Certified ISO/IEC 27005:2022 Information Security Risk Manager Training Course

25 – 29 October 2027
Addis Ababa

AGILE LEADERS
Training Center

AGILE LEADERS
Training Center

Certified ISO/IEC 27005:2022 Information Security Risk Manager Training Course

Ref: 103600292_225120 **Date:** 25 – 29 October 2027 **Location:** Addis Ababa **Fees:** 6000 Euro

Course Overview

The Certified ISO/IEC 27005:2022 Information Security Risk Manager Training Course is a comprehensive and practical program designed to equip participants with the knowledge, skills, and tools necessary to master the iso/iec 27005 risk management framework. This iso/iec 27005 training course focuses on the essential elements of information security risk assessment training, including context establishment, risk identification, risk analysis, risk evaluation, risk treatment, and monitoring and review, as outlined in iso/iec 27005:2022.

Participants will gain a deep understanding of how iso/iec 27005 information security risk management integrates with iso/iec 27001 compliance and how to apply best practices for risk management using various methodologies such as OCTAVE, EBIOS, MEHARI, and harmonized TRA. The course also enhances participants' ability to prepare for the pecb iso/iec 27005 certification, providing both theoretical and hands-on learning experiences through case study training, risk reporting and documentation exercises, and risk communication and consultation training.

This iso/iec 27005 certification training is ideal for professionals aiming to advance their risk management career by acquiring globally recognized credentials and practical capabilities to protect organizational assets and ensure information security risk governance.

Target Audience

- Information security managers
- Risk managers and compliance officers
- IT and cybersecurity professionals
- Internal auditors and governance specialists
- Privacy officers
- Project managers and consultants involved in iso/iec 27005 risk assessment course
- Professionals preparing for iso/iec 27005 lead risk manager certification

Targeted Organizational Departments

- Information security and IT risk departments
- Risk management and compliance teams
- Internal audit and governance offices
- Privacy and data protection teams
- IT operations and incident response departments
- Business continuity and disaster recovery teams

AGILE LEADERS
Training Center

Targeted Industries

- Banking and financial services
- Healthcare and pharmaceuticals
- Government and public sector
- Telecommunications and technology
- Manufacturing and supply chain management
- Energy and utilities
- Consulting and professional services

Course Offerings

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

- Understand the core principles and processes of iso/iec 27005 information security risk management
- Establish and maintain an information security risk management program aligned with iso/iec 27005:2022
- Conduct risk identification, risk analysis, risk evaluation, and risk treatment based on iso/iec 27005 risk management framework
- Apply iso/iec 27005 risk governance training to align with iso/iec 27001 requirements
- Use risk communication and consultation training to inform stakeholders and leadership
- Develop and maintain an iso/iec 27005 risk register and effective risk reporting and documentation processes
- Incorporate best practices for information security risk management into organizational governance programs

Training Methodology

This iso/iec 27005 training course combines instructor-led lectures, case study training, and interactive group workshops. Participants apply iso/iec 27005 process model training directly to simulated risk scenarios, ensuring they gain practical experience alongside theoretical knowledge.

The course uses real-world examples, guided discussions, and hands-on exercises to teach risk identification, risk analysis, risk evaluation, and risk treatment training. Participants work in teams to conduct threat identification training, document risks, and develop risk treatment plans using iso/iec 27005 risk recording and reporting training techniques.

Interactive group work also emphasizes communication and consultation training, ensuring participants can effectively convey risk findings to executive leadership and external auditors. Feedback and peer reviews support collaborative learning, ensuring participants are well-prepared for the iso/iec 27005 lead risk manager exam preparation.

AGILE LEADERS
Training Center

Course Toolbox

- iso/iec 27005 training manual
- iso/iec 27005 risk assessment templates
- Sample iso/iec 27005 risk register
- Risk communication and consultation training templates
- Threat identification and risk prioritization checklists
- Case studies illustrating iso/iec 27005 risk management methodologies
- Tools for monitoring and review training
- Exam preparation guide for pecb iso/iec 27005 certification

Course Agenda

Day 1: Introduction to ISO/IEC 27005 and Risk Management

- Topic 1: Introduction to iso/iec 27005 training course objectives and structure
- Topic 2: Overview of iso/iec 27005 risk management framework and principles
- Topic 3: Establishing context and defining scope using iso/iec 27005 context establishment training
- Topic 4: Understanding risk identification and threat identification training
- Topic 5: Developing an initial risk register and aligning it with iso/iec 27005 for iso/iec 27001 compliance
- Reflection & Review: Discussing key concepts and lessons using iso/iec 27005 communication and consultation training

Day 2: Risk Assessment and Analysis Process

- Topic 1: Conducting risk analysis and assessing impact using iso/iec 27005 risk analysis training
- Topic 2: Applying quantitative risk assessment training techniques
- Topic 3: Developing risk evaluation criteria using iso/iec 27005 risk evaluation training
- Topic 4: Assessing and prioritizing risks using iso/iec 27005 risk prioritization training
- Topic 5: Documenting findings using iso/iec 27005 risk recording and reporting training
- Reflection & Review: Reviewing assessments and evaluations using case study training examples

Day 3: Risk Treatment and Governance Integration

- Topic 1: Selecting and applying iso/iec 27005 risk treatment training options
- Topic 2: Communicating treatment options using iso/iec 27005 communication and consultation training
- Topic 3: Linking risk governance training to iso/iec 27001 compliance frameworks
- Topic 4: Incorporating iso/iec 27005 privacy risk management training for data protection
- Topic 5: Establishing ongoing monitoring and review processes using iso/iec 27005 continual improvement framework
- Reflection & Review: Peer feedback on risk treatment strategies using iso/iec 27005 case study training

Day 4: Advanced Methodologies and Compliance Alignment

- Topic 1: Applying alternative methodologies such as OCTAVE, MEHARI, and EBIOS
- Topic 2: Exploring harmonized threat and risk assessment techniques
- Topic 3: Comparing iso/iec 27005 implementation training to other frameworks
- Topic 4: Applying iso/iec 27005 best practices to regulatory compliance initiatives
- Topic 5: Linking iso/iec 27005 risk governance training to internal audit processes
- Reflection & Review: Sharing lessons and feedback using iso/iec 27005 lead risk manager exam preparation exercises

Day 5: Final Review and Certification Exam

- Topic 1: Reviewing core concepts from iso/iec 27005 training course
- Topic 2: Conducting a mock iso/iec 27005 lead risk manager exam preparation
- Topic 3: Reviewing case study findings and preparing personal action plans
- Topic 4: Understanding the iso/iec 27005 risk manager certification process
- Topic 5: Certification exam
- Reflection & Review: Closing discussion and next steps for iso/iec 27005 lead risk manager career advancement

FAQ

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

There are no formal prerequisites for the certified iso/iec 27005:2022 information security risk manager training course. However, participants with prior experience in information security, iso/iec 27001 compliance, or general risk management practices will benefit the most from the course. The iso/iec 27005 training course is suitable for both beginners seeking foundational knowledge and experienced professionals aiming to enhance their risk management capabilities through iso/iec 27005 certification training.

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 one week, approximately 20-25 hours of instruction.

What is the difference between iso/iec 27005:2022 and other risk management frameworks?

One key difference is that iso/iec 27005:2022 focuses specifically on information security risk management within the context of iso/iec 27001 compliance, while other frameworks such as OCTAVE, EBIOS, and MEHARI offer broader risk management approaches that are adaptable to various industries and organizational types. iso/iec 27005:2022 provides a process model that supports risk identification, risk analysis, risk evaluation, and risk treatment training, while emphasizing risk communication and consultation training, ensuring risks are clearly communicated to stakeholders.

How This Course is Different from Other Certified ISO/IEC 27005:2022 Information Security Risk Manager Training Course

The certified iso/iec 27005:2022 information security risk manager training course stands out from other risk management programs because it provides a deep focus on the iso/iec 27005 risk management framework specifically aligned with the requirements of iso/iec 27001. While many courses offer general risk management concepts, this iso/iec 27005 training course helps participants develop specialized expertise in information security risk assessment training that integrates seamlessly into information security management systems.

This course emphasizes practical application alongside theoretical knowledge. Through case study training, participants work on real-world scenarios to apply iso/iec 27005 risk analysis training, risk recording and reporting training, and risk treatment training. These hands-on workshops ensure participants gain practical experience in developing risk registers, documenting threat identification training results, and applying quantitative risk assessment training techniques.