LEAD AUDITOR TRAINING (IRCA CERTIFIED)
DURATION: 5 DAYS

COURSE OVERVIEW

This five-day intensive course enables participants to develop the expertise needed to audit an Information Security Management System (ISMS) and to manage a team of auditors by applying widely recognized audit principles, procedures and techniques.

During this training, the participant will acquire the skills and knowledge needed to proficiently plan and perform audits compliant with the certification process of the ISO/IEC 27001:2013 standard. Based on practical exercises, the participant will develop the abilities (mastering audit techniques) and skills (managing audit teams and audit program, communicating with customers, conflict resolution, etc.) necessary to the efficient conducting of an audit.

TARGET AUDIENCE

1. Auditor wanting to perform and lead an Information Security Management System (ISMS) audit

2. Project manager or consultant wanting to master the Information Security Management System audit process

3. Person responsible for the Information security or conformity in an organization

4. Member of the information security team

5. Expert advisor in information technology

6. Technical expert wanting to prepare for an Information security audit function

COURSE OBJECTIVES

Includes a real life case study and assignments to:

1. Provide applicable situations and cases

2. Present a real world connect using situations that can happen in the day to day life of participants

3. Perform an audit of an ISMS with a team

COURSE CONTENT

Day 1: Introduction to Information Security Management System (ISMS) concepts as required by

1. ISO 27001
2. Normative, regulatory and legal framework related to information security
3. Fundamental principles of information security
4. ISO 27001 certification process
5. Information Security Management System (ISMS)
6. Detailed presentation of the clauses 4 to 8 of ISO27001

Day 2: Planning and Initiating an ISO 27001 audit

1. Fundamental audit concepts and principles
2. Audit approach based on evidence and on risk
3. Preparation of an ISO 27001 certification audit
4. ISMS documentation audit
5. Conducting an opening meeting

Day 3: Conducting an ISO 27001 audit

1. Communication during the audit
2. Audit procedures: observation, document review, interview, sampling techniques, technical verification, corroboration and evaluation
3. Audit test plans
4. Formulation of audit findings
5. Documentation non conformities

Day 4: Concluding and ensuring the follow-up of an ISO 27001 audit

1. Audit documentation
2. Quality review
3. Conducting a closing meeting and conclusion of an ISO 27001 audit
4. Evaluation of corrective action plans
5. ISO 27001 Surveillance audit
6. Internal audit management program

COURSE PREREQUISITES

ISO 27001 Foundation Certification or basic knowledge of ISO 27001 is recommended

Participants are required to purchase a copy of the ISO/IEC 27001:2013 Standard from www.iso.org

Upon passing the Lead Auditor Exam, the candidate can get registered with PECB to become:

1. A Provisional Auditor – Required: No experience required
2. An Auditor – Required: 2 years of professional experience, 1 year of information security experience, audit activities totaling 200 hours
3. A Lead Auditor - Required: 5 years of professional experience, 2 years of information security experience, audit activities totaling 300 hours