2023

What's changing under the new NIS2 Directive

How a holistic Identity security framework can help

Why Identity is Important Whilst Preparing for NIS2 Compliance

okta

Contents

3 Introduction

4 Overview of NIS2

5 Preparing for NIS2

7 The importance of Identity in NIS2 compliance

9 Holistic Identity security framework with Okta

11 Consequences for non-compliance with NIS2

NIS2 and securing your supply chain

12 Formalise your incident response plan

Educate your people

13 Mapping NIS2 to ISO 27001

15 Conclusion

Introduction

The European Union's Network and Information Systems (NIS) Directive was adopted in 2016 and entered into force in 2018. It aimed to ensure a high common level of security of network and information systems across the EU and required the implementation of security measures and reporting obligations for operators of essential services and digital service providers. The Directive was recently updated with the NIS2 Directive, which further raises the security measures and reporting obligations and expands the scope to new sectors.

This whitepaper aims to provide an overview of NIS2, how it can be mapped to popular security frameworks such as ISO 27001 and highlight the importance of Identity, and what organisations can do to prepare for NIS2 implementation.

Overview of NIS2

NIS2 is an updated version of the original NIS Directive, aimed at enhancing the cybersecurity of organisations in the European Union that provide essential and critical infrastructure to the European economy. The original NIS Directive was adopted in 2016 and came into force in May 2018. NIS2 was formally adopted by the Parliament and then the Council in November 2022. It entered into force on 16 January 2023, and Member States now have until 17 October 2024, to transpose its measures into national law.

As large enterprises incorporate NIS2 controls into their third-party risk programmes, most organisations will need to address NIS2 in order to be competitive.

NIS2 applies to all entities with 50 employees and an annual turnover of 10 million EUR, that provide essential or important services to the European economy and society, including companies and suppliers, which also includes organisations established outside of the EU but provide services within the EU. While the Directive has exclusions for small organisations, one should expect that larger enterprises will incorporate NIS2 controls into their third-party risk programmes, and therefore, most organisations will need to address NIS2 in order to be competitive.

The directive requires entities subject to NIS2 to implement appropriate and proportionate technical and organisational measures to mitigate the risks posed to the security of network and information systems, as well as the physical environment, including data centres. It also mandates organisations to report security incidents to competent authorities and introduces more stringent reporting requirements for those providing digital infrastructure services.

Preparing for NIS2

EU member states have until October 2024 to incorporate the NIS2 Directive into their national laws. Organisations should use this time to begin preparing for the directive by taking the following steps:

- **Identify, assess, and address your risks:** NIS2 requires management bodies of essential and important entities to take appropriate and proportionate technical, operational, and organisational measures to manage the risks posed to the security of network and information systems and the physical environment. Organisations should identify their risks, assess their impact and take steps to mitigate them.
- **Evaluate your security posture:** A risk and security evaluation can assist in pinpointing vulnerabilities, such as unmanaged passwords or misconfigured or inactive accounts that are susceptible to credential theft. Organisations should conduct a comprehensive security assessment to evaluate their security posture and identify areas for improvement such as introducing phishing-resistant authentication factors.
- **Take steps to safeguard privileged access:** Adversaries can exploit privileged accounts to orchestrate attacks, take down critical infrastructure, and disrupt essential services. NIS2 advises critical entities to limit access to administrator-level accounts and to regularly rotate administrative passwords. Organisations should take steps to safeguard privileged access by implementing best practices such as least privilege access, continuous authentication, and threat analytics.

October 2024

Deadline by which NIS2 must be incorporated into national law

- **Strengthen your ransomware defences:** Costly and debilitating ransomware attacks are a major concern for EU regulators and one of the primary drivers of the NIS2 Directive. Organisations should introduce security solutions and best practices to proactively defend against ransomware. This includes using endpoint privilege security solutions to enforce the principle of least privilege, control applications, and augment Next-Generation Antivirus (NGAV) and Endpoint Detection and Response (EDR) solutions.
- **Move to a Zero Trust strategy:** Traditional perimeter-based security architectures, conceived to defend trusted enterprise network borders, aren't suited for the world of cloud services and hybrid workforces. Adopt a Zero Trust approach, implementing several layers of defence such as least privilege access, continuous authentication, and threat analytics to validate all access attempts.
- **Scrutinise your software supply chain:** Supply chain attacks are a major concern for EU regulators and a prime motivator for the NIS2 Directive. Organisations should take a fresh look at their software supply chain and consider implementing a secrets management solution to mitigate risk.

The importance of Identity in NIS2 compliance

Security is difficult as it involves navigating the complex interplay of; people, processes and technology. Within this landscape, Identity assumes a crucial role as a cornerstone of cybersecurity strategies and maintaining robust cyber hygiene while achieving compliance with regulatory frameworks like NIS2.

Identity serves as the bedrock that underpins security policies, operational procedures, and IT systems governing access to critical information within an organisation. It encompasses the verification of user identities, authentication of their access, authorisation of their actions and permissions, and the management of access controls. Effective Identity governance ensures that only authorised individuals are granted access to specific resources, allowing them to utilise those resources appropriately with the least privileges necessary to fulfil their responsibilities. Additional layers of security, such as Multi-Factor Authentication, further enhance the protection of identities.

In the context of regulatory compliance, such as NIS2, Identity provides a powerful tool for mitigating risks associated with unauthorised access. It establishes accountability within the organisation by enabling the identification of individuals responsible for actions, thereby facilitating traceability. Furthermore, Identity management enables efficient user management, streamlining administrative processes while maintaining a secure organisational landscape. A well-developed Identity management solution provides an easily accessible audit trail across an organisation's critical applications that demonstrate appropriate access control and authorisation management.

> Identity is the bedrock underpinning security policies, operational procedures and IT systems governing access to an organisation's critical information.

Here are some of the areas in which Identity management helps with NIS2 compliance:

1. **Access Control:** Properly managing user identities enables organisations to enforce strong access control measures. By assigning unique identities to individuals or entities, organisations can ensure that only authorised personnel can access specific resources or perform certain actions within their network and information systems.
2. **Authentication and Authorisation:** Identity management facilitates the implementation of robust authentication mechanisms, such as multi-factor authentication, to verify the Identity of users before granting access. It also enables organisations to define granular authorisation policies, ensuring that users have appropriate privileges and permissions based on their roles and responsibilities.
3. **Incident Response:** In the event of a security incident, Identity management plays a crucial role in identifying the individuals or entities involved. Properly managing identities allows organisations to track and trace actions performed within their systems, aiding in incident investigation, attribution, and remediation.
4. **Compliance Monitoring:** NIS2 requires organisations to implement measures for managing risks to the security of network and information systems. Identity management provides organisations with the ability to monitor and audit user activities, ensuring compliance with regulatory requirements. It enables organisations to demonstrate accountability by documenting who accessed specific resources and when.

By recognising the importance of identity within cybersecurity strategies and compliance efforts, organisations can establish a solid foundation for safeguarding their information assets, maintaining regulatory adherence, and fostering a resilient and secure environment.

Holistic Identity security framework with Okta

Okta's comprehensive approach to Identity management is designed to protect digital identities and safeguard an organisation's people, applications, and devices. Recognising that any user, whether human or non-human, can become privileged and pose a security risk, Okta emphasises the importance of identities in implementing sound cybersecurity hygiene, particularly within a Zero Trust framework.

By focusing on effective and adaptable mechanisms for regulating access to data and securing information, Okta's solutions incorporate continuous authentication and authorisation practices that align with Zero Trust principles. Through tight control of access to cloud-based resources and continuous monitoring and auditing of user activity, Okta ensures compliance while mitigating risks. Implementing a comprehensive Identity strategy is crucial for protecting critical infrastructure against various threats, including malicious attacks, ransomware, and software supply chain vulnerabilities.

Moreover, it can help organisations comply with NIS2 Article 21 requirements which covers the Cybersecurity risk management measures and reporting obligations and proposes a wide range of recommendations. Okta offers a range of security solutions to safeguard organisations against cyber threats and protect identities and sensitive data including a state-of-the-art, phishing-resistant Multi-Factor Authentication solution - an explicit requirement of NIS2.

Okta's platform is scalable and flexible, enabling organisations to implement policy-based authentication approaches across their systems and environments. This empowers customers to deliver services, enhance user experience, and ensure data privacy and protection.

Implementing a comprehensive Identity strategy is crucial for protecting against threats like malicious attacks, ransomware, and software supply chain vulnerabilities.

Okta's Workforce Identity Cloud (WIC) is a solution that protects access for every user – employees, contractors, and business partners – no matter where they are or what device they're using. It is built to help leaders drive productivity and efficiency, modernise IT and infrastructure, and enhance security. Through easily configurable policies Okta Workforce Identity Cloud (WIC) enables you to fine tune the security measures needed for each access risk category providing the right balance between security friction and ease of access. Features such as Single Sign-On (SSO), Adaptive Multi-Factor Authentication (MFA), and Passwordless Authentication allow organisations to improve their cybersecurity posture and offer a seamless experience for their employees.

API Access Management, Advanced Server Access, and Access Gateway allow organisations to centralise administration, manage privileged access, and automate configuration, driving efficiencies across the business. Okta Identity Governance (OIG) solution combines Okta Workflows, Okta Lifecycle Management & Okta Access Governance to help mitigate modern risks and improve efficiency.

As a result, a modern Identity framework like Workforce Identity Cloud helps organisations simplify compliance with NIS2 by improving cybersecurity, implementing more robust access management processes and guaranteeing reliable delivery of Identity services with a best-in-class uptime.

Consequences for non-compliance with NIS2

€10 million

or 2% of annual revenues fine for non-compliance with NIS2, whichever is higher.

Failure to comply with NIS2 may result in organisations being subject to administrative fines. The NIS2 directive distinguishes between Essential Entities and Important Entities where the former includes public and private companies in sectors such as transportation, energy and utilities, healthcare, public administration, and digital infrastructure (including Cloud service providers) with a fine level of €10 million or 2 % of global annual revenue, whichever is higher, and for Important entities, which includes public and private companies in sectors such as food supply, chemicals, postal services, waste management, manufacturing etc of €7 million or 1.4 % of global annual revenue, whichever is higher. In addition, Article 32(5) foresees that Essential Entities which fail to comply with the enforcement measures can see their certifications frozen, and their chief executive officer may be impeded from exercising his/her managerial functions.

NIS2 and securing your supply chain

Ensuring the integrity and security of the supply chain is a fundamental aspect of NIS2, given the potentially devastating consequences witnessed during events like the pandemic.

To minimise the risk of third-party cyberattacks, organisations must go beyond conducting regular risk assessments of their supply chain. It is crucial to ensure that all supply chain partners comply with NIS2 requirements on a daily basis. This involves implementing security measures within the supply chain, such as conducting vendor risk assessments and audits, establishing contractual agreements that outline specific security requirements, and maintaining ongoing monitoring and communication with suppliers. By ensuring that suppliers adhere to the updated NIS2 requirements, organisations can effectively reduce their overall risk and strengthen the security of their digital infrastructure. Organisations should expect their vendors to provide industry-standard reports such as ISO27001, external penetration testing reports, and allow their customers to perform their own penetration tests.

Okta's Workforce Identity Cloud (WIC) and Customer Identity Cloud (CIC) provide solutions to protect identities in both B2B and B2C relationships and serve as foundational components in ensuring compliance with NIS2.

Formalise your incident response plan

The NIS2 regulation necessitates a swift incident reporting timeline, requiring the initial report to be filed within 24 hours of an event, followed by a technical report under 72 hours. To meet this demand, it is crucial to establish a well-structured incident response plan. Here Okta plays a crucial role in this preparation by providing comprehensive visibility into authorisation and access attempts across various infrastructures and technologies. This capability assists organisations in reconstructing the timelines of network or resource reconnaissance, a crucial component in incident reporting. To ensure compliance with NIS2 requirements, it is advisable to meticulously scrutinise your event notifications, information collection, and reporting procedures. Regular drills might also be essential to evaluate and enhance the effectiveness of your response plan.

Educate your people

NIS2 emphasises the importance of cybersecurity and cyber hygiene training for employees, contractors, and third-party suppliers. Step up efforts to improve cyber awareness and foster a security-first culture within your organisation. Ensure that employees understand their role in maintaining the security of network and information systems and are aware of the potential risks and threats they may encounter.

Mapping NIS2 to ISO 27001

ISO 27001 is an international standard for information security management that provides a framework for establishing, implementing, maintaining and continually improving an information security management system (ISMS). The standard is designed to help organisations manage their information security risks and protect their information assets.

NIS2 and ISO 27001 share a common goal of improving the security of network and information systems. As such, NIS2 can be mapped to ISO 27001, allowing organisations to leverage their existing ISO 27001 certification to meet the NIS2 requirements.

The following table presents a broad yet not comprehensive correlation between the EU's NIS2 Directive requirements and ISO 27001 controls from Annex A in the ISO/EIC 27001:2023 standard. Given the complexity and the unique objectives and scopes of this exercise, it's vital to note that this general mapping is not exhaustive. Specialised professionals should perform an in-depth mapping tailored to your specific context. Thus, consider this table as an initial point of reference. To fully map NIS2 to ISO 27001, organisations should perform a gap analysis to identify any areas where their ISO 27001 implementation falls short of the NIS2 requirements. They should then update their ISMS to address any gaps and ensure compliance with both the ISO 27001 standard and NIS2.

Area	NIS2 Requirements	Relevant ISO 27001 Control
Risk Management	Requires entities to have risk management practices	A.6.1 (Internal organisation) A.8 (Asset management) A.12.1 (Operational procedures and responsibilities)
Security of systems and facilities	Requires entities to ensure the security of their network and information systems	A.11 (Physical and environmental security) A.12.1 (Operational procedures and responsibilities) A.13 (Communications security) A.14 (System acquisition, development and maintenance)
Incident Handling	Entities should be prepared to respond swiftly and appropriately to incidents	A.16 (Information security incident management) A.12.6 (Technical vulnerability management)
Business Continuity Management	Entities should have plans in place to ensure the continuity of their services	A.17 (Information security aspects of business continuity management)
Monitoring, Auditing and Testing	Entities should perform regular audits and tests to validate their security measures	A.18.2 (Internal audit) A.12.7 (Information systems audit considerations)
Compliance with legal and contractual requirements	Entities should comply with all relevant legal and contractual security requirements	A.18 (Compliance) A.15.2 (Information security in project management)
Incident Reporting	Entities should report incidents with a significant impact	A.16.1 (Management of information security incidents and improvements)
Supply Chain Security	Entities should ensure security within their supply chain	A.15 (Supplier relationships)

Conclusion

NIS2 is a comprehensive cybersecurity regulation designed to improve the security of network and information systems across the EU for organisations offering infrastructure of important and critical nature. Organisations that are subject to the directive should take steps to ensure they are compliant with the requirements, including identifying and managing risks, evaluating their security posture, safeguarding privileged access, strengthening their ransomware defences, adopting a Zero Trust strategy, scrutinising their software supply chain, formalising their incident response plan and educating their people.

There are several cyber- and information security frameworks that offer a good match to the requirements. ISO 27001 is one of these. By mapping NIS2 to ISO 27001, organisations can leverage their existing ISO 27001 certification to meet the NIS2 requirements, saving time and resources. Ultimately, compliance with NIS2 and ISO 27001 can help organisations mitigate cybersecurity risks, protect their information assets and maintain the trust of their customers and stakeholders.

To discover how Okta Workforce Identity Cloud and Okta Customer Identity Cloud and other solutions can support your organisation with NIS2 compliance, **reach out to our team.**

About Okta

Learn more at: www.okta.com Okta is the leading independent provider of Identity for developers and the enterprise. The Okta Identity Cloud securely connects enterprises to their customers, partners, and employees. With deep integrations to over 7,000 applications, the Okta Identity Cloud enables simple and secure access for any user from any device.

Thousands of customers, including 20th Century Fox, Adobe, Dish Networks, Experian, Flex, LinkedIn, and News Corp, trust Okta to help them work faster, boost revenue and stay secure. Okta helps customers fulfil their missions faster by making it safe and easy to use the technologies they need to do their most significant work.

okta

EMEA Headquarters
20 Farringdon Road
London EC1M 3HE, UK
info_emea@okta.com
+44 203 389 8779