

SEC11 - NIS2 for Embedded

Objectives

- Understand NIS2 scope, roles, and obligations for essential/important entities.
- Translate Article 21 risk-management measures into an embedded/OT context.
- Apply incident reporting timelines (24h/72h/1-month) with ready-to-use templates.
- Build a 30/60/90-day compliance roadmap and evidence checklist.

Course Environment

- Theoretical course
 - PDF course material (in English) supplemented by a printed version for face-to-face courses.
 - Online courses are dispensed using the Teams video-conferencing system.
 - The trainer answers trainees' questions during the training and provide technical and pedagogical assistance.
- At the start of each session the trainer will interact with the trainees to ensure the course fits their expectations and correct if needed

Target Audience

- Any embedded systems engineer or technician with the above prerequisites.

Evaluation modalities

- The prerequisites indicated above are assessed before the training by the technical supervision of the trainee in his company, or by the trainee himself in the exceptional case of an individual trainee.
- Trainee progress is assessed by quizzes offered at the end of various sections to verify that the trainees have assimilated the points presented
- At the end of the training, each trainee receives a certificate attesting that they have successfully completed the course.
 - In the event of a problem, discovered during the course, due to a lack of prerequisites by the trainee a different or additional training is offered to them, generally to reinforce their prerequisites, in agreement with their company manager if applicable.

Plan

Introduction & Scope

- NIS2 at a glance
- Sectors in scope & “size-cap” rule
- Essential vs Important Entities (EEs vs IEs)
- Roles, authorities, penalties

Governance & Responsibilities

- Management accountability
- Security policy & risk ownership
- Roles/RACI and coordination with product/OT teams

Risk Management Measures

- Business continuity & incident handling

- Identity & Access and logging
- Vulnerability management & secure development
- OT/embedded specifics (segmentation, safety interplay)

Mapping to Engineering Workflows

- From requirements to release (Dev & Test & Release & Update)
- Secure updates & support periods (firmware/RTOS/toolchains)
- Vulnerability intake, triage, remediation, and user communication
- Evidence-by-design: what to capture during builds

Incident Reporting

- Triggers & thresholds (significant incidents)
- Timelines: 24h / 72h / 1-month reports
- Internal playbook, contacts, escalation

Supply Chain & Third-Party Components

- Supplier due diligence & contractual expectations
- Updates, disclosure programs, and support commitments
- Evidence from vendors (SBOM/VEX, security posture)

Evidence & Metrics

- Registers: risks, incidents, assets, suppliers, training
- KPIs & dashboards for management
- Preparing for audits/inspections

Roadmap

- Quick wins
- Priority controls & contracts
- Exercises, metrics, internal audit

Wrap-Up & Q&A

- Key takeaways
- Next steps & optional deep-dives (OT, IoT, CRA alignment)

Renseignements pratiques

Inquiry : 1 day