Makerhub

NIS2 Audit

Arnaud Lombaers

Table of Contents

Introduction – NIS 2

What is NIS 2?

“The European NIS 2 Directive aims to build cybersecurity capabilities across the EU, mitigate threats to networks and information systems used to provide essential services in key sectors, and ensure the continuity of these services in the event of incidents, thereby contributing to the security of the EU and the smooth functioning of its economy and society.”

Which companies are affected?

An organization is considered a medium-sized company when it employs at least 50 people or has a turnover or balance sheet total exceeding €10 million. It is classified as a large company when it has at least 250 employees or exceeds €50 million in turnover and €43 million in balance sheet total.

Sectors affected by NIS2

Highly critical sectors:

- Energy, transport, banking
- Financial infrastructure
- Healthcare, drinking water, wastewater
- Digital infrastructure
- ICT services, public administration, space

Other critical sectors:

- Postal services
- Waste
- Agri-food
- Manufacturing
- Digital suppliers
- Research

Companies outside critical sectors are not directly targeted, but may be impacted via the supply chain.

The application of NIS 2

NIS 2 applies from October 18, 2024, registration is required by the end of 2024/early 2025, and full compliance is expected between April 2026 and April 2027.

Scope

Context:

This audit is part of an end-of-training project aimed at assessing the level of compliance of an SME's infrastructure (LA Cyber) with the requirements of the NIS 2 directive.

This SME has 60 employees, €14 million in revenue, and a balance sheet of €11 million. The organization has a budget of 5 to 10% of the IT budget, which represents €30,000 to €60,000 per year.

The objective of this audit is to identify compliance gaps, assess the associated risks, and make proportionate recommendations to improve the infrastructure's level of compliance.

The audit is carried out using a structured methodology based on a scope, an analysis of the existing situation, a risk register, a gap analysis table, and a conclusion with recommendations.

The organizational scope is limited to the technical infrastructure.
HR, legal, external supplier, and actual end-user processes are not included in the scope of the audit.

The technical scope of the audit includes the following components:

- A user host
- A Layer 2 switch
- A multilayer switch (MLS) configured in layer 3
- A Fortigate perimeter firewall
- A core router providing access to the CGN network
- Network segmentation based on three VLANs
- Access control lists (ACLs)
- A data center integrating Active Directory

The audit focuses mainly on:

- Network segmentation and security
- Access and identity management
- Perimeter security
- Logging and monitoring
- Business continuity mechanisms
- Infrastructure risk management

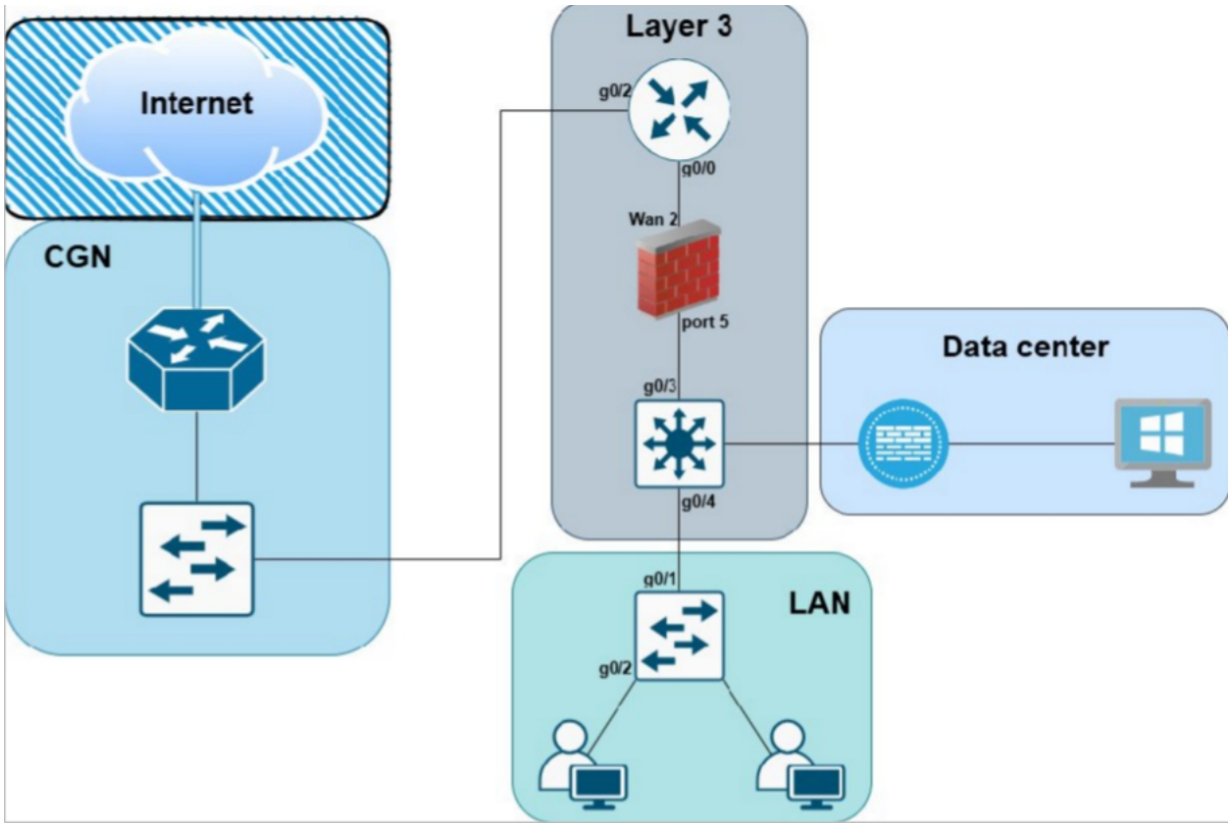
The analysis is mainly based on the requirements of Article 21 of the NIS 2 Directive, relating to risk management measures and the security of networks and information systems.

The following are explicitly excluded from the scope:

- Redundancy of operator WAN links
- Physical audits of premises
- Actual HR procedures
- Contractual management of suppliers

This scope allows for a realistic and proportionate analysis of the requirements of the NIS 2 directive as applied to an infrastructure.

Diagram of the audited infrastructure:



Analysis of existing infrastructure – Audited network infrastructure

1. General overview of the infrastructure:

The audited network infrastructure is organized around a segmented architecture based on the use of VLANs and network equipment providing separate access, routing, and traffic security functions. It includes a main host with Internet access and an architecture designed to integrate future user hosts.

2. Logical segmentation and VLANs

The network is segmented into several VLANs:

- A Management VLAN, which houses the main production host and has Internet access.
- A User VLAN, designed to accommodate any additional user hosts via the access switch.
- A "Trash" VLAN, in which unused network interfaces are placed to prevent unauthorized connections.

This segmentation aims to logically separate the different types of traffic and uses within the infrastructure.

3. Access switch and port control

Network hosts are connected to a Layer 2 access switch configured to support the defined VLANs.
On this switch, a Port Security mechanism is enabled to limit and control connections on physical ports.
Unused ports are associated with the "Trash" VLAN, preventing any active communication on these interfaces.

4. Multilayer Switching (MLS) and Routing

A multilayer switch configured in layer 3 provides routing functions within the infrastructure.
It is responsible for routing:

- the subnetwork associated with the Data Center,
- the subnetwork of the host located in the Management VLAN, and the User VLAN

to the equipment providing security and access to the external network, namely the firewall and router.

The MLS thus acts as a central transit and routing point between the different areas of the network.

Traffic from the VLAN Management, as well as traffic from the Data Center, is routed by the MLS to the firewall and router.

5. Firewall operation

The firewall is configured in stateful mode, which means that it monitors the status of network connections.
This operation automatically authorizes return flows associated with connections initiated from internal zones, in accordance with the defined rules. A security rule authorizes flows from the Management VLAN to the firewall's WAN interface.

The firewall uses static routing to forward network traffic. Two static routes are

configured:

- A default route pointing to the gateway located on the WAN network.
- A specific route to the internal subnetwork, pointing to the internal interface connected to the MLS.

These routes enable communication between internal networks, the firewall, and the external network.

6. Interaction between the MLS, the firewall, and the router

The MLS routes internal subnets to the firewall.
The firewall applies filtering rules and transmits authorized traffic to the router. The router then performs address translation (PAT) to the CGN network to allow access to the external network.

This process constitutes the normal path for outgoing traffic from internal VLANs to the Internet.

In conclusion:

The audited network infrastructure is based on VLAN segmentation, access control at the access switch level via Port Security, and access control lists.

Internal routing is provided by a Layer 3 MLS, while the firewall controls traffic between the internal and external networks. The firewall uses static routing and applies filtering rules.

Access to the external network is provided by a router performing address translation (PAT) to a CGN network.

Risk Register

See Appendix 1

Summary of the Risk Register

The risk register highlights six major risks identified within the analyzed infrastructure, covering technical, operational, and organizational aspects related to the requirements of the NIS 2 Directive. The initial risks are mostly high to critical, mainly due to the lack of formalized security controls, advanced detection mechanisms, and structured incident management capabilities.

The most critical technical risks relate to the firewall, with threats linked to overly permissive rules and the lack of advanced traffic inspection. Weaknesses have also been identified in network access control, in particular the lack of strong equipment authentication (802.1X).

From an operational and organizational standpoint, the lack of logging, event correlation, and incident response capabilities is an aggravating factor, significantly increasing the potential impact of a security incident. Finally, the absence of a clear governance framework limits effective decision-making in crisis situations.

The proposed treatment plans are based primarily on a risk reduction strategy, through the implementation of technical controls (strict filtering, IPS/SIEM, strong authentication) and organizational controls (incident response procedures, clarification of roles and responsibilities).

Following these measures, the majority of residual risks are reduced to a minor level, demonstrating the effectiveness of the controls implemented.

Gap Analysis

See Appendix 2

Summary of the Gap Analysis

The gap analysis table is used to assess the gap between the existing situation of the analyzed infrastructure and the requirements of the NIS2 Directive, in particular those defined in Article 21.

This analysis highlights several shortcomings, both technical and organizational. Current logging mechanisms are decentralized and stored locally on equipment, which limits overall visibility and prevents effective correlation of security events. Furthermore, the lack of intrusion detection and prevention solutions makes it impossible to identify malicious traffic entering the internal network.

In terms of access control, network segmentation relies solely on the use of VLANs, without authentication of devices or users at the local network level. This approach does not meet identity-based access control requirements and exposes the infrastructure to unauthorized connections.

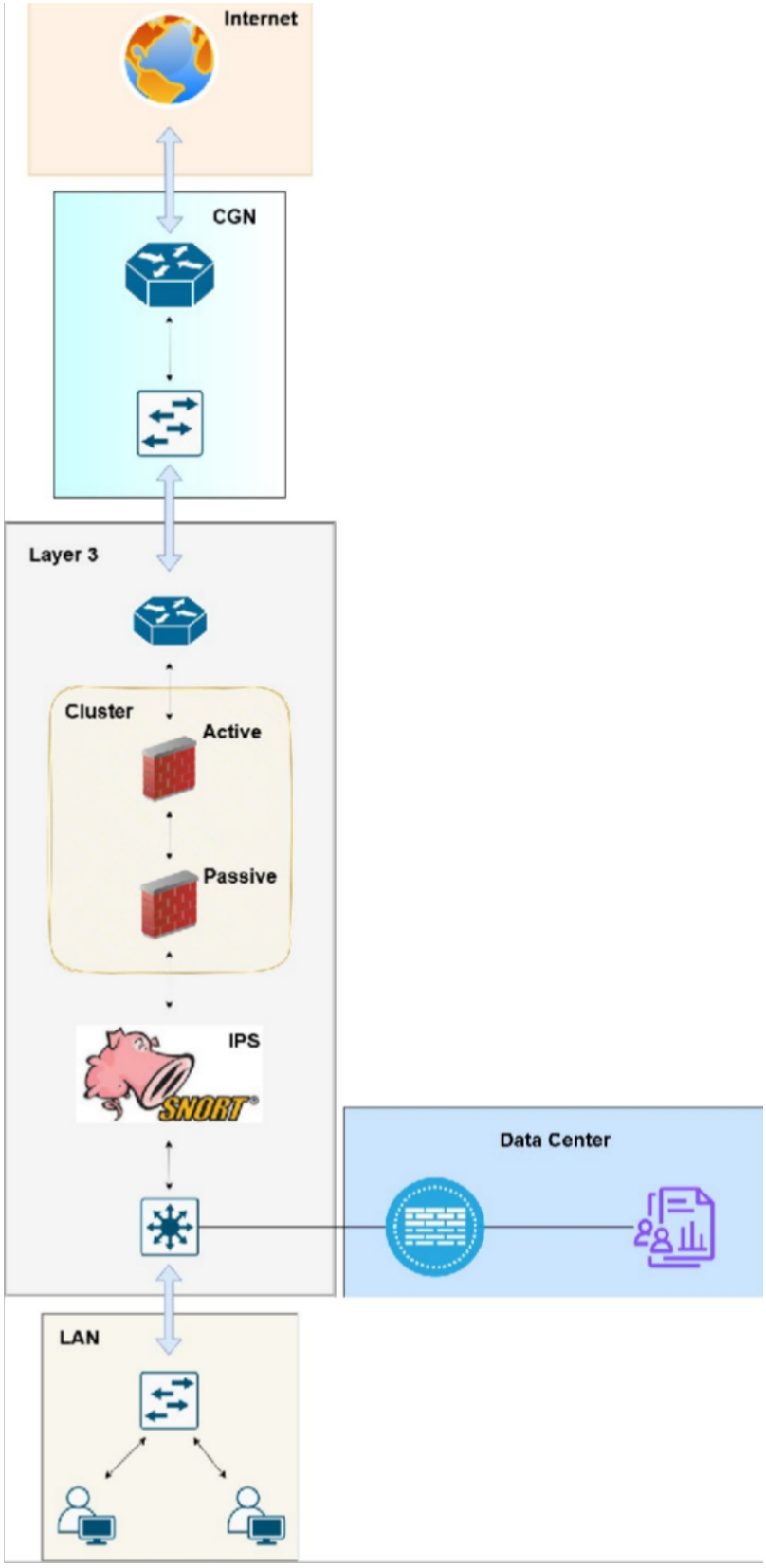
The analysis also reveals excessive exposure of the internal network due to overly permissive firewall rules, which contradicts the principle of least privilege recommended by the NIS2 directive.

Finally, at the organizational level, incident management is currently informal and no structured CSIRT process has been defined. In addition, the absence of a formalized governance framework leads to a lack of clearly established responsibilities and oversight at the management level.

The proposed corrective measures aim to address these gaps by implementing appropriate technical and organizational controls, with high priority given to actions that have a direct impact on risk reduction and NIS2 compliance.

Recommendations after Audit

Recommended infrastructure diagram:



Hardening of firewall rules (least privilege principle)

This recommendation aims to reduce the exposure of the internal network by applying the principle of least privilege. The existing firewall rules are too permissive, increasing the risk of unauthorized access from the Internet. Tightening the rules limits authorized traffic to only those services that are strictly necessary, in accordance with Article 21 of the NIS2 Directive. This measure directly contributes to reducing the attack surface and improving perimeter security.

Implementation of an IPS (SNORT)

Deploying an intrusion prevention system makes it possible to detect and block malicious traffic that would not be filtered by the firewall. This measure meets the incident detection requirements set out in the NIS2 directive and improves the ability to respond to network attacks. It significantly reduces the risk of vulnerabilities being exploited and enhances the security of incoming and outgoing traffic.

Log centralization (SIEM)

Centralizing security logs provides global visibility into infrastructure events and allows incidents to be correlated. This measure is essential for attack detection and incident management, as required by the NIS2 directive.

High availability firewall

High availability firewalls ensure the continuity of critical services in the event of hardware or software failure. This measure contributes to the resilience of the infrastructure, in line with the service continuity and availability objectives imposed by NIS2.

Identity-based network access control (802.1X)

The implementation of identity-based network access control via the 802.1X protocol ensures that only authenticated users and devices can access the internal network. Currently, segmentation is based solely on VLANs, which does not allow the identity of connected entities to be verified. The implementation of 802.1X, combined with a RADIUS server, meets the access control requirements defined by the NIS2 directive and significantly reduces the risk of unauthorized devices connecting to the network.

Incident management procedures – CSIRT

The definition of incident management procedures (CSIRT) is essential to ensure an effective and structured response to security incidents. Currently, incident management is informal and undocumented, which can lead to delays or errors in the event of a crisis. The implementation of a CSIRT clarifies roles, responsibilities, and notification processes in accordance with NIS2 requirements for the management and notification of significant incidents.

Governance framework

The establishment of a governance framework aims to formalize the roles, responsibilities, and decision-making processes related to information security. In the absence of clearly defined governance, cybersecurity relies primarily on isolated technical initiatives. The NIS2 directive requires direct involvement of senior management in the oversight of security measures. This recommendation ensures informed decision-making, clearly established accountability, and the integration of cybersecurity into the organization's overall risk management.

Cybersecurity governance and incident management (CSIRT)

1. Governance

1.1 Objective

The objective of governance is to define a clear framework for managing risks related to network and information system security.

It aims to clarify roles and responsibilities, while ensuring that management is directly involved in decisions related to cybersecurity.

1.2 Organization

In the context of LA Cyber, a cybersecurity governance framework proportionate to the size and complexity of the organization has been defined.

The following roles have been identified:

- Executive/Management:
  Management is responsible for approving cybersecurity risk management measures. It oversees their implementation, allocates the necessary resources, and assumes responsibility for the decisions made.
- Cybersecurity manager:
  The cybersecurity manager coordinates risk management, monitors technical and organizational measures, and oversees the management of security incidents. He or she also acts as the internal point of contact in the event of an incident.
- IT team:
  The IT team is responsible for the operational implementation of security measures, infrastructure operation, and providing the technical elements necessary for incident analysis.

This organization ensures clear and effective governance, while remaining adapted to the capabilities of a medium-sized company.

2. Incident management and CSIRT capability

2.1 General principle

The NIS2 directive requires affected entities to have the capacity to manage and respond to security incidents.
In this project, I opted to set up a simplified internal CSIRT capability, proportionate to the size and needs of the organization.

2.2 Organization of the internal CSIRT

An incident response unit is defined and activated only in the event of a significant security incident.
It is based on the following roles:

- Incident coordinator:
  This role is performed by the cybersecurity manager. He or she coordinates response actions, centralizes information, and ensures internal communication.
- Technical support:
  Technical support, provided by the IT team, is responsible for the technical analysis of the incident, the implementation of containment and remediation measures, and the collection of technical evidence.
- Management:
  Management is involved in strategic decision-making, particularly in the event of a major incident, and oversees crisis management.

2.3 Incident management process

A formalized incident management process has been defined, structured around the following steps:

1. Detection and identification:
   The incident is detected from logs, security alerts, or internal reports.
2. Analysis and qualification:
   The incident is analyzed to determine its nature, impact, and severity.
3. Containment and remediation:
   Technical measures are implemented to limit the impact of the incident and restore the affected services.
4. Notification:
   When the incident is classified as significant, it is notified in accordance with the requirements of the NIS2 Directive.

5. Feedback:
   A post-incident analysis is carried out to identify possible improvements and strengthen existing security measures.

3. Alignment with the NIS2 Directive

The cybersecurity governance structure and CSIRT capacity defined in this project enable compliance with the NIS2 directive's requirements for risk management, incident detection, and response.
The proposed measures comply with the principle of proportionality, taking into account the size of the organization and its level of exposure to risks.

4. Conclusion

The implementation of structured cybersecurity governance and an appropriate incident management capability is an essential step towards NIS2 compliance.
These elements enable the organization to strengthen its resilience to security incidents and respond effectively to regulatory obligations.

Cost estimate

Recommendation	Type	Priority	Estimate Cost	Justification
Governance & CSIRT	Organization	Short term e	**€2,000–5,000**	Internal time, formalization of roles, procedures, documentation, simple exercises
Firewall hardening	Technical	Short term e	**€2,000–4,000**	Review of rules, cleanup, testing, no major hardware purchases
SIEM	Technical	Mediumter me	**€12,000–18,000**	Dedicated server + suitable SIEM solution (open-source or licensed) + integration
IPS	Technical	Mediumter me	**$5,000–$8,000**	SNORT setup / dedicated server
802.1X	Technical	Long term	**$6,000–$10,000**	ServerRadius,configuration, testing, gradual deployment
HA firewall	Technical	Long term	**€10,000–15,000**	Secondfirewall,licensesHA,setup in cluster, gradual deployment

Conclusion of the audit

This audit assessed the maturity level of the infrastructure analyzed in relation to the requirements of the NIS2 directive, using a risk management-based approach.
The analysis highlighted several technical and organizational gaps that could expose the organization to significant cyber risks and regulatory non-compliance.

The main risks identified relate to the exposure of the internal network, the lack of advanced threat detection mechanisms, insufficient access control, and a lack of structure in governance and incident management. These findings confirm that current security relies primarily on isolated technical measures, without a formalized overall framework.

The recommendations made aim to reduce these risks in a proportionate manner, taking into account the size of the organization, its exposure to threats, and the requirements of the NIS2 directive. They combine technical, organizational, and governance measures to improve the resilience and continuity of services in the long term.

Finally, this audit is not an end in itself, but a step in a process of continuous improvement. The gradual implementation of the recommendations will enable the organization to move closer to an acceptable level of NIS2 compliance by 2026–2027, while strengthening its cybersecurity posture in the face of current and future threats.