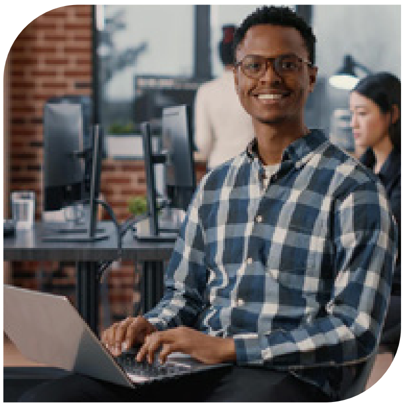
INFOSECTRAIN



ISO 27001:2022 LEAD AUDITOR

TRAINING & CERTIFICATION

ABOUT ISO 27001:2022 Lead Auditor

Any management system's success depends on effective auditing. As a result, it involves a great deal of responsibility and challenges. InfosecTrain's ISO 27001:2022 Lead Auditor training and certification course is a five-day intensive course to inculcate in participants the knowledge to perform an Information Security Management System (ISMS) audit by employing recommended audit fundamentals, principals, procedures, and methodologies.

ISO 27001:2022 LEAD AUDITOR TRAINING INCLUDES

- 40 hrs of instructor-led training
- Authorized Training Partner
- Practical approach for ISO 27001 Audit
- Mock Test and exam guidance session
- Certified & Experienced Trainers

Who Attend?

- Internal Auditors
- Auditors wanting to perform and lead ISMS certification audits
- Project Managers or Consultants wanting to master the ISMS audit process
- CxO and Senior Managers responsible for the IT governance of an enterprise and the management of its risks
- Members of an information security team
- Expert advisors in information technology
- Expert advisors in information security
- Technical experts wanting to prepare for an information security audit function

Pre-Requisites

- Certified ISO/IEC 27001 Foundation Certification or basic knowledge of ISO/IEC 27001 is recommended.

Exam Information

- We provide Exams with PECB, & IGC; for more detail, connect with our experts.

MEET OUR INSTRUCTOR

INSTRUCTOR

RAJESH SANDHEER

CISA | ISO 27001 LA | GDPR CDPO | CDCS | CDCP

INSTRUCTOR

CHANDER S

ISO 27001 | ISO 22301 | ISO 27701 | ISO 9001 | ISO | GDPR | ISACA | LEAN 6-Sigma

What our
Client Says About Us?

SENG SEYHA

I experienced such an amazing and interacted training session. Thanks to the respective trainer who shared us the details knowledge of the standard as well as his practical experiences. I have gain a great amount of knowledge and it has sharpen my perspective as an auditor. I can't wait to make use of it in my career and provide a better audit quality to my organization.

CHRISY ANNIE PUNNEN

Thank you for organizing an amazing training session.Trainer clearly explained the concepts. It was very interactive session with team and lot of group activities.

JUNO DAVID ANTONY

The training was very informative and a good learning experience. Learned and enjoyed it a lot.

Course Content

Introduction to the Information Security Management System (ISMS) and ISO/IEC 27001

Section 1: Training course objectives and structure

> General information
> Learning objectives
> Educational approach
> Examination and certification

Section 2: Standards and regulatory frameworks

> What is ISO?
> The ISO/IEC 27000 family of standards
> Advantages of ISO/IEC 27001

Section 3: Certification process

> Certification process
> Certification scheme
> Accreditation bodies
> Certification bodies

Section 4: Fundamental concepts and principles of information security

> Information and asset

> Information security

> Confidentiality, integrity, and availability

> Vulnerability, threat, and impact

> Information security risk

> Security controls and control objectives

> Classification of security controls

Section 5: Information security management system (ISMS)

> Definition of a management system

> Definition of ISMS

> Process approach

> ISMS implementation

> Overview - Clauses 4 to 10

> Overview - Annex A

> Statement of Applicability

Audit principles, preparation, and initiation of an audit

Section 6: Fundamental audit concepts and principles

> Audit standards

> What is an audit?

> Types of audits

> Involved parties

- > Involved parties
- > Audit objectives and criteria
- > Combined audit
- > Principles of auditing
- > Competence and evaluation of auditors

Section 7: The impact of trends and technology in auditing

- > Big data
- > The three V's of big data
- > The use of big data in audits
- > Artificial intelligence
- > Machine learning
- > Cloud computing
- > Auditing outsourced operations

Section 8: Evidence-based auditing

- > Audit evidence
- > Types of audit evidence
- > Quality and reliability of audit evidence

Section 9: Risk-based auditing

- > Audit approach based on risk
- > Materiality and audit planning
- > Reasonable assurance

Section 10: Initiation of the audit process

> The audit offer

> The audit team leader

> The audit team

> Audit feasibility

> Audit acceptance

> Establishing contact with the auditee

> The audit schedule

Section 11: Stage 1 audit

> Objectives of the stage 1 audit

> Pre on-site activities

> Preparing for on-site activities

> Conducting on-site activities

> Documenting the outputs of stage 1 audit

On-site audit activities

Section 12: Preparing for stage 2 audit

> Setting the audit objectives

> Planning the audit

> Assigning work to the audit team

> Preparing audit test plans

> Preparing documented information for the audit

Section 13: Stage 2 audit

> Conducting the opening meeting
> Collecting information
> Conducting audit tests
> Determining audit findings and nonconformity reports
> Performing a quality review

Section 14: Communication during the audit

> Behavior during on-site visits
> Communication during the audit
> Audit team meetings
> Guides and observers
> Conflict management
> Cultural aspects
> Communication with the top management

Section 15: Audit procedures

> Overview of the audit process
> Evidence collection and analysis procedures
> Interview
> Documented information review
> Observation
> Analysis
> Sampling
> Technical verification

Section 16: Creating audit test plans

Audit test plans

Examples of audit test plans

Guidance for auditing an ISMS

Corroboration

Evaluation

Auditing virtual activities and locations

Closing of the audit

Section 17: Drafting audit findings and nonconformity reports

> Audit findings

> Types of possible audit findings

> Documenting the audit findings

> Drafting a nonconformity report

> The principle of the benefit of the doubt

Section 18: Audit documentation and quality review

> Work documents

> Quality review

Section 19: Closing of the audit

> Determining audit conclusions
> Discussing audit conclusions
> Closing meeting
> Preparing audit report
> Distributing the audit report
> Making the certification decision
> Closing the audit

Section 20: Evaluation of action plans by the auditor

> Submission of action plans by the auditee
> Content of action plans
> Evaluation of action plans

Section 21: Beyond the initial audit

> Audit follow-up activities
> Surveillance activities
> Recertification audit
> Use of trademarks

Section 22: Managing an internal audit program

> Managing an audit program
> Role of the internal audit function
> Main internal audit services and activities
> Audit program resources

> Audit program records
> Follow up on nonconformities
> Monitoring, evaluating, reviewing, and improving an audit program

The above-mentioned content is delivered in 32 hours. In addition to this, we have added 8 hours session.

8 Hours Dedicated Session

ISO 27001 Practical Approach

> ISO 27001 (new 93 controls) Controls to Evidence Mapping
> Practical approach on how to collect evidence while auditing with three scenarios/ case studies paragraphs

ISO 27001 Exam Prep

> Revision of course and open mic session for doubts
> Exam Prep – mock exam
> Discussion on exam questions and answers
> Discussion on different exams (IGC/PECB)

Benefits of ISO/IEC 27001

52% Characterize certifying to ISO/IEC 27001 as “an investment that is fully justified by the benefits

69% To enhance the information security posture

56% To get a competitive advantage

55% To assure legal and regulatory

History of
ISO/IEC 27001

01	SO/IEC 27001:2022	2022
02	ISO/IEC 27001:2013	2013
03	ISO/IEC 27001:2005	2015
04	ISO/IEC 17799 2000	2000
05	British Standards Institute BS7799 1995	1995
06	Code of practice for a Security Management 1992	1992

INFOSECTRAIN

www.infosectrain.com | sales@infosectrain.com