NIS 2 Directive: Cybersecurity Compliance & Risk Management Training Course

10 – 14 May 2027
Vienna

AGILE LEADERS
Training Center

AGILE LEADERS
Training Center

NIS 2 Directive: Cybersecurity Compliance & Risk Management Training Course

Ref: 103600309_99397 **Date:** 10 – 14 May 2027 **Location:** Vienna **Fees:** 7500 Euro

Course Overview

In today's rapidly evolving digital landscape, cybersecurity has become a critical priority for organizations worldwide. The NIS 2 Directive: Cybersecurity Compliance & Risk Management Training Course is designed to provide professionals with the expertise required to navigate the complexities of the NIS 2 Directive, ensuring compliance and strengthening cyber resilience.

This course offers a comprehensive understanding of cybersecurity compliance, IT risk management, critical infrastructure security, and network security under the EU cybersecurity law framework. Participants will gain hands-on experience in cyber threat protection, incident response training, and risk assessment methodologies while learning how to implement NIS 2 Directive requirements effectively.

With interactive sessions, real-world case studies, and practical exercises, attendees will develop a strong foundation in cybersecurity best practices for businesses and how to mitigate risks in sectors such as energy, transport, healthcare, banking, and digital services. Upon successful completion, participants will be prepared for the NIS 2 certification and acquire the skills necessary to lead organizations in cybersecurity governance and regulatory compliance.

Target Audience

- Cybersecurity professionals
- IT managers and network security specialists
- CISOs and IT security officers
- Compliance officers and legal advisors
- Risk management professionals
- Government and regulatory officials
- Business continuity and incident response teams
- Organizations subject to the NIS 2 Directive

Targeted Organizational Departments

- IT & Cybersecurity
- Risk Management
- Compliance & Legal
- Operations & Business Continuity
- Supply Chain & Vendor Management

AGILE LEADERS
Training Center

Targeted Industries

- Energy & Utilities
- Transportation & Logistics
- Banking & Financial Services
- Healthcare & Pharmaceuticals
- Digital Services & Telecommunications
- Public Sector & Government Agencies
- Cloud and IT Service Providers
- Supply Chain & Manufacturing

Course Offerings

By the end of this course, participants will be able to:

- Understand and interpret the NIS 2 Directive requirements for cybersecurity compliance
- Develop and implement cybersecurity risk management frameworks
- Enhance cybersecurity governance and best practices for critical infrastructure
- Identify cybersecurity threats and implement proactive mitigation strategies
- Manage incident response and crisis management programs effectively
- Comply with EU regulations, cybersecurity directives, and reporting requirements
- Lead cybersecurity teams in implementing the NIS 2 Directive across an organization

Training Methodology

This training course utilizes a practical and interactive approach, combining:

- Instructor-led discussions on NIS 2 compliance and cybersecurity strategies
- Case studies and real-world scenarios from critical infrastructure industries
- Role-based simulations for incident response and crisis management
- Hands-on cybersecurity strategy development and policy implementation
- Interactive Q&A sessions and best practice sharing

Course Toolbox

- Cybersecurity best practice guides for compliance and risk management
- Incident response checklists and risk assessment templates
- Case studies and examples from regulated industries
- Reference materials on EU regulatory frameworks and cybersecurity laws

AGILE LEADERS
Training Center

Course Agenda

Day 1: Introduction to NIS 2 Directive and Cybersecurity Compliance

- **Topic 1:** Overview of NIS 2 Directive: Scope, Objectives, and Impact
- **Topic 2:** Understanding EU Cybersecurity Law and Regulatory Requirements
- **Topic 3:** Key Cybersecurity Governance Roles and Responsibilities
- **Topic 4:** Cybersecurity Risk Management: Identifying Threats and Vulnerabilities
- **Topic 5:** Initiation of NIS 2 Compliance Program and Organizational Context
- **Topic 6:** Standards and Regulatory Frameworks for Critical Infrastructure Security
- **Reflection & Review:** Key Compliance Challenges and Strategic Considerations

Day 2: Risk Management, Asset Management, and Compliance Frameworks

- **Topic 1:** Implementing a Cybersecurity Risk Management Framework
- **Topic 2:** Asset Management: Identifying and Protecting Critical Digital Assets
- **Topic 3:** NIS 2 Directive Risk Assessment and Mitigation Strategies
- **Topic 4:** Supply Chain Security and Compliance Obligations under NIS 2
- **Topic 5:** Implementing Cybersecurity Best Practices for Business Resilience
- **Topic 6:** Incident Reporting Requirements and Regulatory Expectations
- **Reflection & Review:** Evaluating Cyber Risks and Implementing Effective Controls

Day 3: Cybersecurity Controls, Incident Response, and Crisis Management

- **Topic 1:** Cybersecurity Controls: Policies, Procedures, and Technical Safeguards
- **Topic 2:** Developing an Effective Incident Response Plan under NIS 2
- **Topic 3:** Crisis Management and Business Continuity Planning
- **Topic 4:** Cyber Threat Protection and Intelligence: Detecting and Responding to Attacks
- **Topic 5:** Network Security Strategies for Protecting IT and OT Systems
- **Topic 6:** Ensuring Compliance with NIS 2 Through Security Audits and Continuous Monitoring
- **Reflection & Review:** Strengthening Incident Response and Crisis Readiness

Day 4: Communication, Training, and Continuous Cybersecurity Improvement

- **Topic 1:** Cybersecurity Awareness and Training for Employees and Leadership
- **Topic 2:** Communicating Cybersecurity Risks to Stakeholders and Regulatory Bodies
- **Topic 3:** Cybersecurity Monitoring, Testing, and Performance Measurement
- **Topic 4:** Business Continuity and Resilience Planning for Cyber Threats
- **Topic 5:** Implementing a Culture of Cybersecurity Compliance and Continuous Improvement
- **Topic 6:** Legal and Ethical Considerations in Cybersecurity and Data Protection
- **Reflection & Review:** Lessons Learned and Key Takeaways from Cybersecurity Compliance

Day 5: NIS 2 Directive and Practical Implementation Strategies

- **Topic 1:** Reviewing Key Elements of NIS 2 Directive Implementation
- **Topic 2:** Preparing for the PECB Certified NIS 2 Directive Lead Implementer Exam
- **Topic 3:** Case Study Analysis: Real-World NIS 2 Compliance Challenges
- **Topic 4:** Developing a Cybersecurity Strategy Aligned with Business Objectives
- **Topic 5:** Evaluating Organizational Cybersecurity Maturity and Readiness
- **Topic 6:** Roadmap for Ongoing Compliance and Cybersecurity Governance
- **Reflection & Review:** Final Q&A, Best Practices, and Next Steps in Cybersecurity Leadership

FAQ

What specific qualifications or prerequisites are needed for participants before enrolling in the course?

There are no formal prerequisites; however, a background in IT security, compliance, risk management, or cybersecurity governance is beneficial.

How long is each day's session, and is there a total number of hours required for the entire course?

Each day's session lasts 4-5 hours, with the total course spanning one week 20-25 hours of instruction.

What are the key compliance challenges organizations face with the NIS 2 Directive?

Key challenges include understanding regulatory requirements, implementing cybersecurity controls, ensuring incident response readiness, and achieving compliance across complex IT infrastructures.

How This Course is Different from Other Cybersecurity Training Courses

This NIS 2 Directive training course stands out from traditional cybersecurity programs by focusing on compliance, regulatory obligations, and risk management strategies specific to the EU framework. Unlike generic cybersecurity training, this course provides:

AGILE LEADERS
Training Center

- A targeted approach to NIS 2 compliance and governance
- Practical implementation strategies for cybersecurity frameworks
- Industry-specific case studies and real-world applications
- A focus on risk management, business continuity, and regulatory reporting
- Preparation for the PECB Certified NIS 2 Directive Lead Implementer certification