netskope

Compliance Series

EU Network and Information Security (NIS2) Directive

Guide for Netskope Products

Table of Contents

INTRODUCTION 2

SUMMARY 2

NIS2 GUIDE FOR NETSKOPE PRODUCTS 4

Version	Name	Email	Date
V1.0	Neil Thacker	nthacker@netskope.com	15 January, 2024

Introduction

The Network and Information Systems Directive 2 (NIS2) is a legislative framework developed by the European Union to address cybersecurity concerns and bolster the resilience of critical infrastructure and digital service providers. Enacted as a successor to the original NIS Directive, NIS2 introduces updated measures to adapt to the evolving threat landscape. The NIS2 Directive entered into force in January 2023 however the deadline for EU member states to transpose NIS2 into national law is 17th October 2024.

Summary & NIS2 updates

The updated NIS2 updates include the following:

Scope Expansion
NIS2 broadens its scope to cover a wider range of sectors, including additional digital service providers and entities considered essential for societal and economic functions.

Risk Management and Incident Reporting
The directive emphasizes the adoption of risk management practices by organizations to identify and mitigate potential cybersecurity threats. It also mandates incident reporting requirements for significant disruptions to essential services.

Cross-Border Cooperation
NIS2 promotes increased collaboration among EU member states, encouraging the sharing of information and best practices to strengthen the collective response to cyber threats.

Security Measures and Standards
Organizations within the scope of NIS2 are required to implement appropriate security measures to safeguard their networks and information systems. The directive references established cybersecurity standards and best practices.

Regulatory Oversight and Competent Authorities
NIS2 establishes competent authorities within each member state responsible for enforcing the directive. These authorities play a key role in ensuring compliance, conducting audits, and managing incident response at the national level.

Penalties and Enforcement
The directive outlines penalties for non-compliance, aiming to incentivize organizations to prioritize cybersecurity. Sanctions may vary based on the severity of the breach and the impact on essential services.

Continuous Monitoring and Adaptation
Recognizing the dynamic nature of cyber threats, NIS2 encourages continuous monitoring and adaptation of security measures to address emerging risks effectively.

Coordinated EU Response
In the event of a cross-border cyber incident affecting multiple member states, NIS2 facilitates a coordinated EU-wide response to minimize the impact and enhance overall cybersecurity resilience. This includes significant incidents to be reported within 24 hours, with details added within 72 hours.

The NIS2 directive represents a concerted effort by the European Union to fortify cybersecurity defences, protect critical infrastructure, and promote a collaborative approach to tackling cyber threats across borders.

NIS2 will apply to organizations within the following key sectors:

Sectors of High Criticality:

- Energy
- Transport
- Banking
- Financial market infrastructures
- Health
- Drinking water
- Waste water
- Digital infrastructure
- ICT service management
- Public administration
- Space

Other Critical Sectors:

- Postal and courier services
- Waste management
- Chemicals
- Food
- Manufacturing
- Digital providers
- Research

The full list with details including type of entity is available here (see Annex I & II) - https://eur-lex.europa.eu/eli/dir/2022/2555

Organizations falling within the directive's scope are therefore urged to proactively implement robust security measures and collaborate with relevant authorities to ensure a resilient and secure digital environment.

NIS2 Guide for Netskope Products

The NIS2 Directive is comprised of 9 chapters and 46 articles in total. Each chapter directs members states on how to adopt the requirements of the Directive. Given that NIS2 is a principle-based Directive, most of the Directive gives guidance to member states however there are several technical, operational, and organisational approaches that can be used to meet the requirements of the Directive for organisations.

At the time of publication of this whitepaper, the European NIS Cooperation Group have not updated their guidelines on security measures to clarify the practical scope of NIS2. Once published, this guide will be updated to include the updated security measures and the direct mapping to Netskope products.

The following table includes the measure referenced under **Chapter IV, Article 21, Section 2** along with a short description of the Netskope control and coverage. The coverage listed is specific to web, cloud, threat protection, data protection and on-premises access control provisions using the Netskope platform and suite of products.

Chapter IV Article 21	Netskope Control & Coverage
Policies on risk analysis and information system security	The Netskope platform provides organisations with the ability to enforce policy throughout their ecosystem of Critical Information Systems (CIS) including web, cloud and on-premises apps and services. The Netskope platform allows for organisations to: - Map and inventory its CIS ecosystem of web and cloud services including suppliers and provision access for internal and external stakeholders who manage critical assets - Perform information system security assessments and audits of web or cloud critical assets and Critical Information Systems (CIS) hosted in the cloud - Report on risk analysis findings with options to auto-remediate for cloud services
Incident handling	The Netskope platform supports event and incident handling and can apply prevent, detect, analyse, or contain actions subject to policy definition. The Netskope platform can: - Apply mitigation controls to contain or limit the impact of CIS compromise from external or internal threat actors - Detect and prevent malicious activity within networks and CIS systems. Detections include both signature and non-signature-based detections (sandbox, Machine-Learning (ML) based detections)
Business continuity	The Netskope platform provides organisations with a fully resilient global network with a 99.999% availability service-level agreement. The agreement supports the NIS2 requirements on the operator to ensure strategic guidelines are applied on business continuity management in the event of a security incident.

Supply chain security	The Netskope platform aids in the identification of security risks to networks and CIS especially on the delivery of essential services deployed via the cloud (both public cloud and Software-as-a-Service). All Netskope resources, both hardware and software used for administration purposes can be managed by the operator and/or by Netskope if authorised. In addition, as referenced in paragraph 3 in Article 21, Netskope's Cloud Confidence Index (CCI) includes the security posture of 78,000+ Cloud Service Providers (CSPs) supporting the operator's due diligence requirements for their direct supplier or service providers.
Security in network and information systems	The Netskope platform provides a Secure Access Service Edge (SASE) capability to ensure a secure connection is applied to network and information systems including maintaining controls including user access rights, risk management metrics and integrations with authentication resources to ensure zero trust principles are applied for access to CIS systems. Data stored or transmitted electronically via the Netskope platform is protected from actions such as unauthorised access, modification or deletion that may cause disruption to essential services. The platform includes both threat protection and data protection controls to provide resiliency to cyber-attacks targeting essential services.
Policy and procedures to assess the effectiveness of cybersecurity risk-management measures	The Netskope platform can provide reporting on the effectiveness of cybersecurity risk management measures including the monitoring and security status of the service. Monitoring includes but is not limited to: - Availability of the service - Digital Experience Management (DEM) including availability/performance of Internet Service Provider (ISP), CSP etc - System risk (Device, Web, Cloud) - Malware/Ransomware risk - Data risk
Basic cyber hygiene practices and cybersecurity training	The Netskope platform can provide several capabilities to ensure basic cyber hygiene for CIS. These include but are not limited to: - Web / Cloud Security - Cloud Security Posture Management (CSPM / SSPM) - Device Intelligence (IT, IoT, OT) - Zero Trust (Network Access, Architecture & Principles) - Threat Protection - Data Protection - Reporting and analytics In addition, the Netskope platform includes the ability to supplement cybersecurity training by offering real-time training, coaching and education for employees when accessing malicious websites and when employees are performing a high-risk activity across the many services the Netskope platform protects (Web, Cloud, On-Prem).

Policies and procedures for use of cryptography and encryption	The Netskope platform can ensure session encryption is supported between physical sites and including but not limited to between client-server, server-client, and client-web/cloud services. In addition, the Netskope platform can support policies and procedures to help identify sensitive information and data files that are not encrypted both through data-at-rest scanning and data-in-motion alerting. Sensitive data can be blocked, held, or alerted to depending on the policy and procedure implemented by the operator pending assessment of the confidentiality, authenticity and/or integrity of the information.
Human resources security, access control policies and asset management	The Netskope platform can ensure access control policies are applied to employees and contractors including the use of Zero Trust principles to prevent misuse of CIS related assets. The platform can further assist in training, coaching and education for employees with CIS related responsibilities, The platform supports the ability to build an inventory of cloud systems supporting the CIS to ensure cloud systems are configured correctly and updated/patched according to baselines.
Multi-factor authentication or continuous authentication solutions	The Netskope platform can integrate with multi-factor authentication (MFA) services to provision access to CIS via MFA. The platform can provision access control and identify suspicious activity or use of redundant accounts. Step-up authentication can also be applied in the event of access and activities to CIS warranting a verification of authentication. In addition, the platform can identify compromised credentials in use and provision alerts and reports for administrators to acknowledge and can even restrict or limit access using zero trust principles.

Disclaimer: The content provided has been created to the best of Netskope's ability and knowledge. However, Netskope cannot guarantee the accuracy, completeness, or timeliness of the information. Netskope are not liable for any errors or omissions in the content, and readers are encouraged to verify the information independently. The use of this content is at the reader's own risk, and Netskope shall not be held responsible for any consequences resulting from reliance on the provided information.