

Whitepaper

IT Asset Management: Building a Complete Inventory for NIS2 Compliance



ITAM & NIS2 Compliance: Tools & Checklist for Holistic Asset Inventory

Date: 04.05.2026

Author: Business Development i-Vertix

IT ASSET MANAGEMENT: THE KEY TO NIS2 COMPLIANCE

In an era where digital infrastructures form the backbone of nearly every business process, knowing precisely what assets exist, where they are deployed, and how they interact is no longer optional—it is essential. Comprehensive visibility of hardware and software across IT and OT environments is the cornerstone of effective cybersecurity and regulatory compliance. With the EU NIS2 directive coming into effect, organizations must act decisively to manage risks, protect critical systems, and ensure operational continuity.

WHY COMPLETE ASSET VISIBILITY MATTERS

Imagine managing a complex factory or corporate IT environment without a full inventory of devices and software. Servers, desktops, and standard software licenses are easy to track, but what about mobile devices, IoT sensors, or industrial controllers running legacy systems? What about unsupported Windows machines controlling production lines or niche Linux servers hosting specialized applications?

Without accurate insight, critical assets can go unnoticed, vulnerabilities remain unaddressed, and operational disruptions become far more likely. A fragmented understanding of IT and OT assets is akin to trying to navigate a city without a map—minor oversights can escalate into major problems.

NIS2 compliance adds another layer of urgency: organizations must not only identify and manage risks internally but also ensure that every component in their ecosystem—including third-party suppliers—is accounted for and secured.

UNDERSTANDING THE NIS2 DIRECTIVE

The NIS2 directive is the EU's updated cybersecurity framework, designed to strengthen resilience against growing digital threats. It expands the scope of the original 2016 NIS

PGUM S.r.l

NOI Techpark
Via Ipazia 2
39100 Bolzano - Italia

Mail: info@i-vertix.com
PEC: pgumgmbh@pec.it
Web: i-vertix.com

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

regulation to include a broader range of sectors, from energy, transport, and healthcare to chemical production, waste management, and digital service providers.

Key elements of NIS2 include:

- Comprehensive risk management covering IT and OT systems.
- Supply chain security to ensure that partner and vendor systems do not introduce vulnerabilities.
- Proactive incident reporting to minimize damage from cyberattacks.
- Business continuity planning to prevent operational downtime.

In short, NIS2 shifts organizations from reactive to proactive cybersecurity practices, requiring full awareness of all assets, their relationships, and potential risks.



ESTABLISHING THE ASSET BASELINE

The first step toward compliance is creating a complete, accurate, and actionable inventory of all assets. This involves:

- Identifying every piece of hardware and software in use, from traditional IT devices to specialized industrial equipment.
- Mapping how these assets interact and depend on one another to ensure business continuity.
- Assessing vulnerabilities and risks associated with each asset.
- Implementing mitigation strategies to address gaps and reduce exposure.

Without this baseline, organizations cannot reliably measure or manage their security posture, leaving them vulnerable to both cyber threats and regulatory penalties.

LEVERAGING IT ASSET MANAGEMENT AS CENTRAL INVENTORY PLATFORM

Network Discovery is instrumental in achieving full asset visibility. Modern platforms, such as the i-Vertix IT Asset Management module go beyond traditional IT tracking by also managing OT systems, mobile devices, and legacy software. Key benefits include:

- Automated discovery of all endpoints, including desktops, servers, mobile devices, IoT equipment, and industrial controllers.
- Lifecycle management from procurement to retirement, ensuring outdated or unsupported systems are addressed.
- Centralized patching and updates, reducing vulnerability windows.

PGUM S.r.l

NOI Techpark
Via Ipazia 2
39100 Bolzano - Italia

Mail: info@i-vertix.com
PEC: pgumgmbh@pec.it
Web: i-vertix.com

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

- Integration with IT Service Management (ITSM) systems for workflow automation, incident reporting, and security alerts.
- Support for industrial OT environments, such as Siemens SIMATIC controllers and other production-critical systems.

By combining Network Discovery with IT Asset Management (ITAM) practices, organizations can maintain a dynamic, real-time view of all assets, which is critical for both day-to-day IT operations and NIS2 compliance.

HOW ITAM SUPPORTS CYBERSECURITY AND COMPLIANCE

IT Asset Management is more than an inventory tool—it is a strategic enabler of robust cybersecurity. A mature ITAM system helps organizations:

- Keep an up-to-date inventory of hardware and software.
- Map dependencies and relationships between assets to ensure continuity.
- Monitor configurations for compliance with internal policies and regulatory standards.
- Automate alerts, reporting, and incident responses.
- Measure and report performance for internal audits and regulatory requirements.

When integrated with service desks or ITSM platforms, ITAM allows organizations to build proactive workflows, categorize security incidents, and accelerate remediation. This aligns directly with NIS2's emphasis on early detection, ongoing monitoring, and rapid response.

ACTING PROACTIVELY MATTERS

The NIS2 compliance deadline varies in different European states and penalties for non-compliance include fines, administrative actions, and potential criminal liability. Beyond

PGUM S.r.l

NOI Techpark
Via Ipazia 2
39100 Bolzano - Italia

Mail: info@i-vertix.com
PEC: pgumgmbh@pec.it
Web: i-vertix.com

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

regulatory consequences, failing to properly manage IT and OT assets exposes organizations to operational disruptions, data breaches, and reputational damage.

Implementing ITAM solutions today enables organizations to:

- Establish a clear, comprehensive view of assets.
- Mitigate risks before they become threats.
- Ensure operational continuity under both regulatory and cyber pressure.
- Demonstrate compliance with auditable processes.

By addressing these requirements proactively, organizations not only satisfy NIS2 obligations but also create a stronger, more resilient cybersecurity posture for the future.

CONCLUSION

Comprehensive IT and OT asset management is no longer a supporting activity—it is a strategic necessity. Organizations that leverage ITAM solutions gain:

- Full visibility of assets and dependencies.
- Enhanced risk management and security control.
- Streamlined compliance reporting.
- Faster recovery from cyber incidents.

In today's evolving threat landscape, ITAM provides the foundation for both regulatory compliance and operational resilience. Organizations that invest in asset visibility and management now are positioning themselves to meet NIS2 requirements while strengthening overall cybersecurity readiness.

Checklist

PGUM S.r.l

NOI Techpark
Via Ipazia 2
39100 Bolzano - Italia

Mail: info@i-vertix.com
PEC: pgumgmbh@pec.it
Web: i-vertix.com

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

The European Union's NIS2 directive has raised the bar for cybersecurity and regulatory compliance, requiring organizations to demonstrate not only strong risk management practices but also a clear, auditable view of all critical assets. This checklist provides a structured, step-by-step approach to help organizations build a complete asset inventory, strengthen cybersecurity, and prepare for NIS2 compliance.

1. PREPARATION & PLANNING

- Define the scope of your inventory, including IT, OT, mobile, cloud, and IoT devices.
 - Identify key stakeholders: IT, OT, cybersecurity, compliance, operations, and procurement teams.
 - Establish goals and objectives: regulatory compliance, risk mitigation, operational resilience.
 - Assign ownership and responsibility for each asset category.
 - Prepare a documentation framework for collecting, storing, and maintaining asset data.
-

2. ASSET DISCOVERY & INVENTORY

Hardware Inventory

- List all servers (physical, virtual, cloud-hosted).
- Include all workstations and laptops (Windows, macOS, Linux).
- Record mobile devices (smartphones, tablets, ruggedized OT devices).
- Capture network devices: switches, routers, firewalls, access points.
- Inventory peripherals: printers, scanners, IoT devices, sensors.

PGUM S.r.l

NOI Techpark
Via Ipazia 2
39100 Bolzano - Italia

Mail: info@i-vertix.com
PEC: pgumgmbh@pec.it
Web: i-vertix.com

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

- Document industrial OT devices: PLCs, SCADA controllers, robotics, production equipment.

SOFTWARE INVENTORY

- Identify all operating systems with version numbers.
- Inventory licensed software, including number of installations and expiration dates.
- Detect unsupported or legacy software (Windows 7/Server 2008, outdated Linux distros).
- Include specialized OT applications (HMI, SCADA, production management software).
- List cloud-based applications and SaaS subscriptions.
- Document open-source and third-party tools in use.

CONFIGURATION & DEPENDENCIES

- Map relationships between assets: network dependencies, client-server interactions, OT integration.
- Document critical configurations impacting security and operations.
- Assign asset owners and responsible teams.
- Identify unmonitored or isolated assets, including remote OT endpoints.

3. RISK ASSESSMENT & VULNERABILITY EVALUATION

- Categorize assets by criticality to business operations.
- Identify high-risk assets, such as legacy software or unsupported devices.
- Assess network exposure, including internet-facing endpoints and remote connections.
- Assign risk levels based on vulnerability, business impact, and likelihood.

PGUM S.r.l

NOI Techpark
Via Ipazia 2
39100 Bolzano - Italia

Mail: info@i-vertix.com
PEC: pgumgmbh@pec.it
Web: i-vertix.com

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

- Define mitigation measures, e.g., patching, access controls, segmentation, monitoring.
-

4. LIFECYCLE MANAGEMENT

- Establish asset lifecycle stages: procurement → deployment → operation → decommissioning.
 - Implement tracking for updates, patches, and maintenance.
 - Set procedures for secure retirement of devices and software, including data wiping.
 - Maintain a change log for additions, removals, or configuration updates.
-

5. INTEGRATION & AUTOMATION

- Integrate asset inventory with ITSM or service desk systems for workflow management.
 - Set up alerts for unauthorized changes or high-risk vulnerabilities.
 - Schedule regular discovery and inventory updates.
 - Ensure alignment with cybersecurity monitoring tools to continuously evaluate risk.
-

6. NIS2 COMPLIANCE REQUIREMENTS

- Confirm all critical assets are identified and monitored.
 - Maintain audit-ready reports demonstrating inventory completeness.
 - Document implemented risk controls and mitigation actions.
 - Track incident history and response actions to prove proactive management.
 - Regularly update asset inventory and risk assessments in line with NIS2 deadlines.
-

PGUM S.r.l

NOI Techpark
Via Ipazia 2
39100 Bolzano - Italia

Mail: info@i-vertix.com
PEC: pgumgmbh@pec.it
Web: i-vertix.com

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

7. CONTINUOUS REVIEW & IMPROVEMENT

- Conduct periodic audits of IT and OT asset inventories.
- Reassess criticality and risk levels for all assets.
- Update security policies and operational workflows according to new threats or regulatory changes.
- Provide ongoing staff training on ITAM best practices and NIS2 requirements.
- Define KPIs to measure inventory accuracy, patch compliance, incident response times, and overall risk reduction.

QUICK REFERENCE: ESSENTIAL ITAM ACTIONS FOR NIS2

1. Discover and document all IT and OT assets, including software and cloud services.
2. Map dependencies and configurations for operational continuity.
3. Assess risks and vulnerabilities across the infrastructure.
4. Ensure licensing, patching, and lifecycle management are up to date.
5. Integrate inventory with service management and monitoring tools.
6. Maintain audit-ready documentation for compliance reporting.
7. Implement continuous review and improvement cycles to stay ahead of threats.

i-Vertex – Contact Details

Address: NOITechpark – Palazzo D1, Via Ipazia, 2

PGUM S.r.l

NOI Techpark
Via Ipazia 2
39100 Bolzano - Italia

Mail: info@i-vertex.com
PEC: pgumgmbh@pec.it
Web: i-vertex.com

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

39100 Bolzano, Italy IT

Phone: +39 0471 1430170

E-Mail: sales@i-vertix.com

Web: www.i-vertix.com

PGUM S.r.l

NOI Techpark

Via Ipazia 2

39100 Bolzano - Italia

Mail: info@i-vertix.com

PEC: pgumgmbh@pec.it

Web: i-vertix.com

Cod. Fisc. e P.IVA: 02923310219

REA: BZ - 216954