# Certified ISO/IEC 27033 Network Security Training Course : Secure IT Networks Effectively

24 – 28 January 2027
Tashkent

AGILE LEADERS
Training Center

AGILE LEADERS
Training Center

# Certified ISO/IEC 27033 Network Security Training Course : Secure IT Networks Effectively

**Ref:** 103600302_99191 **Date:** 24 – 28 January 2027 **Location:** Tashkent **Fees:** 8000 Euro

## Course Overview:

The Certified ISO/IEC 27033 Network Security Training Course: Secure IT Networks Effectively is specifically designed to equip IT professionals with advanced expertise in Network security, Cybersecurity training, and practical implementation of Network security standards. This course addresses key topics including VPN security, Wireless network security, Security gateways, and advanced strategies for Cyber threat protection. Participants will master techniques such as Network risk management, Network security risk assessment strategies, and advanced security measures for enterprise networks.

Emphasizing the implementation of ISO/IEC 27033 for cybersecurity, this training course guides learners through step-by-step network security implementation, teaching best practices for network security compliance, preventing unauthorized access, and secure wireless communication for businesses. Participants will also explore strategies for Firewall security, managing security controls, and enhancing cybersecurity resilience. This comprehensive course ensures that participants can effectively apply guidelines for designing secure network architecture and protecting business networks from cyber threats.

## Target Audience:

- Network Security Managers
- IT Security Professionals
- Cybersecurity Analysts
- Network Administrators
- IT Compliance Officers
- Information Security Officers

## Targeted Organizational Departments:

- IT Security and Cybersecurity Departments
- Network Operations
- IT Infrastructure Management
- Compliance and Risk Management
- Business Continuity and Disaster Recovery

## Targeted Industries:

- Information Technology and Services
- Banking and Finance
- Healthcare and Pharmaceuticals
- Telecommunications
- Government and Public Administration
- Manufacturing and Industrial Automation

## Course Offerings:

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

- Implement ISO/IEC 27033 network security certification standards
- Conduct effective network security risk assessment strategies
- Protect business networks from cyber threats using advanced security measures
- Utilize network encryption techniques for data protection
- Develop and manage secure VPN and wireless network security solutions
- Establish strong firewall security strategies
- Apply technical security controls for enterprise networks
- Strengthen network security governance in organizational IT environments

## Training Methodology:

This training course employs diverse methodologies, including interactive lectures, hands-on exercises, group discussions, and practical case studies. Participants will engage in interactive sessions designed around real-world network security scenarios to apply Network risk management techniques effectively. Case studies on cyber threat protection and data breaches highlight the importance of proactive cybersecurity resilience and compliance. Group activities and workshops allow participants to collaboratively explore secure wireless communication for businesses and firewall security strategies, reinforcing learning through practical exercises. Regular feedback sessions ensure personalized learning experiences, focusing on step-by-step network security implementation and advanced security measures for enterprise networks. This interactive training approach fosters the ability to apply ISO/IEC 27033 effectively, ensuring participants are well-equipped to manage cybersecurity threats and compliance challenges in their organizations.

## Course Toolbox:

- Comprehensive digital course materials and workbooks
- Network security checklists and templates
- Guidelines for Network security compliance
- Online resources for cybersecurity resilience
- Examples and insights into ISO/IEC 27033 network security certification

## Course Agenda:

### Day 1: Introduction to Network Security and ISO/IEC 27033

- Topic 1: Overview of Network security standards and ISO/IEC 27033 compliance
- Topic 2: Importance of network security in IT infrastructure
- Topic 3: Guidelines for designing secure network architecture
- Topic 4: Network risk management fundamentals
- Topic 5: Preventing unauthorized access to networks
- Reflection & Review: Key takeaways in network security and risk management

## Day 2: Implementing Effective Network Security Controls

- Topic 1: Technical security controls for enterprise networks
- Topic 2: Best practices for network security compliance
- Topic 3: Managing security controls in network environments
- Topic 4: Security gateways and firewall security strategies
- Topic 5: Step-by-step network security implementation
- Reflection & Review: Effective strategies for secure IT environments

## Day 3: Advanced Network Security Techniques

- Topic 1: Network encryption techniques for data security
- Topic 2: Cyber threat protection and detection strategies
- Topic 3: Secure digital communication using ISO/IEC 27033
- Topic 4: VPN security and secure remote access networks
- Topic 5: Protecting personal data through secure networks
- Reflection & Review: Insights into advanced network protection methods

## Day 4: Wireless Network Security and Cloud Security

- Topic 1: Wireless network security for business environments
- Topic 2: Cloud network security measures for businesses
- Topic 3: Enhancing cybersecurity resilience through network security
- Topic 4: Protecting remote access networks securely
- Topic 5: Business continuity and network security best practices
- Reflection & Review: Consolidation of network security best practices

## Day 5: Governance and Network Security Risk Management

- Topic 1: Network security governance for organizations
- Topic 2: Implementing cyber risk management for IT professionals
- Topic 3: IT compliance solutions for network security
- Topic 4: Preventing data breaches with strong network security
- Topic 5: Future trends and innovations in cybersecurity training
- Reflection & Review: Overall course reflection and implementation strategies

# FAQ:

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

Participants should have basic knowledge of network infrastructure, cybersecurity principles, and prior IT-related work experience.

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

Each day's session is generally structured to last around 4-5 hours, with breaks and interactive activities included. The total course duration spans five days, approximately 20-25 hours of instruction.

## Does implementing ISO/IEC 27033 standards guarantee total protection against cyber threats?

While ISO/IEC 27033 provides robust frameworks for securing networks, total protection depends on consistent application, ongoing assessment, and continuous updating of security practices.

# How This Course is Different from Other Certified ISO/IEC 27033 Courses:

The Certified ISO/IEC 27033 Network Security Training Course uniquely emphasizes practical, actionable implementation strategies tailored for secure IT networks. Unlike standard IT security certification courses, it combines theoretical knowledge of network security standards with hands-on experiences, ensuring participants gain a deep understanding of cybersecurity training methodologies. The course distinctively covers comprehensive scenarios such as VPN security, wireless network security, and advanced techniques for cyber threat protection, providing learners with real-world approaches to preventing unauthorized access and protecting sensitive data. Its extensive use of practical case studies, group interactions, and reflective reviews further differentiate it from typical certification offerings. Participants will explore detailed strategies for managing security controls, applying technical security controls for enterprise networks, and achieving network security compliance effectively, thus providing a clear competitive advantage over similar network security courses.