ISO/IEC 27001:2013
INFORMATION SECURITY MANAGEMENT SYSTEM
LEAD AUDITOR TRAINING COURSE

TIME (DAY)	5
TRAINING OPTIONS	General Participation & In-House & Online
LANGUAGE	Turkish, English
COURSE CODE/ACCREDITATION	A019677 / CPD

COURSE AIM

The purpose of the training is to provide the participants with information about the establishment, implementation, maintenance and audit of the ISO / IEC 27001: 2013 Information Security Management System.

This CPD certified ISO 27001:2013 Information Security Management Systems Lead Auditor Course provides basic training for potential ISMS Lead Auditors with the knowledge and skills to prepare, conduct, report and follow up 1st, 2nd and 3rd party ISMS audits.

WHO SHOULD ATTEND

- Those who want to manage Information Security Management System (ISMS) audits (2nd party or 3rd party) according to ISO / IEC 27001: 2013,
- Those who want to have information about effective examination practices,
- Current information security auditors who want to expand their audit skills,
- Those who want to provide consultancy on ISO / IEC 27001: 2013 ISMS Audits,
- Information security and quality management process owners.

COURSE CONTENT

- Terms and terminology used in information security management and audits
- Information security management importance, purpose and objectives, scope
- Information security - the relationship between management and processes
- Information assets and protection
- Business continuity
- Communication on information security
- Confidentiality, integrity and accessibility
- Security threats
- Controls to be applied according to risk analysis and results
- ISO / IEC 27001: 2013 requirements
- Interpreting the previous study,
- The role of an auditor in the context of ISO 19011,
- Examination types,
- Laws and other requirements,
- Accreditation and certification,
- Benefits of accreditation,
- Those who have a role in audits and their responsibilities
- Auditor characteristics,
- Examination process,
- Audit scope and audit objectives,
- Selection of auditors and creating an audit team,
- Stage 1 and 2 examinations,
- Audit planning,
- Preparing a list of questions,
- Opening and Closing meeting,
- Conducting an audit interview,
- Determining nonconformity,
- Examination review,
- Recording and reporting nonconformity,
- Audit reporting,
- Follow-up audits and corrective actions
- rehabilitation
- Exam information and course review
- Exam

IMPORTANT NOTES

NOTE 1: Participants should know about Information Security Management or ISO/IEC 27001 before attending this training.
NOTE 2: In order to get a certificate of achievement in this training, the exam passing grade is 70 points, and the Attendance Certificate will be given to those who cannot get a valid grade. You have the right to repeat the lead auditor exam 1 time free of charge within 12 months.
NOTE 3: In order to take the exam, attendance at least 70% is required.
NOTE 4: In order to be an auditor/lead auditor in any certification body, CFECERT does not have any commitments about CANDIDATE INSPECTION and INTERNSHIP, which should be done after training. This training is a prerequisite for being an auditor/lead auditor, and the appointment process must be completed by the certification body you will be assigned to. The conditions required to become an auditor/lead auditor after training are as follows;

- Vocational education or training at a level equivalent to university education,
- Must have at least four years of full-time work experience in information technologies, with at least two years in a role or position related to information security,
- Must have successfully completed at least five days of training, the scope of which can be evaluated in accordance with the ISMS audits and audit management,
- He/she should have gained experience in the entire information security assessment process before taking responsibility to act as an auditor. It is essential that this experience has been provided by participation in at least four certification audits of at least 20 days in total, including the review of documentation and risk assessment, application assessment and audit reporting. Includes re-certification audit and surveillance audit. A maximum of 5 days of 20 days is performed as a surveillance examination.

NOTE 5: Also for Lead Auditors;
Participating in at least three full ISMS audits as an auditor. Participation should include initial scope and planning, document review and risk assessment, implementation assessment, and formal audit reporting.