ISO 27033 Lead Network Security Manager

Lead Management
Online instructor-led
Self-study
Modality

English
Language

5 days
Duration

Master the implementation and management of network security with the ISO/IEC 27033 Lead Network Security Manager course. In just 5 days, you'll gain the knowledge and skills to design, implement, and maintain secure network infrastructures aligned with the ISO/IEC 27033 series of standards.

This course covers everything from network security concepts and architecture to secure communications using gateways, VPNs, and wireless access — as well as incident management, monitoring, and continual improvement. After passing the exam, you can apply for the PECB Certified ISO/IEC 27033 Lead Network Security Manager credential — a recognised validation of your competence in enterprise-level network security.

Learning Objectives

By the end of the course, you will be able to:

⊘ Gain a comprehensive understanding of the concepts, approaches, methods, and techniques of implementing and managing network security

- Acknowledge the correlation between the ISO/IEC 27033 series and other standards and regulatory frameworks

- Interpret ISO/IEC 27033 guidelines in the context of an organisation

- Plan, implement, manage, monitor, and maintain network security

- Advise organisations on best practices for securing communication infrastructures

Who Should Attend?

- Network security and information security professionals seeking to manage network security

- Managers or consultants aiming to master network security best practices

- Individuals involved in the architectural design and implementation of secure network infrastructures

- Technical experts and network security advisors

What's Included?

- 450+ pages of course material with examples, case studies, and practical exercises

- Certification and exam fees included

- Course completion attestation, granting 31 CPD credits.

Course Agenda

Day 1 | Introduction to ISO/IEC 27033 series of standards and initiation of network security implementation.

Day 2 | Network security team, policy, risk management, and documentation management.

Day 3 Internet access services, network segmentation, securing network communications using security gateways, VPNs, and wireless IP network access.

**Day 4** Network security testing, incident management, monitoring, and continual improvement.

Day 5 Certification Exam

Certification & Exam

🎓 Certification Prerequisites

After successfully completing the exam, you can apply for one of the credentials shown on the table below. You will receive a certificate once you meet the requirements related to the selected credential.

	ISO/IEC 27033 Provisional Network Security Manager	ISO/IEC 27033 Network Security Manager	ISO/IEC 27033 Lead Network Security Manager	ISO/IEC 27033 Senior Lead Network Security Manager	Other requirements
General Work Experience	None	2 Years	5 Years	10 years	
Network security Work experience	None	1 year	2 Years	7 years	Signing the PECB Code of Ethics
Hours of NSMS project experience	None	200 hours	300 hours	1000 hours	

📄 **Exam:** 3 hours, taken on Day 5

It covers the following competency domains:

Domain 1 Fundamental principles and concepts of network security.

Domain 2 Network security planning.

Domain 3 Network security policy and documentation management.

Domain 4 Securing network communications based on ISO/IEC 27033 series of standards and best practices.

Domain 5 | Network security competence, training, awareness, and team.

Domain 6 | Network security incident management and business continuity.

Domain 7 | Network security testing, monitoring, and continual improvement

✓ **Retake:** Free retake within 12 months if needed

📄 **Maintenance Fee:** First year included; fees applies from second year. Pay $120/year or save 10% by paying three years upfront.