DNV

WHEN TRUST MATTERS

NIS2 DIRECTIVE

What new cyber security laws mean for industrial companies in Europe, and what you need to do to get ready to comply

WHITEPAPER

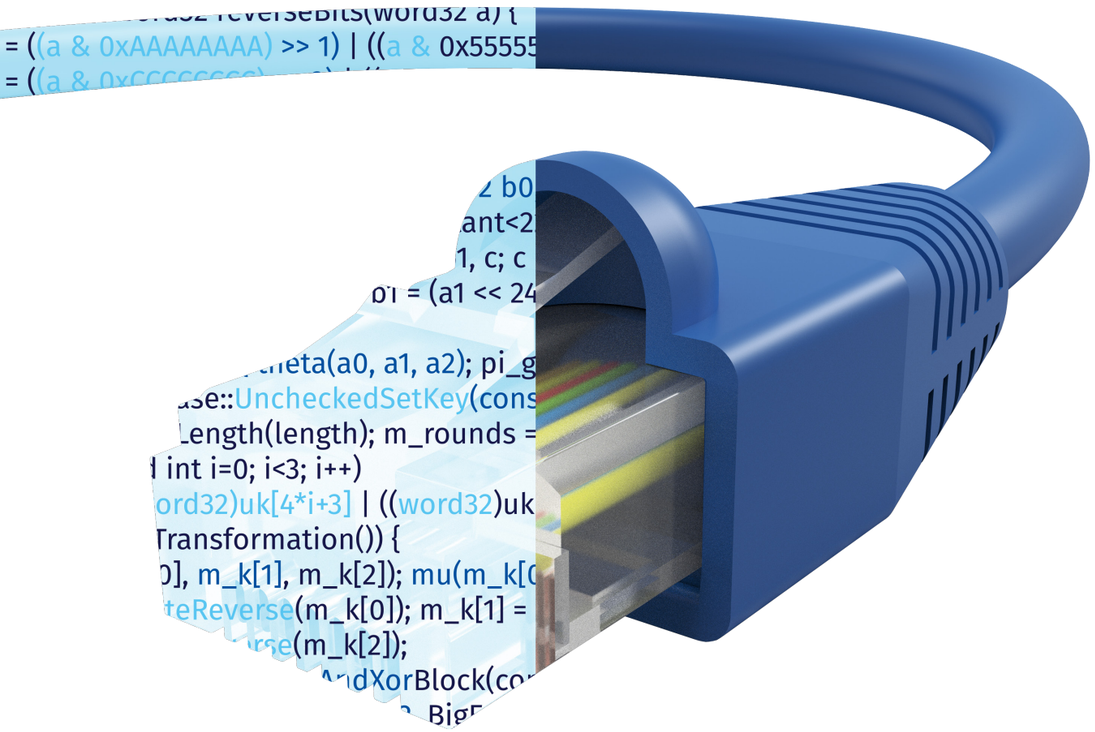
Contents

1.	**Introduction**	**4**
2.	**Overview of NIS and NIS2**	**6**
2.1	NIS2 main changes in a nutshell	7
2.2	NIS2 covers more sectors	7
2.3	NIS2 requirements on organizations, management, and supply chains	8
2.4	Why regulating supply-chain cyber security matters	8
2.5	NIS2 reporting obligations	8
2.6	Adoption timelines	9
3.	**Key steps for NIS2 readiness**	**10**
3.1	Understanding the scope	10
3.2	Risk-based cyber security management systems	10
3.3	Documentation for demonstration	10
4.	**Conclusion**	**11**
Appendix A: Table – NIS/NIS2 scope by sector/subsector		**12**
Appendix B: Abbreviations		**13**

This whitepaper was published in February 2023

1. Introduction

Organizations providing essential services in the European Union (EU) will soon face tougher cyber security regulation than ever, with the threat of more and greater fines and/or withdrawal of license to operate if they do not comply. This follows the January 2023 entry into force of a directive that the EU's 27 Member States must transpose into national laws by late 2024.[1] The revised Directive on Security of Network and Information Systems (NIS2) builds on the NIS Directive (NIS)[2] of 2016, which has been in force in national regulations since 2018.



NIS and industrial cyber security

The original NIS Directive's stated aim was to 'build cyber security capabilities across the Union, mitigate threats to network and information systems used to provide essential services in key sectors and ensure the continuity of such services when facing incidents, thus contributing to the Union's security and to the effective functioning of its economy and society'.

Effectively, NIS was the first EU-wide framework to address concern that threats to critical infrastructure cyber security are becoming more common, complex, and creative as digital transformation continues. Deeply digitally connected infrastructure is critical to efforts to create more efficient decentralized systems and cross-border networks of critical infrastructure within the EU.

NIS2 is NIS on steroids

NIS2 can be regarded as 'NIS on steroids' for an era in which organizations operating essential services need more than ever to manage the cyber risk of both their IT and operational technology (OT), the control systems that manage, monitor, automate and control industrial operations. Greater risk arises from greater connections between OT/IT and externally through the internet.
NIS2 covers more sectors than NIS; see Appendix A for a summary of those deemed 'essential' or 'important' services. Those defined as essential now include, for example, energy, transport, health, and digital infrastructure.

While NIS was about establishing a framework for EU-wide cyber security of essential services, NIS2 is about regulation and enforcement.

NIS2 strengthens requirements for cyber risk assessment by essential and important organizations in the sectors within its scope, and covers risk from supply chains and supplier relationships.

Management bodies of organizations in scope will become legally obliged and accountable for implementing cyber security requirements mandated by NIS2-related laws. This raises the possibility that they could be fined and that their managers, including c-suite, could be temporarily barred from duties.

The EU's Member States must ensure that management bodies comply; and as is the case with NIS, Member States can impose even stricter requirements than those in the NIS2 Directive for cyber security, monitoring, and reporting. Organizations' cyber security teams, IT/OT managers, C-Suites and directors must understand the requirements.

The clock is ticking on compliance

Companies working in energy, transport, health, space, banking and other selected sectors with critical infrastructure need to start preparing.

DNV estimates that organizations will have to start complying with national laws incorporating NIS2 requirements by mid-2024. So, the clock is already ticking on what will be a lengthy risk assessment, management, and training challenge for many medium and large[3] organizations within NIS2 scope.

Preparing for compliance will take many months and will be more complex for organizations operating across multiple Member States. Many organizations with industrial operations will need to set plans in motion from early 2023.

This white paper summarizes the scope and requirements of NIS2 and suggests how to prepare for compliance following three key steps. We hope these insights from our team will be useful to you, and we welcome your comments and questions.

Jalal Bouhdada
Global Segment Director for Cyber Security, DNV
and Founder, Applied Risk

1. Directive (EU) 2022/2555, aka the NIS2 Directive, entered into force 16 January 2023, from which date Member States have 21 months to homologate it into national laws.
2. Directive (EU) 2016/1148 of the European Parliament and of the Council of 6 July 2016 concerning measures for a high common level of security of network and information systems across the Union. https://eur-lex.europa.eu/eli/dir/2016/1148/oj
3. The EU defines 'medium-sized enterprises' as those that employ 50 to 250 persons and either have annual turnover not exceeding EUR 50 million, or an annual balance sheet not exceeding EUR 43 million. It defines large enterprises as employing more than 250. For definition of 'persons employed' see https://ec.europa.eu/eurostat/statistics-explained/index.php?title=Glossary:Persons_employed_-_SBS

2. Overview of NIS and NIS2

NIS applies to companies involved in or responsible for 'essential services' but leaves it to Member States to decide which organizations fall into this category. Energy, drinking water supply and distribution, banking, transport, and health are among the essential services providers (see Appendix A) within the scope of the NIS framework which:

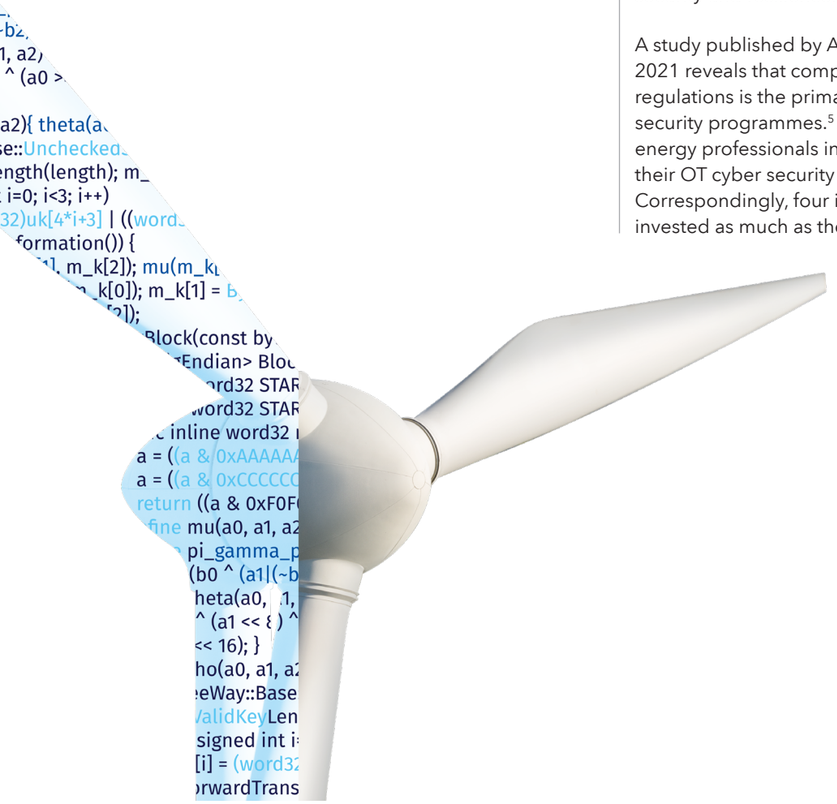
1. Defines 'essential services' and sets thresholds for them
2. Requires a notification process to be in place for cyber incidents
3. Requires relevant organizations to demonstrate compliance with additional cyber security controls.

The application of NIS provisions has been evolving and changing across Member States depending on risk appetites, timing, and maturity. Enforcement of NIS is already in effect in certain countries such as Germany France and UK while others are still working on this.[4]

We are not aware of any penalties arising so far from non-compliance with the original NIS framework. However, we are certain that the EU is very serious about compliance and that the threat of fines and/or loss of license to operate are very real under NIS2.

The upside is that the two directives help to focus organizations on the need to do something about compliance and on thinking about the financial, technology, and human resources they need to allocate to OT/IT cyber security and resilience.

A study published by Applied Risk, a DNV company, in 2021 reveals that compliance with standards or regulations is the primary driver of investment in OT security programmes.[5] According to DNV research of 940 energy professionals in 2022, less than half (47%) believe their OT cyber security is as strong as their IT security.[6] Correspondingly, four in 10 (38%) admit that they have not invested as much as they need to in OT cyber security.



4. At the time of writing, it is unclear if the UK, no longer within the EU, will intentionally and/or specifically reflect any or all of the EU's NIS2 requirements in the UK's own Network and Information Systems Regulations, which are being updated.
5. 'Architecting the Next Generation for OT Security', Applied Risk, November 2021, https://applied-risk.com/resources/press-release-architecting-the-next-generation-for-ot-security-report-released
6. The Cyber Priority', DNV, May 2022, download at https://www.dnv.com/cybersecurity/cyber-insights/thecyberpriority.html

2.1 NIS2 main changes in a nutshell

NIS2 seeks to correct shortcomings of the previous NIS Directive, modernize it for the present, and ensure its viability in the future. To achieve these goals, NIS2:

1. Broadens the application of the current NIS Directive by including new sectors (see Section 2.2) based on how important they are to the economy and society, and by introducing a clear size cap, which includes all medium and large businesses in some sectors. NIS2 also gives Member States significant latitude in identifying smaller organizations with a high security risk profile. Additionally, NIS2 ends the distinction between digital services providers (DSPs) and operators of basic services. According to their importance, entities will be categorized into essential and important categories and divided into subgroups that would be subject to various types of oversight.
2. Establishes requirements for 'management body' oversight and accountability for security risk management. Establishes a risk management method stipulating a minimal set of fundamental security features that must be used, strengthening and streamlining security and reporting requirements for businesses.
3. Adds more specific guidelines for incident reporting, report content, and delivery schedules. These require the implementation of a stricter incident response process.
4. Adjusts fines and penalties for non-compliance.
5. Suggests forcing individual businesses to address cyber security risks in supply chains and supplier partnerships to address the security of these ties. The idea improves supply-chain cyber security for important information and communication technology at the European level. Building on the successful strategy used in the framework of the European Commission's Recommendation on Cybersecurity, Member States may conduct coordinated risk assessments of vital supply chains in collaboration with the Commission and the European Union Agency for Cybersecurity (ENISA).
6. Calls for tighter enforcement standards, more rigorous oversight of national agencies, and more alignment of penalties policies among Member States. Additionally, NIS2 strengthens the NIS Cooperation Group's[7] influence over strategic policy choices and expands information exchange and cooperation among Member State authorities. The new directive also improves operational coordination, notably in terms of managing cyber crises.
7. Creates an EU registry in this area, run by ENISA, and sets a fundamental framework with accountable key actors on coordinated vulnerability disclosure for recently discovered vulnerabilities throughout the EU.

2.2 NIS2 covers more sectors

The broader scope of NIS2 defines more sectors as 'essential services', or sectors of 'high criticality', that must implement cyber security risk management and prove that they are doing so (see Appendix A). This impacts on medium and large organizations. The EU also lists 'important services' protected under NIS2, which could be redefined as 'essential' in the future. Organizations not in NIS2 scope include central banks, parliaments, and those engaged in defence, law enforcement, the judiciary, and national and public security. Member States must establish a list of essential and important entities as well as entities providing domain name registration services.

It should be noted that Appendix A includes broad headings and that there is more nuanced detail in both NIS and NIS2 about what is, what is not, and what could be, in scope in some of the sectors/subsectors covered by the directive. We recommend seeking advice on this aspect as it becomes clearer what will be in scope in national laws homologating NIS2 while applying local variations.

7. The Network and Information Systems Cooperation Group was established by the first NIS Directive to ensure cooperation and information exchange among EU Member States.

2.3 NIS2 requirements on organizations, management, and supply chains

To reduce discrepancies in cyber security resilience across in-scope industries, NIS2 aspires to a more coordinated cyber security management approach. To control the risks presented to the security of those entities' network and information systems when providing their services, NIS2 recommends seven fundamental steps that all essential and important entities shall implement:

1. Risk analysis and information system security policies;
2. Incident handling (prevention, detection, and response to incidents);
3. Business continuity and crisis management;
4. Supply chain security, including security-related aspects of relationships between each entity and (i) its suppliers, or (ii) service providers (such as data storage providers and processing services or managed security services providers);
5. Security in network and information systems acquisition, development and maintenance, including vulnerability handling and disclosures;
6. Policies and procedures to assess the effectiveness of cyber security risk management measures; and
7. The use of cryptography and encryption.

Fortunately, most of these security controls are not brand-new, and many businesses are likely already engaged in these fields. We anticipate that key performance indicators for these controls will emerge in due course from the EU.

2.4 Why regulating supply-chain cyber security matters

The inclusion of supply chain cyber security is timely and important. It will drive a much-needed change in the mindsets of organizations when it comes to cyber risk management. Most OT security professionals say their organizations are at risk because of their inability to ascertain the security practices of relevant third parties and to mitigate cyber risks across the OT external supply chain, according to research conducted by Applied Risk in 2021.[8]

Only 33% of OT professionals say their organizations conduct regular audits of their own main suppliers, and only 27% conduct due diligence prior to contracting with new suppliers. Just half (49%) of OT security professionals say their contracts with suppliers include cyber security requirements.

Research conducted by DNV in 2022 reveals that 28% of energy professionals working with OT say their company is making the cyber security of their supply chain a high priority for investment.[9] This contrasts with the 45% of OT-operating respondents who say expenditure in IT system upgrades is a high investment priority.

2.5 NIS2 reporting obligations

NIS2 aims to boost information sharing and collaboration on managing cyber crises between Member States at EU level. It mandates a greater degree of EU-wide harmonization of reporting obligations for organizations within scope and for national cyber security incident response teams (CSIRTs) or, where applicable, competent authorities.

For example, NIS2 obliges organizations to issue 'without undue delay and in any event within 24 hours of becoming aware of the significant incident, an early warning, which, where applicable, shall indicate whether the significant incident is suspected of being caused by unlawful or malicious acts or could have a cross-border impact'.

Within 72 hours of becoming aware of the significant incident, the organization must file an incident notification updating if applicable the first information and indicating an initial assessment of the significant incident, including its severity, impact and, where available, the indicators of compromise. The national CSIRT or competent authority can request a more detailed follow-up report one month after the 72-hour notification.

8. 'Architecting the Next Generation for OT Security', Applied Risk, November 2021, https://applied-risk.com/resources/press-release-architecting-the-next-generation-for-ot-security-report-released
9. 'The Cyber Priority', DNV, May 2022, download at https://www.dnv.com/cybersecurity/cyber-insights/thecyberpriority.html

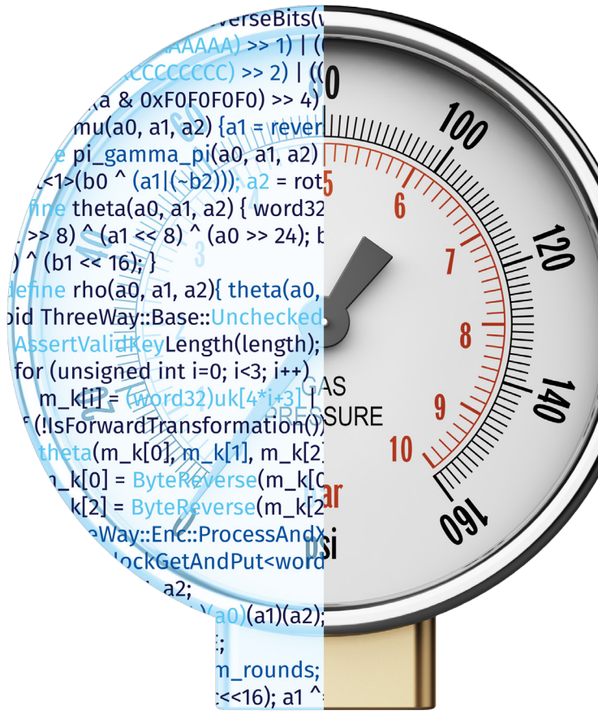
This means that organizations with OT/IT within scope must have or develop compliant incident response processes that report incidents within prescribed deadlines (Section 3.2). This could be quite challenging for OT companies as many do not yet include incident response as part of daily security routines despite it being a critical aspect of cyber security.[10]

2.6 Adoption timelines

Organizations should now think about NIS2's scope and if their operations fit within it. An organization should think about the organizational, financial, and technical actions that will be necessary to get ready for NIS2 compliance if it determines that it is likely to fall under the new legislation's purview. For instance, the European Commission anticipates that organizations' ICT security spending will increase by up to 22% in the first few years following the introduction of NIS2 (a maximum increase of 12% is anticipated for organizations already covered by the present NIS Directive). In-scope organizations should also monitor how NIS2 is implemented in the important EU jurisdictions where they conduct business.

Organizations that provide products or services related to information and network security should also be ready for due diligence from in-scope NIS2 organizations. Therefore, in preparation for any such due diligence, such out-of-scope organizations should make sure that efficient, documented processes are in place to handle security risks related with their product or service offering.

The European Parliament approved NIS2 on 10 November 2022 and the directive came into force on 16 January 2023, from which date Member States have 21 months to homologate it into national laws. It is unlikely to be ratified and legally incorporated into the national legislation of all EU Member States until the end of 2024 at the earliest.



10. 'Cyber Security Incident Response & Decision-making strategies in OT environments', Applied Risk, Blog [online], 08 June 2022, https://applied-risk.com/resources/blog-cyber-security-incident-response-ot-environments

3. Three key steps to prepare for NIS2-based regulation

We advise any organization now beginning to consider how to prepare to comply with regulation based on NIS2 to follow these three practical steps for success:

- **Step1:** know from the start which systems are within scope for NIS2-based regulations (Section 3.1)
- **Step 2:** adopt risk-based cyber security management and enforce security controls (Section 3.2)
- **Step 3:** document everything needed to demonstrate compliance with controls (Section 3.3).

3.1 Understanding the scope

Deciding what OT/IT systems are within scope for NIS2 is the initial step towards successful compliance. Key questions include:

- What essential services is the organization providing?
- Does or might the organization fall within the scope of NIS2?
- What new requirements would need to be implemented by the organization within NIS2 scope?
- If the organization is not itself directly within NIS2 scope, does it deal with suppliers or customers subject to the new rules?
- What obligations do organizations need to attribute to their suppliers or business customers in their contractual arrangements?

As a result, understanding the regulatory requirements will be important for organizations not directly impacted by the new Act. It will also be important to determine whether any additional local IT/OT security regulations need to be adopted because of any national regulations.

3.2 Risk-based cyber security management systems

Essential and important entities within the scope of NIS2 will be required to take appropriate technical, operational, and organizational measures to manage the risks posed to the security of the IT/OT assets they use for their operations or providing services. They will also need to prevent or minimize the impact of incidents both on people who use their services and on other services.

To protect networks and systems, and their physical environment, against incidents, such measures must take a risk-based approach. In addition to this broad need, the new Directive includes more specific information on cyber security risk management methods, specifying that they shall include at least the following:

- A governance and operating model with clear roles and responsibilities and senior management accountability;
- Risk analysis and information system security policies;
- 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 cyber security risk management measures;
- Basic computer hygiene practices and cyber security training;
- Policies and procedures regarding the use of cryptography and, where appropriate, encryption;
- Human resources security, access control policies, and asset management; and
- The use of multi-factor authentication or continuous authentication solutions, secured voice, video and text communications, and secured emergency communications systems within the entity, where appropriate.

3.3 Documentation for demonstration

Compliance requires documentation – if it is not documented, it did not happen. Auditors can ask for a wide range of documentation in assessing organizations for proof of compliance with NIS2. This step can be overwhelming especially for organization that are just starting their compliance journey. A holistic governance systems can not only aid in tracking progress and improving documentation, it can also provide a multi-disciplinary perspective and a solid framework of how companies can manage cyber threats in a pro-active manner and work towards counteracting cyber threats both now and in the future.

4. Conclusion

Despite being a relatively new regulatory obligation, NIS has many elements that were already defined in best practices (e.g. standards and frameworks such as IEC 62443, NIST, ISO27001) and have been included in compliance requirements for sectors like financial services and telecoms for more than 20 years. Investment in comprehensive IT and OT security programmes based on established cyber security standards and frameworks can enable organizations to address risks covered by NIS and other legislation. They also enable businesses with industrial operations to reduce downtime and improve resilience. Having better security will also secure valuable business models, and future-proof organizations.

In parallel, preparing for NIS2 can be seen as a wider opportunity to review and fix cyber security to future-proof OT/IT across the organization and its supply chains. The opportunity is to embed robust cyber security practices vital to organizations' digital transformations while also building regulatory compliance into operations.

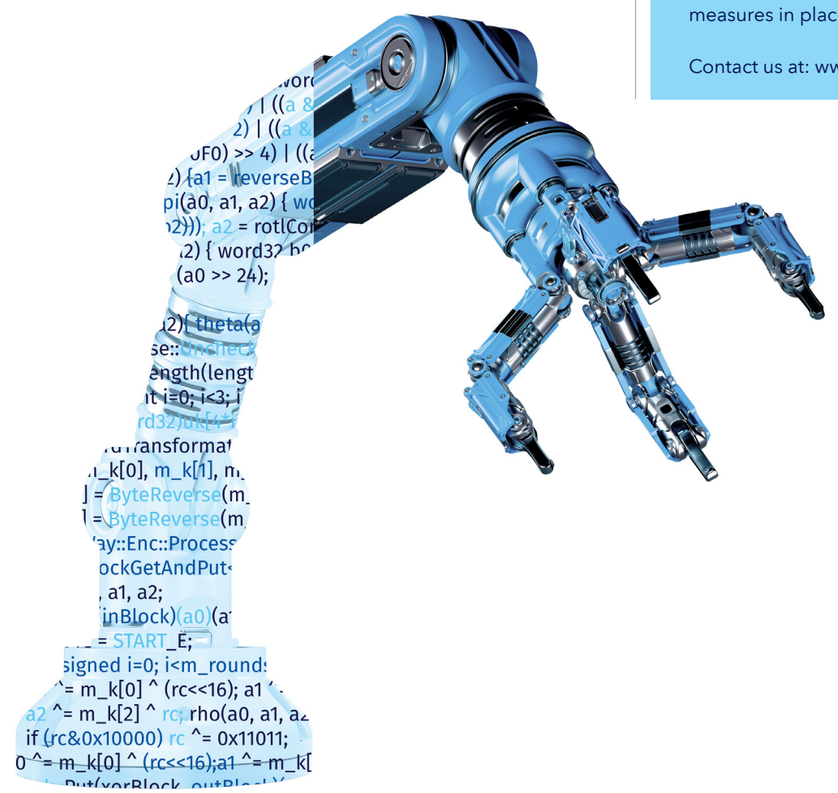
Developing a culture of security and compliance involves adequately funding and resourcing sustainable and long-term security improvement. This should focus on an approach based on risk and consequences. This approach in turn involves diversifying controls and activities to include offensive capabilities, training and simulation, monitoring and testing.

The requirements for evidence of compliant policy being in place and adhered to should be consistent, enforced on all users, and current (version control is needed). Technical and organizational cyber security controls should ensure compliance with policies and be subject to review, performance assessment, and compliance assessment. The good news is that all of this is achievable given sufficient time, resources, and with buy-in from the boardroom down.

NEED ADVICE?

DNV's experts are on hand to help your business identify relevant NIS2 requirements, and put measures in place to comply.

Contact us at: www.dnv.com/cybersecurity



Appendix A

TABLE: NIS AND NIS 2 SCOPE BY SECTOR AND SUBSECTOR

NIS DIRECTIVE ANNEX II	NIS2 DIRECTIVE ANNEX I
Essential services and Digital Service Providers • Energy – electricity, oil, natural gas • Drinking water supply and distribution • Transport – air, rail, water, road • Banking • Financial market infrastructures • Health – health care settings including hospitals and private clinics • Digital Infrastructure – internet exchange points (IXPs), DNS service providers, TLD name registries • Public administrations identified as operators of essential services	**Essential services** • Energy – electricity, district heating and cooling, oil, natural gas, hydrogen • Manufacture of pharmaceutical products including vaccines • Drinking water and waste water • Transport – air, rail, water, road • Banking (except for central banks) • Financial market infrastructures • Health • Digital infrastructure – internet exchange points (IXPs), DNS providers, TLD name registries, cloud computing service providers, data centre service providers, content delivery networks, trust service providers, public electronic communications networks, electronic communications services • ICT service management (business-to-business) • Space industry • Central and regional public administrations, though Member States can if wished regulate local authorities' cyber security **Important services (NIS2 Directive Annex II)** • Postal and courier services • Waste management • Chemicals – manufacture, production, distribution • Food – production, processing, distribution • Manufacture of medical devices (but these can be redefined as essential services during a public health emergency) • Manufacture of computers, electronic and optical products, electrical equipment, machinery and equipment, and motor vehicles and other transport equipment • Digital providers – online marketplaces, online search engines, and social networking service platforms

Appendix B

ABBREVIATIONS

CSIRT: Computer security incident response team

DSP: Digital service provider

ENISA: The European Union Agency for Cybersecurity

IEC: International Electrochemical Commission

ISO: International Organization for Standardization

IT: Information technology

NIS: Network and Information Systems Directive (EU) 2016/1148

NIS2: Second Network and Information Systems Directive (EU) 2022/2555

NIST: (US) National Institute of Standards and Technology

OT: Operational technology

ABOUT DNV

DNV is an independent assurance and risk management provider, operating in more than 100 countries. Through its broad experience and deep expertise, DNV advances safety and sustainable performance, sets industry standards, and inspires and invents solutions.

DNV combines specialist energy industry knowledge with engineering expertise and information system best practice to keep critical infrastructure projects and operations confidently cyber secure. We provide many of the sector's most successful and forward-thinking companies with clear and practical advice to uncover their risks, build a powerful force of defence against threats, recover from attacks, and unite stakeholders behind security programmes that everyone can believe in.

dnv.com/cybersecurity

Disclaimer
All information is correct to the best of our knowledge. Contributions by external authors do not necessarily reflect the views of the editors and DNV AS.

17680_JSW.30.01 2023