ISO 27001 Lead Auditor / Information security

★★★★★

SII-422 **5 Days (35 Hours)**

Description

The "ISO/IEC 27001 Lead Auditor" training will allow you to develop the expertise required to conduct an information security management system (ISMS) audit using principles, procedures and techniques widely recognized in audit.

Through this training, you will be able to plan and carry out internal and external audits in accordance with the ISO 19011 and ISO/IEC 17021-1 certification processes, while acquiring the necessary knowledge and skills.

Who is this training for ?

For whom

- Managers or consultants involved in information security management.
- Specialized advisors wishing to master the implementation of an information security management system.
- Any person responsible for maintaining compliance with ISMS requirements. Members of an SMSI team.

Prerequisites

Good knowledge of the ISO/IEC 27001 standard and in-depth knowledge of implementation principles.

Training objectives

- Understanding the relationship between ISO/IEC 27001, ISO/IEC 27002, and other standards and regulatory frameworks
- Mastery of the concepts, approaches, methods and the techniques necessary to set up and effectively manage an ISMS
- Interpret the requirements of the ISO/IEC 27001 standard in a context specific to the organization
- Support the organization in planning , implementation, management, monitoring and updating of the ISMS
- Acquire the expertise necessary to advise an organization on the implementation of best practices in terms of IT management system

- information security

Training program

Jour 1: introduction au système de management de la sécurité de l'information (SMSI) et la norme ISO/IEC 27001

- Leverage training to acquire new knowledge and skills about information security and the information security management system (ISMS).
- Get familiar with the standards and regulatory frameworks relevant to the field of information security by completing the training.
- Understand the information security certification process through the training.
- Learn the fundamental concepts and principles of information security by following the training.
- Acquire knowledge on the implementation and management of an information security management system information (ISMS) through training.

Jour 2 : Les fondements, la planification et l'initiation de l'audit

- The fundamental concepts and principles of auditing are the foundations of the audit process, including integrity, objectivity, competence, confidentiality, planning and supervision.
- The impact of trends and technology in auditing is growing, with the use of AI, blockchain and other tools improving audit efficiency and quality.
- Evidence-based auditing involves collecting tangible, verifiable evidence to assess compliance with internal standards and procedures, as well as to identify non-conformities and opportunities for improvement.
- Risk-based auditing involves assessing the risks associated with the company's activities and planning the audit accordingly, in order to cover the highest risk areas.
- Initiating the audit process involves notifying relevant stakeholders of the audit, planning the audit activities and collecting the necessary information.
- Audit Step 1 involves defining the audit objectives, selecting the audit team and identifying the areas to be audited. This is an important step to ensure the success of the audit.

Jour 3 : Les activités d’audit sur site

- Preparing for the second stage of the audit involves planning the activities and gathering the information necessary to successfully complete this stage.
- Stage 2 of the audit is the phase during which the collected information is evaluated and verified to confirm compliance with internal standards and procedures.
- Communication during the audit is an important step to ensure transparency and collaboration between parties stakeholders involved in the audit.
- Audit procedures are detailed instructions that guide the auditor through the audit process.
- Creating test plans audit is a key step to ensure that all risk areas are covered during the audit and that the results are reliable.

Jour 4 : Clôture de l’audit

- Audit findings and non-compliance reports are drawn up at the end of the audit.
- The audit documentation is examined as well as the quality review.
- Audit closure is the final stage of the audit process during which results are presented and possible corrective actions are identified.
- The evaluator verifies the the effectiveness of the action plans put in place following the audit.
- After the initial audit, corrective measures are put in place to improve the processes.
- Management An internal audit program is necessary to ensure compliance with standards and regulations.
- The training close marks the end of the training session.

Jour 5 : Révision pour préparer les candidats à passer l'examen de certification

- Review of concepts for certification and mock exam
- A voucher allowing you to take the certification test is sent at the end of the session