NAVIGATING THE NIS 2 DIRECTIVE: STRENGTHENING CYBER RESILIENCE

Honeywell

TABLE OF CONTENTS

INTRODUCTION

Amid the digital revolution, efficiencies emerge alongside unprecedented risks. Interconnected infrastructures face escalating cyber threats, necessitating regulation to counteract them. Regulations establish security standards, foster awareness and help improve effective defense mechanisms. Compliance can help ensure adherence to best practices, reduce breach risks and promote a culture of security. It also can help establish protocols for incident response and minimize impact.

The European Union's Network and Information Security Directive (NIS Directive or NIS-D) (Directive (EU) 2016/1148) was passed into law in 2018,[1] with the aim to harmonize cybersecurity efforts across European Union member states, focusing on critical infrastructure sectors. In 2023, the EU updated its cybersecurity legislation with the NIS 2 Directive (Directive (EU) 2022/2555), elevating cybersecurity standards and expanding the sectors covered, as outlined in Illustration-1.

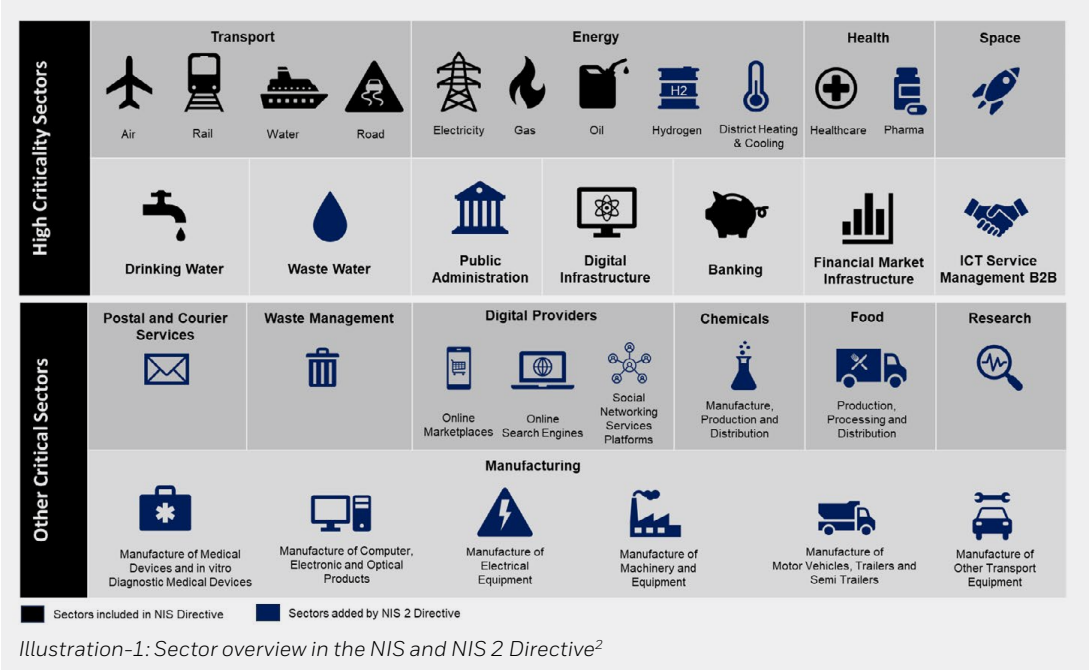


Illustration-1: Sector overview in the NIS and NIS 2 Directive[2]

This whitepaper explores the NIS 2 Directive and its operational technology (OT) aspects, providing insights into its objectives, provisions and implications for stakeholders. It aims to foster understanding and protection of Europe's digital ecosystem. Robust cybersecurity measures are essential for embracing digital transformation and realizing its benefits. NIS 2 signifies the European Union's effort to enhance its cybersecurity framework in response to evolving digital challenges.

1. Security of Network and Information Systems Targeted consultation on Digital Service Providers, March 2018, Paragraph 2, https://assets.publishing.service.gov.uk/media/605e473cd3bf7f7184489500/DSP_Targeted_Consultation__Final__V2.pdf
2. Source (and amendments introduced by Honeywell): https://www.wavestone.com/en/insight/Directive-nis-2-cybersecurity-impact-european-companies/

ENHANCED CYBERSECURITY IN THE EU: UNPACKING THE CHANGES IN THE NIS 2 DIRECTIVE

The NIS 2 Directive represents a significant step forward in enhancing cybersecurity, particularly for OT systems across the European Union. Its comprehensive approach addresses the unique challenges and vulnerabilities associated with OT environments, which are integral to the functioning of critical infrastructure sectors.

Important changes and additions to the NIS 2 Directive include:

1. **Expanded Scope:** Unlike its predecessor, the NIS Directive, NIS 2 extends its reach to include additional sectors like waste management, postal services and public administration alongside traditional sectors such as energy and transport. This broadened scope provides a more inclusive and protective cybersecurity framework across essential services that rely on OT systems.
2. **Increased Importance of OT Security:** Given OT systems' pivotal role in critical infrastructure, NIS 2 emphasizes improving security for these systems against cyber threats. The interconnectedness and digitalization of OT environments heightens their vulnerability, making them potential targets for cyber attacks that could disrupt vital services.
3. **Economic and Safety Implications:** The updated NIS 2 Directive recognizes the severe economic and public safety consequences of cyber attacks on industrial systems. By enforcing stringent cybersecurity measures, NIS 2 aims to mitigate these risks, helping to better protect the economic stability and the public welfare of EU member states.
4. **Enhanced Cybersecurity Requirements:** NIS 2 sets a higher standard for cybersecurity practices, urging organizations within its purview to adopt comprehensive measures that address various aspects of cybersecurity, from governance to incident response and business continuity.
5. **Inclusion of SMEs:** Acknowledging the role small and medium enterprises (SMEs) play in the European economy, NIS 2 includes provisions that cater to these entities, recognizing their vulnerabilities and offering frameworks to bolster their cybersecurity defenses.
6. **All-Hazard Approach[3]:** The updated NIS 2 Directive advocates for an all-encompassing strategy for cybersecurity, urging organizations to consider a wide array of risks and vulnerabilities. This holistic approach is designed to foster a more resilient and robust cybersecurity posture across the board.
7. **Compliance and International Cooperation:** Compliance with NIS 2 is mandatory for designated entities, and also aims to facilitate international cooperation to help address cross-border cyber threats effectively. This is crucial in the context of the globalized nature of cyber threats and the interconnectedness of digital infrastructure.

In summary, the NIS 2 Directive is a pivotal piece of legislation that underscores the EU's commitment to enhancing cybersecurity, particularly for OT systems within critical infrastructure sectors. It establishes a new benchmark for cybersecurity, urging entities across various sectors to adopt proactive and comprehensive measures to protect against the evolving landscape of cyber threats.

3. Source: Art. 21.2 NIS-2, cybersecurity risk-management measures.

NIS 2: ENTITY CLASSIFICATION AND KEY REQUIREMENTS

The NIS 2 Directive broadens the range of entities subject to cybersecurity obligations, including more companies and organizations based on their size and the sector in which they operate.

The NIS 2 Directive also provides flexibility and allows each EU member state to adopt the classification of entities through its own laws. Importantly, national cybersecurity authorities (NCAs) in each country will be at the forefront, applying the Directive and determining the classification of entities to ensure a tailored and effective approach to cybersecurity across the EU.

Entities are categorized based on their criticality and assigned different compliance requirements to each category. Large and medium-sized organizations, as well as other entities from sectors specified in Annex I or II of the NIS 2 Directive, that offer services or conduct operations within the EU (as outlined in Article 3(1) of the NIS 2 Directive[4]), are encompassed by the scope of the NIS 2 Directive.

The operator of essential services (OES) will be expanded in the NIS 2 Directive along with the relevant sectors listed in Illustration-2, with new sectors that have been added since the NIS Directive highlighted in bold.

Entities Impacted by Size and Sector[6]

Some entities are covered by the NIS 2 Directive irrespective of their size, particularly if they play a pivotal role in communication and trust services or are sole providers of essential services within EU member states. This includes:

- Public electronic communications network providers
- Trust service providers
- Domain name system (DNS) service providers (a reference to Article 6 No. 20 of the NIS 2 Directive)
- Entities essential for maintaining critical social or economic activities
- Providers whose service disruption could significantly impact public safety or create systemic risks

Other entities must adhere to the following criteria if they offer services or conduct activities within the European Union:

- Large and Medium-Sized Entities: Companies or organizations operating in the EU and in sectors (as listed in Annex I or II of the NIS 2 Directive) are subject to the Directive as stated in EU[7] (Article 3(1) of the NIS 2 Directive). These sectors include energy, transport, banking, healthcare, digital infrastructure and more, with specific sectors being newly added under the NIS 2 Directive.
- Sectors of Critical Importance: Entities in sectors deemed highly critical, such as energy and transport, are particularly focused on. Other sectors, while still important, have a different set of criteria and implications under the Directive.

ANNEX - I
ESSENTIAL ENTITY
(Sectors of high criticality)

	Large Entities (>= 250 employees or more than €50 M in revenues)	Medium Entities (50-249 employees or more than €10 M in revenues)	Smal/Micro Entities
Energy	**Essential**	**Important**	**Not in Scope**
Transport	Essential	**Important**	Not in Scope
Banking	Essential	**Important**	Not in Scope
Financial Market Infrastructure	Essential	**Important**	Not in Scope
Health	**Essential**	**Important**	**Not in Scope**
Drinking Water	Essential	Important	Not in Scope
Waste Water	**Essential**	**Important**	**Not in Scope**
Digital Infrastructure	Essential	Essential	Essential
ICT Service Management (B2B)	**Essential**	**Important**	**Important**
Public Administration Entities	Essential	Essential	Essential
Space	**Essential**	**Important**	**Not in Scope**

ANNEX - II
(Other critical sectors)

	Large Entities (>= 250 employees or more than €50 M in revenues)	Medium Entities (50-249 employees or more than €10 M in revenues)	Smal/Micro Entities
Postal and Courier Services	**Important**	**Important**	**Not in Scope**
Waste Management	**Important**	**Important**	**Not in Scope**
Chemicals	**Important**	**Important**	**Not in Scope**
Food	**Important**	**Important**	**Not in Scope**
Manufacturing	**Important**	**Important**	**Not in Scope**
Digital Providers	**Important**	**Important**	**Not in Scope**
Research	**Important**	**Important**	**Not in Scope**
Entities Providing Domain Name Registration Services	**All sizes, but only subject to Article 3(3) and Article 28**		

Newly Added Sectors in NIS 2 Directive (Bolded)

Reference: Sectors listed in Annex-1 or II that provide their services or carry out their activities in the EU (Article 3 (1) of the NIS 2 Directive

Illustration-2: NIS 2 scope covered by two annexes for public and private entities[5]

4. Source: Article 3(1) of the NIS 2 Directive, https://eur-lex.europa.eu/eli/dir/2022/2555
5. Source: www.ncsc.gov.ie, NCSC, National Cyber Security Centre, paper NIS 2 Essential and Important Entities, https://www.ncsc.gov.ie/pdfs/NCSC_NIS2_2_ENTITIES.pdf
6. Source: The NIS 2 Directive categorizes entities into size classes based on Article 2 of the Annex to Recommendation 2003/361/EC, setting specific thresholds to define its application scope

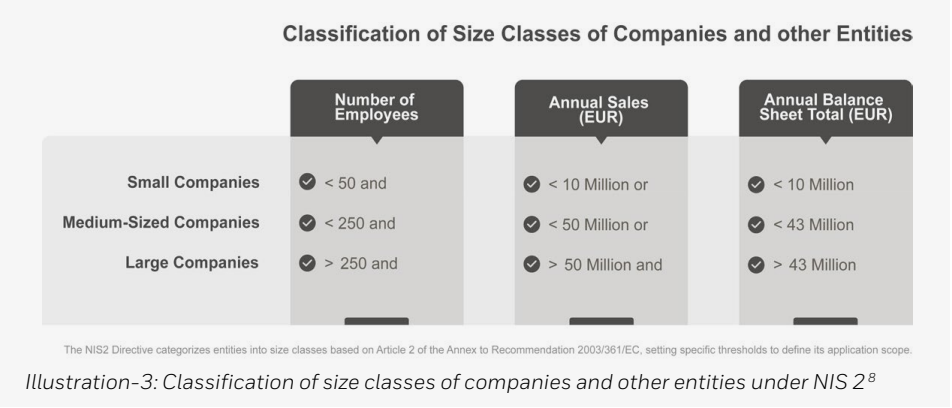


Illustration-3: Classification of size classes of companies and other entities under NIS 2[8]

Impact on Supply Chain and Small Entities

The NIS 2 Directive introduces significant changes in cybersecurity with a shift toward a more integrated and holistic approach. Implementing these measures requires careful planning, ample resources and continuous adaptation to meet evolving standards and assessments. Businesses must actively engage with these processes to ensure compliance and protect their operational integrity against emerging cyber threats. While primarily targeting larger entities, the NIS 2 Directive indirectly affects smaller companies through supply chain requirements.

As stated in Article 21 (3) of the NIS 2 Directive, service providers and suppliers to larger entities must adhere to cybersecurity measures, ensuring the security of the entire supply chain. The NIS 2 Directive notably influences how organizations approach and manage supply chain security as part of a comprehensive strategy to enhance cybersecurity across the European Union and its affiliated regions. By ensuring robust security practices at every stage of the supply chain, the Directive aims to create a unified cybersecurity front, enhancing protection against potential disruptions and threats originating from less secure elements in the supply chain.

The NIS 2 Directive introduces several mechanisms to enhance supply chain security, which include:

1. **Coordinated Risk Assessment:** This is an EU-level procedure aimed at assessing the risk associated with specific supply chains. This assessment involves the Cooperation Group, European Union Agency for Cybersecurity (ENISA) and the European Commission and may include consultations with stakeholders. This comprehensive assessment evaluates technical and non-technical factors impacting supply chain security, such as dependence on a single supplier, the critical nature of the supply services and undue influence by third-party countries.
2. **National Risk Assessment:** This mechanism allows member states to extend the scope of the Directive to include entities that might not initially be covered but are crucial for national security or economic stability. This flexible approach ensures that national authorities can address emerging threats or vulnerabilities specific to their region.
3. **Internal Risk Assessment:** Entities are required to conduct their own risk assessments focusing on direct suppliers and service providers. This includes evaluating the cybersecurity practices and products of suppliers and considering their secure development processes.

The practical implementation of the NIS 2 Directive poses multiple challenges for organizations, especially those with limited resources or existing systems. Smaller entities may find it particularly difficult to comply with the rigorous demands of conducting internal and coordinated risk assessments. Furthermore, the complexity of involving multiple stakeholders in these assessments can make consensus and thorough evaluations challenging. Variability in compliance and enforcement across EU member states adds another layer of complexity, as they have the authority to tailor the Directive's scope and conduct national assessments. This leads to inconsistent requirements that complicate efforts for multinational corporations.

Additionally, integrating new Directives with existing security frameworks may require significant adjustments, especially for those that previously placed less emphasis on supply chain security. Strategically, it is crucial for businesses to stay abreast of assessment progress and adapt their security measures to align with EU-wide and national risk assessments, ensuring compliance and avoiding potential financial penalties. This proactive approach to managing and mitigating supply chain risks is essential to maintain operational integrity in the face of evolving cyber threats.

8. Source: Article 2 of the Annex to Recommendation 2003/361EC, https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32003H0361

Classification of Entities

The NIS 2 Directive's Article 3[9] introduces a pivotal framework for classifying entities into "Essential" and "Important" categories, underscoring a nuanced approach to cybersecurity across various sectors. This classification is instrumental in customizing cybersecurity measures, ensuring they are proportionate to different organizations' roles and potential impacts on the EU's collective cyber resilience.

Whether a company or other entity is deemed essential or important under the NIS 2 Directive does not affect the required obligations and measures they must implement. However, the classification does influence the potential regulatory actions and the risk of sanctions for failing to comply with the NIS 2 Directive (see Illustration 4). It is paramount to note the significant difference in the supervision regimes between the two categories: essential entities are subject to proactive supervision, while important entities are supervised only ex-post, meaning after an incident has occurred. This distinction in supervision regimes underscores the varied regulatory scrutiny and response mechanisms based on the classification under the NIS 2 Directive.

"Essential entities" and "important entities" are what the NIS 2 Directive calls companies and other organizations that must comply with NIS 2.

1. **Essential Entities[10]:** These entities are the linchpins in maintaining vital societal and economic functions. Any disruption in their services could severely impact public safety, security, economic stability and health. The sectors that typically house these essential entities include, but are not limited to, energy, transportation, banking, health and digital infrastructure.

2. **Important Entities[11]:** These are entities that, while not as critical as essential ones, still play a vital role in the socio-economic fabric. Disruptions in their operations would have significant, albeit less catastrophic, consequences. Sectors under this category often include postal and courier services, waste management and food production.

Illustration-4: Entity classification and key requirements table under NIS 2.

OPERATIONAL TECHNOLOGY IN NIS 2

While operational technology (OT) is not explicitly mentioned in the Directive, due to the coverage of industries and the definition of network and information systems outlined in Article 6 (DIRECTIVE (EU) 2022/2555), distributed control systems (DCS) such as Honeywell's Experion PKS® fall under the scope, along with any communication used by third-party systems.

This classification scheme under the NIS 2 Directive provides a targeted and tiered approach to cybersecurity, aligning the level of regulatory scrutiny and obligation with the degree of risk and potential impact an entity has on the EU's collective security and economic stability. It reflects an astute understanding that, while all sectors are integral to the digital ecosystem, the level of criticality and the potential fallout from cyber incidents vary, necessitating a differentiated approach to protecting Europe's cyber and economic landscape.

New Obligations for Affected Entities

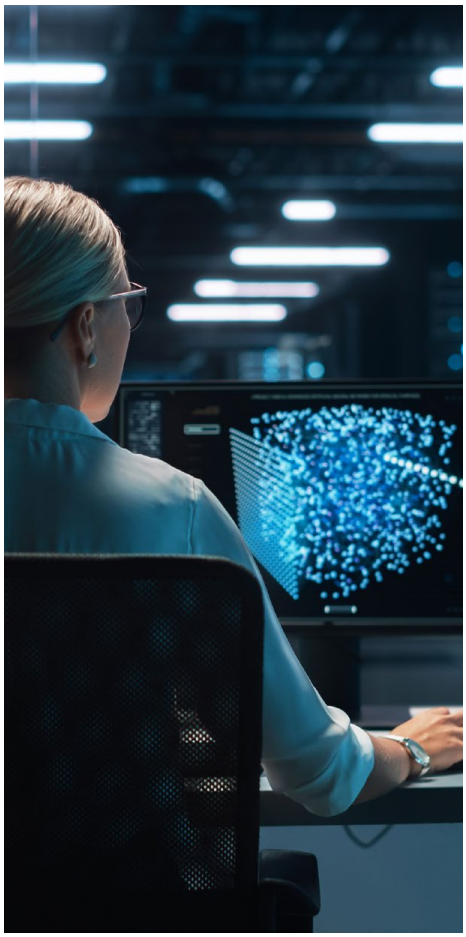
Entities impacted by the NIS 2 Directive must meet enhanced cybersecurity obligations, including risk management practices, incident reporting and compliance with national cybersecurity Directives. They are required to implement effective security measures, report significant cyber incidents and comply with stricter regulatory oversight to ensure a high level of cybersecurity across the EU.

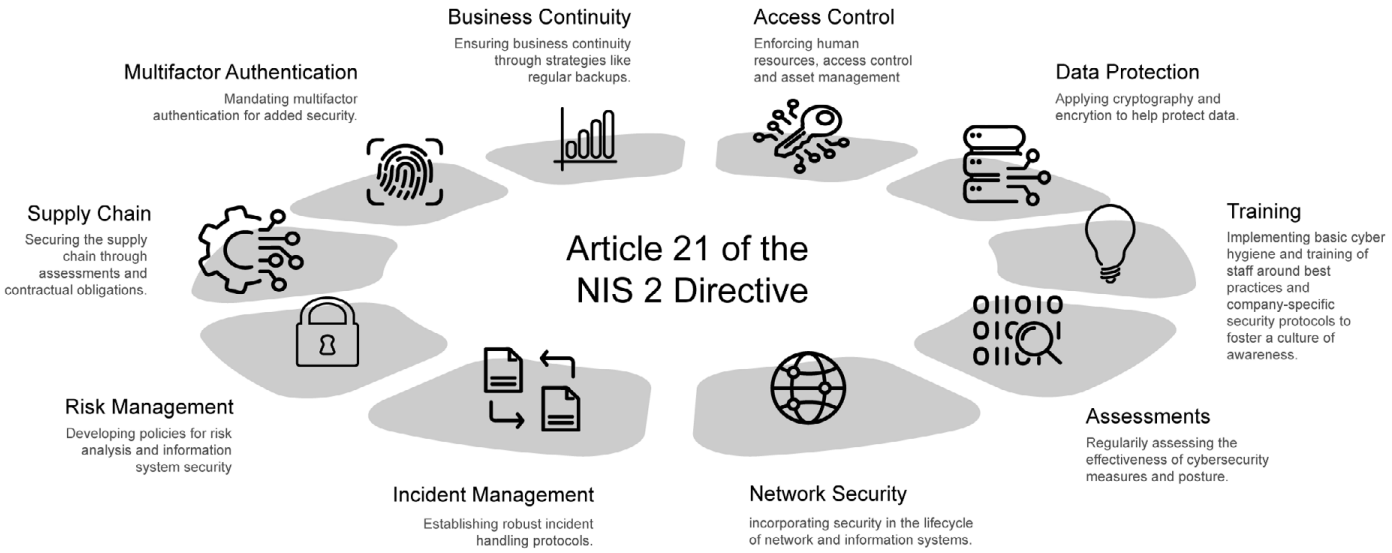
9. Source: Official Journal of the European Union as Directive (EU) 2022/2555, Article 3, Scope, https://eur-lex.europa.eu/eli/dir/2022/2555.
10. Source: Article 2, para. 1, sentence 2, NIS 2 together with Article 2, para. 2 in Annex to Commission Recommendation, 2003/361/EC of 6 May 2003, OJ L 124, 20.05.2003, p.36.
11. Source: Preamble, 121-130, https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX%3A32022L2555.

Article 21 of the NIS 2 Directive mandates essential and important entities in EU member states to implement specific risk management measures to strengthen cybersecurity. These measures, varying based on the national context and organizational specifics, include:

1. Developing policies for risk analysis and information system security.
2. Establishing robust incident-handling protocols.
3. Ensuring business continuity through strategies like regular backups.
4. Securing the supply chain through assessments and contractual obligations.
5. Incorporating security in the lifecycle of network and information systems.
6. Regularly assessing the effectiveness of cybersecurity measures.
7. Implementing basic cyber hygiene and training for staff.
8. Applying cryptography and encryption to help protect data.
9. Enforcing human resources, access control and asset management policies.
10. Mandating multifactor authentication for added security.

These measures are part of the framework to prepare organizations for compliance with the NIS 2 Directive before its transposition into national law by 17 October 2024.





A HOLISTIC APPROACH TO INDUSTRIAL CYBERSECURITY

The NIS 2 Directive signifies a pivotal shift in cybersecurity strategy, emphasizing a holistic approach for entities deemed "Essential" and "Important."

This strategy, grounded in both policy and technology, focuses on:

- Governance
- Risk management
- Incident detection and response
- Reporting obligations.

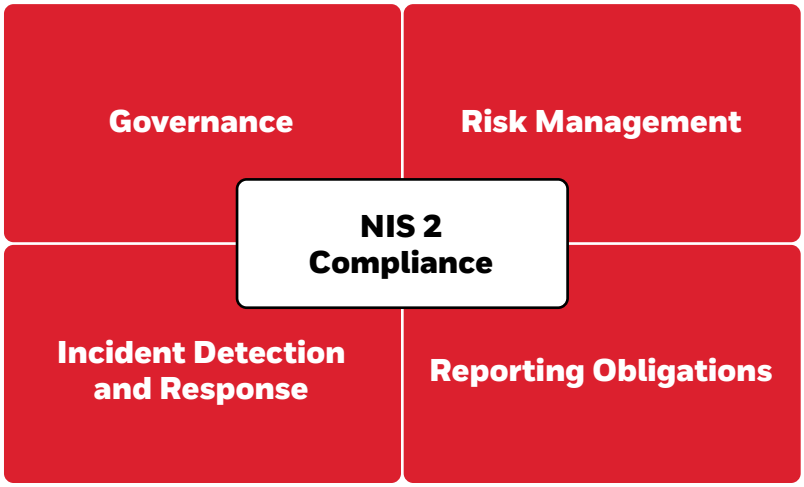


Illustration-5: Policy and technology strategy framework for cybersecurity.

Governance

Governance, as outlined in Article 20 Governance, **Directive (EU) 2022/2555 (NIS 2 Directive)**, involves the implementation of risk management measures and the accountability of entities for any infringements. Training is integral to governance, ensuring employees gain sufficient knowledge and skills to identify and assess cybersecurity risk and impact.

Article 20 of the NIS 2 Directive establishes a comprehensive framework to ensure that entities critical to cybersecurity maintain stringent governance standards. It emphasizes the accountability of management bodies, mandating their active involvement in approving and overseeing cybersecurity risk management measures. This aligns with the Directive's broader goal of strengthening cybersecurity resilience through top-down commitment.

The Directive also prioritizes continuous learning and skill development, requiring management body members and employees to undergo regular training. This initiative aims to build a workforce adept at identifying and mitigating cybersecurity risks, enhancing the entity's defensive posture.

Significantly, the NIS 2 Directive elevates the role of Chief Information Security Officers (CISOs), transforming them from advisors to key players in strategic decision-making related to cybersecurity. They are now instrumental in implementing security practices and educating senior management on cybersecurity risks and strategies.

Furthermore, the Directive underscores the importance of governance and risk management, advocating for a culture where cybersecurity is a fundamental concern across all organizational levels. This approach facilitates a systematic risk identification, assessment and mitigation process, ensuring a robust defense mechanism.

Legal and regulatory compliance is another critical aspect, with entities facing liability for non-compliance. This legal structure underscores the imperative of complying with established cybersecurity measures, highlighting the severe consequences of lapses.

Ultimately, the Directive aims to protect the services these entities provide, minimizing the risk of disruptions that could have broader societal and economic impacts. In summary, Article 20 of the NIS 2 Directive adopts a holistic strategy to help enhance cybersecurity, emphasizing governance, accountability and continuous learning as key pillars in building a resilient cybersecurity framework, aligning with global trends that integrate cybersecurity into the strategic core of vital organizations.

12. Source: Article 20 Governance, Directive (EU) 2022/2555 (NIS 2 Directive), https://eur-lex.europa.eu/eli/dir/2022/2555.

Risk Management, Incident Detection and Response

Cybersecurity risk management, as outlined in Article 21.2 NIS 2, cybersecurity risk-management measures, is a critical area addressed by the NIS 2 Directive, encompassing the following key components:

1. **Policies on Risk Management and Information System Security:** Organizations must develop robust risk management and information system security policies, particularly for OT systems. Such policies are vital administrative controls that shape the organization's cybersecurity strategies and show adherence to pertinent regulations and standards. When supported by the right technology, these policies can help improve security for OT systems against cyber threats. Therefore, organizations must create detailed policies addressing their unique needs and risk profiles.
2. **Incident Management:**[13] Effective management and mitigation of cyber incidents require thorough preparedness. Organizations benefit from having skilled cybersecurity professionals who can comprehend, contain and reduce the damage from such incidents. Tabletop Exercise services can help test and enhance an organization's readiness for cyber incidents. Through simulations of realistic cyber scenarios, organizations can evaluate their response strategies, pinpoint improvement areas and improve their incident-handling processes.

MANDATED RISK MANAGEMENT

All entities must conduct **regular risk assessments** and implement suitable cybersecurity measures.

3. **Business Continuity:** Business impact analysis and risk assessment are critical components of business continuity planning and disaster recovery, aiming to enhance operational resilience.
4. **Supply Chain Security:** With systems supplied and connected globally, the security of OT assets is paramount. NIS 2 requires the implementation of security measures for third-party vendors and suppliers, recognizing the crucial interconnected nature of the supply chain in protecting critical infrastructure.
5. **Security in Network and Information Systems Acquisition:** This area encompasses security in acquisition, development and maintenance, including vulnerability handling and disclosure.
6. **Policies and Procedures to Assess Effectiveness:** Periodic reviews of an organization's relevant cybersecurity policies and procedures help ensure that those policies and procedures remain relevant to evolving challenges.
7. **Basic Cyber Hygiene Practices and Training:** Training in cybersecurity, particularly in OT, is crucial for enhancing organizational security.

INCIDENT MANAGEMENT

Essential Entities:

- Should report not only actual incidents but also near misses and attempted incidents.
- A 24/7 dedicated contact for incident reporting is mandatory.
- Regular penetration testing may be required, with results reported to the relevant authority.
- Subject to higher fines for non-compliance than important entities.

Important Entities:

- Must report significant incidents to the CSIRT or the competent authority in the form of an early warning, an incident report, an interim report, an intermediate report or a final report.
- Depending on the country's specific rules, a dedicated contact for incident reporting might not be necessary.
- Penetration testing and its reporting could be less frequent or not mandatory.
- Incur lower fines for non-compliance compared to essential entities.

13. Source: Honeywell interpretation leaning on Preamble 86-87, https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX%3A32022L255512.

It includes learning fundamental cyber hygiene practices and may extend to advanced techniques like penetration testing. This training aims to equip personnel with the necessary skills to incorporate cybersecurity measures into their daily operations, fostering a culture of vigilance and proactive security within the organization.

8. **Cryptography and Encryption:** Cryptography and encryption are vital for securing the data exchange between systems and remote connections.

9. **Human Resources Security, Access Control Policies and Asset Management:** Security in OT systems should encompass all interaction points.

10. **Multifactor Authentication:** Multifactor authentication (MFA) adds critical layers of security by requiring two or more verification factors to gain access to a system, significantly enhancing its defense against unauthorized access. This method goes beyond the traditional username and password by incorporating elements like something the user knows (password or PIN), something the user has (a security token or mobile phone) and something the user is (biometric verification). By employing MFA, organizations can ensure that additional barriers protect sensitive information and system access, even if one factor is compromised.

Reporting Obligations

In the context of the evolving cybersecurity landscape in the European Union, the role of the cybersecurity incident response teams (CSIRTs) and their network is crucial. The CSIRT network serves as a cornerstone of the EU's strategy to enhance cybersecurity across member states, particularly under the NIS and NIS 2 Directives. These Directives extend and fortify the functions of CSIRTs, emphasizing their pivotal role in ensuring coordinated responses to cybersecurity incidents and risks.

One of the primary functions of the CSIRT network includes enhancing incident response capabilities through rapid information sharing about threats, vulnerabilities and incidents. This coordination is vital in mitigating the impact of cross-border cyber incidents that can simultaneously affect multiple countries. Additionally, the network is tasked with strengthening security and resilience by supporting the development of capabilities to prevent, detect and respond to cybersecurity incidents. This involves sharing best practices, tools and techniques among the CSIRTs, thereby enhancing the overall cybersecurity posture of each member state.

Furthermore, the network plays a key role in promoting awareness and education about cybersecurity risks. It facilitates educational initiatives to improve security practices among public and private sector entities. In terms of operational capabilities, CSIRTs are empowered to monitor assets connected to the internet, provide direct support in managing cybersecurity incidents, conduct detailed risk analyses and forensic investigations, and facilitate collaborative analysis of cybersecurity trends and threats.

INCIDENT REPORTING

Essential and Important Entities:

- **Early Warning:** Within 24 hours
- **Incident Notification:** Within 72 hours
- **Final Report:** Within 1 month

The reporting obligations under the NIS 2 Directive are significant.[14] Member states ensure that essential and important entities notify CSIRTs or competent authorities of incidents that significantly impact service provision. These incidents are deemed significant if they cause operational disruption, financial loss or materially or non-materially affect other parties.[15] Reporting must occur within specified time frames, with updates and final reports provided as necessary.

Conclusively, fostering a culture of cybersecurity awareness among employees is paramount. Training is a vital tool in empowering employees to recognize and assess potential risks. For CISOs and other cybersecurity professionals, implementing the NIS 2 Directive presents a unique opportunity to elevate their organizational positions by underscoring managerial responsibility in cybersecurity risk mitigation and imposing rigorous consequences for negligence. This collective approach helps strengthen the security posture, ensuring a safer digital landscape for all stakeholders.

14. Source: Preamble 102, https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX%3A32022L2555.
15. Article 20, NIS 2 Directive (Proposal 16.12.2020), https://www.nis-2-Directive.com/NIS_2_Directive_Article_20_(Proposal_16.12.2020).html

EU STRATEGY: THE CYBER RESILIENCY ACT (CRA) AND EUROPEAN CERTIFICATION SCHEMES

The Cyber Resilience Act (CRA) and the Directive on measures for a high common level of cybersecurity across the union (NIS 2) are key components of the European Union's strategy to enhance cybersecurity. The CRA serves as a complement to NIS 2 by addressing legislative gaps in digital product security. It establishes fundamental requirements for hardware manufacturers, software developers, distributors and importers who introduce digital products or services into the EU market.

While NIS 2 provides a broad framework for overall cybersecurity across member states, the CRA specifically targets digital products' resilience and supply chains. Together, they cover a comprehensive range of cybersecurity aspects, ensuring both systemic resilience and product-level security within the EU.

Certification Under CRA

The certification under CRA[16] serves as a compliance mechanism, indicating that a product meets the established cybersecurity standards necessary for obtaining a CE marking[17] – meaning the manufacturer takes responsibility for a product's compliance with all applicable European health, safety, performance and environmental requirements.

SCOPE AND FOCUS	**CRA:** Primarily focuses on products with digital elements, requiring them to meet specific cybersecurity standards throughout their lifecycle. This includes design, development and market placement.	**NIS 2:** Targets critical entities and essential services, mandating robust cybersecurity measures, risk management practices and incident reporting obligations to ensure a high level of network and information system security across the EU.
COMPLEMENTARY GOALS	Both regulations aim to enhance overall cybersecurity in the EU from different angles. The CRA ensures that digital products are secure from the point of design and throughout their lifecycle. NIS 2 ensures that critical sectors and services maintain high levels of cybersecurity to prevent and minimize the impacts of cyber incidents.	
WHO IS AFFECTED	**CRA:** Affects manufacturers, developers and distributors of digital products, including hardware and software.	**NIS 2:** Affects operators of Essential services and Important entities, including sectors like energy, transportation, banking, health, digital infrastructure and public administration.
WHAT IT MEANS AND REQUIRED ACTIONS	**CRA:** Manufacturers must ensure that their digital products meet the essential cybersecurity requirements before being marketed in the EU. They need to: • Implement a comprehensive security-by-design approach. • Provide regular updates and patches. • Maintain compliance documentation and conduct vulnerability assessments. • Provide clear and detailed information to consumers about the cybersecurity features of the products. • Importers and distributors must verify compliance with the CRA before products are marketed in the EU.	**NIS 2:** Entities under NIS 2 Essential services and Important entities must: • Adopt risk management practices and report significant cyber incidents to national authorities. • Take appropriate security measures based on an assessment of risks potentially affecting the security of network and information systems. • Notify the relevant national authority of any adverse effects from cyber incidents or risks.

Illustration-6:

Achieving systemic resilience and product-level security with NIS 2, CRA and certifications.

16. Source: https://digital-strategy.ec.europa.eu/en/policies/cyber-resilience-act

17. Conformité Européenne; French for "European conformity", https://www.tuvsud.com/en-us/services/product-certification/ce-marking#:~:text=CE%20stands%20for%20Conformit%C3%A9%20Europ%C3%A9enne,and%20the%20European%20Economic%20Area.

EU Cybersecurity Certification Framework[18]

Offers different assurance levels (basic, substantial, high) depending on the risk associated with the information and communication technology (ICT) product or service identified in Annex I, high-criticality sectors.

- Managed by ENISA, which develops and maintains cybersecurity certification schemes in coordination with member states and stakeholders.

Impact of Certification

- Certification aims to harmonize cybersecurity standards across the EU, providing a single market for cybersecurity-certified ICT products.
- It helps entities demonstrate compliance with CRA requirements, facilitating access to the EU market.
- Enhances consumer trust as certified products must disclose security features and support periods.

In summary, entities affected by either CRA or NIS 2 must undertake substantial cybersecurity and compliance efforts. Manufacturers dealing with digital products must ensure they meet the strict cybersecurity criteria set out in the CRA, often demonstrated through EU cybersecurity certification. Simultaneously, entities covered by NIS 2 must focus on robust cybersecurity management and incident management practices to comply with the Directive. Member states may require essential and important entities to use certified ICT products, services and processes under European cybersecurity certification schemes to demonstrate compliance with Article 49 of Regulation (EU) 2019/881 requirements.

18. Source: https://digital-strategy.ec.europa.eu/en/policies/cybersecurity-certification-framework.

NON-COMPLIANCE AND PENALTIES

Competent authorities in member states can set deadlines for essential entities to remedy deficiencies or comply with requirements. If deadlines are not met, authorities can, as outlined in Article 33 NIS 2, cybersecurity risk-management measures: (a) temporarily suspend certifications or authorizations concerning relevant services or activities, and (b) temporarily prohibit responsible individuals from exercising managerial functions in essential entities.

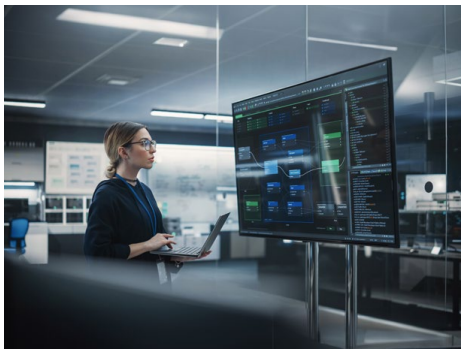
Management bodies, such as boards of directors, are responsible for approving cybersecurity measures and overseeing implementation and can be held liable.

Under NIS 2, penalties for non-compliance vary for essential and important entities. As outlined in Article 49 of Regulation (EU) 2019/881, they can impose the following:

FAILURE TO COMPLY WITH NIS 2 CARRIES STRICTER PENALTIES THAN THE PREVIOUS DIRECTIVE, NIS-D.

PENALTIES FOR NIS 2 VIOLATIONS

- **Administrative fines**
- **Criminal sanctions**
- **Non-monetary remedies,** including compliance orders, binding instructions, security audit implementation orders and threat notification orders to entities' customers.
- **Additional Sanctions:** Member states may be able to impose sanctions on organizations that fail to comply with the NIS 2 Directive. These sanctions may include suspending or revoking licenses, permits and authorizations.



Essential Entities	Administrative Fines	**Up to €10,000,000**	or **2%** of the total annual worldwide turnover; **whichever is higher.**
Important entities	Administrative Fines	**up to €7,000,000**	or **1.4%** of the total annual worldwide turnover; **whichever is higher.**

Illustration-7: Penalty schedule for NIS 2 violations.[18]

18. Source: Penalty schedule for NIS 2 violations, https://NIS 2Directive.eu/NIS 2-fines/.

HONEYWELL'S COMMITMENT TO NIS 2 COMPLIANCE SUPPORT IN EUROPE

Table 1, "Aligning Honeywell's cybersecurity offerings with NIS 2 requirements," delineates various cybersecurity services, solutions and strategies offered by Honeywell that are designed to help organizations augment their industrial cybersecurity in automation systems and OT. It highlights Honeywell's capability of assisting European organizations to elevate their cybersecurity protocols and align with the NIS 2 Directive, set to be enacted on October 17, 2024. Honeywell resources maintain the skills and experience that can help organizations enhance their cybersecurity measures and improve their ability to comply with legal mandates that specifically target sectors engaged in automation and OT.

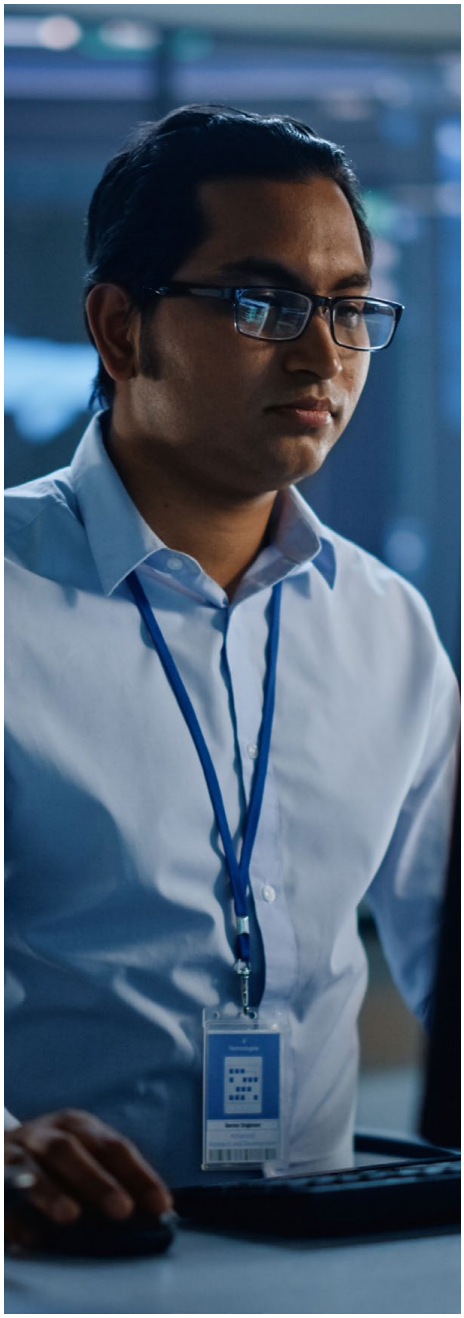
NIS 2 REQUIREMENT	HONEYWELL OFFERING	INCLUDED FUNCTIONALITY DESIGNED TO HELP ORGANIZATIONS
VULNERABILITY MANAGEMENT	Managed Security Services	Managed Security Services are designed to support organizations in receiving the latest updates for Microsoft Windows and antivirus software, improving access to patches and updates.
USE OF EUROPEAN CYBERSECURITY CERTIFICATION SCHEMES	Consultation Services	These services are designed to provide gap assessments and help organizations compare their security posture against standards like IEC 62443, ISO 27001 and NIS 2 or a cybersecurity certification scheme as suggested by ENISA.
BUSINESS CONTINUITY	Consultation Services	Designed to help organizations with business continuity and disaster recovery planning.
NETWORK SECURITY AND INFORMATION SYSTEM ACQUISITION	Consultation Services	These services are designed to help organizations with security-by-design principles, helping with the implementation of rigorous security measures and reviews for its developed systems. Honeywell's services can be utilized by an organization to help conduct regular security reviews and scans for all applicable third-party components and applications.
CYBER RESILIENCE, CYBER HYGIENE FOR SMALL AND MEDIUM-SIZED ENTERPRISES (SMEs)	Consultation Services	Consulting services designed to help an organization improve network resilience by offering support with the design of network architectures, implementing perimeter controls, segmentation and continuous monitoring.
BASIC CYBER HYGIENE, HUMAN RESOURCES, ACCESS CONTROL AND TRAINING	Consultation Services	Honeywell offers a range of cybersecurity training courses, including courses on basic awareness, advanced workshops, industrial standards, offensive cybersecurity and incident management. Consultation services include services designed to help customers develop policies and procedures and conduct penetration testing on industrial assets. Training on tools like Secure Media Exchange (SMX) are designed to help an organization protect USB-borne threats and enforce zero-trust policies.
MULTIFACTOR AUTHENTICATION (MFA) AND ENCRYPTION	Managed Security Services and Consultation Services	Many Honeywell solutions are designed to include encryption and MFA for systems and communications, with a focus on systems requiring heightened security based on risk assessment.

Illustration-8.1: Mapping of Honeywell's cybersecurity product and service portfolio against NIS 2 requirements.

NIS 2 REQUIREMENT	HONEYWELL OFFERING	INCLUDED FUNCTIONALITY DESIGNED TO HELP ORGANIZATIONS
RISK ANALYSIS AND MANAGEMENT	Cybersecurity Vulnerability Assessment (CSVA)	Organizations are assisted in identifying and addressing cybersecurity flaws in automation systems, including issues related to design, software and firmware. Risk reduction measures can be prioritized based on the urgency of observations or customer preferences.
	Cybersecurity Hazard and Operability Analysis (csHAZOP)	This approach of semi-quantitative risk assessments can help organizations gauge cyber-physical risks by correlating the impact of cyber attacks with process losses, providing quantitative insights into cybersecurity resilience. Results from these assessments can help guide an organization in the identification of countermeasures and inform the specification of cybersecurity requirements. Regular reassessment by an organization is recommended before significant technical alterations in the IACS, and periodical assessments are endorsed to help an organization accommodate to shifts in the threat landscape.
	Risk Assessments	Organizations are supported in the identification of threat scenarios, helping them assess their vulnerabilities and associated risks. Regular reassessments are recommended to address threat landscape or process design changes.
INCIDENT MANAGEMENT, RESPONSE AND REPORTING	Advance Monitoring and Incident Response (AMIR)	AMIR is designed to assist customers in complying with the NIS 2 Directive's incident management requirements and provide Managed Security Services. These services include helping customers develop incident response plans, and are designed to provide 24/7 monitoring, with alerting incident reporting, and support in analyzing incidents for continuous improvement.
VULNERABILITY MONITORING AND ASSET MANAGEMENT	Cyber Insights	Cyber Insights is a transformational and vendor-agnostic solution designed to provide insights into a company's cybersecurity posture, vulnerabilities threats and asset detection. The software's core capabilities are designed to provide a foundation for site-specific and enterprise-wide OT cybersecurity, including passive and active network visibility, vulnerability and risk management, a compliance dashboard and automated reporting. Capable of being seamlessly integrated, this solution is designed to be a unified suite that helps a company transform its industrial cybersecurity program into a proactive, strategic asset and helps reduce OT cybersecurity risks.
GOVERNANCE AND COMPLIANCE	Cyber Watch	Cyber Watch is designed to enhance the cybersecurity of OT environments. It offers a centralized dashboard designed to provide near real-time and historical data on threats, vulnerabilities and compliance across multiple operational sites. This tool is engineered to help organizations improve the detection and management of cyber threats, reduce false positives and support compliance with various standards. Its scalability is helpful to integrating and monitoring data from numerous locations, designed to provide a comprehensive view of an organization's cybersecurity posture and to enable proactive responses to potential threats. Cyber Watch is designed to offer a multi-site view and helps to provide visibility across multiple cyber standards, including IEC 62443.

Illustration-8.2: Mapping of Honeywell's cybersecurity product and service portfolio against NIS 2 requirements.

CHALLENGES IN IMPLEMENTING NIS 2 DIRECTIVE IN OT ENVIRONMENTS



Implementing the requirements of Articles 20 and 21 of the NIS 2 Directive in Operational Technology (OT) environments presents a series of significant challenges. The NIS 2 Directive, which builds on the original NIS Directive, aims to strengthen the security and resilience of critical infrastructure across the European Union.

Articles 20 and 21 focus on security requirements and incident reporting, respectively. While these articles are crucial for helping provide a robust cybersecurity framework, the unique nature of OT environments makes compliance particularly complex.

Background on OT Environments and the NIS 2 Directive:

OT systems are integral to the operations of critical infrastructure sectors, such as energy, transportation and manufacturing. Unlike traditional Information Technology (IT) systems, OT systems are designed to control physical processes and machinery. This fundamental difference means that OT systems often prioritize availability and real-time operation over security considerations, which are more common in IT systems. Consequently, integrating stringent cybersecurity measures mandated by the NIS 2 Directive can take time and effort.

Key Challenges in Implementing NIS 2 Directive in OT Environments:

- **Legacy Systems:** Many OT systems are outdated and not designed to accommodate modern cryptographic methods, leading to high costs and potential operational disruptions when upgrades or replacements are necessary.
- **Performance Impact:** Cryptographic operations can introduce latency, affecting the performance of time-sensitive OT processes that rely on near real-time data processing. Balancing security and performance is crucial.
- **Compatibility Issues:** Ensuring compatibility between different systems and devices can be challenging, requiring extensive testing and integration efforts to avoid communication breakdowns.

GRASPING CHALLENGES OF IMPLEMENTING SECURITY MEASURES UNDER ARTICLE 21

Multi-Factor Authentication (MFA)[19]:

1. **User Experience:** OT environments often require quick and seamless access to systems, and implementing MFA can slow down access, potentially facing resistance from operational staff accustomed to faster login processes.
2. **Device Limitations:** Many OT devices do not support modern authentication methods, necessitating additional hardware or software solutions, which increases complexity and cost.
3. **Environmental Constraints:** Harsh industrial environments with high levels of dust, moisture or extreme temperatures can make implementing MFA solutions that rely on mobile devices or biometric systems impractical.
4. **Air-Gapped Environments:** Air-gapped environments, which are isolated from external networks, present additional challenges for implementing MFA. These environments are designed to enhance security by preventing any form of remote access, which complicates the use of MFA methods that rely on network connectivity, such as SMS-based codes or app-based authentication. In such scenarios, offline-capable MFA solutions are required. For instance, time-based one-time passwords (TOTP) generated by hardware tokens or smart cards that do not require an internet connection can provide a feasible alternative.

Asset Management:

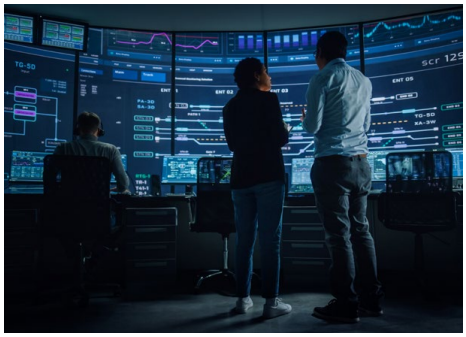
1. **Visibility and Inventory:** OT environments typically involve a vast array of devices that may not be regularly updated or managed, making comprehensive visibility and accurate inventory management difficult.
2. **Diverse Ecosystems:** OT environments often consist of heterogeneous systems from multiple vendors with different protocols and management interfaces, complicating centralized asset management.
3. **Near Real-Time Monitoring:** Continuous near real-time monitoring and management of assets are crucial but challenging to implement without disrupting ongoing operations, as many OT systems cannot afford downtime or performance degradation.

Tailored Approaches for Effective Implementation[20]:

To effectively address these challenges and comply with the NIS 2 Directive, organizations should consider the following tailored approaches:

- Phased Upgrades: Gradually upgrade legacy systems to support modern cryptographic methods, prioritizing the most critical systems to minimize disruptions.
- Performance Optimization: Optimize cryptographic operations to balance security and performance, ensuring that real-time processes remain unaffected.
- **Compatibility Testing:** Conduct thorough compatibility testing to ensure that cryptographic measures do not disrupt communication between systems.
- **User-Centric MFA Solutions:** Implement MFA solutions that are user-friendly and minimally intrusive, possibly using hardware tokens or smart cards for quick authentication.
- **Robust Asset Management Tools:** Deploy advanced asset management tools are designed to provide near real-time visibility and inventory management across diverse ecosystems.
- **Environment-Specific MFA Implementation:** Choose MFA methods suitable for industrial environments, such as ruggedized biometric scanners or offline-capable authentication devices.

By addressing these challenges with industry-appropriate solutions, organizations can improve their cybersecurity in line with the NIS 2 Directive while maintaining operational efficiency and resilience. This approach can not only help improve compliance, but also strengthen the protection of critical infrastructure that is vital to societal well-being and economic stability.



19. Source: https://industrialcyber.co/vendors/beyond-mfa-can-we-make-accessing-critical-infrastructure-even-in-air-gaps-safe-in-2023/
20. Source: https://www.cyber.gc.ca/en/guidance/steps-effectively-deploying-multi-factor-authentication-mfa-itsap00105, May 2023, Awareness Series, ITSAP.00.105

CONCLUSION AND ACTIONABLE STEPS

The Network and Information Security Directive (NIS) was passed into law in 2018 and was a significant milestone in tackling cybersecurity challenges across vital sectors within the European Union. NIS aimed to bolster cybersecurity capabilities and establish a unified framework for member states. Building upon this foundation, the NIS 2 Directive expanded its scope to encompass small and medium-sized enterprises (SMEs) and address emerging digital landscape threats.

NIS 2 mandates compliance with cybersecurity strategies, emphasizing a holistic approach to risk management, incident management and business continuity. Essential entities face comprehensive supervision, while important entities follow a lighter, ex-post supervisory regime. Stricter penalties for non-compliance underscore the importance of adhering to NIS 2 requirements. To help its customers respond and comply with NIS 2, Honeywell offers a comprehensive portfolio of services designed to support industrial organizations in their efforts to satisfy their required compliance standards, enhance cyber resilience and improve their security programs for their critical assets. Through continuous improvement, proactive measures and collaboration with trusted service providers like Honeywell, organizations can increase their ability to adapt to the dynamic cybersecurity landscape and mitigate risks.

Honeywell provides a spectrum of industrial cybersecurity solutions, from helping improve OT cybersecurity defenses with vendor-agnostic solutions designed to assist organizations in identifying, prioritizing and reducing OT cyber risks and potential vulnerabilities.

NIS 2 CALENDAR

- **Official Adoption:** November 10, 2022
- **Entry into Force:** January 16, 2023 (became officially part of EU law)
- **Transposition Deadline:** October 17, 2024. EU member states must adapt their national laws to comply with NIS 2 by this date.
- **Enforcement Deadline:** 18 months after the transposition deadline (this varies slightly between member states, but most will start enforcing NIS 2 around mid-2025.)

SCHEDULE YOUR NIS 2 CONSULTATION

Honeywell
715 Peachtree Street NE Atlanta,
Georgia 30308
www.honeywell.com

Navigating the NIS 2 Directive: Strengthening Cyber Resilience | V1 | 05/2024

THE FUTURE IS WHAT WE MAKE IT

Honeywell

GLOSSARY

NIS Directive	Directive on Security of Network and Information Systems, enacted into law 2018.
NIS 2 Directive	Directive on Security of Network and Information Systems, updated in 2023.
Ex-ante	Based on forecasts rather than actual results.
Ex-post	It being imposed retrospectively to address conduct on the market which has already occurred.
OT	Operational technology
CSIRT	Computer Security Incident Response Team
ICT Products	Information and communication technology (ICT), which covers any product that will store, retrieve, manipulate, transmit or receive information electronically in a digital form. For example, personal computers, digital television, email and robots.
IACS	The energy infrastructure's industrial automation and control systems (IACS) (e.g., SCADA systems), which are vulnerable to cybersecurity incidents.
SCADA	Supervisory Control and Data Acquisition (SCADA) systems control, monitor and analyze industrial devices and processes. The system consists of both software and hardware components and enables remote and on-site gathering of data from the industrial equipment
SME	Small and medium-sized enterprises
AMIR	Advanced Monitoring and Incident Response; a Honeywell Managed Security Service
csHAZOP	A Honeywell Professional Service assessment
Cyber Insights	A Honeywell Forge Cybersecurity+ suite portfolio product/solution
Cyber Watch	A Honeywell Forge Cybersecurity+ suite portfolio product/solution
SMX	A Honeywell solution
MFA	Multifactor authentication
PIN	Personal identification number
DNS	Domain name system
NCA	National Cybersecurity Authorities
CRA	The Cyber Resilience Act
CE	Conformité Européenne; French for "European conformity" CE stands for Conformité Européenne, which translates from French to English as 'European Conformity'. CE certification is an EU safety directive that indicates that a product has passed certain tests and means that a product can legally be sold anywhere within the EU and the European Economic Area.
DSPs	Digital Service Providers

Resources: NIST Glossary, https://csrc.nist.gov/glossary?index=A.