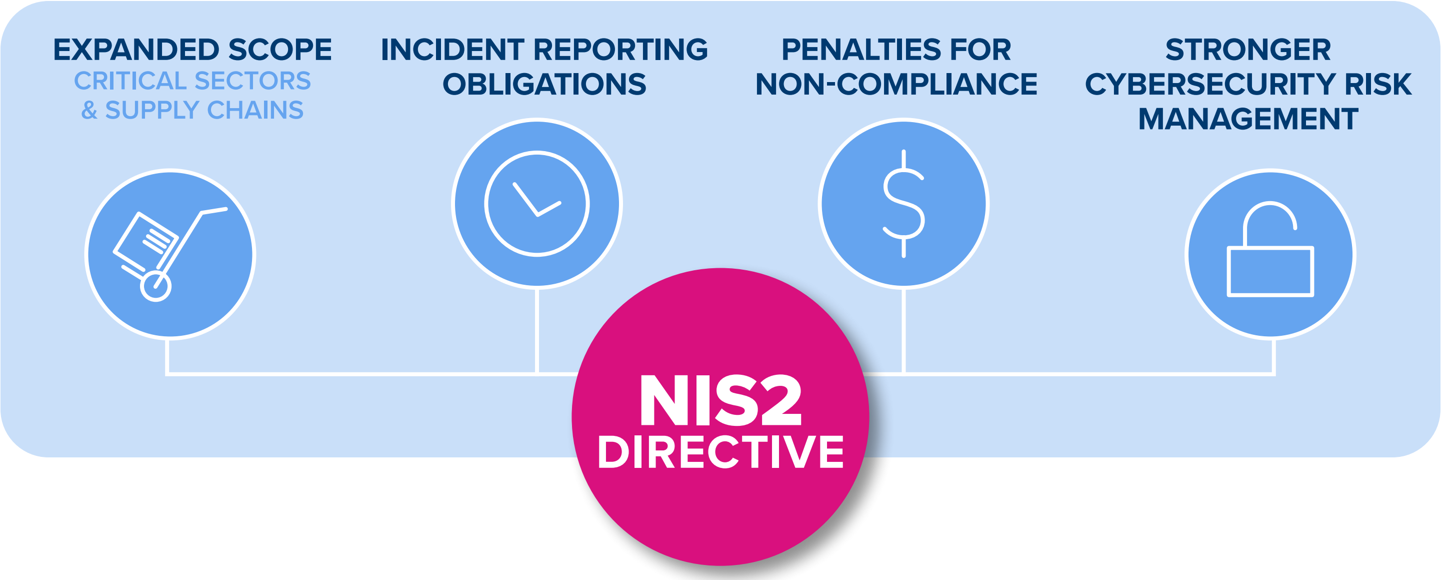
Cambium Networks™

SOLUTION PAPER

NSE and NIS2 Compliance Mapping



EXPANDED SCOPE
CRITICAL SECTORS
& SUPPLY CHAINS

INCIDENT REPORTING OBLIGATIONS

PENALTIES FOR NON-COMPLIANCE

STRONGER CYBERSECURITY RISK MANAGEMENT

NIS2
DIRECTIVE

Executive Summary

The NIS2 Directive establishes security and resilience requirements for essential and important entities across the EU. Compliance demands stronger governance, incident response, access control, resilience, and supply-chain risk management.

Cambium Networks' Network Service Edge (NSE) solutions, managed through cnMaestro™ Network Management, provide capabilities that directly address these domains. With built-in device identification, centralized management, vulnerability scanning, access controls, network segmentation, secure configuration, logging, and redundancy, NSE helps organizations demonstrate alignment with NIS2 requirements and strengthen overall cyber resilience.

©2025 Cambium Networks, Ltd.

DOMAIN	NIS2 Requirement	How NSE Supports the Requirement
GOVERNANCE AND POLICIES	Maintain asset inventory	Device identification and fingerprinting (type, OS, make, vulnerabilities)
	Secure configuration policies	cnMaestro centralized management, role-based access
RISK MANAGEMENT	Regular vulnerability assessment	NSE firmware scrubbed against CVEs; LAN vulnerability scans
	Ensure patches and updates	Regular firmware and security patch releases
MONITORING	Enable logging and reporting	Syslog, cnMaestro dashboards, APIs
ACCESS AND AUTHENTICATION	MFA for administrators	MFA support through cnMaestro
	Restrict access to authorized staff	Role-based access in cnMaestro
	Strong password policies	Cambium account rules + MFA recommendations
INCIDENT RESPONSE	Configure alerts	Alerts on threats, DNS filtering, failed logins
	Retain logs for forensics	Configurable log retention, export via syslog
NETWORK BEST PRACTICES	Segmentation of critical systems	VLANs, firewall policies for inter-VLAN isolation
	Encrypted management protocols	HTTPS, SSH, SNMPv3
	Disable unused services/ports	Default WAN→LAN block, admin-enabled exceptions
RESILIENCE	Redundancy for critical devices	WAN redundancy, high-availability pairs
TRAINING AND AWARENESS	IT staff training	Cambium structured training for secure deployment

NIS2 → NSE Compliance Mapping

GOVERNANCE AND POLICIES

- **Inventory of critical assets:** NSE automatically fingerprints connected devices, recording type, make, OS, and vulnerabilities.
- **Secure configuration:** Centralized through cnMaestro with role-based policies that ensure only authorized administrators can make changes.
- **Documentation:** cnMaestro dashboards and inventory views support compliance reporting.

RISK MANAGEMENT AND PROTECTION

- **Vulnerability management:** NSE firmware scrubbed against known vulnerabilities prior to release. Periodic LAN scans identify vulnerable devices.
- **Patch management:** Regular security updates and firmware releases keep systems hardened.
- **Monitoring:** Logs and events are available via cnMaestro, syslog, and APIs for continuous oversight.

©2025 Cambium Networks, Ltd.

NIS2 → NSE Compliance Mapping *continued*

ACCESS AND AUTHENTICATION

- **MFA:** cnMaestro requires/supports multifactor authentication for admin logins.
- **Role-based access:** Administrative functions are restricted to authorized personnel.
- **Password policies:** Cambium enforces minimum length, dictionary/keyboard pattern avoidance, and breach-list checking. MFA is strongly recommended.

INCIDENT DETECTION AND RESPONSE

- **Alerting:** Anomalous activity (vulnerability findings, intrusion prevention, DNS filtering, repeated login failures) triggers alerts.
- **Forensics:** Alerts and audit logs are retained for compliance reporting and can be exported for forensic analysis.

NETWORK SECURITY BEST PRACTICES

- **Segmentation:** VLAN-based segmentation + inter-VLAN firewalling isolates critical systems.
- **Secure protocols:** HTTPS, SSH, and SNMPv3 are supported for secure device management.
- **Default deny posture:** WAN→LAN traffic is blocked by default; admins explicitly allow services.

MONITORING AND AUDITING

- **Log review:** All NSE activities are logged and can be forwarded to external servers for SIEM integration.
- **Audit readiness:** Supports compliance audits with centralized visibility and exportable logs.

RESILIENCE AND CONTINUITY

- **Redundancy:** WAN redundancy ensures continuity during internet failures; high-availability pairs cover hardware failure.
- **Backups and rollback:** Regular backup and automatic rollback to last-known-good configurations prevent prolonged downtime.

TRAINING AND AWARENESS

- **Staff enablement:** Cambium provides structured training for IT staff on secure deployment and configuration of NSE devices.
- **Best-practice guidance:** Documentation and support materials reinforce NIS2-aligned security practices.

About Cambium Networks

Cambium Networks enables service providers, enterprises, industrial organizations, and governments to deliver exceptional digital experiences and device connectivity with compelling economics. Our ONE Network platform simplifies management of Cambium Networks' wired and wireless broadband and network edge technologies. Our customers can focus more resources on managing their business rather than the network. We make connectivity that just works.

©2025 Cambium Networks, Ltd.