zscaler™

WHITE PAPER

Working towards NIS2 compliance – how Zero Trust needs to be a critical part of this journey

Table of Contents

Executive Summary

NIS2 and the Role of a Zero Trust Model in Enhancing Cyber Resilience

The enactment of the Network and Information Security Directive 2 (NIS2) marks a significant evolution in the European Union's (EU) commitment to bolstering cybersecurity across its member states. NIS2 replaces the earlier NIS Directive, and expands its scope to a broader array of sectors and subsectors while also tightening security requirements, including elevating cybersecurity to a management and governance imperative. While NIS2 came into force in 2023, the key deadline is October 2024, when EU member states must have enforceable national laws in place implementing NIS2 Because NIS2 implementation may vary slightly in each member state, this whitepaper focuses on the high-level requirements and principles of the Directive itself.

No single solution or software vendor can guarantee compliance with NIS2. An adherence to Zero Trust principles, however, (which the Directive itself suggests entities adopt as a basic cyber hygiene practice) addresses a number of criteria called for by the Directive. Implementing Zero Trust architecture within an organization's environment, distributed elements of a network, and those of an organization's third parties can radically shrink attack surfaces and remove a range of technical variables that can hinder progress towards NIS2 compliance. Zero Trust should be a primary vehicle organizations use to enhance resilience; a strong Zero Trust vendor partner can support organizations' compliance journeys.

The journey to compliance must be structured and communicated across organizations in scope of the new Directive. Recent surveys of European IT teams by Zscaler explored the state of readiness of organizations to comply.

Seventy-one percent of the IT leaders surveyed believe that security modernization requires a significant mindset change, not just a compliance exercise.

Yet the attitudes held by different stakeholders that will drive compliance varies dramatically. While 80% of IT leaders surveyed feel confident their organizations will be compliant by the deadline, only 53% believe their teams fully understand the scope of obligations under NIS2. When asked about corporate leadership understanding of compliance obligations, that number falls to 49%. More than 60% of survey respondents believe that NIS2 will require a significant departure from their current security strategy.

Zscaler is positioned uniquely to assist organizations in navigating changes introduced by NIS2 given our expertise in cloud security. By adopting Zscaler's Zero Trust Architecture, organizations of all sizes can address the Directive's core requirements—enhancing their defensive mechanisms, reducing their exposure to cyber risks, and streamlining compliance activities. Zero Trust principles align closely with the goals of NIS2 by systematically eliminating unnecessary access rights, rigorously verifying all connections, and minimizing the potential impact of security incidents. Zscaler provides an array of capabilities and tools that support compliance efforts with specific provisions of NIS2, including policy enforcement, incident detection, and response processes.

Overview of the NIS2 Directive and Its Scope

NIS2 came into force in 2023, with an EU member state implementation deadline of October 2024. EU policymakers enacted this critical new legislation in response to the need for the EU to raise its cyber resilience in an era of increasing cyberattacks on European citizens, businesses, and economies. NIS2 emphasizes the responsibility of entities to ensure network and information system security, calling on them to have a culture of governance and comprehensive risk management frameworks. NIS2 is consistent with a growing trend in the EU towards more direct regulation of cyber resilience efforts. (For example, the Digital Operational Resilience Act (DORA), which will come into force in January 2025, is a separate framework for managing and mitigating ICT risk in the financial sector.)

The NIS2 Directive adds new industry sectors, as well as new types of entities within existing sectors, to the original NIS Directive. This expansion responds to the growing realization that a wide array of economic and societal activities are critically dependent on IT infrastructure, that cyberthreats to these sectors are growing, and that disruptions can have cascading effects across the entire EU.

Industry sectors in NIS2 are categorized as either "essential" or "important," to reflect their criticality or the service they provide. While cybersecurity and incident reporting requirements for both groups are the same, the two categories of entities will fall under slightly different supervision and enforcement regimes, including size of potential fines for non-compliance (more on this below).

> "With the deadline on the horizon, organizations face hastened compliance efforts, potentially at the expense of other vital cybersecurity facets. 60% of survey participants voice apprehensions that the concentrated efforts on NIS 2 compliance may result in the neglect of other critical areas of security. Consequently, it is imperative for organizational leaders to extend substantial support to IT departments, ensuring a holistic approach to compliance that mitigates risks of vulnerabilities and operational setbacks."
>
> **James Tucker,** Head of EMEA CISOs in Residence at Zscaler

Sectors and sub-sectors covered by NIS2[1]

Essential Entities ("Sectors of High Criticality")	
Energy	Includes electricity, oil, gas, district heating and cooling, and hydrogen
Transport	Includes air, rail, water, and road
Banking (credit institutions)	
Financial market infrastructures	
Health	Includes healthcare, pharmaceuticals
Drinking Water	
Waste Water	
Digital infrastructure	Includes Internet Exchange Point (IXP) providers, DNS service providers, TLD name registries, cloud computing service providers, data center service providers, content delivery network providers, trust service providers, providers of public electronic communications networks, and providers of publicly available electronic communications services
ICT service management (business-to-business)	Includes managed service providers and managed security service providers
Public administration	Public administration entities of central governments and regional levels as defined by member states' national laws
Space (operators of ground-based infrastructure)	
Important Entities ("Other Critical Sectors")	
Postal and courier services	
Waste management	
Manufacture, production and distribution of chemicals	
Production, processing and distribution of food	
Manufacturing	Includes a wide range of manufacturing such as medical devices, computers and electronics, electrical equipment, machinery and equipment, motor vehicles, transport equipment
Digital providers	Includes providers of online marketplaces, providers of online search engines, and providers of social networking services platforms
Research organizations	

1. There are some exceptions to these categories; see Annex I and II of the Directive for more details. Public administration entities whose activities are predominantly national security, public security, defense or law enforcement are also excluded. Further, the Directive applies only to entities which qualify as "medium-sized enterprises" in the EU (enterprises with more than 250 persons and annual turnover exceeding EUR 50 million). At the same time, some exceptions in turn apply NIS2 to some smaller entities.

Zscaler's Zero Trust Approach Supports the NIS2 Directive

Zscaler's Zero Trust Exchange™ Platform reduces the complexity associated with traditional network security, making it easier for organizations to meet the requirements of the NIS2 Directive. The Zero Trust Exchange™ is a cloud-native, SASE-based architecture that has been purpose-built to satisfy the demands of global business operations with diverse technology and operating requirements. Employing granular segmentation to compartmentalize a network, enforcing least-privileged access to restrict user permissions, and maintaining continuous traffic monitoring are proactive measures that help to identify and respond to threat actors, minimizing potential damage and the impact of attacks.

The Zero Trust Exchange™ also allows organizations to reduce their attack surface, prevent lateral movement, and lower breach risks by abstracting security from network infrastructure. This ensures that users securely connect to applications without exposing networks to the internet, significantly reducing the risk of attacks. The platform's capabilities support compliance efforts required under NIS2 mandates for secure data handling, access controls, and incident management.

The platform enhances security by protecting all traffic, users, and devices, ensuring real-time threat blocking and comprehensive traffic inspection. Zscaler also improves administrator productivity with unified global management and policy administration, eliminating the need for hardware maintenance and enabling a focus on value-added activities. The Zscaler platform improves internet performance for end users, and direct connections to the internet, and our compliance with major security frameworks such as ISO 27001 and SOC2 Type II further enhance the overall user experience and organizational security posture.

Further details regarding Zero Trust and Zscaler's approach to Zero Trust Architecture can be found on Zscaler's Zpedia.

Zscaler Alignment with NIS2

Zscaler's comprehensive approach to security and compliance allows us to quickly react and align with existing, new, and emerging regulations such as NIS2. Zscaler's internal cybersecurity risk management program ensures adherence to internationally recognized standards such as ISO 27001 and SOC 2. Aligning with these foundational standards allows Zscaler to effectively embed a diverse set of security controls to identify, prevent, detect, respond, and recover from associated threats within our products and services. Zscaler leverages a structured common controls framework that focuses on core cybersecurity competencies such as the establishment of an information security risk management program, secure supply chain practices, third-party risk management, continuous risk assessments, incident reporting, vulnerability disclosure and more. An up-to-date list of security and compliance standards that Zscaler maintains can be found on Zscaler's compliance overview **page**.

In addition, Zscaler maintains the Zscaler Trust **Portal** to provide customers real-time insights into Zscaler operations, serving as the primary communications forum for Zscaler-related **incidents** and **advisories**.

Key NIS2 Compliance Areas and How Zscaler Can Help

NIS2 delineates the responsibility of entities to ensure network and information system security, calling on them to have a culture of governance and established, comprehensive, and well-integrated risk management frameworks. To meet these goals, NIS2 includes cybersecurity risk management measures, governance measures, incident reporting requirements, and supervision and enforcement, all described below.

In the European IT leader survey referenced above, 56% of respondents told Zscaler that their teams feel like they lack support from leadership to meet the NIS2 compliance deadline. To support their compliance journeys, IT leaders surveyed said that the most significant changes required in their organizations were the following:

- Updating technology stacks and cybersecurity solutions: 34%
- Educating employees: 20%
- Educating leadership: 17%

NIS2 Cybersecurity Risk Management Measures

Entities in scope of the Directive must adopt proactive technical, operational, and organizational measures to manage the risks posed to the security of network and information systems which those entities use for their operations or for the provision of their services, and to prevent or minimize the impact of incidents on recipients of their services and on other services organizations may provide.

Article 21 of the Directive lists the minimum cybersecurity risk management measures organizations must take, while Recitals 78 and 89 provide more information about what the law's authors expect.

- **Article 21 (minimum cybersecurity risk management measures)**, specifies that entities must implement policies on risk analysis and information system security; business continuity and crisis management; supply chain security, including the quality and secure development procedures of products and cybersecurity practices of their suppliers and service providers; basic cyber hygiene practices and cybersecurity training; policies and procedures regarding the use of cryptography/encryption; human resources security, access control policies and asset management; and use of multi-factor authentication or continuous authentication solutions.
- **Per Recital 78**, cybersecurity risk management measures implemented by entities in scope of the Directive should take into account the degree of dependence of the entity on network and information systems; identify any risks of incidents; prevent, detect, respond to and recover from incidents and mitigate their impact; cover stored, transmitted and processed data; and provide for systemic analysis, taking into account the human factor.
- **Recital 89** urges entities to implement a range of recommended basic cyber hygiene practices namely, Zero Trust principles, software updates, device configuration, network segmentation, identity and access management or user awareness, and training for staff and awareness-raising concerning cyber threats, phishing or social engineering techniques. Recital 89 also urges entities to pursue cybersecurity enhancing technologies, such as artificial intelligence (AI) or machine-learning (ML) systems, to enhance their capabilities and the security of network and information systems.

How Zscaler Can Help: Below we describe generally how Zscaler can help entities align with particular aspects of these provisions. For a detailed mapping of specific Zscaler solutions and tools that support these provisions, please contact your local Zscaler representative. General content and white papers on Zscaler solutions can be found at https://www.zscaler.com/resources?type=white-papers.

NIS2 Governance and Risk Management

NIS2 places ultimate responsibility on company leadership. Management must approve and oversee implementation of the entity's cybersecurity risk-management measures. Management must also follow cybersecurity training, and offer similar training to their employees on a regular basis, so that they gain sufficient knowledge and skills to enable them to identify risks and assess cybersecurity risk-management practices and their impact on the entity's services.

How Zscaler Can Help: Zscaler provides comprehensive security features across its suite of services, designed to assist organizations in minimizing their attack surface and ensuring the effectiveness of applied security controls across a customer's governance and risk management program.

Zscaler Resilience™ is a complete set of capabilities that ensures uninterrupted business continuity during blackouts, brownouts, or catastrophic black swan events.

Zscaler Internet Access (ZIA) and Zscaler Private Access (ZPA) enforce traffic flows and provide security event and transaction logs for correlation and management, enabling organizations to monitor and mitigate potential threats effectively.

Zscaler's Zero Trust Exchange™ ensures that users are not placed on the network and applications are never exposed to the internet, significantly reducing the attack surface. The solution also lets organizations create and enforce policies around the generative AI sites users can interact with to ensure protection of sensitive data.

Zscaler's SSL inspection capabilities further enhance security by decrypting HTTPS traffic to detect and block malicious content.

Zscaler's Risk360™ and Zscaler Posture Control (ZPC) offerings enable continuous monitoring and vulnerability detection, allowing organizations to proactively address security risks.

Zscaler Digital Experience (ZDX) provides device inventory inventory tracking, ensuring that service components are appropriately identified and securely retired when necessary, contributing to minimizing the attack surface.

Zscaler's Nanolog Streaming Service (NSS) facilitates seamless communication between Zscaler cloud and third-party security solution devices, enabling real-time streaming of logs to customers' SIEM systems through VM-based or Cloud NSS options.

Zscaler Cloud Intrusion Prevention Service (IPS), integrated with technologies like firewalls and sandboxes, provides comprehensive threat protection against various attacks, leveraging custom and industry-leading signatures for real-time monitoring and policy enforcement. Moreover, organizations can proactively identify and remediate vulnerabilities using Zscaler capabilities such as ZIA's Advanced Threats Protection and Mobile Malware Protection policies, while Risk360 offers insights into the external attack surface and lateral propagation risk, enabling informed decisions to enhance an organization's security posture and reduce their mean-time-to-respond (MTTR).

Finally, all customers can register to use the ZScaler Trust Portal to report incidents/suspected incidents.

NIS2 Incident Reporting Requirements (Article 23)

Entities must notify authorities of any incident that has a significant impact on the provision of their services. Where appropriate, entities also must notify the recipients of their services of significant incidents that are likely to adversely affect service provision. NIS2 defines a significant incident as one that has caused or is capable of causing severe operational disruption of the services or financial loss for the entity concerned, or it has affected or is capable of affecting other natural or legal persons by causing considerable material or non-material damage.

The incident reporting timeline is as follows:

- An "early warning" within 24 hours of becoming aware of the significant incident;
- A formal incident notification within 72 hours of becoming aware of the significant incident, providing an initial assessment of the incident, including its severity and impact, as well as (where available) indicators of compromise;
- A final report within one month detailing the incident, including its severity and impact; the type of threat or root cause likely to have triggered the incident; applied and ongoing mitigation measures; and (where applicable) cross-border impacts.
- During this process authorities can request an intermediate report on relevant status updates.

How Zscaler Can Help: Zscaler's cloud-based security solutions offer real-time threat detection and mitigation capabilities, ensuring that organizations can quickly identify and mitigate threats. Also, by deemphasizing traditional perimeter-based defenses in favor of ongoing identity verification and authorization, Zscaler's Zero Trust Architecture helps to prevent lateral movement that could worsen the severity should a breach occur. By evaluating each access request based on identity, authorization, and the surrounding context, the entire environment is better protected from cyber incidents.

NIS2 Supervision and Enforcement (Articles 32 and 33)

EU member states can use supervision and enforcement powers on entities that breach NIS2's cybersecurity risk-management measures and reporting obligations. The supervisory and enforcement regimes for essential and important entities are slightly differentiated: for essential entities supervision is ex-ante whereas for important entities it is ex post (when there is evidence, indication or information that an entity does not comply with NIS2).
In general, authorities can subject covered entities of either category to:

- On-site inspections and off-site supervision
- Targeted security audits carried out by an independent body or a competent authority
- Security scans
- Requests for information necessary to assess the cybersecurity risk-management measures adopted, including documented cybersecurity policies
- Requests to access data, documents and information necessary for supervision
- Requests for evidence of implementation of cybersecurity policies

NIS2 also states that management can be held personally liable for infringements of NIS2, including potential temporary bans from holding management positions, and as a last resort authorities have the power to temporarily suspend a certification or authorization related to the entity's relevant services provided or activities carried out.

EU member states can also impose administrative fines for instances of NIS non-compliance. For essential entities, administrative fines can reach €10 million or 2% of total worldwide annual turnover in the preceding financial year, whichever is higher. For important entities, fines can reach €7 million or 1.4 % of total worldwide annual turnover in the preceding financial year, whichever is higher.

How Zscaler Can Help: Zscaler supports organizations in preparing for and responding to audits and regulatory scrutiny through comprehensive logging, consistent policy enforcement, and detailed reporting.

For more information about NIS2 and Zscaler's capabilities, please contact your local Zscaler representative.

+1 408.533.0288 Zscaler, Inc. (HQ) • 120 Holger Way • San Jose, CA 95134 zscaler.com