# ISO/IEC 27005 Risk Manager («HSR»)

Master the Information Security Risk Management process based on ISO/IEC 27005 and other risk assessment methods.

**Duration:** 3 days
**Price:** 3'550.–

## Content

1. st Day: Introduction to ISO/IEC 27005 and implementation of a risk management programme
    - Course objectives and structure
    - Standard and regulatory framework
    - Concepts and definitions of risk
    - Risk management programme
    - Context establishment
2. nd Day: Information security risk assessment, risk treatment and acceptance as specified in ISO/IEC 27005
    - Risk identification
    - Risk analysis
    - Risk evaluation
    - Risk assessment with a quantitative method
    - Risk treatment
    - Information security risk acceptance
3. rd Day: Risk communication, consultation, monitoring, review and risk assessment methods
    - OCTAVE method
    - MEHARI method
    - EBIOS method
    - Harmonized Threat and Risk Assessment (TRA) method
    - Applying for certification and closing the training

## Key Learnings

- Acknowledging the correlation between Information Security risk management and security controls
- Understanding the concepts, approaches, methods and techniques that enable an effective risk management process according to ISO/IEC 27005
- Interpreting the requirements of ISO/IEC 27001 in Information Security Risk Management
- Acquiring the competence to effectively advise organizations in Information Security Risk Management best practices

## Methodology & didactics

- This training is based on both theory and best practices used in Information Security Risk Management
- Lecture sessions are illustrated with examples based on cases studies
- Practical exercises are based on a case study which includes role playing and discussions
- Practice tests are similar to the Certification Exam

## Target audience

Information Security risk managers, Information Security team members. Individuals responsible for Information Security, compliance, and risk within an organization or individuals implementing ISO/IEC 27001, seeking to comply with ISO/IEC 27001 or involved in a risk management program.

## Requirements

A fundamental understanding of ISO/IEC 27005 and comprehensive knowledge of Risk Assessment and Information Security.

- ISO/IEC 27001 Lead Auditor («HSI»)
- CISA – Certified Information Systems Auditor («CAM»)

## Certification

The exam covers the following competency domains:

- Domain 1: Fundamental principles and concepts of Information Security Risk Management
- Domain 2: Implementation of an Information Security Risk Management program
- Domain 3: Information Security risk management framework and process based on ISO/IEC 27005
- Domain 4: Other Information Security risk assessment methods

## Additional information

- Certification fees are included on the exam price
- Training material containing over 350 pages of information and practical examples will be distributed
- A participation certificate of 21 CPD (Continuing Professional Development) credits will be issued
- In case of exam failure, you can retake the exam within 12 months for free

## Further courses

- ISO/IEC 27001 Lead Implementer («HSL»)

## Any questions?

We are happy to advise you on +41 44 447 21 21 or info@digicomp.ch. You can find detailed information about dates on www.digicomp.ch/courses-security/information-security-data-protection/course-isoiec-27005-risk-manager