ManageEngine
AD360

A comprehensive handbook for

NIS2 DIRECTIVE COMPLIANCE

www.manageengine.com/active-directory-360/

Introduction

In a world dominated by digital transformation, adhering to compliance standards isn't just a legal requirement but a crucial aspect of sustaining trust, credibility, and long-term success.

Organizations must navigate an ever-evolving regulatory landscape, ensuring that they meet stringent data protection and privacy standards. This adherence not only safeguards sensitive information but also enhances customer confidence and business reputation. Cybersecurity compliance is a continuous effort to meet legal requirements while securing your organization against the relentless onslaught of cyberthreats.

What is the NIS2 Directive?

The second Network and Information Security (NIS2) Directive is an EU-wide cybersecurity legislation that brings in stricter requirements focused on risk management and incident reporting. Its goal is to enhance the resilience of cybersecurity in networks and information systems by enforcing the adoption of suitable security protocols and requiring operators to report any incidents to the pertinent authorities promptly.

The NIS Directive vs. the NIS2 Directive

The focus of the NIS Directive was on ensuring the security of essential services and digital service providers. It required implementing measures to handle risks and prevent and mitigate the consequences of security incidents.

Compared to its predecessor, NIS2 expands the scope of covered organizations and sectors to include online marketplaces and search engines. It introduces further security prerequisites for ensuring communication network security, along with specific responsibilities for cloud computing services. It also simplifies reporting obligations and enforces stricter measures.

Penalties of NIS2 violations

Penalties for gross negligence of NIS2 are:

Administrative fines

Non-monetary penalties

Criminal sanctions

Non-monetary penalties

NIS2 gives national authorities the right to enforce non-monetary penalties, such as:

- Compliance orders.
- Binding instructions.
- Security audit implementation orders.
- Threat notification orders to entities' customers.

Administrative fines

When it comes to administrative fines, NIS2 differentiates between essential and important entities:

- Essential entities are fined at least **€10,000,000 or 2%** of the global annual revenue, whichever is higher.
- Important entities are fined at least **€7,000,000 or 1.4%** of the global annual revenue, whichever is higher.

Criminal sanctions

NIS2 has included new measures to hold top management accountable in case of non-compliance. It enables the Member State authorities to:

- Require organizations to disclose compliance violations publicly.
- Issue a public statement disclosing the individuals, both natural and legal persons, accountable for the violation and its nature.
- Temporarily ban individuals from taking management roles within essential entities in cases of repeated violations.

Source: *nis2directive.eu/nis2-fines/*

The timeline

2016	2020	2023	2024
Original NIS Directive comes into effect	NIS2 Directive is introduced	NIS2 Directive comes into effect	Deadline to meet the regulations

The 15 sectors covered by NIS2

The sectors that should comply with NIS2 are categorized into essential and important entities. Essential entities consist of large companies operating in sectors deemed crucial, with either more than 250 employees or a turnover exceeding €50M. Important entities include large companies in other vital sectors or medium-sized companies with 50 to 249 employees, or a turnover ranging from €10M to €50M, operating within the other sectors in the scope.

Essential sectors	Important sectors
Transport	Food
Finance	Digital providers
Energy	Chemicals
Water supply	Postal services
Health	Waste management
Space	Manufacturing
Digital infrastructure	Research
Public administration	

New organizational requirements of NIS2

NIS2 has implemented new requirements for organizations across four overarching areas aimed at strengthening resilience against cyberthreats. These areas are risk management, corporate accountability, reporting obligations, and business continuity.

Risk management

Organizations are advised to implement measures for mitigating cyber risks, such as improving incident management, strong supply chain security, enhanced access control, and encryption techniques.

Corporate accountability

Corporate management must supervise, approve, and undergo training on cybersecurity protocols. Failure to address security incidents could result in penalties for the management team.

Reporting obligations

Both essential and important entities are required to establish procedures that facilitate the timely reporting of security incidents. NIS2 mandates specific notification deadlines, such as the "early warning" requirement within 24 hours.

Business continuity

Organizations need to prepare strategies to maintain business continuity in the event of cyber incidents. This strategy should include system recovery protocols, emergency procedures, and the establishment of a crisis response team.

The 10 minimum requirements of NIS2

NIS2 requires the above-mentioned essential and important sectors to adopt the following fundamental security measures aimed at mitigating likely cyberthreats.

01

Comprehensive risk assessment

Ensure that there are risk assessments and security policies tailored to the information systems within your organization. These risk assessments should involve thorough evaluations of potential threats and vulnerabilities, considering factors such as data sensitivity, system architecture, and potential attack vectors.

02

Advanced authentication

Implement measures such as MFA, continuous authentication solutions, and text encryption in your organization as required.

03

Incident response plan

Prepare an instant response plan to promptly address potential security breaches as they arise. This plan should include swift and decisive actions to mitigate risks and safeguard sensitive assets against unauthorized access or compromise.

04

Security effectiveness

Establish and enforce policies and procedures to evaluate the efficiency of the security measures implemented within your organization. This involves conducting regular evaluations and audits to gauge the solidity of security protocols, identify potential vulnerabilities, and determine the overall effectiveness of the security infrastructure in place.

05

Access control management

Implement security procedures for employees that have access to sensitive or important data and establish policies for data access. Also, have an overview of all the relevant assets in your organization and ensure that they are properly utilized and handled.

06

Encryption policies

Implement policies and procedures regarding the use of cryptography and encryption for managing sensitive data within your organization. These policies should outline guidelines for the proper application of cryptographic methods to protect data at rest, in transit, and during processing.

07

Disaster recovery

Prepare a backup and recovery plan to manage your business operations after a potential security attack. Ensure regular backups and have a plan for ensuring proper access to IT systems during and after a security incident.

08

Security measures

Secure the procuring, developing, and operating of systems and establish policies for handling and reporting vulnerabilities that could arise.

09

Supply chain risk management

Ensure tight security around supply chains. Establish security measures that fit the vulnerabilities of each direct supplier and assess the overall security levels of all suppliers.

10

Cybersecurity training

Provide training not only to management, but also to employees to enhance their understanding of cybersecurity.

IAM and NIS2

The NIS2 comprises nine chapters that are further divided into 46 articles. Among these chapters, Chapter IV: Cybersecurity-risk management measures and reporting obligations defines the cybersecurity steps that the essential and important entities must take to comply with the NIS2. This chapter includes six articles (Articles 20 to 25).

This section elaborates the IAM requirements mandated by the NIS2.

Article	NIS2 requirement
Article 19, Peer reviews	• Peer reviews will be carried out by cybersecurity experts. • They will cover various aspects, including the level of implementation of cybersecurity and reporting measures and cybersecurity information-sharing arrangements.
Article 20, Governance	• This aims to guarantee that the governing bodies of essential and important entities approve the cybersecurity risk-management measures implemented by these entities to adhere to Article 21, supervise their execution, and assume responsibility for any breaches committed by the entities. • The governing bodies should also ensure that the management bodies follow cybersecurity training and encourage the companies to offer similar training to all their employees.
Article 21, Cybersecurity risk-management measures	• Ensure that appropriate measures are taken to manage security risks that can affect networks and information systems and to prevent or reduce the impact of security incidents. • These measures should include: ◦ 21.2.b- Incident handling. ◦ 21.2.c- Business continuity, such as backup management, disaster recovery, and crisis management. ◦ 21.2.i- Access control policies and asset management. ◦ 21.2.j- The use of MFA or continuous authentication solutions where appropriate.
Article 22, Union level coordinated security risk assessments of critical supply chains	• The Cooperation Group, collaborating with the Commission and the European Union Agency for Cybersecurity (ENISA), may conduct security risk assessments of particular critical Information and Information Communications Technology (ICT) services, ICT systems, or ICT product supply chains. • These assessments consider both technical and, when applicable, non-technical risk elements.

ManageEngine AD360 to the rescue

ManageEngine AD360 is an enterprise IAM solution designed to help you manage identities and secure access. With its comprehensive features, AD360 simplifies the process of meeting compliance standards.

Secure access to the organization's IT systems

(helps with Article 21.2.i)

- Perform role-based access control (RBAC) across your organization easily.
- Identify and review the access users have to resources in your organization periodically using AD360's access certification campaign.

Implement comprehensive risk management

(helps with Article 21.2.b, Article 7.1.d, Article 18.1.a, Article 22)

- Identify, analyze, and evaluate the risk elements in your organization with the Identit Risk Assessment report.
- Perform remediation measures and monitor your IT infrastructure closely to identify and mitigate risk indicators.

Get incident reports to manage the system's security

(helps with Article 11.3.b)

- Receive real-time email alerts regarding any suspicious activity happening in your systems.
- View all the potential vulnerabilities in your AD environment and mitigate them with actionable recommendations.

Maintain an overview of all your digital assets

(helps with Article 11.3.a)

- With AD360's intuitive reporting and monitoring capabilities, you can gain insights and get detailed audit reports about your AD, Exchange, and Microsoft 365 environments.
- Keep an eye on all your resources from a single console.

Implement MFA

(helps with Article 21.2.j)

- AD360's adaptive MFA feature, along with SSO and conditional access policies, can help you create a Zero Trust environment in your organization.
- Secure multiple resources and manage access to the network without compromising the user experience.

Perform up-to-date backups

(helps with Article 9.3, Article 21.2.c)

- Easily back up and restore your AD, Azure AD, Microsoft 365, Google Workspace, and Exchange environments.
- Schedule backups to happen automatically to ensure that you have backed up the updated versions of your data.

Your local distributor

inuit by ELOVADE

Inuit AB

inuit.se | sales@inuit.se | support@inuit.se

Our Products

Log360 | ADManager Plus | ADAudit Plus | ADSelfService Plus

Exchange Reporter Plus | RecoveryManager Plus

ManageEngine

AD360

ManageEngine AD360 is a unified identity and access management (IAM) solution that helps manage identities, secure access, and ensure compliance. It comes with powerful capabilities like automated identity life cycle management, access certification, risk assessment, secure single sign-on, adaptive MFA, approval-based workflows, UBA-driven identity threat protection and historical audit reports of AD, Exchange Server and Microsoft 365. AD360's intuitive interface and powerful capabilities make it the ideal solution for your IAM needs, including fostering a Zero Trust environment. For more information, please visit www.manageengine.com/active-directory-360/.

$ Get Quote   ⤓ Download