



How Eye Security can help

NIS2 in Practice: Where Eye Security Strengthens Your Compliance Readiness.

Many of the responsibilities under NIS2, such as governance decisions, risk ownership, and formal accountability, remain firmly with the organisation and its management. No security provider can transfer or replace those duties.

A critical operational requirement under NIS2 is the ability to detect and respond to security incidents. Organisations must continuously monitor environments, identify threats early, and act quickly to contain and manage incidents. Eye Security supports exactly these requirements through 24/7 SOC monitoring and incident response, helping you investigate, contain, and remediate incidents while meeting reporting obligations. We help you implement, operationalise, and evidence the key NIS2 requirements to identify, detect, and respond.

Beyond detection and response, the overview below maps out your responsibilities under NIS2 and shows where Eye Security can provide support, tooling, expert guidance, or templates or advisory input while governance, final decision-making, and legal accountability stay with you.



For security leaders, the assume breach principle requires a shift from compliance-driven activity to continuous readiness. This involves testing response plans, training teams, monitoring systems 24/7, and partnering for expertise. The organisations that will thrive under NIS2 are those that treat the directive as a blueprint for long-term resilience.

Marcel van Asperdt
CISO, Eye Security

↘ The highlighted areas indicate where Eye Security provides direct support or enables implementation through its certified partners. The final responsibility for compliance, reporting, and remediation always stays with the entity, even if Eye Security supports operational execution.

Governance and accountability

- ✓ Appoint a responsible person or team for NIS2 compliance
- ✓ Ensure board-level approval of cybersecurity policies
- ✓ Provide management training on NIS2 obligations
- ✓ Document roles and responsibilities for incident response

Risk management

- ✓ Conduct regular risk assessments for IT and OT systems
- ✓ Maintain an information security policy aligned with ISO 27001 or NIST
- ✓ Implement asset inventory and classification
- ✓ Apply encryption for sensitive data (at rest and in transit)

Technical and organisational measures

- ✓ Access control with multi-factor authentication
- ✓ Patch and vulnerability management process in place
- ✓ Secure system acquisition, development, and maintenance
- ✓ Implement network segmentation and firewall rules
- ✓ Ensure secure communications (TLS, VPN)

Business continuity

- ✓ Create and test disaster recovery plans
- ✓ Maintain backup strategy (offline and immutable backups)
- ✓ Define Recovery Time Objectives (RTO) and Recovery Point Objectives (RPO)

Training and awareness

- ✓ Conduct regular cybersecurity training for staff
- ✓ Implement phishing simulations and awareness campaigns

Incident handling

- ✓ Develop and test an incident response plan
- ✓ Assist in preparing reports for:
 - o Early warning within 24 hours
 - o Detailed report within 72 hours
- ✓ Establish contact with national CSIRT

Supply chain security

- ✓ Assess third-party risk for critical suppliers
- ✓ Include cybersecurity clauses in vendor contracts
- ✓ Continuous monitoring of service provider security posture

Documentation and evidence

- ✓ Facilitate audit logs for security events
- ✓ Maintain records of compliance activities
- ✓ Prepare for audits and inspections by authorities

Governance reporting

- ✓ Schedule annual compliance reviews
- ✓ Report to management and regulators as required



About Eye Security

Eye Security helps small and medium-sized businesses identify cyber risks proactively and strengthen operational resilience. As one of Europe's leading MDR providers, the company blends advanced AI technology, expert guidance, and integrated cyber insurance into one cohesive solution. More than 800 organisations across Europe rely on this unified approach to safeguard their digital operations.

eye.security



Incident response hotline

Experiencing a cyber incident? Call the Eye Security Incident Response hotline at **+31 88 644 4898** (24/7 availability) or contact the IR team via email at cert@eye.security for non-urgent cases.