

*Partner Briefing NIS 2*

## NIS 2 Compliance & Cyber Resilience

*Leveraging Log Management and SIEM for EU Security Compliance*



Date: 22.03.2026

Author: Business Development i-Vertix

---

---

# IMPLEMENTING NIS2 COMPLIANCE THROUGH LOG MANAGEMENT AND CYBERSECURITY PRACTICES

## INTRODUCTION

The NIS2 Directive establishes a comprehensive framework for managing cybersecurity risks and ensuring reporting obligations across the European Union. At its core, NIS2 aims to strengthen the resilience of essential and important entities against evolving cyber threats, mandating a structured approach to risk management. One of the most effective ways to achieve compliance is through the integration of advanced log management and Security Information and Event Management (SIEM) systems. This whitepaper provides an in-depth analysis of how NIS2 compliance can be operationalized through technical and organizational cybersecurity measures.

## MINIMUM CYBER RISK MANAGEMENT MEASURES UNDER NIS2

Article 21 of the NIS2 Directive lists ten minimum measures for cyber risk management that all regulated entities must implement:

1. Policies for risk analysis and information system security.
2. Incident management procedures.
3. Business continuity, including backup management, disaster recovery, and crisis handling.
4. Supply chain security, addressing security relationships between entities and their suppliers or service providers.
5. Security in the acquisition, development, and maintenance of networks and information systems, including vulnerability management and disclosure.

---

### PGUM S.r.l

NOI Techpark  
Via Ipazia 2  
39100 Bolzano - Italia

Mail: [info@i-vertix.com](mailto:info@i-vertix.com)  
PEC: [pgumgmbh@pec.it](mailto:pgumgmbh@pec.it)  
Web: [i-vertix.com](http://i-vertix.com)

Cod. Fisc. e P.IVA: 02923310219  
REA: BZ - 216954

6. Policies and procedures for assessing the effectiveness of cyber risk management measures.
7. Basic cybersecurity hygiene practices and personnel training.
8. Policies and procedures regarding encryption and, where applicable, cryptographic solutions.
9. Human resource security, access control policies, and asset management.
10. Implementation of multi-factor authentication or continuous authentication solutions.

While specific technical and organizational measures may vary by national implementation, these requirements will largely remain consistent throughout the EU. Article 21 emphasizes that compliance with NIS2 requires organizations to implement multiple essential technical measures.

## TECHNICAL MEASURES REQUIRED BY NIS2

The NIS2 Directive, together with draft national implementations, establishes a broad spectrum of technical competencies that regulated entities must develop to ensure compliance and strengthen their cybersecurity posture. These competencies go far beyond simple IT hygiene, encompassing physical, digital, and organizational aspects of security. Below is an in-depth examination of each area:

### 1. Physical Security

While often overlooked, physical security is a foundational component of cybersecurity. NIS2 mandates that entities secure all premises and facilities that house critical IT infrastructure. This includes data centers, server rooms, and offices where sensitive information is processed. Measures may include controlled access points, surveillance systems, environmental monitoring (e.g., temperature, humidity, fire detection), and physical protection of critical hardware against theft, tampering, or sabotage.

### 2. Network Security

Securing network infrastructure is central to preventing unauthorized access, data breaches,

---

#### PGUM S.r.l

NOI Techpark  
Via Ipazia 2  
39100 Bolzano - Italia

Mail: [info@i-vertix.com](mailto:info@i-vertix.com)  
PEC: [pgumgmbh@pec.it](mailto:pgumgmbh@pec.it)  
Web: [i-vertix.com](http://i-vertix.com)

Cod. Fisc. e P.IVA: 02923310219  
REA: BZ - 216954

and service disruptions. Organizations must implement firewalls, intrusion detection and prevention systems (IDPS), network segmentation, and continuous monitoring of network traffic for anomalies. Encryption of data in transit, secure remote access solutions, and real-time threat intelligence integration are also essential to meet NIS2 expectations.

### 3. Identity Management and Authentication

Managing user identities and ensuring robust authentication mechanisms are critical to maintaining secure access to systems. NIS2 emphasizes the implementation of multi-factor authentication (MFA), single sign-on (SSO) solutions, and regular review of user credentials. Identity lifecycle management, including provisioning and de-provisioning of accounts, ensures that only authorized individuals have access to sensitive systems and data.

### 4. Access Rights Management

Access rights management involves defining, enforcing, and regularly reviewing permissions for users, applications, and systems. Role-based access control (RBAC), principle of least privilege, and periodic audits are required to prevent overprivileged accounts from creating security vulnerabilities. NIS2 also requires documenting and justifying access decisions to support accountability and compliance.

### 5. Cybersecurity Incident Detection

NIS2 underscores the importance of proactive detection of cybersecurity incidents. This requires organizations to implement systems that can continuously monitor IT environments, identify suspicious behavior, and trigger alerts in real time. Detection capabilities include anomaly detection, signature-based monitoring, behavioral analytics, and automated threat intelligence integration. Timely detection is essential for rapid containment and mitigation of cyber incidents.

### 6. Logging of Security-Relevant and Operational Events

Effective logging is the backbone of incident detection, reporting, and auditability. NIS2 requires organizations to maintain comprehensive, tamper-proof logs of all security-relevant and operational events. Logs should include activity type, user or system account, affected assets, timestamps, and the outcome of actions. Proper log management ensures transparency,

---

#### **PGUM S.r.l**

NOI Techpark  
Via Ipazia 2  
39100 Bolzano - Italia

Mail: [info@i-vertix.com](mailto:info@i-vertix.com)  
PEC: [pgumgmbh@pec.it](mailto:pgumgmbh@pec.it)  
Web: [i-vertix.com](http://i-vertix.com)

Cod. Fisc. e P.IVA: 02923310219  
REA: BZ - 216954

enables forensic investigations, supports audit obligations, and facilitates reporting to regulatory authorities within prescribed timeframes.

#### 7. Cybersecurity Incident Assessment

Beyond detection, NIS2 emphasizes the systematic assessment of cybersecurity incidents. Organizations must collect, correlate, and analyze relevant data to evaluate incident severity, potential impact, and remedial actions. This continuous evaluation helps organizations improve resilience, identify systemic weaknesses, and optimize incident response strategies over time.

#### 8. Application Security

Securing software applications is critical to prevent exploitation of vulnerabilities. NIS2 expects entities to implement secure development practices, including code reviews, vulnerability assessments, penetration testing, and patch management. Security must be embedded throughout the software lifecycle, from acquisition and development to deployment and maintenance.

#### 9. Cryptographic Algorithms

The directive mandates the use of strong cryptographic algorithms to protect data confidentiality, integrity, and authenticity. Organizations should apply encryption for data at rest and in transit, manage cryptographic keys securely, and periodically review cryptographic practices to align with evolving standards.

#### 10. Ensuring the Availability of Regulated Services

NIS2 stresses service continuity as a core responsibility. Organizations must implement robust measures to maintain the availability of critical services, including disaster recovery plans, redundancy, failover systems, and real-time monitoring of service health. The goal is to minimize downtime and ensure operational continuity even in the face of cyberattacks or other disruptive events.

#### 11. Security of Industrial, Control, and Specialized Technical Assets

Entities operating industrial or specialized control systems face unique risks. NIS2 requires implementing specific safeguards for industrial control systems (ICS), SCADA environments, IoT

devices, and other specialized technical assets. Measures include network segmentation, real-time monitoring, anomaly detection, and secure configuration management to prevent unauthorized access or operational disruption.

## ENHANCING DETECTION THROUGH LOG MANAGEMENT AND SIEM

Integrating log management and Security Information and Event Management (SIEM) systems transforms raw data into actionable intelligence. Together, these tools enable:

- **Proactive Threat Detection:** By continuously monitoring activities across endpoints, servers, network devices, and cloud environments, organizations can identify potential security incidents before they escalate. Advanced analytics, anomaly detection, and threat intelligence integration allow for early identification of malicious activity.
- **Alerts on Malicious Patterns and Anomalies:** SIEM systems correlate data from multiple sources to recognize patterns indicative of potential attacks. Whether it's unusual login attempts, abnormal data transfers, or unauthorized changes to critical systems, these systems generate automated alerts to ensure immediate attention.
- **Centralized Observability of the IT Environment:** A unified view of all assets—ranging from industrial control systems to cloud infrastructure—allows security teams to monitor activities holistically. This observability is crucial for identifying lateral movements, advanced persistent threats, and previously unknown attack vectors.
- **Effective Investigation and Incident Response:** By providing a detailed historical record of events, SIEM and log management systems enable forensic investigation, root cause analysis, and timely response. This reduces dwell time for threats and enhances resilience against recurrent attacks.

## ROLE OF LOG MANAGEMENT IN MEETING NIS2 REQUIREMENTS

Log management tools are indispensable in operationalizing the detection measures required by NIS2. Their contributions include:

---

### PGUM S.r.l

NOI Techpark  
Via Ipazia 2  
39100 Bolzano - Italia

Mail: [info@i-vertix.com](mailto:info@i-vertix.com)  
PEC: [pgumgmbh@pec.it](mailto:pgumgmbh@pec.it)  
Web: [i-vertix.com](http://i-vertix.com)

Cod. Fisc. e P.IVA: 02923310219  
REA: BZ - 216954

- **Verification and Monitoring of Data Transmission:** Monitoring the flow of data within and across networks ensures that sensitive information is protected and helps identify potential breaches or misuse.
- **Continuous, Automated Protection Against Malware:** By logging system events and network traffic, organizations can detect malware infections or unauthorized software activity and trigger automated containment measures.
- **Communication Monitoring Between Applications, Services, and Processes:** Tracking inter-application and inter-service communications ensures that all data exchanges follow policy and reveals irregular activity that may indicate a compromise.
- **Detection of Security Events:** Log data enables the identification of security incidents, from failed authentication attempts to privilege escalation, ensuring that no critical event goes unnoticed.
- **Behavioral Anomaly Monitoring:** By analyzing user, administrator, and asset behaviors, systems can detect deviations from normal patterns, which may indicate insider threats, compromised accounts, or system misconfigurations.

## LOGGING SECURITY-RELEVANT AND OPERATIONAL EVENTS FOR REPORTING AND AUDITS

Under NIS2, regulated entities are subject to extensive reporting obligations, including:

- Incident reporting within tight deadlines (e.g., 24 hours)
- On-site inspections by regulatory authorities
- Regular and extraordinary cybersecurity audits
- Continuous supervisory measures

To comply, organizations must collect detailed, contextual data on all security incidents and operational events. Log management systems make this possible by storing comprehensive, tamper-proof records in an accessible format. This enables:

---

### PGUM S.r.l

NOI Techpark  
Via Ipazia 2  
39100 Bolzano - Italia

Mail: [info@i-vertix.com](mailto:info@i-vertix.com)  
PEC: [pgumgmbh@pec.it](mailto:pgumgmbh@pec.it)  
Web: [i-vertix.com](http://i-vertix.com)

Cod. Fisc. e P.IVA: 02923310219  
REA: BZ - 216954

- **Efficient Incident Investigation:** Analysts can trace the origin, scope, and impact of security events accurately and quickly.
- **Impact Assessment:** Understanding the full extent of a security incident allows organizations to implement corrective actions and prevent recurrence.
- **Secure Archival of IT Activity Logs:** Maintaining a reliable historical record supports regulatory audits, forensic investigations, and internal compliance monitoring.

## TYPICAL DATA CAPTURED BY CENTRALIZED LOG MANAGEMENT SYSTEMS

### INCLUDES:

- **Type of Activity:** What action was performed (login, file access, configuration change, etc.).
- **Affected Asset Identification:** Which system, device, or application was involved.
- **User or Account Performing the Activity:** Including administrator actions and automated processes.
- **Activity Outcome:** Success, failure, or partial completion of the event.
- **Additional Operational Metadata:** Timestamps, location, protocol used, and other relevant contextual information.

These capabilities are essential to meet NIS2's stringent reporting requirements, including the obligation to notify competent authorities within 24 hours of identifying significant incidents. By providing real-time visibility, detailed historical records, and correlation capabilities, log management and SIEM systems form the backbone of NIS2-compliant incident detection and response programs.

## CYBERSECURITY INCIDENT ASSESSMENT

NIS2 requires essential entities to continuously assess detected cybersecurity events. This involves collecting, investigating, and correlating information to identify and evaluate incidents.

---

### PGUM S.r.l

NOI Techpark  
Via Ipazia 2  
39100 Bolzano - Italia

Mail: [info@i-vertix.com](mailto:info@i-vertix.com)  
PEC: [pgumgmbh@pec.it](mailto:pgumgmbh@pec.it)  
Web: [i-vertix.com](http://i-vertix.com)

Cod. Fisc. e P.IVA: 02923310219  
REA: BZ - 216954

The goal is not only to respond proactively to emerging threats but also to continuously improve organizational resilience by identifying and addressing vulnerabilities.

Advanced log management platforms, such as i-Vertix Log Management, collect the necessary information and enable correlation and evaluation of events—essentially functioning as a SIEM—thereby fulfilling this compliance requirement.

## CONCLUSION

The NIS2 Directive mandates a structured, proactive approach to cyber risk management for essential and important entities in the EU. Effective log management and SIEM integration are not optional—they are fundamental tools for meeting detection, response, reporting, and audit requirements. By deploying centralized log management solutions and aligning technical controls with NIS2 standards, organizations can significantly strengthen their cybersecurity posture while ensuring compliance with regulatory obligations.

---

### i-Vertix – Contact Details

**Address:** NOI Techpark – Palazzo D1, Via Ipazia, 2

39100 Bolzano, Italy IT

**Phone:** +39 0471 1430170

**E-Mail:** [sales@i-vertix.com](mailto:sales@i-vertix.com)

**Web:** [www.i-vertix.com](http://www.i-vertix.com)

---

### PGUM S.r.l

NOI Techpark  
Via Ipazia 2  
39100 Bolzano - Italia

Mail: [info@i-vertix.com](mailto:info@i-vertix.com)  
PEC: [pgumgmbh@pec.it](mailto:pgumgmbh@pec.it)  
Web: [i-vertix.com](http://i-vertix.com)

Cod. Fisc. e P.IVA: 02923310219  
REA: BZ - 216954