WHITEPAPER

Network and information security directive 2 (NIS2)

Enhancing cybersecurity compliance: Navigating the NIS2 Directive

protiviti®
Global Business Consulting

Table of contents

Introduction

The European Commission has revised the NIS Directive, expanding its scope to include numerous new sectors. This revision aims to enhance cybersecurity across the entire European region by unifying national laws with common minimum requirements. For many companies located within European Union (EU) Member States, as well as non-EU organisations that provide services within the EU, NIS2 represents their initial regulatory obligation in the field of information security. All EU countries were required to transpose the NIS2 directive into their national law by October 2024.

The European Commission has the power to issue regulatory requirements and compel Member States to implement them in order to ensure a secure European Economic Area. These requirements are often driven by emerging threats that pose a risk to EU members, particularly the increasing number of attacks on IT infrastructure and network and information systems in recent years. The EU classifies these attacks as cyber threats and defines them as "a possible circumstance, event or action that could harm, disrupt or otherwise affect the network and information systems(s) that harm the users of those systems and other persons." These cyber threats, which can have global reach and cross-border consequences, are more significant than ever due to the growing interconnectedness of our economy and society. As the trend toward increased digitalisation continues, it is likely that the resulting damage from these threats will only increase.

For the EU Commission, cyber threats are not a new phenomenon, but for years have been a serious factor, which can have a negative impact on the stability of the economy. Back in 2016, the "Directive (EU) 2016/1148 of the European Parliament and of the Council of 6 July 2016 concerning measures to ensure a high common level of security of network and information systems across the Union," also known as the NIS Directive due to its focus on network and information systems, was published. This directive has been revised by the EU Commission and entered into force at the end of 2022 as "Directive (EU) 2022/2555 of the European Parliament and of the Council of 14 December 2022 on measures for a high common level of cybersecurity across the Union, amending Regulation (EU) No 910/2014 and Directive (EU) 2018/1972 and repealing Directive (EU) 2016/1148 (NIS2 Directive," *this* directive is also called the NIS2 Directive. The aim is to create a legal framework for a uniform minimum level of cyber resilience in the EU area.

Compliance with NIS2 is particularly challenging for organisations that have not been regulated or are only marginally regulated, as they must now consider the specific regulatory requirements in addition to self-motivated implementation of cybersecurity measures. This white paper primarily focuses on identifying the entities impacted by NIS2, explaining the core content and requirements of NIS2, the resulting actions that need to be taken and recommended steps for compliance. It also addresses the classification of companies into different sectors.

The requirements of NIS2 apply not to every company that operates in Member States, but only to companies that make significant contributions to the economy or the common good. The NIS2 Directive introduces a revised approach to determining regulated entities by implementing a size cap rule and further defines how microenterprises and small and medium-sized enterprises are impacted. All medium-sized and large companies operating or providing services in the sectors covered in NIS2 fall under its scope. However, small enterprises and microenterprises are included in NIS2 only in exceptional circumstances. For instance, they may be included if they are the sole provider of a service essential for maintaining critical societal or economic activities within a Member State or if they offer domain name registration services. NIS2 also establishes distinct rules for essential entities and important entities. Additional guidance is offered under Article 2, Annex I and Annex II of the directive.

There are essentially two types of companies that must comply with the NIS2 Directive: essential entities and important entities.

Under NIS2, the key difference between an essential entity and an important entity is the level of oversight and potential consequences of non-compliance:

Essential Entities: Defined by operating in a critical sector and meeting a specific size threshold:

- Critical sectors include energy, transportation, banking, waste management, etc.
- These sectors are subject to stricter oversight and enforcement measures, including regular audits.

Important Entities: Typically, medium-sized enterprises in critical sectors that don't meet the essential entity-size threshold.

- May also include some entities designated as critical under a separate EU directive.
- Face less stringent oversight but must still comply with the same basic cybersecurity requirements.

The European Commission's revised NIS Directive expands its scope to include new sectors, aiming to unify national laws with common minimum requirements.

Additionally, institutions classified as essential or important entities constitute two main criteria:

Sector: The entity operates in one of the sectors identified as critical infrastructure by NIS2. These sectors include:

- Energy (electricity, oil, gas)
- Transport (airlines, railways, maritime)
- Banking
- Financial market infrastructure
- Waste and water management
- Postal services
- Digital infrastructure providers
- Waste and wastewater treatment & transport
- Providers of waste collection services
- Manufacture of essential goods (medicines, food, etc.)
- Public administration

Figure 1

Size: The entity meets a certain size threshold, which is defined by the Member State implementing the directive.

It's important to note that some entities may be designated as "important" even outside these sectors if a Member State deems them critical.

While important entities have the same basic cybersecurity requirements as essential entities, they tend to have less stringent oversight and enforcement measures.

An institution is classified as an essential institution if at least one of the following criteria is met:

- Services or goods are offered for a fee and the company is located in a sector that is particularly important according to NIS2 criteria (the sectors are shown in Figure 1). An organisation must also either employ at least 250 people or have an annual turnover of more than 50 million euros and a balance sheet total of over 43 million euros.
- The setup is a qualified trust service provider, top level domain name registry or DNS service provider.
- It provides telecommunications services or publicly accessible telecommunications networks that either employ at least 50 people or whose annual turnover and balance sheet total are each more than 10 million euros.
- It operates of critical assets.

On the other hand, an institution is classified as an important institution if none of the criteria for a "very important" facility apply, but at least one of the following criteria is met:

- Services or goods are offered for a fee and the company is located in an important sector according to the NIS2 (the sectors are shown in Figure 1). In addition, an organisation must have either a minimum of 50 employees or an annual turnover and an annual balance sheet total of more than 10 million euros each.
- The company is a trust service provider.

NIS2 represents the first regulatory obligation in information security for many companies within the EU and non-EU organisations providing services in the EU. Compliance was mandatory by 18 October 2024.

Regardless of their characteristics, NIS2 also applies to all regulated financial services providers. In this context, the NIS2 requirements should be considered as additional requirements, which, however, deviate only slightly from the already extensive regulatory requirements of BaFin or other supervisory authorities.

In addition to companies from these sectors, state institutions and state-related institutions are also affected by the NIS2. The exact organisational and technical measures required of the companies concerned are not yet fully certain due to the draft status of the law in many Member States. However, based on similar legislations and the existing requirement to have an effective information security management system (ISMS), it is largely foreseeable which requirements companies will face.

If non-regulated companies do not have an ISMS in place, the introduction of an ISMS is not only sensible but also mandatory due to the regulatory requirement of NIS2. Companies that are already regulated, such as financial services providers, will need to adapt their processes for dealing with cyber threats according to NIS2, but they are already operating on a strong foundation and can expect minimal adjustments to their existing processes in terms of cyber resilience, such as reporting the first-time use of critical components to related agencies or ministries.

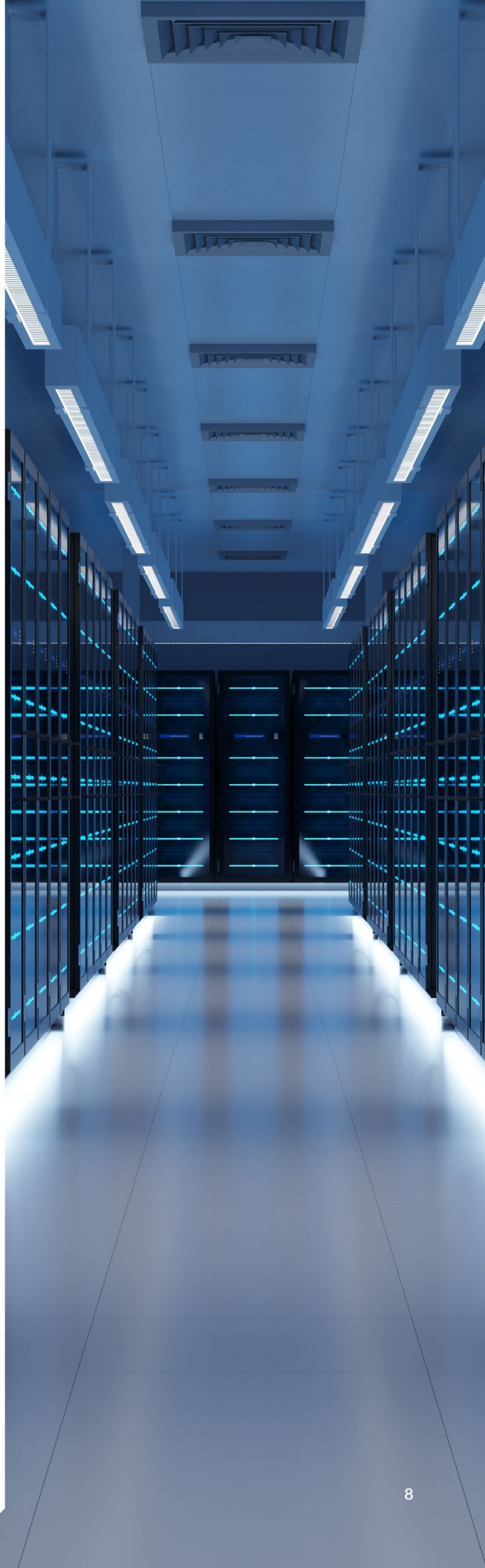
The NIS2 requirements should be considered as additional requirements, which, however, deviate only slightly from the already extensive regulatory requirements of BaFin or other supervisory authorities.

(New) requirements for companies

Protecting against cyber threats should have been a concern for organisations even before NIS2, as the past has seen a steady increase in reputational and monetary losses due to cyberattacks. In fact, by the end of 2020, cyberattacks had caused the global economy to lose nearly 5.5 trillion euros.

NIS2 proposes new and more extensive regulations to combat cyber threats. These regulations require affected companies to prioritise suitable, proportionate, and effective technical and organisational risk management measures in order to safeguard the availability, integrity, authenticity, and confidentiality of their information technology systems, components and processes.

NIS2 establishes the minimum requirements for risk management that must be met by impacted entities, and those entities may be further impacted by the requirements set forth by the Member State they operate within.



NIS2 outlines 10 minimum cybersecurity risk management measures that obligated entities must implement. These measures focus on various aspects of cybersecurity risk management, including:

Management oversight and approval: Corporate management's training on and oversight and approval of the entity's cybersecurity measures.

Risk assessments: Regular risk assessments to identify potential threats and vulnerabilities.

Incident reporting: Procedures for reporting cyber incidents to the relevant authorities.

Business continuity and crisis management: Plans for maintaining critical operations during and after a cyber incident.

Supply chain security: Measures to assess and mitigate risks from third-party vendors and suppliers.

Cyber hygiene practices: Implementing basic security measures like strong passwords and user access controls.

Cybersecurity awareness and training: Training employees on cybersecurity best practices to identify and prevent cyber threats.

It's important to note that these measures need to be adapted based on the specific size, sector and risk profile of the entity.

These minimum requirements, along with the other requirements of NIS2, can be categorised into three main areas that companies should prioritise. These areas include implementing a functional ISMS to ensure cybersecurity, involving the supply chain in information security to manage risks at service providers and establishing a reporting capability to communicate security incidents to regulators.

Requirement 1: Cybersecurity in the ISMS

An Information Security Management System (ISMS) is a systematic and continuous approach to managing and protecting digital, data and informational assets. It ensures the confidentiality, integrity, authenticity and availability of information through various methods, processes, measures and policies. In the context of information security, cybersecurity is also a crucial aspect of an ISMS. The NIS2 regulations prioritise addressing cyber threats and strengthening cyber resilience.

To comply with NIS2 requirements, entities classified as important must conduct risk analyses and assessments as part of their risk management practices. These analyses aim to identify potential threats and vulnerabilities and derive technical and organisational measures to minimise or prevent potential damage. These measures may include implementing access controls, encryption technologies, incident response procedures and providing regular cybersecurity training to employees.

The company's IT infrastructure is impacted by vulnerabilities and external threats. Therefore, it is important to have state-of-the-art security technologies that are tailored to the company's characteristics. Secure network management and configuration are vital for external interfaces and internal areas. This includes network segmentation, zoning, hardening of IT systems, and encryption for data at rest, in processing and in transit.

Additionally, it involves the use of antivirus programs, firewalls, anti-malware software and rule-based file checks. Regular vulnerability scans, penetration tests and simulated attacks are necessary to assess the effectiveness of these measures. This assessment is important for business continuity management and should be considered an essential aspect within the corporate context. Business continuity management extends not only to the company itself but also to business-critical service providers and suppliers that must follow or implement these practices.

To comply with NIS2 requirements, entities classified as important must conduct risk analyses and assessments as part of their risk management practices.

Suppliers should review new and existing contracts with regard to cybersecurity, risk management and security incident management.

Requirement 2: Involvement of supply chains

NIS2 considers the growing networking and collaboration among companies, both within a country and across borders. In the production of a product or the provision of a service, it is rare for only one company to be involved. Instead, companies focus on their core processes, outsource secondary processes, and purchase sub-products and services from suppliers and service providers. For "particularly important" and "important" entities, this means that their supply chain must also be secure.

When planning and implementing information security measures, a company regulated under NIS2 must also consider that a cyber attack on a supplier can impact its own operations or bring them to a halt. Cybersecurity practices need to be strengthened and supply chain risks actively managed. In the service management process, it is important to ensure that potential suppliers are aware of cyber threats and proactively address information security risks from the selection stage of new service providers.

Suppliers should review new and existing contracts with regard to cybersecurity, risk management and security incident management. Only requirements agreed upon in the contract should be met by suppliers, and these can be reliably considered in risk management. Additionally, contractual regulations regarding cybersecurity should be audited periodically and on a case-by-case basis, which is why it is important to establish an audit right. Depending on the size, audit complexity and market power of the supplier, audits can be conducted independently, by another service provider or collectively as part of an audit pool involving multiple companies.

Aside from controls and verification, it is also beneficial to have a collaborative security process between companies and suppliers, such as a joint ISMS, or integrating suppliers into an existing security process. A coordinated process, regularly tested, helps effectively manage cyber threats. Such a process must also ensure that security incidents at suppliers are promptly reported, enabling companies to fulfill their reporting obligations regarding significant security incidents under NIS2.

Requirement 3: Reporting and communication with supervisors

In addition to internal requirements and requirements with suppliers for "particularly important" and "important" facilities, NIS2 requires the reporting of significant security incidents to Member State authorities. Furthermore, general information, such as registration data, also needs to be communicated in accordance with NIS2. Registration data includes the extent to which a company is affected by NIS2, including the company's name, legal form, address, contact details with IP address range, applicable NIS2 sectors and a list of EU Member States where the company operates.

Effective reporting is crucial. Security incident reporting has specific deadlines: initial reporting within 24 hours of becoming aware of a significant incident (as defined by the NIS2 and any Member State legislation), a detailed assessment of the incident within 72 hours, and reporting the completion of treatment or providing a progress report with an update within one month. To achieve this, mechanisms must be established to ensure fast and accurate recording and reporting of security incidents. This involves creating suitable internal and external communication channels and developing a reliable internal company system for documenting, analysing, and classifying security-related events and incidents.

Security incident reporting has specific deadlines: Initial reporting within 24 hours of becoming aware of a significant incident, a detailed assessment of the incident within 72 hours, and reporting the completion of treatment or providing a progress report with an update within one month.

Conclusion: Need for action for previously unregulated companies

The requirements of NIS2 should not be considered individually, but rather as interconnected obligations aimed at improving information and cybersecurity in the EU. An effective ISMS focuses on protecting company information and should be designed independently of regulatory requirements. However, an ISMS that complies with NIS2 may also need to meet specific requirements outlined in a Member State's regulations. This means that previously unregulated companies with basic or no ISMS face the challenge of setting up an ISMS quickly and addressing the unique aspects of NIS2.

Companies need to promptly adapt their existing ISMS to incorporate the necessary changes, as there is no transition period for compliance. Failure to comply with NIS2, which came into effect in October 2024, can result in fines. Non-compliance can lead to significant penalties, including personal liability. For important facilities, the penalty can be up to 7 million euros or 1.4% of the worldwide annual turnover. For "particularly important" facilities, the penalty can reach 10 million euros or 2% of the worldwide annual turnover, whichever is higher. These penalties aim to raise awareness of cybersecurity among decision-makers and responsible individuals in companies.

In addition to raising awareness, regulators will have expanded powers, including authorisation for on-site inspections, regular safety audits, ad hoc inspections during emergencies and security scans. As a result, companies must continuously monitor and adapt their security measures to keep up with evolving threats and regulatory requirements. It is advisable for companies to proactively establish a good relationship with their local supervisory authority for NIS2, and stay updated on information from the European Union Agency for Cybersecurity (ENISA) and other cybersecurity interest groups. For companies that have not yet engaged with information security institutes, prioritising engagement and communication within their ISMS is crucial.

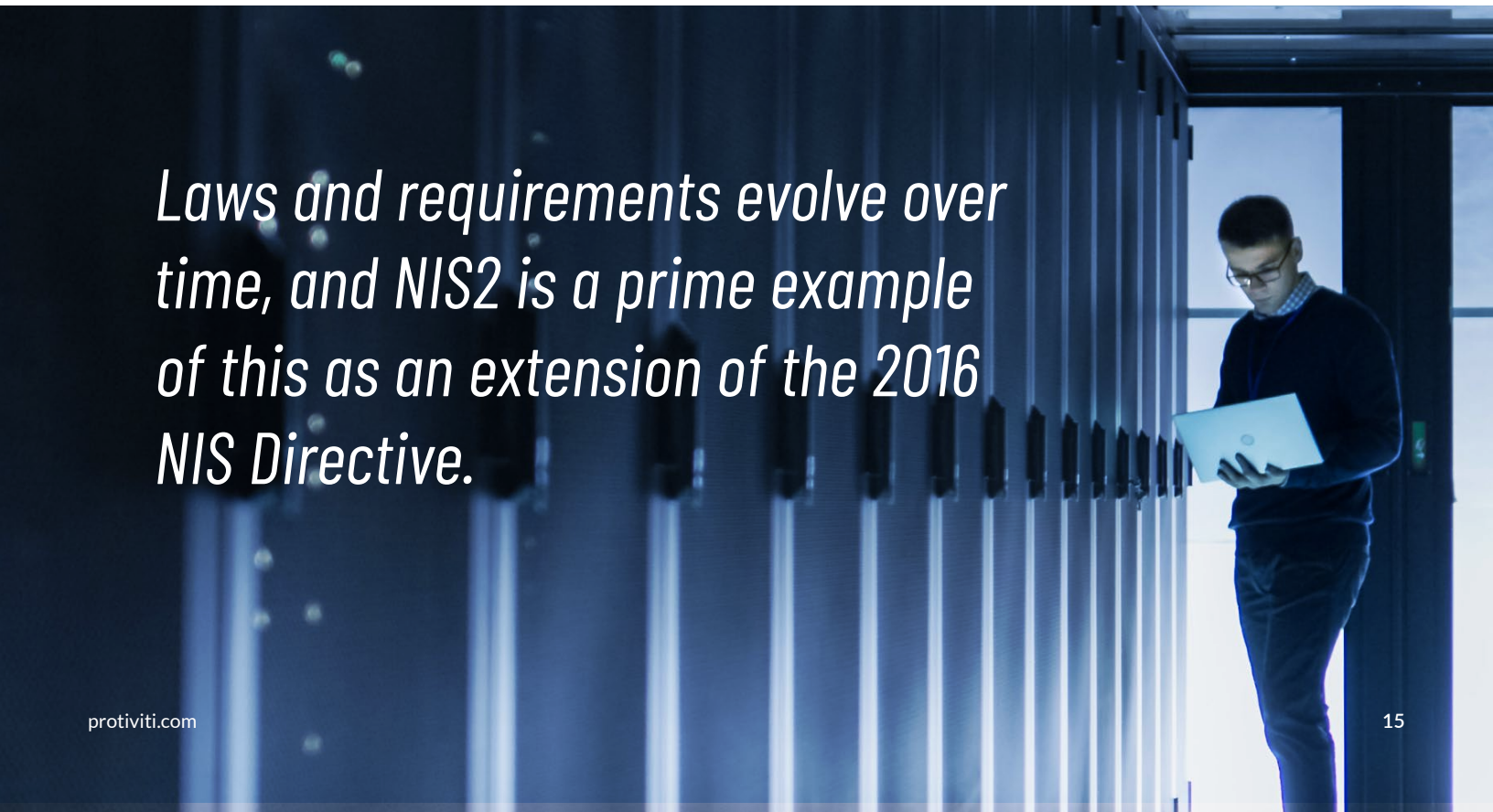
Non-compliance can lead to significant penalties, including personal liability. For important facilities, the penalty can be up to 7 million euros or 1.4% of the worldwide annual turnover.

Our recommendation for dealing with NIS2 (until enacted)

In addition to the outlined need for action, we recommend taking a generalist approach to address the entry into force of NIS2. This will ensure that your company is adequately prepared for NIS2 and on track to enhance your cybersecurity measures. Those actions include the following:

1. Examination of NIS2 concern with associated categorisation
   To ensure NIS2 compliance, the first step is to determine if your company falls into one of the relevant sectors and meets the required criteria, such as having a certain number of employees or reaching a specific annual turnover and balance sheet. Additionally, if your company is a critical infrastructure operator or considered an essential or important institution based on another criterion, NIS2 regulations are applicable.
2. Derivation of company-specific requirements
   Based on the results of step one, you need to determine your company-specific requirements. These requirements primarily involve developing risk management measures to address cyber threats to your network and information systems. The extent and complexity of these measures will depend on your company's unique circumstances. However, it is important to note that 10 non-negotiable minimum requirements must be met by the technical and organisational measures in place to protect company information.
3. Implementation of the NIS2 gap assessment
   Based on the requirements that pertain to your company, we suggest conducting a gap assessment. This assessment will compare your company's control framework with the requirements outlined in the NIS2. If your company is already regulated and operates within a consolidated ISMS, you can prioritise exploring the innovations that arise from NIS2. The objective of the NIS2 gap assessment is to identify any gaps that exist so that they can be evaluated and addressed within your organisation's risk management process.

4. Setting up or adapting the ISMS for NIS2 through continuous improvement
   As part of the ongoing improvement process of your ISMS, it is crucial to address the identified gaps. If your ISMS is not yet fully developed, it is important to commence its development promptly. Initially, when focusing on the continuous-improvement process and the development of an ISMS, prioritise the following three key areas: cybersecurity within the ISMS, inclusion of the supply chain in risk management, and the establishment of a reporting process and communication with the Member State supervisory authority.
5. Monitoring of changes to the NIS2 and related online platforms of the supervisory authorities
   Laws and requirements evolve over time, and NIS2 is a prime example of this as an extension of the 2016 NIS Directive. It is crucial to continuously monitor for further updates in the NIS2 domain to ensure that you do not overlook any changes or lag behind. In addition to keeping an eye on developments within Member States' supervisory authority, we strongly advise regularly visiting the ENISA's online platform to stay informed about the latest information on cybersecurity.



Face the Future with Confidence®

protiviti®
Global Business Consulting