TRECCERT

NIS2 Essentials
Training Course



TRECCERT NIS2 Essentials is an awareness-level course designed to provide participants with a solid understanding of the NIS2 Directive and its practical relevance in the workplace. The course explores the directive's strategic purpose, scope of application and key principles while also highlighting its evolution from the original NIS1 Directive. Participants will develop the competence to recognize and proactively respond to common cyber threats and vulnerabilities in their day-to-day activities. They will learn to identify security risks associated with third-party services and vendors, supporting the security of the broader supply chain.

TARGET AUDIENCE

The NIS2 Essentials training course is designed for individuals aiming to understand their role in cybersecurity under the NIS2 Directive.

This course is particularly suitable for:

- Compliance Officers, Risk Managers, or Policy Advisors addressing cybersecurity governance
- IT and security teams
- Legal and data protection officers
- Team leaders and managers

LEARNING OBJECTIVES

- Learn the purpose of NIS2 and its strategic objectives in strengthening cybersecurity across the EU.
- Describe the development timeline of the Network and Information Systems (NIS) Directives and their evolution.
- Recognize key principles of the NIS2 Directive.
- Identify the key sectors and types of organizations affected by the NIS2 Directive.

COURSE MATERIAL FACTSHEET

Training Slides
200

Quiz Questions
25

Exercises
1

COURSE OUTLINE

1. Introduction to NIS2 Directive

- Background and Objectives of NIS2
- Scope of NIS2
- Key Principles of NIS2

2. Organizational Obligations Under NIS2

- Risk Management Requirements
- Governance and Management Responsibilities
- Supply Chain and Third-Party Risk Management

3. Incident Reporting and Response

- What constitutes an Incident
- Reporting Obligations and Timelines
- Internal Escalation Procedures

4. Security Requirements and the Role of Employees

- Human Factors in Cybersecurity
- Employee Good Practices
- Recognizing and Reporting Suspicious Activity

5. Compliance Support and Continuous Improvement

- How Your Organization Ensures Compliance
- Whistleblower Rights and Reporting Concerns
- Employee Involvement in Long-Term Security Culture

EXAMINATION DETAILS



Nr. of questions
20



Type of exam
Multiple choice



Duration
60 minutes



Location
Online

COURSE DETAILS



Duration
One (1) day



Language
English



CPE Credits
8



Training mode
Classroom and online

PATH TO RECOGNITION

info@treccert.com | www.treccert.com

TRECCERT