Certified NIS2 Lead Auditor / Lead Implementer

Implement, Evidence, and Audit NIS2 Readiness

The C)NIS2-LA/LI – Certified NIS2 Lead Auditor / Lead Implementer prepares professionals to implement, manage, and audit cybersecurity programs aligned with the EU NIS2 Directive and ISO/IEC 27001 management-system principles.

The program combines two progressive pathways. The Lead Implementer pathway focuses on applicability, scope, governance, risk, controls, incident and supplier readiness, evidence, monitoring, and improvement. The Lead Auditor pathway builds on that foundation with audit principles, planning, evidence collection, control testing, findings, reporting, and follow-up.
The course emphasizes defensible evidence and professional boundaries: ISO/IEC 27001 can organize readiness, while national NIS2 laws, competent authorities, registration duties, and country-specific reporting requirements still require local validation.

Key Course Information

Live Class Duration: 4 Days
CEUs: 32
Language: English

Class Formats Available:

- Instructor Led
- Self-Study
- Live Virtual Training

Suggested Prerequisites:

- Basic information-security knowledge
- Experience in risk, governance, compliance, implementation, or auditing
- Prior ISO/IEC 27001 or NIS2 experience helpful, but not required

Modules/Lessons

Module 01: ISO/IEC 27001 and NIS2
Module 02: Organizational Context
Module 03: Leadership, Governance
Module 04: Competence
Module 05: Risk Assessment
Module 06: Organizational, People
Module 07: Incident Reporting,
Module 08: Monitoring, Mgmt
Module 09: Audit Principles
Module 10: Audit Scope, Criteria
Module 11: Collecting & Evaluating
Module 12: Auditing Governance
Module 13: Auditing Security
Module 14: Auditing Incidents
Module 15: Nonconformities
Module 16: Audit Reporting

Full Titles Below

Who Should Attend

- IS Security Officers
- CISOs & Security Managers
- NIS2 Program Leads
- Risk Managers
- Compliance Professionals
- Internal / External Auditors
- IT Auditors
- ISO/IEC 27001 Implementers
- Security Consultants
- Business Continuity Professionals
- Supplier / Third-Party Risk Managers
- Management responsible for cyber oversight

Accreditations

www.mile2.com 10213 Wilsky Blvd, Tampa, FL 33625 813-920-6779

Certified NIS2 Lead Auditor / Lead Implementer

Upon Completion

Upon completion, students will be able to:

- Determine and document NIS2 applicability and scope
- Establish governance and management accountability
- Conduct cybersecurity risk assessments and treatment
- Develop and maintain a defensible Statement of Applicability
- Implement organizational, people, physical, and technological controls
- Manage incident reporting, continuity, and supplier security
- Monitor effectiveness and support continual improvement
- Plan and conduct risk-based audits
- Collect and evaluate sufficient audit evidence
- Test controls and write defensible findings
- Evaluate corrective action and closure
- Report conclusions and perform audit follow-up

Exam Information

The C)NIS2-LA/LI exam is taken online through Mile2's Learning Management System and is accessible on you Mile2.com account. The exam will take approximately 2 hours and consist of 100 multiple choice questions. A minimum grade of 70% is required for certification.

Re-Certification Requirements

All Mile2 certifications will be awarded a 3-year expiration date.

There are two requirements to maintain Mile2 certification:

1) Pass the most current version of the exam for your respective existing certification
2) Earn and submit 20 CEUs per year in your Mile2 account.

Course FAQ's

Question: Do I have to purchase a course to buy a certification exam?

Answer: No

Question: Do all Mile2 courses map to a role-based career path?

Answer: Yes. You can find the career path and other courses associated with it at www.mile2.com.

Question: Are all courses available as self-study courses?

Answer: Yes. There is however 1 exception. The Red Team vs Blue Team course is only available as a live class.

Question: Are Mile2 courses transferable/shareable?

Answer: No. The course materials, videos, and exams are not meant to be shared or transferred.

Course and Certification Learning Options

www.mile2.com 10213 Wilsky Blvd, Tampa, FL 33625 813-920-6779

Detailed Outline:

PART I – NIS2 IMPLEMENTATION & MANAGEMENT SYSTEM FOUNDATIONS

Module 01: ISO/IEC 27001 and NIS2 Foundations
01.1 Integrated Lead Implementer and Lead Auditor Pathways
01.2 NIS2 Directive Foundation, National Implementation, and Professional Boundaries
01.3 ISO/IEC 27001 Management-System Structure and Risk-Based Approach
01.4 Evidence, Audit Readiness, and the EuroCore Continuing Scenario

Module 02: Organizational Context, Applicability, and Scope
02.1 Organizational Context and Interested Parties
02.2 Obligations Register, Conflicts, Overlap, and Change Monitoring
02.3 NIS2 Applicability, Entity Classification, Jurisdiction, and Registration
02.4 Legal Scope, ISMS Scope, Audit Scope, Boundaries, Interfaces, and Dependencies

Module 03: Leadership, Governance, and Management Accountability
03.1 Management-Body Accountability and Executive Sponsorship
03.2 Roles, Responsibilities, RACI, Risk Owners, and Control Owners
03.3 Security Policy, Objectives, Resources, and Decision Authority
03.4 Management Reporting, Training, Approvals, Minutes, and Governance Evidence

Module 04: Competence, Communication, and Documented Information
04.1 Competence, Role Requirements, and Training Evidence
04.2 Awareness, Cyber Hygiene, and Security Culture
04.3 Internal, External, Incident, Crisis, and Supplier Communication
04.4 Documented Information, Records, Lifecycle Control, and Evidence Quality

PART II – RISK, CONTROLS, OPERATIONS & IMPROVEMENT

Module 05: Risk Assessment, Treatment, and Statement of Applicability
05.1 Risk Methodology, Criteria, Assets, Threats, Vulnerabilities, and Dependencies
05.2 Risk Analysis, Evaluation, Prioritization, and Documentation
05.3 Risk Treatment, Ownership, Residual Risk, Acceptance, and Action Planning
05.4 Statement of Applicability, Control Justification, Status, and Traceability

Module 06: Organizational, People, Physical, and Technological Controls
06.1 Organizational Controls: Policies, Assets, Suppliers, Projects, and Governance
06.2 People Controls: Screening, Awareness, Responsibilities, and Role Changes
06.3 Physical Controls: Secure Areas, Entry, Equipment, Environment, and Media
06.4 Technological Controls: IAM, MFA, Cryptography, Vulnerabilities, Logging, Backups, Cloud, and Development

Module 07: Incident Reporting, Continuity, and Supply Chain
07.1 Incident Readiness, Detection, Triage, Escalation, and Evidence
07.2 NIS2 Significant-Incident Assessment and Staged Reporting
07.3 Business Impact Analysis, RTO/RPO, Recovery, Backups, Testing, and Crisis Management
07.4 Supplier Criticality, Due Diligence, Contracts, Monitoring, Fourth Parties, and Exit Readiness

Module 08: Monitoring, Management Review, and Implementation Planning
08.1 Monitoring, Measurement, Analysis, and Evaluation
08.2 Internal-Audit Readiness and Management Review
08.3 Nonconformity, Root Cause, Corrective Action, and Continual Improvement
08.4 Gap Assessment and Implementation Roadmap with Owners, Dependencies, and Evidence

PART III – AUDIT PLANNING, EVIDENCE & GOVERNANCE ASSURANCE

Module 09: Audit Principles and Auditor Responsibilities
09.1 Audit Purpose, Criteria, Evidence, Relationships, and Limitations
09.2 Integrity, Fair Presentation, Confidentiality, Independence, Evidence-Based and Risk-Based Auditing
09.3 Auditor Independence, Competence, Safeguards, and Role Boundaries
09.4 Audit Program, Risk-Based Scheduling, Methods, Records, and Quality

Module 10: Audit Scope, Criteria, and Planning
10.1 Audit Objectives, Scope, Boundaries, and Criteria
10.2 Auditee Understanding, Risk Prioritization, Methods, and Team Competence
10.3 Schedule, Evidence Requests, Audit Trails, Checklists, and Interview Strategy
10.4 Sampling, Expansion Triggers, Audit Risk, Constraints, and Limitations

Module 11: Collecting and Evaluating Evidence
11.1 Evidence Sources, Collection Methods, and Audit Questions
11.2 Reliability, Sufficiency, Relevance, Completeness, and Traceability
11.3 Interviews, Observations, Walkthroughs, Screenshots, and Technical Demonstrations
11.4 Workpapers, Evidence Indexing, Confidentiality, Integrity, and Preliminary Conclusions

Module 12: Auditing Governance and Risk Management
12.1 Connected Governance-to-Risk Audit Trail
12.2 Context, Scope, Legal Assumptions, Leadership, Policy, Objectives, and Resources
12.3 Competence, Communication, Documented Information, and Records at the Point of Use
12.4 Risk Methodology, Populations, Treatment, Acceptance, Exceptions, and Statement of Applicability
12.5 Metrics, Internal Audit, Management Review, Improvement, and EuroCore Interview Activity

PART IV – CONTROL ASSURANCE, FINDINGS, REPORTING & CAPSTONE

Module 13: Auditing Security Controls
13.1 Control Design, Objectives, Criteria, Implementation, and Intended Scope
13.2 Control Operation, Exceptions, Waivers, Compensating Controls, and Sample Expansion
13.3 Auditing Organizational and People Controls
13.4 Auditing Physical and Technological Controls

Module 14: Auditing Incidents, Continuity, and Suppliers
14.1 Incident Detection, Escalation, Significance Decisions, Reporting, Records, and Learning
14.2 Continuity and Recovery: BIA, Objectives, Strategies, Backups, Exercises, and Corrective Action
14.3 Suppliers and Cloud Providers: Population, Criticality, Due Diligence, Contracts, Monitoring, Shared Responsibility, and Exit
14.4 Integrated Resilience Conclusion and Cross-Domain Corroboration

Module 15: Findings, Nonconformities, and Corrective Action
15.1 From Evidence to Findings: Criteria, Condition, Evidence, Scope, and Significance
15.2 ISO Nonconformities, NIS2 Gaps, Observations, and Unresolved Legal Questions
15.3 Correction, Containment, Root Cause, Corrective Action, Ownership, Milestones, and Effectiveness Criteria
15.4 Follow-Up, Sustained Effectiveness, Escalation, Recurrence, and Closure Authority

Module 16: Audit Reporting, Follow-Up, and Integrated Capstone
16.1 Controlled Audit Reporting, Approval, Distribution, and Record Protection
16.2 Executive Communication of Conclusions, Priorities, Limitations, and Decisions
16.3 Action Tracking, Management Response, Implementation Evidence, Effectiveness, and Escalation
16.4 Closure, Integrated Assurance Conclusions, and EuroCore Capstone

APPENDICES / PRACTICAL DELIVERABLES

- EuroCore continuing case-study evidence set
- Applicability and scope worksheet
- Governance / RACI and evidence register
- Risk register and risk-treatment plan
- Statement of Applicability working template
- Incident-reporting and supplier-readiness exercises
- Audit plan and evidence request list
- Audit workpaper and evidence index
- Finding / corrective-action worksheet
- Executive audit report and follow-up plan