISO) or Security Officer, or you might have some other person acting as a security manager – e.g., Chief Technology Officer (CTO), Chief Information Officer (CIO), etc.

Preview of related section

Objectives and measurement

General objectives for the information security management system are the following: [general security objectives]. [job title for setting general security objectives] is responsible for reviewing these general ISMS objectives and setting new ones.

Objectives for individual security controls or groups of controls are proposed by heads of departments, and approved by [job title for security manager].

All the objectives must be reviewed at least once a year.

[company name] will measure the fulfillment of all the objectives:
[job title for measurement methodology] is responsible for setting the methods for measuring the achievement of the objectives.
The measurements will be performed at least once a year.
[job title for reporting measurement results] will analyze and evaluate the

NIS 2 and ISO 27001 Documentation Toolkits

NIS 2 and ISO 27001 Company-wide Training & Awareness

Q&A

Advisera

Thank You

https://advisera.co/Where-to-Start-NIS2

Advisera