Course : ISO 27005:2022 Risk Manager, LSTI preparation and certification

Practical course - 3d - 21h00 - Ref. RMG
Price : 2690 CHF E.T.

★★★★☆ **4,2 / 5**

BEST

On completion of the course, students will be able to assess and manage information security risks, with a view to defining and implementing appropriate policies and procedures. They will also be in a position to obtain the certification "Risk Manager ISO 27005" linked to risk management within the framework of an ISMS.

Teaching objectives

At the end of the training, the participant will be able to:

- Know the requirements of ISO 27005 on information security risk management
- Managing a risk assessment as part of an ISMS
- Establish an ISO 27005-compliant risk management process
- Prepare for and pass ISO 27005 Risk Manager certification successfully

Intended audience

Project managers, consultants, technical architects, IS security managers, anyone in charge of information security, compliance and risk management within an organization.

Prerequisites

Be familiar with a best practice guide (ANSSI hygiene, ISO 27002 or equivalent), have completed the introductory cybersecurity course or have equivalent knowledge.

PARTICIPANTS

Project managers, consultants, technical architects, IS security managers, anyone in charge of information security, compliance and risk management within an organization.

PREREQUISITES

Be familiar with a best practice guide (ANSSI hygiene, ISO 27002 or equivalent), have completed the introductory cybersecurity course or have equivalent knowledge.

TRAINER QUALIFICATIONS

The experts leading the training are specialists in the covered subjects. They have been approved by our instructional teams for both their professional knowledge and their teaching ability, for each course they teach. They have at least five to ten years of experience in their field and hold (or have held) decision-making positions in companies.

ASSESSMENT TERMS

The trainer evaluates each participant's academic progress throughout the training using multiple choice, scenarios, hands-on work and more.
Participants also complete a placement test before and after the course to measure the skills they've developed.

Certification

L'examen de certification est dirigé en partenariat avec l'organisme de certification LSTI. Il se déroule pendant la dernière demi-journée. Ce diplôme international officiel ISO vous apportera la plus grande crédibilité dans la conduite de vos projets d'analyse de risques. Il est à noter qu'un travail personnel important est à prévoir pour se préparer au mieux à l'examen.

Remote certifications

See the certifier's official documentation for the list of prerequisites for completing the online certification exam.

Course schedule

1 Introduction

- ISO 27000 terminology, definitions of threat. Vulnerability. Risk...
- Availability, integrity and confidentiality requirements.
- Taking traceability/evidence into account.
- Reminder of regulatory and standards constraints (RGPD, LPM/NIS, PCI DSS...).
- The role of the CISO versus the Risk Manager.
- The 31000 standard, the value of the "umbrella" standard as a universal reference.

2 The "IS risk" concept

- Risk identification and classification.
- Origin of threats (accidental, deliberate, environmental).
- The consequences of risk (financial, legal, human, etc.).
- Risk management (reduction/reduction, risk avoidance, sharing).
- The special case of digital risk in "persistence" (APT).
- How to act on the risk (before, during and after the incident).

3 ISO risk management

- The 27001:2022 method and its risk governance process.
- The initial assessment in the planning phase of section 6 - Planning.
- The major evolution of standard 27005:2022: Information Security Risk Management.
- Implementing a PDCA risk management process.
- Risk context, assessment, treatment, acceptance and review.
- Steps in risk assessment (identification, analysis and evaluation).
- Drawing up a treatment plan based on ISO 27002 measures.
- The process of selecting measures based on attributes (preventive, detective or corrective).
- Selection of safety measures for the declaration of applicability (SoA).

4 The ISO 27005:2022 standard

- Introduction to the new ISO 27005:2022 standard, the influence of EBIOS RM.
- Linking risk management processes to ISMS processes.
- Targeted cyber risk analysis, how to analyze APTs.
- The cyber kill chain, new sources of risk and their objectives.
- Example of a likelihood/consequence scale.
- The event-based versus asset-based approach to risk management.
- Description of strategic and operational scenarios.
- Taking risk into account through the ecosystem.

(5) Preparation and final review

- Role-playing, MCQ-type knowledge tests, case studies.
- Asset inventory, threat and vulnerability assessment.
- Development of risk management plans, etc.
- Mock exam and interactive answer key.
- Tips to avoid the pitfalls.

(6) Taking the exam

- On the first day of training, we'll explain the content and rules of the online exam.
- Technical requirements for the online exam (webcam enabled, Internet connection).
- Administrator privilege to install anti-cheat software, etc.
- This exam takes place on the TESTWE online testing platform (testwe.eu).
- If the exam is taken on Orsys premises, Orsys will take care of preparing the candidate's workstation.
- When you take the exam at Orsys, you will also receive a paper copy of the standards described during the training course.
- To take this distance-learning exam, candidates must acquire all the standards themselves, in paper format.

Dates and locations

REMOTE CLASS
2026 : 9 Mar., 13 Apr., 27 May, 24 June, 9 Sep.,
14 Oct., 2 Dec., 16 Dec.