Sepio NIS2 Compliance Cross Reference Guide

Executive summary

NIS2 requires covered entities to demonstrate effective cybersecurity governance, risk management, incident reporting, and audit readiness. In practice, many programs fail at the first step: maintaining a reliable inventory of what is actually connected to the environment.

Sepio addresses that gap by delivering device truth validation through AssetDNA, complete visibility across managed and unmanaged assets, policy based hardware access control, and automated mitigation workflows. This makes Sepio especially relevant to NIS2 requirements for physical asset management, supply chain security, incident handling, and evidence driven control effectiveness.

Best fit: organizations that need reliable discovery and control of IT, OT, IoT, and peripheral assets, including shadow or spoofed devices.

Strongest NIS2 alignment: Article 21 controls related to asset management, risk analysis, supply chain security, incident handling, and effectiveness assessment.

Shared responsibility model: Sepio supports the technical control and evidence layer, while customers retain responsibility for governance, legal reporting submissions, business continuity, IAM, MFA, and cryptography programs.

Audit value: Sepio outputs can be packaged into recurring evidence sets for internal audit, customer assurance, and regulator inquiries.

How to use this guide

- ✔ Use the summary matrix to quickly understand where Sepio has direct, partial, or supporting alignment to NIS2.
- ✔ Use the detailed sections to build customer facing responses, audit narratives, and implementation work plans.
- ✔ Use the evidence checklist to define what reports and records should be exported and retained on a recurring basis.
- ✔ Use the shared responsibility notes to set accurate expectations and avoid over stating tool scope.

NIS2 applicability context

NIS2 applies to a broad set of sectors and introduces obligations for essential and important entities. Final implementation and enforcement details are defined in each national law.

NIS2 creates requirements across governance, cyber risk management, incident reporting, and supervisory evidence.

Sector specific EU rules may override overlapping NIS2 obligations where equivalent requirements exist, such as DORA for many financial entities.

Sepio supports its customers' NIS2 compliance through strong security controls, risk management, and incident handling and should be mapped into the customer's existing control framework, not treated as a standalone compliance program.

Sepio's EU operation itself - strongly align with NIS2 requirements.

Customers should confirm scoping, local reporting thresholds, and regulator expectations before finalizing their compliance operating model.

Sepio capability baseline for NIS2 mapping

AssetDNA based device truth validation using physical layer and hardware level characteristics

Authoritative asset inventory across network assets, endpoints, peripherals, and cyber physical environments.

Policy based hardware access enforcement and automated mitigation workflows

Continuous monitoring with device location context, historical activity, and evidence generation

Trafficless visibility model that remains effective in environments with encrypted traffic.

Integration support with SIEM, SOAR, NAC, and ticketing tools to operationalize response and reporting.

NIS2 to Sepio alignment summary matrix

Part A - core technical control areas

NIS2 article / theme	Sepio role	Coverage	Typical customer gap to close
Article 20 - Governance	Management visibility and enforcement evidence for oversight	Partial	Board training, governance process, accountability records
Article 21(2)(a) - Risk analysis	Trusted asset baseline and policy inputs for hardware risk	Strong	Enterprise risk process and policy governance
Article 21(2)(b) - Incident handling	Detects rogue devices and supports containment workflows	Strong technical support	IR process, CSIRT playbooks, legal and comms
Article 21(2)(c) - BC/DR and crisis	Improves impact analysis and device level containment	Supporting	Backup, DR, crisis process and tooling
Article 21(2)(d) - Supply chain security	Validates device identity and enforces trusted hardware policy	Strong	Supplier due diligence and contracts
Article 21(2)(i) - Asset Management and Access Control	Provides authoritative, hardware-validated asset inventory and device-level access control policies (allow/alert/deny)	Strong	Workforce IAM and HR processes remain customer responsibilities

Part B - reporting, assurance, and complementary controls

NIS2 article / theme	Sepio role	Coverage	Typical customer gap to close
Article 21(2)(e) - Vulnerability handling	Asset context and prioritization signals for remediation.	Partial	Patching, SDLC, CVE lifecycle tooling
Article 21(2)(f) - Effectiveness assessment	Measurable policy violation, risk level metrics and mitigation outputs for effectiveness assessment and audit evidence.	Strong support	Formal KPI program and audits
Article 21(2)(g)(h)(j) - Training, crypto, MFA	Complements with device trust and policy enforcement.	Supporting	LMS, IAM, MFA, PKI, secure comms
Article 23 - Incident reporting	Faster detection, triage, and evidence for reporting deadlines.	Strong support	Submission process to CSIRT or regulator
Articles 32 to 34 - Supervision and fines	Audit ready evidence for implementation and due diligence.	Strong evidence layer	Program governance and regulator engagement

Detailed control mapping

Article 20 - Governance and management accountability

Coverage level: Partial

NIS2 expectation

Management bodies are expected to approve and oversee cybersecurity risk management measures, and ensure appropriate management training and awareness.

How Sepio supports

- Delivers a trusted view of connected assets and device identity that leadership can use to understand cyber physical exposure.
- Provides policy enforcement outputs, alerts, and mitigation evidence that support board and executive oversight reviews.
- Helps demonstrate due diligence by showing measurable improvements in visibility and hardware risk control.

Customer and ecosystem responsibilities

- Customer must maintain governance structures, approval workflows, and management accountability records.
- Customer must run management training and awareness programs, and retain attendance and completion evidence.
- Legal and compliance teams must align policies to the national NIS2 implementation in each jurisdiction.

Recommended evidence for auditors and customers

- Executive summary reports showing asset posture and enforcement trends.
- Approved hardware access policy documents and change records.
- Management review minutes and sign off records.
- Quarterly compliance review packs referencing Sepio outputs.

Article 21(2)(a) - Risk analysis and information system security policies

Coverage level: Strong

NIS2 expectation

Entities must define and maintain policies for risk analysis and information system security, with controls that reflect the organization's exposure and environment.

How Sepio supports

- Builds a reliable asset truth layer, including unmanaged or shadow devices that software only tools may not identify accurately.
- Supports policy decisions based on device type, identity, location, interface, and observed risk context.
- Improves risk analysis quality by grounding decisions in verified hardware and connectivity information.

Customer and ecosystem responsibilities

- Customer must maintain enterprise risk methodology, risk acceptance criteria, and policy approval governance.
- Customer must connect Sepio outputs to broader risk registers and control frameworks.
- Customer should define policy exceptions and compensating controls for non standard devices.

Recommended evidence for auditors and customers

- Asset inventory exports and classification reports.
- AssetDNA and device identity verification reports.
- Policy definitions, owners, and approvals.
- Exception and waiver register for hardware policy deviations.

Article 21(2)(b) - Incident handling

Coverage level: Strong technical support

NIS2 expectation

Entities must maintain incident handling capabilities, including detection, triage, containment, remediation, and coordination.

How Sepio supports

- Detects unauthorized, rogue, spoofed, or unmanaged hardware activity and policy violations.
- Supports automated containment, isolation, blocking, and escalation workflows through policy enforcement and integrations.
- Provides device history and context that improve incident triage and forensic timelines.

Customer and ecosystem responsibilities

- Customer must operate a formal incident response process, severity model, and decision authority.
- Customer must maintain legal, communications, and customer notification procedures.
- IR teams must document root cause, impact, and recovery actions across the full stack.

Recommended evidence for auditors and customers

- Alert logs and incident timelines from Sepio and integrated tools.
- Mitigation action history including blocks, isolates, and escalations.
- IR playbooks that reference Sepio data and triggers.
- Post incident reports with hardware and device evidence attached.

Article 21(2)(c) - Business continuity, backup, disaster recovery, and crisis management

Coverage level: Supporting

NIS2 expectation

Entities must maintain resilience measures such as backups, disaster recovery plans, crisis procedures, and continuity capabilities.

How Sepio supports

- Improves situational awareness during incidents by identifying affected or untrusted devices quickly.
- Supports containment of suspicious hardware to reduce spread and operational impact.
- Provides device level evidence that can improve impact analysis and recovery prioritization.

Customer and ecosystem responsibilities

- Customer must maintain backup platforms, restoration testing, and disaster recovery runbooks.
- Customer must define crisis communication, business continuity, and executive escalation procedures.
- Infrastructure teams must execute system recovery and validation outside Sepio.

Recommended evidence for auditors and customers

- Crisis runbooks that include device quarantine and validation steps.
- Recovery drill reports referencing Sepio discovery and containment outputs.
- Continuity plans mapped to critical sites and asset groups.
- Post event lessons learned including hardware level findings.

Article 21(2)(d) - Supply chain security

Coverage level: Strong for hardware and device assurance

NIS2 expectation

Entities must address supply chain and supplier related cyber risk, including risks from direct suppliers, service providers, and product trust concerns.

How Sepio supports

- Validates what a device actually is, not only what it claims to be on the network.
- Detects spoofed, hidden, or unapproved hardware and peripherals that may indicate supply chain compromise or unauthorized replacement.
- Enables policy enforcement by vendor, model, device type, and location to reduce exposure from untrusted hardware.

Customer and ecosystem responsibilities

- Customer must run supplier due diligence, contracting, and third party risk management processes.
- Procurement and legal teams must define supplier security clauses and evidence requirements.
- Customers should combine Sepio controls with SBOM, vendor attestations, and supplier reviews for full coverage.

Recommended evidence for auditors and customers

- Approved device and vendor policy lists.
- Detection reports for rogue, spoofed, or non compliant hardware.
- Exception approvals for temporary or high risk supplier devices.
- Supplier assurance records cross referenced to device policy controls.

Article 21(2)(i) - Asset Management and Access Control

Coverage level: Strong for physical assets

NIS2 expectation

Entities must maintain "human resources security, access control policies and asset management." [nis-2-directive.com]. That single clause is short, but it is intentionally broad and is one of the most operationally significant parts of Article 21.

How Sepio supports

- Verified asset inventory: Sepio provides a hardware validated inventory of all connected assets, including unmanaged and spoofed devices.
- Hardware access control: Sepio enforces device level access policies (allow/alert/block) to prevent unauthorized or high risk hardware connections.
- Policy enforcement evidence: Sepio generates continuous logs and enforcement records to evidence effective asset and access control governance.

Customer and ecosystem responsibilities

- HR security: Manage workforce onboarding, role changes, offboarding, and periodic access reviews.
- Access governance: Define and enforce user and administrative access policies (IAM, MFA, least privilege, exceptions).
- Asset accountability: Assign asset ownership and lifecycle governance, integrating technical discovery tools into the control framework.

Recommended evidence for auditors and customers

- Asset inventory: Hardware validated visibility of all connected assets, including unmanaged and spoofed devices, new devices that were added at any cadance (day, week, etc.)
- Device level control: Policy based control (allow / alert / block) of device connections at the point of access.
- Audit ready evidence: Continuous logs and reports showing asset presence, policy enforcement, and access control outcomes.

Article 21(2)(e) - Secure acquisition, development, maintenance, and vulnerability handling

Coverage level: Partial

NIS2 expectation

Entities must manage cybersecurity in acquisition, development, and maintenance, including vulnerability handling and disclosure processes.

How Sepio supports

- Provides hardware and asset context that improves remediation prioritization and operational decision making.
- Identifies risky or unmanaged devices and can trigger workflow actions through integrations.
- Helps security teams focus patching and response actions based on verified device presence and exposure.

Customer and ecosystem responsibilities

- Customer must operate patching, vulnerability scanning, and remediation governance.
- Development teams must maintain secure SDLC and vulnerability disclosure processes.
- GRC teams must track remediation timelines, exceptions, and compensating controls.

Recommended evidence for auditors and customers

- Asset exposure reports used for vulnerability triage.
- Integrated workflow tickets and remediation action records.
- Policy based enforcement logs for unpatched or restricted devices.
- Exception and risk acceptance documentation tied to device inventory.

Article 21(2)(f) - Assessing effectiveness of cybersecurity measures

Coverage level: Strong support

NIS2 expectation

Entities must assess the effectiveness of cybersecurity risk management measures through policies, procedures, and evidence based review.

How Sepio supports

- Provides measurable outputs such as detected rogue devices, policy violations, and mitigation actions executed.
- Supports continuous monitoring and historical evidence for trend analysis and control validation.
- Helps demonstrate that hardware trust controls are active, enforced, and producing outcomes.
- Generates measurable risk based indication for all physical assets.

Customer and ecosystem responsibilities

- Customer must define KPIs, testing frequency, audit scope, and review ownership.
- Customer should run periodic control testing, incident simulations, and tabletop exercises.
- Audit and compliance teams must consolidate evidence from Sepio and other systems into a formal assessment package.

Recommended evidence for auditors and customers

- Monthly and quarterly KPI dashboards.
- Trend analysis of policy violations and response times.
- Audit trails of enforcement actions and policy changes.
- Control effectiveness review minutes and corrective action plans.
- Pivot reports based on risk levels and asset types, location, proximity to the enterprise “crown jewels”.

Article 21(2)(g), (h), and (j) - Cyber hygiene, cryptography, training, and MFA handling

Coverage level: Supporting

NIS2 expectation

NIS2 also expects basic cyber hygiene and training, cryptography and encryption policies, and secure authentication and communications practices.

How Sepio supports

- Strengthens these controls indirectly by enforcing trusted hardware and reducing unauthorized device pathways.
- Provides practical incident examples and policy evidence that can be used in awareness and training programs.
- Complements IAM, MFA, and secure communications controls by validating the device side of trust.

Customer and ecosystem responsibilities

- Customer must run training and awareness programs and retain completion records.
- Customer must implement IAM, MFA, PKI, encryption, and secure communications controls.
- Architecture and security teams must define integration points between Sepio, NAC, IAM, and network security controls.

Recommended evidence for auditors and customers

- Training content that references device trust and hardware policy scenarios.
- Architecture diagrams showing Sepio integration with IAM, NAC, and SIEM.
- Device policy reports demonstrating support for least privilege access principles.
- Control mapping that documents scope boundaries for Sepio versus IAM and crypto tools.

Article 23 - Significant incident reporting

Coverage level: Strong support (not submission itself)

NIS2 expectation

Entities must report significant incidents according to national NIS2 rules, typically requires early warning within 24 hours, formal notification within 72 hours, and final reporting timelines.

How Sepio supports

- Accelerates detection and triage of hardware related events through verified device identity and continuous monitoring.
- Provides exact device context such as type, location, and policy enforcement status for reporting accuracy.
- Captures mitigation evidence and history that supports incident narratives and regulator ready reporting packages.

Customer and ecosystem responsibilities

- Customer must define thresholds for reportable incidents and align to national CSIRT or regulator requirements.
- Customer must maintain submission workflows, legal review, and communication approvals.
- Incident owners must consolidate Sepio data with broader forensic, network, and business impact analysis.

Recommended evidence for auditors and customers

- Detection timestamp and event timeline.
- Affected devices and verified identity details.
- Mitigation actions taken and current status.
- Cross functional approval records and final incident report package.

Articles 32 to 34 - Supervision, audits, enforcement, and fines

Coverage level: Strong evidence layer

NIS2 expectation

NIS2 gives authorities supervisory powers and allows them to request evidence, audits, and proof of implementation. It also introduces significant fine exposure for non compliance.

How Sepio supports

- Produces audit ready evidence for asset inventory, policy enforcement, incident actions, and monitoring outcomes.
- Supports due diligence narratives by showing continuous control operation and measurable risk mitigation.
- Enables repeatable evidence packages for internal audit, customer assurance, and regulator inquiries.

Customer and ecosystem responsibilities

- Customer remains responsible for legal compliance, responses to authorities, and formal audit management.
- Compliance teams must organize evidence from Sepio alongside governance, IAM, BC/DR, and reporting procedures.
- Customers should assign an owner for recurring evidence exports and regulator readiness reviews.

Recommended evidence for auditors and customers

- Recurring evidence pack including inventory baseline, AssetDNA validation, policy catalog, and enforcement logs.
- Vulnerability intelligence, location aware reporting, and historical device activity logs.
- Integration evidence from SIEM, SOAR, NAC, and ticketing workflows.
- Audit response templates and named owners for regulator requests.

Customer implementation roadmap

The roadmap below is designed for customer facing planning discussions. It positions Sepio as a foundational control while clearly showing the shared responsibilities needed for NIS2 readiness.

Phase	Primary objective	Key Sepio actions	Customer actions	Deliverables
1. Scope and baseline	Define applicability and establish device truth baseline	Deploy discovery, validate coverage, and baseline inventory and AssetDNA visibility	Confirm scope, sector obligations, priority sites, and target control framework	Scope memo, baseline inventory, initial risk findings
2. Policy design	Translate policy objectives into enforceable hardware controls	Create policy sets for approved devices, rogue detection, and location or role based restrictions	Approve policy owners, exceptions, change process, and enforcement thresholds	Policy catalog, exception process, pilot plan
3. Integration and response	Operationalize detection and mitigation	Integrate with SIEM, SOAR, NAC, and ticketing; enable automated actions and evidence logging	Update IR playbooks and validate legal and comms paths	Integrated workflows and tested playbooks
4. Audit and reporting readiness	Create recurring evidence and reporting capability	Schedule exports and dashboards for inventory, policy, incidents, and enforcement	Define reporting templates, review cadence, and evidence owners	Quarterly evidence pack and readiness review

Recommended Sepio evidence pack for NIS2 programs

Customers should build a recurring evidence package monthly or quarterly. The goal is to show that controls are not only defined, but operating and producing measurable outcomes.

- **Asset inventory baseline -** complete inventory by site, segment, and critical asset class, including unmanaged and shadow assets.
- **AssetDNA and identity validation evidence -** records of unknown, spoofed, or policy violating device detections and their disposition.
- **Policy catalog and approvals -** policy versions, owners, enforcement mode, and exception records.
- **Policy enforcement and mitigation logs -** alerts, block or isolate actions, escalations, and workflow outcomes.
- **Vulnerability and exposure context reports -** prioritized device groups and remediation support outputs.
- **Location aware and asset history reporting -** device location context and historical activity to support investigations.
- **Integration evidence -** SIEM, SOAR, NAC, and ticketing records proving end to end workflow execution.
- **Effectiveness review package -** KPI trends, control testing results, and management review decisions.

Shared responsibility model

Sepio is a critical control layer for device trust and hardware risk mitigation, but NIS2 compliance remains a program that spans people, process, and multiple technologies.

Sepio responsibility	Customer responsibility	Shared outcomes
Device discovery and identity validation	Governance, policy approval, and legal accountability	Trusted, auditable risk management controls
Hardware policy enforcement and mitigation triggers	Incident response decisions and regulator reporting submissions	Faster containment and stronger reporting evidence
Continuous monitoring and technical evidence generation	Control testing, audit management, and evidence retention	Demonstrable due diligence and effectiveness
Integration to ecosystem tools	Operating model, staffing, and cross team coordination	Operationalized NIS2 readiness across the stack

Sector specific note for financial entities

For many financial entities, DORA may define the primary cybersecurity and incident reporting obligations where it overlaps with NIS2. In these cases, position Sepio as NIS2 aligned and DORA supportive, then confirm the governing requirements through the applicable national implementation and supervisory guidance.

- ✓ Use this guide as a control alignment reference for hardware trust and asset visibility.
- ✓ Validate the primary reporting and oversight obligations under the sector specific regime.
- ✓ Preserve a single evidence model where possible so the same Sepio outputs support both regulatory and customer assurance needs.

Suggested customer facing positioning statement

Sepio helps organizations operationalize key NIS2 control requirements by delivering verified device identity through AssetDNA, complete asset visibility, policy driven hardware access enforcement, and automated mitigation workflows. Sepio is especially effective for unmanaged, rogue, and spoofed devices that traditional software only tools often miss, and it provides the evidence needed to support incident handling, audit readiness, and regulator focused reporting.

Next steps for customer projects

1. Run a short discovery assessment to baseline asset visibility and identify unmanaged or untrusted devices
2. Prioritize one or two high impact policy use cases, such as blocking unapproved USB devices or enforcing approved network adapter policy
3. Integrate Sepio alerts into the existing incident handling workflow and test a reporting scenario
4. Define the recurring NIS2 evidence package and assign owners for export, review, and retention
5. Review the final control mapping against the national NIS2 implementation with legal and compliance counsel

Important note: This guide explains how Sepio supports NIS2 control objectives. It is a technical and operational alignment document, not legal advice. NIS2 is implemented through national laws, so customers should confirm final obligations with legal and compliance counsel in each country of operation. Sepio is positioned here as a core technical control layer for hardware trust, visibility, and policy enforcement within a broader compliance program.

Disclaimer: This document is intended for compliance alignment planning and customer communication. It does not constitute legal advice.