Unlocking Compliance to NIS2

January 2024

Infinity
IT Consulting

LEGAL DISCLAIMER

The information provided herein serves solely for general informational and educational purposes. It is not intended to, nor should it be construed as, legal advice. The content contained herein may not be applicable "as-is" to every situation and may not reflect the most current circumstances. Nothing contained herein should be solely relied upon or acted upon without the guidance of legal counsel, based on the specific facts and circumstances at hand, and nothing in this document should be interpreted otherwise. Infinity ITC retains the right to modify the contents of this document at any time without prior notice.

Despite Infinity ITC reasonable efforts to include accurate and current information in this document, Infinity ITC makes no warranties or representations of any kind regarding its accuracy, currency, or completeness. By accessing, using, or relying on this document and its contents, you acknowledge that you do so at your own risk. Infinity ITYC disclaims all warranties, whether express or implied. Neither Infinity ITC nor any party involved in the creation, production, or delivery of this document shall be liable for any consequences, losses, or damages, including but not limited to direct, indirect, special, consequential, loss of business profits, or other special damages, arising from access to, use of, or the inability to use, or in connection with the use of this document, or any errors or omissions in its content. The utilization of this information signifies acceptance of its "as is" condition.

Meet us

Bianca Ioana

Certified NIS2 Lead Implementer | ISMS | ISO27001 implementation, audits and certification | Information Security specialist | Streamlined, simplified security processes | Security in Mergers and Acquisitions

PECB ISO/IEC 27001 Lead Implementer

PECB NIS 2 Directive Lead Implementer

PECB ISO/IEC 27001 Lead Auditor

Meet us

Infinity
IT Consulting

✓ Established

Serving Swedish/Nordics and global customers and partners since 2009

✓ Industry Sectors

Our services are spanning sectors like telecommunications, security, engineering, retail, sports, fashion, and beyond

✓ How we work

Swift and flexible in our approach, we ensure top-tier quality to meet consultancy requirements

✓ Ethos

Strong company ethos that makes the well-being of our consultants' part of our success

✓ Our Services

IT Management
DevOps Information
Security

Key Talking Points

WHAT'S ON THE AGENDA

Understanding the NIS 2 directive and its context
Organizations in scope
Clarity on NIS2 requirements
Supervisory and enforcement measures of NIS2 directive (and fines)
Implementing the NIS 2 directive: A practical approach
Keep it simple – recommended methodology
How we can support
Q&A

05.

Understanding the NIS 2 Directive and its context

NIS vs NIS2

NIS Directive (Network and Information Security directive) was the first EU-wide cyber security piece of legislation. It aimed to achieve a high common level of network and information system security across the EU's critical infrastructure, and it was initially released in 2016.

Since it has not resulted in a sufficient level of resilience, the European Commission proposed a retake of NIS so NIS2 was released and will become effective October 17, 2024.

NIS2 covers therefore the minimum requirements needed to bring European companies in line with a high common level of cybersecurity across all member states.

Transposition into national legislation

In Sweden, the Swedish Government decided to commission a special investigator to assess and report on how the Directive will be transposed into national law. However, the basic requirements are mandatory across the EU irrespective of the country.

The assignment shall be released no later than 23 February 2024.

NIS2 will be subject for a new revision in 2027.

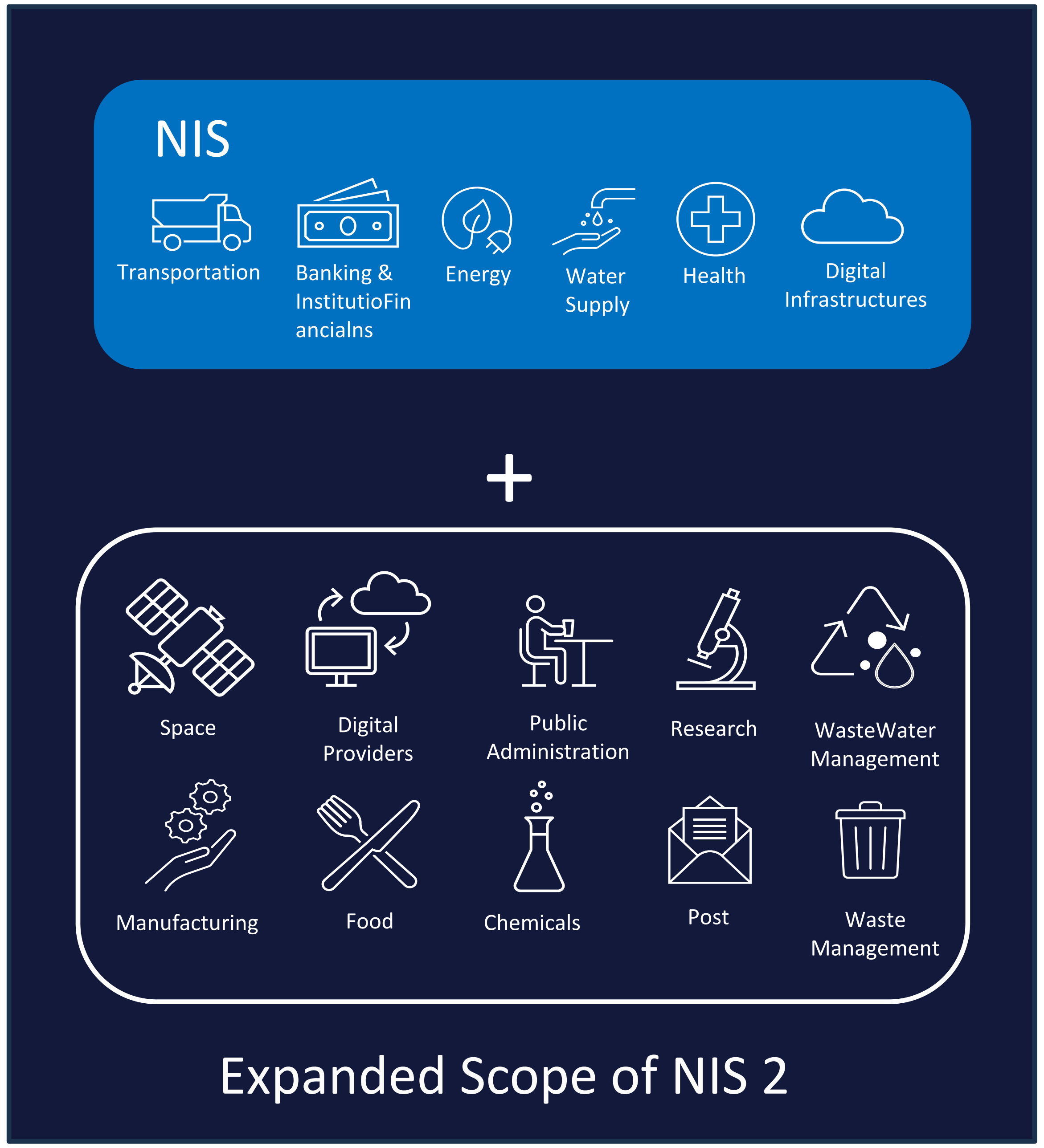
Organizations in NIS2 Directive scope

07.

08.

(Revised and Expanded) Scope

The scope extension recognizes that various industries play essential roles in the digital economy and must also be safeguarded against cyber threats.



Enterprises under NIS2 scope

Essential Entities – Public or Private large organizations in the sectors mentioned in NIS2 Annex I that have
-min. 250 employees,
- annual turnover >50 mil euro OR an annual total balance sheet of min 43 mil euro

Annex I • Energy • Transport • Banking • Financial market infrastructures • Health • Drinking water • Wastewater • Digital infrastructure • ICT Service Management (B2B) • Public administration • Space

Important Entities – Public or Private medium sized enterprises in the sectors mentioned in NIS2 Annex II that have
- min. 50 employees and
- an annual turnover/balance sheet of > 10 mil euro

Annex II • Postal and courier services • Waste management • Chemicals • Food • Manufacturing • Digital providers • Research

Also in scope

- **In scope regardless of the enterprise size (Article 21)**

- The providers of public electronic communications networks or of publicly available electronic communications services
- Trust service providers (electronic signature)
- Top domain name administrators and domain name system providers
- The entity is the only provider in a Member State of a service essential for the maintenance of critical societal or economic activities
- A disruption to the service provided by the entity could have a significant impact on public safety or public health
- A disruption of the service provided by the unit could lead to a significant systemic cross-border risk
- The unit is critical due to its specific importance at national or regional level for the sector/type of service/other interdependent sectors concerned
- The entity is a public administration unit under central administration as defined by a Member State or at regional level which could have a significant impact on critical societal or economic activities if disrupted
- The entities identified as critical according to Directive (EU) 2022/2557 (CER Directive)
- Entities that provide domain name registration services
- **Entities that Member States will have decided to when transposing the NIS2 Directive into national laws** (e.g. education, research and local public administration units etc)

Exceptions

10.

- **Exceptions (Article 2 paragraphs 7 and 8)**

  NIS2 does not apply to public administration entities that carry out their activities in the areas of national security, public security, defense or law enforcement, including the prevention, investigation, detection and prosecution of criminal offences.

  Member States may exempt specific entities which carry out activities in the areas of national security, public security, defense or law enforcement, including the prevention, investigation, detection and prosecution of criminal offences, or which provide services exclusively to the public administration entities

- **Other exceptions (Article 3 paragraph 3)**

  List the entities and activities considered not considered to be operators of essential services therefore not in scope based on nature of the entity, services and location criteria.

11.

Clarity on NIS2 requirements

▪ Governance (Article 20)

Management approves the cybersecurity risk management measures taken to comply, oversee its implementation and can be held liable for infringements.
Training is mandated for management as well as employees on regular basis.

▪ Cybersecurity risk-management measures (Article 21)

(…) entities take appropriate and proportionate technical, operational and organizational measures to manage the risks (…) and to prevent or minimize the impact of incidents on recipients of their services (…)
Considering the state-of-the-art and, where applicable, relevant European and international standards, cost of implementation, the measures shall ensure an appropriate level of security of network and information systems to the risks posed.
All-hazards approach and undue delay that shall include at least:

- risk analysis and information system security-incident handling
- business continuity, such as backup management and disaster recovery, and crisis management
- *supply chain security, including security-related aspects concerning the relationships between each entity and its direct suppliers or service providers
- security in network and information systems acquisition, development, and maintenance, including vulnerability handling and disclosure
- policies and procedures to assess the effectiveness of cybersecurity risk-management measures
- basic cyber hygiene practices and cybersecurity training
- use of cryptography and, where appropriate, encryption
- human resources security, access control policies and asset management
- the use of multi-factor authentication or continuous authentication solutions, secured voice, video and text communications and secured emergency communication systems within the entity, where appropriate

*remember to consider the coordinated security risk assessments of specific critical ICT services, ICT systems or ICT products supply chains Article 22(1)

- **Reporting obligation (Article 23)**

  Early warning within 24 hours of detection of a significant incident or potential harm (potential significant damage or disruption of services or financial loss)

- **Supervisory and enforcement modalities (Article 32)**

  Don’t worry, it’s coming up next - too important not to have a slide of its own.

14.

Supervisory and enforcement measures (and fines)

Measures (Article 32)

The competent authorities have the power to impose effective, proportionate, and dissuasive supervisory or enforcement measures, considering the circumstances of each individual case:
- on-site inspections and off-site supervision, including random checks
- regular and targeted security audits
- justified ad hoc audits (significant incident or an infringement of this Directive)
- security scans
- requests for information to assess the cybersecurity risk-management measures adopted including other documentation
- requests to access data, documents, and information
- requests for evidence of implementation of cybersecurity policies, (ex. results of security audits carried out by a qualified auditor and the respective underlying evidence)

Other measures

- issue warnings about infringements
- order the entities concerned to cease conduct that infringes this Directive
- order the entities concerned to ensure that their cybersecurity risk-management measures comply with Article 21 or 23 under time constrain and in a specific manner
- order the entities concerned to implement the recommendations provided as a result of a security audit within a reasonable deadline
- designate a monitoring officer with well-defined tasks for a determined period to oversee the compliance.

If enforcement measures are ineffective

Impose an administrative fine
Set a deadline to remedy the deficiencies or to comply with the requirements.

If the company fails, then temporary suspension of a certification or authorization concerning part, or all the relevant services will be imposed, and a court of law will be requested to discharge managerial responsibilities at CEO or legal representative level from exercising managerial functions in that company.

Penalties and fines

- 10mil euro or min 2% of the annual global turnover of the company the entity at fault belongs to (for essential entities)

- 7mil euro or min 1.4% of the annual turnover of the company the entity at fault belongs to, whichever is higher (for important entities)

Implementing NIS 2 Directive: A Practical Approach

- **Overall Assessment**

  Start by assessing whether your organization is in scope for NIS2 or not – MSB already have additional clarifying guidelines.

  Determine the scope of the compliance and what are the gaps towards NIS2 Directive that must be addressed in order to acquire compliance.

- **Management commitment and support to secure the funding for cybersecurity**

  We all agree this doesn’t require additional explanation, right?

Plan

Do

Check

Act

Plan
Establish the NIS2 Compliance Framework

- **Gap analysis**

  Assess the current and the targeted maturity level of the organization, existing systems and processes, in-house competence, and knowledge and cybersecurity measures against the NIS 2 requirements and identify areas that need improvement to achieve compliance.

- **Risk assessment**

  Conduct a detailed risk assessment to understand where your organization is most vulnerable to cybersecurity threats in the context of NIS2.

- **Deadlines and Speed of implementation**

  Start early and plan carefully. Allow room for delays. Certain tasks take more time than initially planned.

- **Other applicable laws and regulations, authorities**

  Industry sectors specific regulations applicable, engage with relevant authorities and cooperate with them

- **Create a NIS2 compliance framework and the NIS2 Implementation Plan**

  Develop a comprehensive compliance plan, detailing the actions needed to meet each requirement of the NIS2 Directive. The plan should include budget, timelines, responsibilities, and metrics for success.

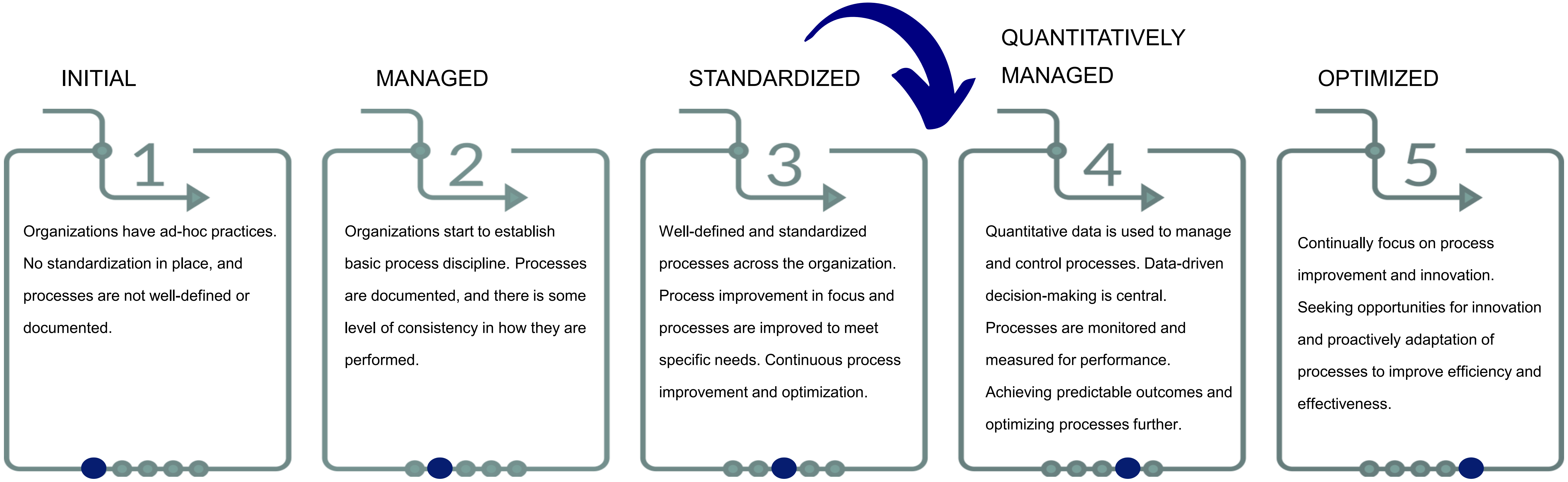
Targeted maturity level

Level 3: Defined (NIS2 Compliance)

Standardized documentation and processes
NIS2 Framework is integrated in existing ISMS (or other frameworks)
Cybersecurity training and awareness are in place
NIS2 compliance is monitored and measured

Level 4: Quantitatively Managed (NIS2 Compliance)

Quantitative data is collected and used by management to take informed decisions and improve the organization's cybersecurity posture.
Continuous improvement is happening as NIS2 framework is regularly reviewed and updated.
Risk management process is aligned with NIS2 requirements.
Automation and optimization in place
Incident Management is mature, has well defined procedures and response times and lessons learned are shared.



INITIAL

1

Organizations have ad-hoc practices. No standardization in place, and processes are not well-defined or documented.

MANAGED

2

Organizations start to establish basic process discipline. Processes are documented, and there is some level of consistency in how they are performed.

STANDARDIZED

3

Well-defined and standardized processes across the organization. Process improvement in focus and processes are improved to meet specific needs. Continuous process improvement and optimization.

QUANTITATIVELY MANAGED

4

Quantitative data is used to manage and control processes. Data-driven decision-making is central. Processes are monitored and measured for performance. Achieving predictable outcomes and optimizing processes further.

OPTIMIZED

5

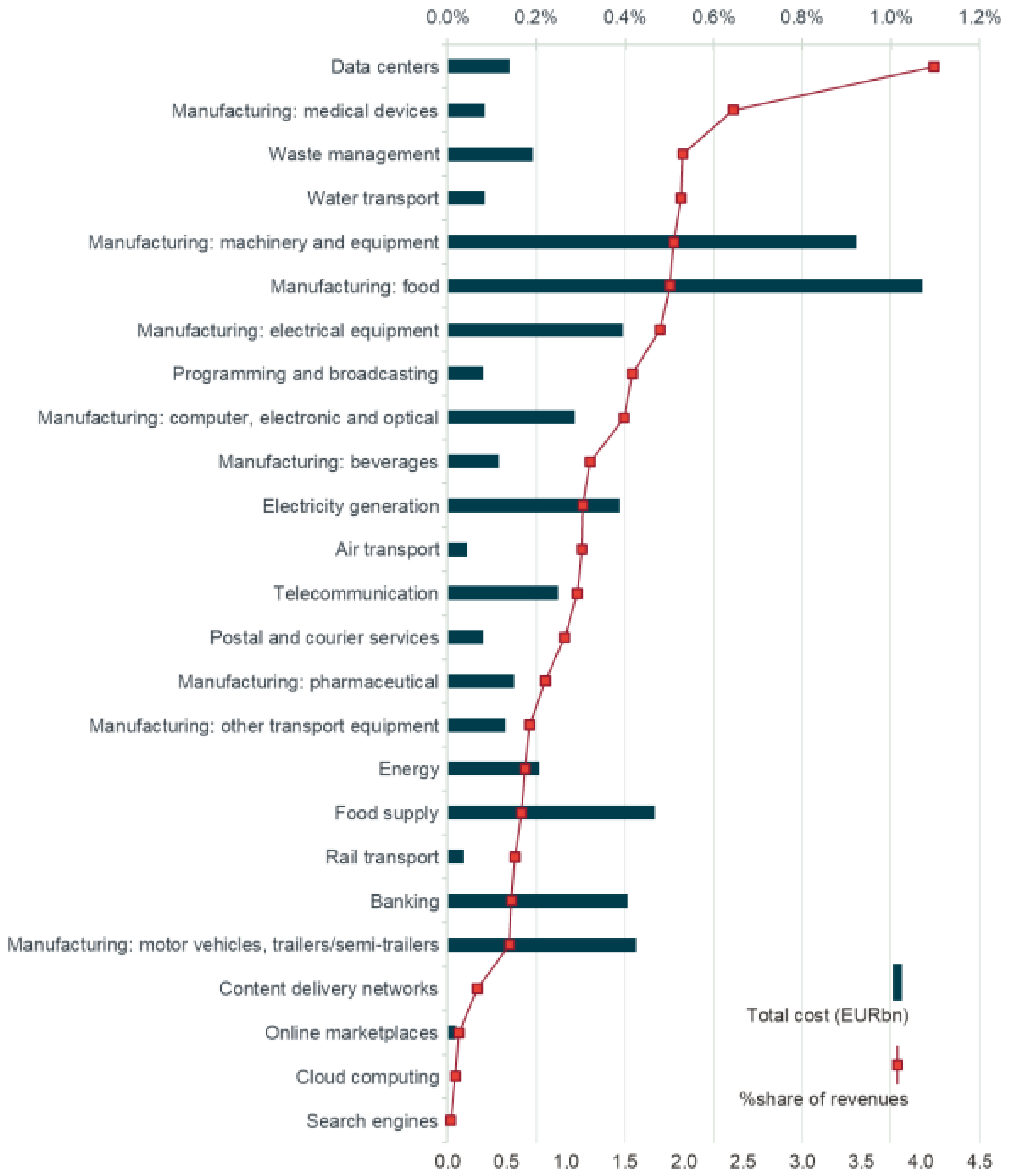
Continually focus on process improvement and innovation. Seeking opportunities for innovation and proactively adaptation of processes to improve efficiency and effectiveness.

Cost Implications

Money, money, money

Target security maturity level, risk treatment plans and other measures to close the gaps and achieve NIS2 compliance will impact the cost of NIS2 compliance Cost associated with the resources required for the compliance project: required competence, technology and tools will also need to be considered

Source [*Frontier Economics*]



Source: Frontier Economics

Note: Small business have <50 employees; Medium businesses have between 50 and 249 employees; Large and very large businesses have more than 250 employees

Do

Implementing the compliance measures

- **Security measures/controls**

  Implement security measures to close gaps and security controls to mitigate cybersecurity risks

- **Update policies and procedures**

  Revise or develop new policies and procedures to align with the NIS2 requirements.

- **Perform supply chain risk assessments**

  Assess the security of your supply chain and establish appropriate third-party risk management procedures.

- **Training and Awareness**

  Roll out training programs to ensure all employees understand their role in compliance and the importance of cybersecurity. Do not forget to train the management

- **Technology Deployment**

  Implement any necessary technologies or security measures that support compliance efforts.

- **Engage with authorities**

  Engage proactively with relevant authorities and cooperate with them as required by the directive. This includes reporting incidents and assisting, assisting with investigations if necessary.

- **Process development, revision and adjustments**

  Adjust existing processes or implement new ones to fulfill the compliance objectives set in the planning phase.

  Develop or enhance your business continuity and disaster recovery plans.

  Streamline incident reporting and enhance incident management procedures

24.

Check

Monitoring and reviewing compliance progress

- **Monitor cybersecurity controls**

  Regularly monitor and evaluate the implemented cybersecurity controls against the NIS2 aligned metrics to ensure they are functioning as intended.

- **Compliance auditing**

  Regularly assess compliance to NIS2 requirements to assess the effectiveness of the NIS2 compliance program, either internally or with external auditors.

- **Performance measurement**

  Measure the effectiveness of the processes (Security Incident Management process, Crisis Management, BCM etc) using the metrics defined in the planning phase

- **Reporting**

  Create compliance boards that document the outcomes of the audits and performance measurements and present them to relevant stakeholders.
  Identify trends and patterns in compliance data to identify areas for improvement.

26.

Act

Taking corrective actions

- **Review Findings**

  Review the results from the 'Check' phase to identify areas that need improvement.

- **Continuous Improvement**

  Apply lessons learned to refine policies, training, and processes. Ensure that the organization is not only compliant but also maintains an adaptive stance to emerging threats and changing requirements.

- **Update Documentation**

  Update all compliance documentation to reflect the changes made during the 'Act' phase.

- **Stakeholder Communication**

  Communicate any changes and improvements to internal and external stakeholders to demonstrate ongoing commitment to compliance

Repeat

29. How we can support

NIS2 Implementation Training

Audience

By providing training to a diverse range of stakeholders, NIS2 Implementation training can help organizations achieve a comprehensive understanding of NIS2 requirements and ensure that all relevant personnel are equipped to implement and maintain a compliant cybersecurity posture:

- Cybersecurity and IT professionals (Security Managers and Officers)
- Executives and senior management
- Compliance officers
- IT procurement and supply chain personnel
- HR professionals

Delivery methods

The modalities for delivering NIS2 Implementation training can vary depending on the specific needs of the organization and the target audience: in-person, online and blended training.

Training content

The training is crafted onto the P-D-C-A model and consists of practical deep dives in the “at least” elements marked as mandatory by the Directive: Risk Management, BCM, Supply chain management, Human resource security, security in network and information systems acquisition, development, and maintenance, including vulnerability handling and disclosure, MFA, encryption etc

For more details, please contact us.

NIS2 Implementation Support

- ## NIS2 Consulting Services

At Infinity, we provide tailored support to companies required to implement NIS2 requirements and demonstrate compliance to the Directive.

- ## NIS2 Preliminary Assessment

Comprehensive evaluation of an organization's cybersecurity posture against the requirements of the NIS2 Directive. It provides a baseline understanding of the company’s current cybersecurity practices, identifies gaps between the organization's current state and NIS2 compliance, and recommends a roadmap for implementation.

- ## NIS2 Implementation support

Ongoing engagement that provides dedicated support to customer’s NIS2 implementation team. This support encompasses tailored trainings, guidance, and hands-on assistance to ensure a smooth and successful transition to NIS2 compliance.

- ## Post-implementation NIS2 framework validation

Comprehensive evaluation of an organization's NIS2 compliance posture after the completion of the implementation project. It involves a thorough review of all NIS2 implementation documentation, processes, procedures, and systems to ensure that the organization is fully compliant with all NIS2 requirements.

Questions & Answers

What is the difference between Dora and NIS2?

There are many differences but here are some mentioned below:

- NIS2 is a Directive and DORA is a Regulation, meaning that in Directives the EU aims to achieve specific goals and results and the Member States must adjust the national laws to fulfill the Directive requirements. The Regulation becomes law immediately, and Member States are required to apply it as is.
- DORA is “lex specialis” for NIS2
- Different objectives: cybersecurity across EU vs operational resilience for financial sector.
- NIS2 emphasizes supply chain security, whereas DORA focuses on third-party risk management.
- Financial penalties are heavy and quantified for NIS2. DORA leaves the Member states to decide upon.

I work in a bank/insurance company. What applies to my organization, NIS2 or DORA?

If your organization is in scop of DORA, then it prevails over NIS2. DORA is “lex specialis” of NIS2 for the financial sector.

Thank you!

For questions
email us at
info@infinityitc.se
bianca.ioana@infinityitc.se

You are welcome to call us at
(0046)706181313.

or visit us on Luxgatan 10,
Stockholm.