{Certible®}
international certification body

Certible® certified

ISO/IEC 27001 Lead Auditor

Syllabus

Version: v2024.15
Status: Released
Release Date: 2024-08-14
Confidentiality: Public

Table of Contents

i Legal Notices and Compliance

i.1 Disclaimer

The information contained in this document is provided ”as is” without warranty of any kind. Certible® disclaims all warranties, either express or implied, including the warranties of merchantability and fitness for a particular purpose. In no event shall Certible® be liable for any damages whatsoever including direct, indirect, incidental, consequential, loss of business profits, or special damages, even if Certible® has been advised of the possibility of such damages. The use of the information provided in this document is solely at the user’s risk. Certible® reserves the right to make changes to the content of this document at any time without notice.

i.2 Copyright

i.3 Use of ISO Standards

Certible®’s certification exams require a thorough understanding of the relevant ISO standards. It is crucial for candidates to ensure they are using the correct and legally obtained versions of these standards for exam preparation purposes, as well as exclusively in paper form for use during the multiple-choice examination.

It is the candidate’s responsibility to ensure that they have the correct version of the required ISO standards. Certible® does not provide copies of the ISO standards and will not be held liable for any issues arising from the use of unauthorized or incorrect versions.

i.4 Trademarks

Certible® the Certible® logo, and all other trademarks, certification marks, service marks, graphics, and logos used in connection with Certible®’s products and services are trademarks or registered trademarks of Certible®. Other trademarks, service marks, graphics, and logos used in this document may be the trademarks of their respective owners. The use of any third-party trademarks does not imply any affiliation, sponsorship, or endorsement between Certible® and the owners of these trademarks. All trademarks are the property of their respective owners and are used in this document for identification purposes only. Unauthorized use, duplication, or distribution of these trademarks is strictly prohibited and may result in civil and criminal penalties.

ii Contact Information

Europe:

Certible GmbH
Loewelstrasse 20/2-3
1010 Vienna
Austria

office@certible.com

North America:

Certible Inc.
800 West El Camino Real, Suite 180
Mountain View, 94040
USA

us@certible.com

iii Syllabus Guide and Overview

Welcome to the Certible® ISO/IEC 27001 Lead Auditor certification syllabus. This overview is designed to provide you with a comprehensive understanding of the course structure, learning objectives, and examination process. To help you navigate this syllabus effectively, please familiarize yourself with the following key components:

1. **Cognitive Levels**: Learn how we classify learning objectives based on the depth of knowledge and skills required.
2. $\{\lambda\}$ **Symbol**: Understand the significance of objectives marked with the lambda ($\{\lambda\}$) symbol and their role in your professional development.
3. **Syllabus Structure**: Gain an overview of the competency areas covered, recommended training duration, and examination format.

iii.1 Cognitive Levels and Learning Objectives

In this syllabus, learning objectives are categorized according to cognitive levels based on Bloom's Taxonomy, a framework for classifying educational goals. These cognitive levels help to define the depth of understanding and the complexity of skills that learners are expected to achieve for each objective.

The cognitive levels used in this syllabus range from C1 to C5, representing a progression from basic recall of information to more complex evaluation skills:

C1 - Remember
: Retrieve relevant knowledge from long-term memory. This involves recognizing or recalling key facts, terms, concepts, or answers without necessarily understanding what they mean.

C2 - Understand
: Construct meaning from instructional messages, including oral, written, and graphic communication. This involves interpreting, exemplifying, classifying, summarizing, inferring, comparing, or explaining.

C3 - Apply
: Carry out or use a procedure in a given situation. This involves executing or implementing knowledge to solve problems in new situations by applying acquired knowledge, facts, techniques, and rules.

C4 - Analyze
: Break material into constituent parts and determine how parts relate to one another and to an overall structure or purpose. This involves differentiating, organizing, and attributing.

C5 - Evaluate
: Make judgments based on criteria and standards. This involves checking and critiquing, leading to assessments or conclusions about the value of ideas, works, solutions, methods, or materials.

Each learning objective in this syllabus is associated with one of these cognitive levels. This classification serves several purposes:

1. It helps learners understand the depth of knowledge expected for each topic.
2. It guides instructors in designing appropriate teaching strategies and assessment methods.

3. It ensures a balanced curriculum that covers various levels of cognitive engagement.
4. It aids in the development of exam questions that accurately reflect the intended depth of learning.

As you progress through the syllabus, you'll notice that objectives move from lower cognitive levels (C1, C2) to higher ones (C3, C4, C5), reflecting the increasing complexity and depth of the material.

Understanding these cognitive levels will help you gauge the expectations for each learning objective and prepare accordingly.

iii.2 {λ} Symbol: Beyond the Exam - Enriching Your Knowledge

Throughout this syllabus, you will encounter learning objectives marked with the $\{\lambda\}$ (Lambda) symbol. These objectives represent topics that, while not directly tested in the exam, are crucial for a comprehensive understanding of the subject matter.

Why $\{\lambda\}$?

- In mathematics and computer science, λ often represents a function or an abstraction.
- Here, it symbolizes the application and extension of your knowledge beyond the basic requirements.

$\{\lambda\}$-marked objectives aim to:

- Broaden your perspective on the subject
- Connect theoretical concepts to real-world applications
- Enhance your professional competence beyond exam preparation

While these topics won't appear in your exam, we strongly encourage trainers to cover them and students to engage with them. They provide valuable insights, practical knowledge, and a deeper understanding of the field, ultimately making you a more well-rounded professional.

Remember: Learning extends beyond exam preparation. The $\{\lambda\}$ objectives are your gateway to advanced understanding and practical expertise.

iii.3 Syllabus Structure

This syllabus is structured around key competency areas essential for an ISO/IEC 27001 Lead Auditor. Here's a brief overview:

- **Competency Areas**: The syllabus covers 8 main competency areas, each focusing on critical aspects of information security management systems auditing.
    1. ISO 27000 Family and Relationship to other Standards
    2. ISMS as a Management System
    3. Accreditation, Certification and Legal Context
    4. Information Security Management 27001 Foundation

5. Audit Principles
6. Audit Methodologies and their Application
7. Process Perspective of an Audit
8. Auditor Competencies and Skills

- **Training Duration** The recommended total training duration for this course is 31 hours, typically delivered over 4 to 5 days. For each competency area and chapter, you will find an information box detailing:
  - Recommended training duration (in minutes)
  - Number of exam questions related to this section
  - Exam weight - percentage of all points allocated in the exam

  For the entire Certible® ISO/IEC 27001 Lead Auditor syllabus, the values are:

Recommended Training Duration	1890 minutes (31 hours 30 minutes)
Exam Questions	75
Exam Weight	100.00%

- **Learning Objectives**: Each competency area contains specific learning objectives, classified by cognitive levels (C1-C5) or $\{\lambda\}$ to indicate the depth of knowledge required. In each chapter, a info box indicates the number of recommended hours

This syllabus is designed to ensure you develop both the theoretical knowledge and practical skills necessary to excel as an ISO/IEC 27001 Lead Auditor. We encourage you to engage fully with all aspects of the course, including the $\{\lambda\}$-marked objectives, to maximize your learning experience and professional growth.

1 ISO 27000 Family and Relationship to other Standards

Recommended Training Duration	170 minutes (2 hours 50 minutes)
Exam Questions	7
Exam Weight	8.99%

This competency area focuses on the ISO 27000 family of standards and their relationship to other relevant security frameworks. Candidates will gain a comprehensive understanding of the structure, scope, and application of the ISO 27000 series, including key standards for Information Security Management Systems (ISMS) implementation and auditing. The area also covers other significant IT security standards and regulations, emphasizing the importance of integrated management systems. By mastering this competency, candidates will be equipped to navigate the complex landscape of information security standards, interpret their requirements effectively, and understand how they can be integrated within organizational processes. This knowledge is fundamental for Lead Auditors to assess ISMS implementations, conduct combined or joint audits, and provide guidance on aligning multiple management systems with ISO/IEC 27001 requirements.

1.1 Overview of ISO 27000 family of standards

Recommended Training Duration	75 minutes (1 hour 15 minutes)
Exam Questions	3
Exam Weight	3.97%

Understanding the ISO 27000 family of standards is crucial for ISO/IEC 27001 Lead Auditors, as it provides a comprehensive framework for information security management. This chapter equips learners with essential knowledge about the structure, scope, and interrelationships within the ISO 27000 series, enabling them to navigate and apply these standards effectively. Proficiency in the terminology, requirements, and specific roles of each standard allows auditors to confidently assess an organization's Information Security Management System (ISMS) against the relevant criteria. Furthermore, this foundational knowledge enhances the auditor's ability to interpret and apply sector-specific requirements, ensuring a thorough and accurate evaluation of an organization's information security practices. Ultimately, this chapter forms the basis for developing the expertise necessary to lead successful ISO/IEC 27001 audits and contribute to the continuous improvement of information security management systems across various industries.

Id	Learning Objectives	CL	Sources
1.1.1 1F80AD6B	Know the scope of the ISO 27000 family of standards.	C1	[4: 1]
1.1.2 435E6DDB	Know where to locate terms and definitions within the family of standards.	C1	

Table continued on next page

Id	Learning Objectives (cont.)	CL	Sources
1.1.3 260C74AD	Know which standard contains the requirements for an ISMS.	C1	[4: 5.1]
1.1.4 7CDC750C	Know which documents in the series are normative and which are informative.	C1	[1: 2] [3: 2] [4: 2] [7: 2] [6: 2] [5: 2]
1.1.1 CF2D1BFE	Know how the terms ”shall,” ”should,” ”may,” and ”can” are used in ISO standards.	C1	[6: 0.0]
1.1.2 11369B65	Know where to find sector-specific requirements within the ISO 27000 family.	C1	[4: 5.1]
1.1.7 152ABD25	Understand the objective and purpose of ISO/IEC 27006 and ISO/IEC 27007.	C2	[4: 5.3, 5.4]

1.2 Overview of other relevant standards

Recommended Training Duration	30 minutes
Exam Questions	1
Exam Weight	1.59%

Expanding beyond the confines of ISO/IEC 27001, this chapter broadens the perspective of Lead Auditors by highlighting other significant IT security standards and regulations. Understanding the landscape of related frameworks, such as the NIST Cybersecurity Framework, GDPR, and ISO/IEC 22301, enhances the auditor’s ability to contextualize ISO/IEC 27001 within the information security ecosystem. While not directly tested in the exam, this knowledge fosters a holistic approach to information security management and encourages continuous professional development. By exploring these complementary standards, Lead Auditors can better appreciate the interconnectedness of various security frameworks and their applicability in diverse organizational contexts, ultimately enriching their expertise and adaptability in the field of information security auditing.

Id	Learning Objectives	CL	Sources
1.2.1 13C86A53	Know other relevant IT security standards, including NIST Cybersecurity Framework (CSF), NIST Special Publication 800-53, General Data Protection Regulation (GDPR), NIS Directive on Security of Network and Information Systems, and ISO/IEC 22301 Business Continuity Management Systems.	$\{\lambda\}$	

1.3 Integrated Management System (IMS)

Recommended Training Duration	65 minutes (1 hour 5 minutes)
Exam Questions	3
Exam Weight	3.44%

This chapter focuses on the concept of Integrated Management Systems (IMS) and their relationship to ISO/IEC 27001 implementation. Candidates will explore the benefits of integrating multiple management systems, including simplified implementation and alignment with organizational processes. The chapter covers ISO's harmonized approach to standards and the requirement for integrating information security management systems within an organization's existing structure. Learners will distinguish between combined and joint audits, and study guidelines for integrating different management systems, such as ISO/IEC 20000-1 and ISO/IEC 27001.

Id	Learning Objectives	CL	Sources
1.3.1 EAAD7BF2	Understand the concept of an integrated management system and recognize that a management system can be implemented independently or as part of an integrated approach.	C2	[3: 3.2, 3.18] [2: 4.2]
1.3.2 7650808C	Know that ISO has aligned standards (harmonized approach) to simplify the implementation of multiple management systems.	C1	[7: 0.2]
1.3.3 B59587F4	Understand that integrating the information security management system with the organization's processes and management structure is a requirement of ISO/IEC 27001.	C2	[7: 0.1]
1.3.4 7B6AE21C	Explain the differences between a combined audit and a joint audit.	C2	[3: 3.2, 3.1, 3.13, 3.18, 3.3]
1.3.5 8B5D68F3	Know guidelines for integrated implementations of different management systems (e.g., ISO/IEC 20000-1 and ISO/IEC 27001).	C1	[4: 5.4]

2 ISMS as a Management System

Recommended Training Duration	210 minutes (3 hours 30 minutes)
Exam Questions	7
Exam Weight	11.11%

This competency area equips auditors with the knowledge to evaluate the effectiveness of an organization's ISMS implementation, including its scope, establishment process, and critical success factors. It covers the fundamental principles of auditing management systems, emphasizing the importance of establishing and maintaining a robust audit programme. By exploring the Plan-Do-Check-Act (PDCA) cycle, auditors gain insights into continuous improvement processes within an ISMS. Furthermore, this area prepares auditors to assess audit programme actions, ensuring they align with organizational objectives and effectively address potential risks and opportunities in information security management.

2.1 Information Security Management Systems (ISMS)

Recommended Training Duration	50 minutes
Exam Questions	2
Exam Weight	2.65%

This chapter provides a comprehensive overview of Information Security Management Systems (ISMS) and their role within organizational security frameworks. Candidates will learn the scope and definition of a security management system, along with the step-by-step process of establishing an ISMS. The chapter covers the identification of various information assets that can be protected using an ISMS, emphasizing the importance of the CIA triad (Confidentiality, Integrity, Availability) in information security. Furthermore, it explores the critical success factors for effectively implementing an ISMS, equipping candidates with the knowledge to evaluate and contribute to ISMS initiatives.

Id	Learning Objectives	CL	Sources
2.1.1 FA301C45	Understand the scope and definition of a security management system.	C1	[3: 3.18, 3.24] [4: 4.2]
2.1.2 8115ADFC	List the steps involved in establishing an ISMS.	C1	[4: 4.5]
2.1.1 FF4903DB	Identify the types of information assets that can be protected using an ISMS.	C1	[4: 0.1]

Table continued on next page

Id	Learning Objectives (cont.)	CL	Sources
2.1.1 D92005A7	Know the CIA triad (Confidentiality, Integrity, Availability).	C1	[4: 3.28, 3.10, 3.36, 3.7, 3.6, 3.48, 3.55] [6: 3.4]
2.1.5 3D6D3816	Recall the critical success factors for the successful implementation of an ISMS.	C1	[4: 4.6]

2.2 Auditing Management Systems

Recommended Training Duration	35 minutes
Exam Questions	1
Exam Weight	1.85%

This chapter focuses on auditing management systems, with a specific emphasis on understanding the application of ISO 19011 in relation to Information Security Management Systems (ISMS) audits. Candidates will learn about the scope of ISO 19011, including its relevance to different company sizes and audit team compositions. The chapter distinguishes between the non-normative nature of ISO 19011 and the normative status of ISO/IEC 27006. Additionally, it clarifies that ISO 19011 primarily addresses first-party and second-party audits, while ISO/IEC 17021-1 provides supplementary requirements for third-party audits.

Id	Learning Objectives	CL	Sources
2.2.1 154D2383	Understand the scope of ISO 19011 in relation to company size and audit team composition.	C2	
2.2.2 11B83095	Know that ISO 19011 has no normative reference, while ISO/IEC 27006 is normative.	C1	[3: 2] [6: 2]
2.2.3 9C0D4C13	Know that ISO 19011 primarily focuses on first-party and second-party audits, while additional requirements for third-party audits are found in ISO/IEC 17021-1 and ISO/IEC 27007.	C1	

2.3 Establish and Maintain an Audit Programme

Recommended Training Duration	35 minutes
Exam Questions	1
Exam Weight	1.85%

Understanding the structure and purpose of an ISMS audit programme is fundamental for ISO/IEC 27001 Lead Auditors, even though they may not have direct control over its establishment. This chapter equips auditors with essential knowledge about the components, objectives, and key roles involved in creating an effective audit programme. By grasping these elements, Lead Auditors can better contextualize their individual audit activities within the broader organizational framework. This understanding enables auditors to align their work with the overall goals of the Information Security Management System.

Id	Learning Objectives	CL	Sources
2.3.1 82F51CDF	Understand the purpose and objectives of an ISMS audit programme.	C2	[3: 5.1]
2.3.2 147C6FA8	Know the components of an audit programme.	C1	[3: 5.1]
2.3.3 8EF0F3C1	Know typical roles involved in establishing an audit programme.	C1	[3: 5.1]

2.4 PDCA Cycle

Recommended Training Duration	35 minutes
Exam Questions	1
Exam Weight	1.85%

The Plan-Do-Check-Act (PDCA) cycle serves as the central driving force behind every management system, making it an indispensable component of the ISO/IEC 27001 Lead Auditor certification syllabus. Understanding this cyclical approach is necessary for auditors to effectively evaluate and improve Information Security Management Systems (ISMS). In this chapter, Lead Auditors gain insight into the continuous improvement process and learn to distinguish between the responsibilities of audit programme owners and individual auditors. This knowledge enables them to accurately assess which actions contribute to each phase of the cycle, ensuring a comprehensive and systematic approach to ISMS auditing.

Id	Learning Objectives	CL	Sources
2.2.1 AAF17E59	Know the Plan-Do-Check-Act (PDCA) cycle.	C1	[3: 5.1]
2.4.2 16AA7F8D	Know which actions are performed by the audit programme owner and which are performed by an auditor.	C1	[3: 5.1]
2.2.1 1736E4D4	Understand to which PDCA phase different actions contribute.	C2	[3: 5.1]

2.5 Audit Programme Actions

Recommended Training Duration	55 minutes
Exam Questions	2
Exam Weight	2.91%

This chapter focuses on the critical aspects of audit programme actions within the context of an Information Security Management System (ISMS). Candidates will learn about typical audit programme objectives and how to identify associated risks and opportunities during program development. The chapter distinguishes between an audit programme and an individual audit, emphasizing the broader scope of the former. It also covers methods for monitoring and maintaining ISMS effectiveness, which is vital for ongoing security management. Additionally, the chapter explores the objectives, inputs, and results of management reviews, providing a comprehensive understanding of how these reviews contribute to the continuous improvement of the ISMS.

Id	Learning Objectives	CL	Sources
2.5.1 15ABD31C	Know what audit programme objectives typically include.	C1	[3: 5.1, 5.2] [7: 9.2]
2.5.2 631762A8	Know how to identify risks and opportunities when developing an audit programme.	C1	[3: 5.3]
2.5.3 826A90E9	Understand the difference between an audit programme and an individual audit.	C2	
2.5.4 1613DE6B	Know how to monitor and maintain ISMS effectiveness.	C1	[3: 5.6] [7: 9.1]
2.5.5 C7B2702E	Know the objectives, inputs, and results of a management review.	C1	[3: 5.7] [7: 9.3]

3 Accreditation, Certification and Legal Context

Recommended Training Duration	265 minutes (4 hours 25 minutes)
Exam Questions	10
Exam Weight	14.02%

This competency area is a cornerstone of the ISO/IEC 27001 Lead Auditor Syllabus, reflecting the critical need for Lead Auditors to possess a comprehensive understanding of the legal and regulatory landscape in which they operate. Unlike internal auditors, Lead Auditors must navigate complex relationships between accreditation bodies, certification bodies, and client organizations, necessitating a deep knowledge of the certification process and its legal implications. This competency area equips auditors with the skills to maintain impartiality and integrity throughout the audit process, ensuring compliance with relevant laws and regulations while upholding the highest standards of professional conduct. Lead Auditors can effectively manage the certification cycle, handle appeals and complaints, and recognize potential conflicts of interest, thereby safeguarding the credibility and value of the ISO/IEC 27001 certification process.

3.1 Accreditation bodies and their role

Recommended Training Duration	50 minutes
Exam Questions	2
Exam Weight	2.65%

This chapter explores the relationships between key players in the certification process, focusing on the International Accreditation Forum (IAF), accreditation bodies, and certification bodies. It emphasizes the concept of certification as a third-party conformity assessment activity, highlighting the importance of independent evaluation in management system certification, the use of accreditation marks, and how accredited conformity assessment bodies are required to use specific marks as mandated by their respective accreditation bodies. Additionally, it covers the rights and obligations related to witnessing activities conducted by accreditation bodies, providing auditors with relevant knowledge for navigating the certification landscape. This information is essential for Lead Auditors to understand the broader context of certification processes and their role within the accreditation framework.

Id	Learning Objectives	CL	Sources
3.1.1 921F6045	Understand the relationship between the International Accreditation Forum (IAF), accreditation bodies, and certification bodies.	C2	
3.1.2 80AC5B2E	Understand that certification of a management system is a third-party conformity assessment activity.	C2	[1: 1]

Table continued on next page

Id	Learning Objectives (cont.)	CL	Sources
3.1.3 70B830AC	Know that accredited conformity assessment bodies are required to use an accreditation mark as specified by their accreditation body.	C1	
3.1.4 10B22D5B	Know the obligations and rights regarding witnessing activities of the accreditation body.	C1	[1: 9.2]

3.2 Overview of Certification Process

Recommended Training Duration	85 minutes (1 hour 25 minutes)
Exam Questions	3
Exam Weight	4.50%

Understanding the certification process from a certification body's perspective is highly relevant for Lead Auditors, especially when conducting third-party audits. This enables auditors to navigate the complexities of the three-year certification cycle, including initial certification, maintenance, and potential scope changes. Familiarity with stage 1 and stage 2 audit requirements, as well as the information necessary for granting initial certification, helps prevent formal errors during audits. Moreover, recognizing situations that may lead to certification changes and understanding the appeal and complaint handling process equips Lead Auditors to effectively manage various scenarios and to confidently guide organizations through the ISO/IEC 27001 certification journey, maintaining professionalism and accuracy in their role as representatives of certification bodies.

Id	Learning Objectives	CL	Sources
3.2.1 5459CB67	Know the typical process flow for a certification process from the perspective of a certification body.	C1	
3.2.2 12113912	Understand the three-year certification cycle and the process of maintaining a certificate.	C2	[1: 9.1, 9.6]
3.2.3 11375492	Know the requirements for stage 1 and stage 2 audits within the initial ISMS certification audit.	C1	[6: 9.3]
3.2.4 E58E5B7E	Apply, in a scenario as a lead auditor, knowledge of which information must be provided to a certification body prior to granting initial certification.	C3	[1: 9.5]
3.2.5 A2F2FA16	Recognize situations that could lead to suspending, withdrawing, or reducing the scope of certification.	C1	[1: 9.6]
3.2.6 29FE994B	Know the requirements for an appeal and complaint handling process of a certification body.	C1	[1: 9.7, 9.8]

3.3 Legal and Regulatory Compliance

Recommended Training Duration	75 minutes (1 hour 15 minutes)
Exam Questions	3
Exam Weight	3.97%

This chapter focuses on the legal and regulatory aspects of ISO/IEC 27001 certification, emphasizing the importance of impartiality, compliance, and proper documentation. Candidates will learn about the financial and legal obligations of certification bodies, including the requirement for legally enforceable agreements with clients. The chapter covers the attributes and usage requirements of certification documents and marks, as well as the distinctions between management system certification audits and legal compliance audits. Additionally, candidates will gain an understanding of compliance terminology and the auditee's responsibility in identifying relevant statutory and regulatory requirements.

Id	Learning Objectives	CL	Sources
3.3.1 132BF09F	Understand that the certification body must evaluate its finances and sources of income to ensure that commercial, financial, or other pressures do not compromise its impartiality.	C2	[1: 5.3] [6: 5.3]
3.3.2 F9E4AB9C	Understand the importance of having a legally enforceable agreement between the certification body and its clients for the provision of certification activities.	C2	[1: 5.1]
3.3.3 7836C341	Know the attributes of a certification document, a certification mark, and requirements for their use.	C1	[1: 8.1, 8.2, 8.3]
3.3.4 D9ECABE7	Know the terms "compliance" and "non-compliance".	C1	[3: 3.7]
3.3.5 1454EE51	Distinguish between a management system certification audit and a legal compliance audit.	C2	[3: 5.2, 5.4] [2: 9.2]
3.3.6 1635094F	Know the obligation of the auditee to identify its statutory and regulatory requirements.	C1	[4: 4.4]

3.4 Maintaining impartiality and integrity

Recommended Training Duration	55 minutes
Exam Questions	2
Exam Weight	2.91%

Maintaining impartiality and integrity is a critical aspect of the ISO/IEC 27001 Lead Auditor role, with far-reaching

implications for the entire audit process. As the cornerstone of credible and trustworthy audits, impartiality must be safeguarded against various threats that can emerge at different stages of the audit. Lead Auditors must be equipped to recognize potential conflicts of interest and understand the profound impact that compromised impartiality can have on audit outcomes. By exploring typical threats and scenarios, this chapter empowers auditors to uphold the highest standards of integrity in their practice, enabling Lead Auditors to navigate complex situations and ensure compliance with accreditation requirements.

Id	Learning Objectives	CL	Sources
3.4.1 16C4C552	Understand the importance of impartiality of an auditor.	C2	[1: 4.2]
3.4.2 791F0533	Know typical threats to impartiality.	C1	[1: 4.2]
3.4.3 167E9612	Recognize a conflict of interest in a given scenario as an auditor.	C3	[1: 5.2] [3: 5.2] [7: 9.2] [6: 5.2]

4 Information Security Management 27001 Foundation

Recommended Training Duration	295 minutes (4 hours 55 minutes)
Exam Questions	12
Exam Weight	15.61%

The Information Security Management 27001 Foundation competency area serves as a refresher for essential knowledge that is fundamental to the ISO/IEC 27001 Lead Auditor role. It covers key aspects of Information Security Management Systems (ISMS), including organizational context, management commitment, security policies, and risk assessment. This foundational knowledge is not only a prerequisite for Lead Auditors but is also implicitly and explicitly tested in the certification exam. By revisiting these core concepts, auditors can strengthen their understanding of ISMS principles, ensuring they are well-equipped to evaluate an organization's compliance with ISO/IEC 27001 standards. The competency area also emphasizes the importance of continuous improvement, resource management, and the application of controls as outlined in the ISO/IEC 27001 Annex A, providing auditors with a comprehensive framework for assessing and enhancing information security practices within organizations.

4.1 General overview of ISMS

Recommended Training Duration	25 minutes
Exam Questions	1
Exam Weight	1.32%

This chapter provides an overview of Information Security Management Systems (ISMS) within the context of ISO/IEC 27001. It emphasizes the flexibility and adaptability of ISO/IEC 27001 requirements, highlighting that these are designed to be tailored to suit various organizational contexts. The chapter stresses the importance of understanding that while processes can be customized, all requirements of ISO/IEC 27001 must be addressed for an organization to claim conformity with the standard.

Id	Learning Objectives	CL	Sources
4.1.1 14B7B51B	Understand that the requirements in ISO/IEC 27001 are generic and processes are meant to be tailored.	C2	[7: 1]
4.1.2 62D44557	Know that no requirements of ISO/IEC 27001 can be excluded when conformity is claimed.	C1	[7: 1]

4.2 Context of the organization

Recommended Training Duration	25 minutes
Exam Questions	1
Exam Weight	1.32%

This chapter focuses on understanding the context of the organization. Candidates will learn the importance of identifying interested parties as an important step in determining the context of the ISMS. The chapter emphasizes the necessity of documenting the scope of the ISMS, which is essential for defining the boundaries and applicability of the information security management system. Understanding these concepts will enable auditors to effectively assess whether an organization has properly established the foundation for its ISMS in alignment with ISO/IEC 27001 requirements.

Id	Learning Objectives	CL	Sources
4.2.1 CBC59D57	Know that identifying the interested parties is necessary for determining the context of the ISMS.	C2	[7: 4.2]
4.2.2 954D5B3B	Know that the scope of the ISMS must be documented.	C1	[7: 4.3]

4.3 Management commitment

Recommended Training Duration	25 minutes
Exam Questions	1
Exam Weight	1.32%

Management commitment forms a critical cornerstone of an effective Information Security Management System (ISMS). Lead Auditors must understand the requirements placed on senior leadership, as their engagement is paramount to the success of an organization's information security initiatives. Given the significance of management commitment, Lead Auditors rarely delegate interviews with top management to their team members. This chapter, though concise, prepares auditors for an essential element of every audit: evaluating and assessing the level of management involvement and support for the ISMS.

Id	Learning Objectives	CL	Sources
4.3.1 112256D6	Understand the requirements top management must fulfill when establishing an ISMS.	C2	[7: 5]

Table continued on next page

Id	Learning Objectives (cont.)	CL	Sources
4.3.2 1106A9BF	Know that top management not only has to assign relevant ISMS roles but also has to communicate them.	C1	[7: 5.3]

4.4 Security Policy

Recommended Training Duration	30 minutes
Exam Questions	1
Exam Weight	1.59%

The Security Policy is the foundation for effective information security management within organizations. This chapter equips ISO/IEC 27001 Lead Auditors with essential knowledge about security policy requirements and the importance of its organizational communication. Understanding the elements of a Statement of Applicability (SoA) is vital for auditors to assess an organization's implementation of ISO/IEC 27001 controls.

Id	Learning Objectives	CL	Sources
4.4.1 F523D103	Know the requirements for a security policy.	C1	[7: 5.2]
4.4.2 161050A5	Know that a security policy must be communicated within the organization.	C1	[7: 5.2]
4.4.3 5F877CA0	Know which elements a Statement of Applicability (SoA) contains.	C1	[7: 6.1]

4.5 Risk assessment and treatment

Recommended Training Duration	30 minutes
Exam Questions	1
Exam Weight	1.59%

This chapter focuses on the critical processes of risk assessment and treatment within the context of ISO/IEC 27001 information security management. Candidates will learn the step-by-step approach to conducting a comprehensive risk assessment and implementing effective risk treatment measures. The chapter explores the components of a risk treatment plan and its importance in managing information security risks. Additionally, students will gain an understanding of the role played by risk owners in the risk management process.

Id	Learning Objectives	CL	Sources
4.5.1 109BD767	Know the risk assessment and treatment steps.	C1	[7: 6.1]
4.5.2 560514F5	Know the risk treatment plan.	C1	[7: 6.1]
4.5.3 D908B5C5	Know the role of a risk owner.	C1	[7: 6.1]

4.6 Resources

Recommended Training Duration	40 minutes
Exam Questions	2
Exam Weight	2.12%

This chapter focuses on the essential resources required for an effective Information Security Management System (ISMS) within the context of ISO/IEC 27001. It explores the key competencies for personnel involved in the organization's ISMS implementation and maintenance. Additionally, the importance of documented information within an ISMS is examined, outlining necessary documentation types and providing guidance on creating and updating these documents effectively.

Id	Learning Objectives	CL	Sources
4.6.1 D74DA9CA	Know the key requirements an ISMS has for the competence of persons involved in the organization.	C1	[7: 7.1, 7.2]
4.2.1 13E4E46F	Know the main objectives persons doing work under the organization shall be aware of.	C1	[7: 7.3]
4.2.2 11467E37	Know what documented information is in an ISMS.	C1	[4: 3.19, 3.50, 3.41, 3.54]
4.6.4 25E913FE	Recognize essential elements when creating and updating documented information.	C1	[7: 7.5]

4.7 Controlling and Improvement

Recommended Training Duration	40 minutes
Exam Questions	2
Exam Weight	2.12%

Control and Improvement is a key element of effective Information Security Management Systems (ISMS) implementation and maintenance. This chapter equips Lead Auditors with essential knowledge on monitoring, mea-

suring, and enhancing ISMS processes to ensure continuous improvement and compliance with ISO/IEC 27001 standards. By exploring elements such as internal audit programmes, management reviews, and nonconformity handling, participants gain valuable insights into evaluating and optimizing an organization's information security practices. Proficiency in these areas enables auditors to provide comprehensive evaluations and recommendations, hence contributing to the overall success of information security initiatives within organizations.

Id	Learning Objectives	CL	Sources
4.7.1 672FC13B	List the elements that an organization must determine for monitoring and measuring information security processes.	C1	[7: 9.1]
4.3.2 4E4A6588	Know factors an organization must consider when establishing an internal audit programme.	C1	[7: 9.2]
4.7.3 6D9ED87D	Identify the main purpose of management reviews in the context of an ISMS.	C1	[7: 9.3]
4.7.4 9AB88CEC	List the actions an organization should take when a nonconformity is identified within its ISMS.	C1	[7: 10.2]

4.8 The renowned Annex A

Recommended Training Duration	80 minutes (1 hour 20 minutes)
Exam Questions	3
Exam Weight	4.23%

Understanding Annex A is fundamental for ISO/IEC 27001 Lead Auditors, as it forms the normative foundation of information security controls. Thorough comprehension of the four control types - organizational, people, physical, and technological - enables auditors to comprehensively assess an organization's security posture. While Lead Auditors may not possess expert-level knowledge of every control, a solid grasp of Annex A principles is essential for assembling and guiding an effective audit team.

Id	Learning Objectives	CL	Sources
4.4.1 B18306A0	Know that Annex A is normative.	C1	
4.8.2 BD1F24F9	Know the four control types (organizational, people, physical, and technological) and their controls.	C1	
4.8.3 165AFA8B	Evaluate the adequacy of physical access controls in restricting unauthorized entry to sensitive areas and protecting critical assets, following the principles outlined in Annex A.	C3	

Table continued on next page

Id	Learning Objectives (cont.)	CL	Sources
4.8.4 B4F8A09B	Contrast the key objectives between technological and organizational controls.	C3	

5 Audit Principles

Recommended Training Duration	230 minutes (3 hours 50 minutes)
Exam Questions	9
Exam Weight	12.17%

The Audit Principles competency area equips candidates with essential knowledge and skills to conduct effective information security audits in accordance with ISO standards. Candidates will learn about various audit types, stakeholder roles, and the fundamental principles that govern the audit process. This area emphasizes the importance of integrity, independence, and evidence-based approaches in auditing, while also addressing the challenges and opportunities presented by remote and virtual audit activities. By mastering these concepts, candidates will be prepared to plan, execute, and lead audits that assess an organization's Information Security Management System (ISMS) compliance and effectiveness.

5.1 Audit stakeholders

Recommended Training Duration	65 minutes (1 hour 5 minutes)
Exam Questions	3
Exam Weight	3.44%

Understanding the roles and responsibilities of various stakeholders in an audit process is important for effective auditing, especially in complex organizational environments. As audits often involve multiple parties with diverse interests and expertise, a Lead Auditor must possess a clear understanding of each stakeholder's role, motives, and potential impact on the audit outcome. This knowledge enables the Lead Auditor to navigate complex organizational structures, manage relationships effectively, and ensure a comprehensive and unbiased audit process. Through a thorough understanding of audit team composition, including the roles of technical experts, guides, and observers, Lead Auditors can optimize team selection and performance. Furthermore, recognizing the importance of being accompanied by a guide enhances the auditor's ability to navigate the audited organization efficiently, ensuring access to necessary information and resources throughout the audit process.

Id	Learning Objectives	CL	Sources
5.1.1 5C4AF84E	Define the role of an auditor.	C1	[3: 3.15]
5.1.2 BE0E58E6	Know who can be part of an audit team.	C1	[3: 3.14, 5.5]
5.1.3 ED0C60BF	Summarize the considerations for selecting audit team members.	C2	[3: 5.5]
5.1.4 4303F2B0	Know the role of a technical expert.	C1	[3: 3.16]

Table continued on next page

Id	Learning Objectives (cont.)	CL	Sources
5.1.5 17046020	Know the responsibilities of guides and observers.	C1	[3: 6.4, 3.17, 6.3]
5.1.6 18102675	Know that an auditor shall be accompanied by a guide.	C1	[1: 9.2]

5.2 Audit types

Recommended Training Duration	35 minutes
Exam Questions	1
Exam Weight	1.85%

This chapter focuses on the various types of audits in the context of ISO/IEC 27001 certification. Candidates will learn to differentiate between first-party, second-party, and third-party audits, gaining a comprehensive understanding of their distinct characteristics and applications. Different scenarios constituting second-party audits are examined, providing practical insights into their implementation. Additionally, the nuances of third-party audits are explored, including initial certification, surveillance activities, and recertification processes. Proficiency in these areas is vital for Lead Auditors to effectively plan, conduct, and evaluate audits across different organizational contexts and stages of the ISO/IEC 27001 certification lifecycle.

Id	Learning Objectives	CL	Sources
5.2.1 120ADCC9	Know the difference between first-party, second-party, and third-party audits.	C1	[3: 3.1]
5.2.2 49CBBBC0	Understand various scenarios that constitute second-party audits.	C2	
5.2.3 F61BBE7A	In the context of third-party audits, know the difference between initial certification, surveillance activities, and recertification.	C1	[1: 9.5, 9.6]

5.3 Audit principles conform to 19011

Recommended Training Duration	80 minutes (1 hour 20 minutes)
Exam Questions	3
Exam Weight	4.23%

This chapter covers the audit principles as outlined in ISO 19011, providing a comprehensive understanding of the fundamental guidelines for auditing management systems. Candidates will learn about the seven key audit principles and how to recognize their application or violation in various audit situations. The chapter explores factors that can influence audit integrity and discusses the appropriate use of audit information. It also addresses

the management of internal auditor independence in small organizations and compares evidence-based and risk-based audit approaches. This knowledge is essential for conducting effective and ethical audits, ensuring the integrity of the audit process.

Id	Learning Objectives	CL	Sources
5.3.1 3E34A0B1	Know the seven audit principles of ISO 19011.	C1	[1: 4] [3: 4]
5.3.2 A24C91D3	Know factors that influence the integrity of an audit or audit programme.	C1	
5.3.3 882727EB	Recognize inappropriate use of audit information.	C1	
5.3.4 7FADC7ED	Know how independence of internal auditors should be managed in small organizations.	C1	
5.3.5 899B9F13	Know the advantages and disadvantages of evidence-based compared to risk-based audit approaches.	C1	
5.3.6 18080460	Be able to recognize adherence to or violation of different audit principles in audit situations.	{λ}	[1: 4] [3: 4]

5.4 Audit principles in the information security context

Recommended Training Duration	30 minutes
Exam Questions	1
Exam Weight	1.59%

Navigating the multitude of ISO audit standards can be challenging, particularly in the realm of information security. This focused exploration of ISO/IEC 27007 equips Lead Auditors with essential guidance for auditing Information Security Management Systems (ISMS). By understanding the structure and documentation requirements of ISO/IEC 27007, auditors gain insights into conducting effective ISMS audits. Familiarity with the Statement of Applicability (SoA) requirements further enhances an auditor's ability to assess ISMS implementation comprehensively.

Id	Learning Objectives	CL	Sources
5.4.1 40C4F428	Know the structure of the ISO/IEC 27007 guidance for auditing an ISMS.	C1	

Table continued on next page

Id	Learning Objectives (cont.)	CL	Sources
5.4.2 107D712C	Know the requirements for documented information conforming to ISO/IEC 27007.	C1	
5.4.3 326DD60A	Know where to find detailed information on what a Statement of Applicability (SoA) should contain.	C1	

5.5 Remote auditing and technology considerations

Recommended Training Duration	20 minutes
Exam Questions	1
Exam Weight	1.06%

This chapter focuses on the implementation of remote auditing techniques and the technological considerations involved in conducting ISO/IEC 27001 audits. It explores the comparative advantages and disadvantages of on-site, remote, and hybrid audit approaches, providing auditors with the knowledge to select the most appropriate method for each situation. The distinctions between remote and virtual audit activities are examined, emphasizing the critical technical preparations required, particularly for virtual audits. Proficiency in these areas equips auditors to effectively plan and execute audits using various modalities, ensuring thorough assessments of information security management systems regardless of physical constraints.

Id	Learning Objectives	CL	Sources
5.5.1 EC1DE9F8	Know the advantages and disadvantages of conducting audits on-site, remotely, or as a combination of both.	C1	[3: 5.5] [6: 9.4]
5.5.2 140304A6	Differentiate between remote and virtual audit activities and know the importance of technical preparations, especially for virtual audits.	C1	

6 Audit Methodologies and their Application

Recommended Training Duration	285 minutes (4 hours 45 minutes)
Exam Questions	12
Exam Weight	15.08%

Audit methodologies and their application form a critical component of the ISO/IEC 27001 Lead Auditor's skill set. This competency area is particularly important as the selection and planning of audit methods significantly influence the audit's effectiveness and outcomes. Lead Auditors must possess comprehensive knowledge of various information sources, audit techniques, and sampling methods to conduct thorough and objective assessments. Through deep understanding of document-focused and people-focused approaches, auditors can adapt their strategies to different organizational contexts and gather robust evidence. Furthermore, grasping the nuances of on-site visits and interview techniques enables Lead Auditors to navigate complex organizational dynamics and extract valuable insights. Expertise in these methodologies empowers Lead Auditors to make informed decisions, ensure compliance, and add value to the audited organization's Information Security Management System (ISMS).

6.1 Sources of information

Recommended Training Duration	45 minutes
Exam Questions	2
Exam Weight	2.38%

This chapter focuses on the sources of information relevant to ISO/IEC 27001 auditing processes. Candidates will learn to utilize Table E.1 from ISO/IEC 27006 as a guide for identifying potential information sources for each ISO/IEC 27001 Annex A control. The chapter covers the conditions under which a Lead Auditor may determine that a certification audit cannot proceed due to insufficient access to ISMS-related information. It emphasizes the importance of understanding that certification procedures should not assume a specific ISMS implementation method or documentation format. Additionally, candidates will explore various sources of information, equipping them with the knowledge to effectively gather and assess relevant data during the auditing process.

Id	Learning Objectives	CL	Sources
6.1.1 137138B0	Know different sources of information.	C1	
6.1.2 88F01977	Know Table E.1 from ISO/IEC 27006 as a guide to identify possible sources of information for each individual ISO/IEC 27001 Annex A control.	C1	

Table continued on next page

Id	Learning Objectives (cont.)	CL	Sources
6.1.3 33268BCD	Know the conditions under which a lead auditor can advise that a certification audit cannot take place due to lack of access to necessary ISMS-related information.	C1	[3: 6.4] [6: 8.4]
6.1.4 3AD1CE9C	Understand that certification procedures should not presuppose a particular manner of implementation of an ISMS or a specific format for documentation and records.	C2	[6: 9.1]

6.2 Audit method selection and preparation

Recommended Training Duration	50 minutes
Exam Questions	2
Exam Weight	2.65%

This chapter focuses on the critical process of selecting and preparing appropriate audit methods for ISO/IEC 27001 audits. Candidates will explore the advantages and disadvantages of various audit methodologies, enabling them to make informed decisions when planning audits. The chapter emphasizes the importance of method selection as a key component of audit planning, ensuring that auditors choose the most effective approaches for each unique audit scenario. Learners will also understand the significance of documenting audit trails and methods used in the final audit report, promoting transparency and accountability in the audit process.

Id	Learning Objectives	CL	Sources
6.2.1 CCCA8599	Analyze advantages and disadvantages of different audit methods.	C4	
6.2.2 56173DC1	Know that choosing audit methods is an important part of planning an audit.	C1	[6: 7.1]
6.2.3 E2CC3E53	Know that audit trails and utilized audit methods shall be part of the audit report.	C1	[6: 9.4]

6.3 Document-focused approaches

Recommended Training Duration	40 minutes
Exam Questions	2
Exam Weight	2.12%

This chapter covers document-focused approaches in ISO/IEC 27001 auditing, with emphasis on mandatory documentation requirements and initial audit stages. Candidates will learn to identify and apply knowledge about

the specific information that ISO/IEC 27001 mandates to be documented in various scenarios. The chapter introduces the commonly used terms ”documentation review” and ”readiness review” in the context of stage 1 audits, providing a foundation for understanding preliminary audit processes. The skills acquired in this chapter will enable auditors to conduct thorough document-based evaluations and determine an organization’s readiness for full ISO/IEC 27001 certification.

Id	Learning Objectives	CL	Sources
6.3.1 12BC4BC6	Apply knowledge about which information ISO/IEC 27001 requires to be documented (mandatory documents) in a given scenario.	C3	[7: 4.3, 5.2, 6.1, 6.2, 7.2, 7.5, 8.1, 8.2, 8.3, 9.1, 9.2, 9.3, 10.1]
6.3.2 3C0C768B	Know the commonly used terms ”documentation review” and ”readiness review” for stage 1 audit.	C1	[6: 9.3]

6.4 People-focused approaches

Recommended Training Duration	95 minutes (1 hour 35 minutes)
Exam Questions	4
Exam Weight	5.03%

People-focused approaches form the cornerstone of effective auditing, embodying the essence of an auditor’s role and expertise. Proficiency in interview techniques and understanding the nuances of human interaction are important skills for ISO/IEC 27001 Lead Auditors, as they directly impact the quality and depth of evidence gathered. By developing expertise in various interview methods and appreciating the dynamics of different organizational roles, auditors can navigate diverse scenarios with finesse and objectivity. This competency not only enhances the auditor’s ability to collect meaningful data but also adds a compelling dimension to the profession, making it both challenging and rewarding. Ultimately, the judicious application of people-focused approaches, balanced with other audit methodologies, enables auditors to conduct comprehensive assessments that yield valuable insights for organizational improvement and compliance.

Id	Learning Objectives	CL	Sources
6.4.1 46A3A78C	Know the protocols for conducting interviews, such as explaining the reason for the interview, taking notes, and summarizing the interview results with the interviewee.	C1	
6.4.2 C89D6CA2	Know that audit methods with or without human interaction should be purposefully applied in specific situations.	C1	

Table continued on next page

Id	Learning Objectives (cont.)	CL	Sources
6.4.3 139EBCF8	Recognize the dynamics that can develop in interviews and be consciously aware of the chosen interview technique.	{λ}	
6.4.4 7C04DC73	Judge different interview techniques (e.g., question types, appreciative inquiry) to determine their effectiveness in collecting objective evidence in a given scenario.	C4	
6.4.5 AE662523	Understand how interviews with different roles and levels of the organizational chart contribute to gathering audit evidence.	C2	

6.5 Visiting the auditee's location

Recommended Training Duration	30 minutes
Exam Questions	1
Exam Weight	1.59%

Understanding the intricacies of visiting an auditee's location is key for ISO/IEC 27001 Lead Auditors, as they must be acutely aware of potential risks and unique characteristics at various sites. This knowledge enables effective planning, execution, and evaluation of on-site activities, which are fundamental to a comprehensive audit process. Proficiency in the essential steps for planning visits and considering key factors during on-site activities allows Lead Auditors to ensure thorough and accurate assessments of organizational controls. The ability to make astute observations during these visits contributes significantly to the overall evaluation of an organization's information security management system. Developing these skills is particularly vital for Lead Auditors, as they bear the primary responsibility for identifying and mitigating potential risks associated with different auditee locations, ultimately enhancing the effectiveness and reliability of the audit process.

Id	Learning Objectives	CL	Sources
6.5.1 89F2F6F5	Identify the essential steps required for planning a visit to the auditee's location.	C1	
6.5.2 6A033FB9	Know what to consider for on-site activities.	C1	
6.5.3 D53B9615	Know how observations contribute to the evaluation of organizational controls during an audit.	C1	

6.6 Sampling techniques

Recommended Training Duration	25 minutes
Exam Questions	1
Exam Weight	1.32%

Sampling techniques are essential for ISO/IEC 27001 Lead Auditors, particularly in complex audit situations requiring formal decision-making processes. This competency is essential when conducting third-party audits, where an auditor's judgment can have significant implications. Lead Auditors must be well-versed in the standard's requirements for sampling, especially in multi-site certifications. Proficiency in sampling techniques enables auditors to effectively plan and execute audits, ensuring comprehensive coverage while optimizing time and resources. Understanding the nuances of sampling decisions during the audit planning phase enables auditors to make informed choices, maintain objectivity, and produce reliable results.

Id	Learning Objectives	CL	Sources
6.6.1 F47EF331	Understand the need for sampling decisions and sampling-type decisions in the planning phase of the audit.	C2	[6: 6.3]
6.6.2 4CF00EEA	Know requirements for a sample-based approach to a multiple-site certification.	C1	[6: 9.1]

7 Process Perspective of an Audit

Recommended Training Duration	365 minutes (6 hours 5 minutes)
Exam Questions	15
Exam Weight	19.31%

The Process Perspective of an Audit is a critical competency area for ISO/IEC 27001 Lead Auditors, as it encompasses the formal procedures and responsibilities essential for conducting a successful audit. Understanding the audit process, from initiation to finalization, is necessary for ensuring compliance with ISO standards and maintaining the integrity of the audit. Lead Auditors must not only know the procedural requirements but also comprehend the underlying rationale behind each step, as deviations can lead to formal errors with significant consequences. This competency area equips auditors with the knowledge to effectively plan, execute, and conclude audits while adhering to the Plan-Do-Check-Act cycle. Proficiency in these skills enables Lead Auditors to navigate complex audit scenarios, gather objective evidence, identify nonconformities, and communicate findings effectively, ultimately contributing to the continuous improvement of information security management systems.

7.1 Audit Initiation

Recommended Training Duration	50 minutes
Exam Questions	2
Exam Weight	2.65%

This chapter focuses on the critical first steps of conducting an ISO/IEC 27001 audit. It emphasizes the non-delegable responsibilities of the audit team leader and explores how different audit stages align with the Plan-Do-Check-Act (PDCA) cycle. Candidates will learn the key objectives for establishing initial contact with the auditee and understand the process of determining audit feasibility. The chapter also covers the essential components of an audit scope description, providing auditors with the necessary knowledge to effectively plan and initiate an audit and to ensure a well-structured and purposeful audit process from the outset.

Id	Learning Objectives	CL	Sources
7.1.1 FD05347C	Know that the responsibility of the audit team leader cannot be delegated.	C1	[3: 6.2]
7.1.2 14B42B59	Know which step of an audit programme or audit contributes to which phase of the PDCA-Cycle.	C1	[3: 6.2]
7.1.3 F57E4D40	Identify key objectives for establishing contact with the auditee.	C1	[3: 6.2]
7.1.4 14F2EF7C	Know the initiation step determining feasibility of an audit.	C1	[3: 6.2]

Table continued on next page

Id	Learning Objectives (cont.)	CL	Sources
7.1.5 16F28296	Know the content of an audit scope description.	C1	[3: 3.5]

7.2 Audit Preparation and Planning

Recommended Training Duration	45 minutes
Exam Questions	2
Exam Weight	2.38%

This chapter covers the aspects of audit preparation and planning. Candidates will learn about the standardized procedures for determining audit time, including specific requirements for multi-site audits. Key objectives of audit planning are explored, emphasizing their importance in ensuring a comprehensive and effective audit process. Students will gain an understanding of audit criteria and their purpose in establishing a benchmark for evaluation. Mastering these concepts is essential for auditors to efficiently organize their approach, allocate resources appropriately, and set clear expectations for the audit process, ultimately contributing to a more structured and successful ISO/IEC 27001 audit.

Id	Learning Objectives	CL	Sources
7.2.1 11579032	Know which standard defines the procedure for determining audit time.	C1	
7.2.2 39DA2263	Know audit time requirements for multi-site audits.	C1	
7.2.3 40AAC5C2	Know key objectives of audit planning.	C1	[3: 3.6, 3.1, 6.3]
7.2.4 7D0ABA53	Understand the purpose of audit criteria.	C2	[3: 3.7, 3.23, 3.8]

7.3 Performing Audit Activities

Recommended Training Duration	205 minutes (3 hours 25 minutes)
Exam Questions	8
Exam Weight	10.85%

Performing audit activities forms a critical core component of the ISO/IEC 27001 Lead Auditor certification, focusing on the practical execution of audits within information security management systems. This comprehensive chapter covers the processes of collecting and verifying information, conducting effective opening meetings, and maintaining regulated audit communication. Participants will gain essential skills in distinguishing audit findings,

evaluating compliance with Annex A controls, and identifying areas requiring further investigation. The importance of objective evidence and proper documentation is emphasized, while also addressing the key task of grading nonconformities. Exploring the relationship between nonconformities, corrective actions, and the PDCA cycle helps auditors-in-training develop a holistic understanding of the audit process. This extensive coverage ensures that certified Lead Auditors are well-equipped to conduct thorough, accurate, and impactful information security audits.

Id	Learning Objectives	CL	Sources
7.3.1 258B31FA	Know a typical process of collecting and verifying information.	C1	[3: 6.4]
7.3.2 B7A0C001	Know the purpose, objectives, and required agenda topics of an opening meeting.	C1	[3: 6.4]
7.3.3 7362F433	Understand the necessity and key elements of regulated audit communication.	C1	[3: 6.4]
7.3.4 734BB4C9	Understand what objective evidence is.	C2	[3: 3.8]
7.3.5 7B115E27	Know different ways of obtaining audit evidence.	C2	[3: 3.8, 3.9]
7.3.6 5BC29D8F	Be able to distinguish what is an audit finding and what is not.	C4	[3: 3.10]
7.3.7 4C337947	Evaluate auditors' decisions regarding their compliance with Annex A controls in different scenarios.	C4	[3: 3.10, 3.9, 3.7]
7.3.8 158D198C	Analyze areas for further investigation that require additional clarification or evidence in an audit scenario.	C3	
7.3.9 1349E3DF	Note gaps, inconsistencies, or potential nonconformities in documentation.	C1	
7.3.10 3F33A1E1	Know the need for records of audit findings.	C1	[3: 6.4]
7.3.11 13C1DDBB	Understand grading nonconformities.	C2	[3: 6.4]
7.3.12 E2B707AA	Know the difference between nonconformities and corrective actions.	C1	
7.3.13 130093C3	Know how nonconformities and corrective actions contribute to the PDCA cycle.	C1	

7.4 Finalizing the Audit

Recommended Training Duration	65 minutes (1 hour 5 minutes)
Exam Questions	3
Exam Weight	3.44%

This chapter focuses on the final stages of an ISO/IEC 27001 audit, emphasizing the evaluation of management system results and the conclusion of the audit process. Candidates will learn how to define conformity and non-conformity, as well as how to prepare and deliver an effective audit report. The chapter covers the essential steps for conducting a closing meeting and the mandatory post-audit procedures. Additionally, students will gain an understanding of the proper communication channels for distributing the audit report.

Id	Learning Objectives	CL	Sources
7.4.1 651410D9	Know the focus on the results of the management system.	C1	
7.4.2 75C82EDD	Know how conformity and nonconformity are defined.	C1	[3: 3.20, 3.21]
7.4.3 166913B7	Know the audit conclusion and content of the audit report.	C1	[3: 3.11, 6.5]
7.4.4 BF47D665	Know how to prepare and conduct an audit closing meeting.	C1	[3: 6.4]
7.4.5 E367E0E7	Know the mandatory steps after the audit closing meeting.	C1	[3: 6.6, 6.7]
7.4.6 1096BE87	Understand the correct communication path for the audit report.	C2	[3: 6.5, 3.12]

8 Auditor Competencies and Skills

Recommended Training Duration	70 minutes (1 hour 10 minutes)
Exam Questions	3
Exam Weight	3.70%

The Auditor Competencies and Skills competency area focuses on developing the essential qualities and capabilities required for effective ISMS auditors and Lead Auditors. Candidates will learn about the specific competence requirements, personal behaviors, and responsibilities associated with auditing roles, as well as the importance of effective team management and communication within audit teams. This area also emphasizes the ongoing nature of auditor development, including the need for continuous evaluation and professional growth. Proficiency in these concepts equips candidates to lead and participate in ISMS audits, select and manage audit teams, and maintain their professional competence in the field of information security management systems auditing.

8.1 Skill Requirements

Recommended Training Duration	25 minutes
Exam Questions	1
Exam Weight	1.32%

This chapter focuses on the essential competencies and skills required for ISMS auditors, with a particular emphasis on personal behavior and professional conduct. Candidates will explore the specific competence requirements outlined for auditors working within the ISO/IEC 27001 framework, understanding the knowledge, skills, and attributes necessary for effective auditing. The critical importance of personal behavior during audits is examined, highlighting how an auditor's conduct can impact the audit process and outcomes. Lead Auditors are required to develop a professional demeanor, maintain objectivity, and build trust with auditees throughout the ISO/IEC 27001 audit process.

Id	Learning Objectives	CL	Sources
8.1.1 FADBDEDA	Know the competence requirements for ISMS auditors.	C1	[3: 7.1, 7.2] [6: 7.1]
8.1.2 116F2D4D	Understand the importance of personal behavior as an auditor.	C2	[3: 7.2]

8.2 Managing Audit Teams

Recommended Training Duration	25 minutes
Exam Questions	1
Exam Weight	1.32%

Managing audit teams is an important skill for ISO/IEC 27001 Lead Auditors, particularly when overseeing larger organizations that require multiple auditors. This chapter prepares Lead Auditors to effectively manage teams of varying sizes, from solo audits to those involving numerous professionals. Understanding the criteria for selecting an ISMS Lead Auditor and their responsibilities is essential for certification bodies when assigning auditors to specific engagements. Equally important is the Lead Auditor's ability to maintain strict and close communication within the audit team, ensuring cohesive and efficient auditing processes.

Id	Learning Objectives	CL	Sources
8.2.1 16FE8673	Understand the criteria for selecting an ISMS lead auditor and their responsibilities.	C2	[3: 6.3] [6: 7.2]
8.2.2 1369CE89	Know the necessity for a lead auditor to ensure strict and close communication within the audit team.	C1	[3: 6.4]

8.3 Auditor Evaluation

Recommended Training Duration	20 minutes
Exam Questions	1
Exam Weight	1.06%

In the realm of information security auditing, the evaluation of auditors themselves is a fundamental aspect often overlooked. This chapter emphasizes that auditors, while responsible for assessing others, are also subject to ongoing assessment and evaluation. Understanding the certification bodies' obligations to continuously evaluate auditor competence is essential for maintaining high standards in the profession. Lead Auditors must be aware of these requirements and commit to continuous professional development to stay current with evolving industry practices and standards. By focusing on auditor evaluation, this chapter underscores the importance of accountability and continuous improvement within the auditing profession, ensuring that those who assess information security management systems are themselves held to rigorous standards of competence and professionalism.

Id	Learning Objectives	CL	Sources
8.3.1 4566D299	Know the obligation of certification bodies to continuously evaluate and assess auditor competence.	C1	[3: 7.3, 7.4, 7.5] [6: 7.2]
8.3.2 FF484C6A	Know the obligation for continuous professional development as an auditor.	C1	[3: 7.6]

References

[1] ISO/IEC 17021-1:2015. Standard, International Organization for Standardization, Geneva, CH, 2015. URL https://www.iso.org/standard/61651.html. https://www.iso.org/standard/61651.html.

[2] ISO/IEC 27021:2017. Standard, International Organization for Standardization, Geneva, CH, 2017. URL https://www.iso.org/standard/61003.html. https://www.iso.org/standard/61003.html.

[3] ISO 19011:2018. Standard, International Organization for Standardization, Geneva, CH, 2018. URL https://www.iso.org/standard/70017.html. https://www.iso.org/standard/70017.html.

[4] ISO/IEC 27000:2018. Standard, International Organization for Standardization, Geneva, CH, 2018. URL https://www.iso.org/standard/73906.html. https://www.iso.org/standard/73906.html.

[5] ISO/IEC 27007:2020. Standard, International Organization for Standardization, Geneva, CH, 2020. URL https://www.iso.org/standard/77802.html. https://www.iso.org/standard/77802.html.

[6] ISO/IEC 27006-1:2024. Standard, International Organization for Standardization, Geneva, CH, 2024. URL https://www.iso.org/standard/82908.html. https://www.iso.org/standard/82908.html.

[7] ISO27001. ISO/IEC 27001:2022. Standard, International Organization for Standardization, Geneva, CH, 2022. URL https://www.iso.org/standard/27001. https://www.iso.org/standard/27001.

9 Imprint

Publisher:
Certible GmbH
Löwelstraße 20/2-3
1010 Vienna
Austria

Represented by:
Maria-Therese Teichmann
Alexander Feder

Contact:
Phone: +43 1 348 3993
Email: office@certible.com
Website: www.certible.com

Register entry:
FN: 564300d, Commercial Register at the Commercial Court in Vienna Registered office: Vienna

VAT ID:
ATU77279026

Responsible for content:
Maria-Therese Teichmann
Alexander Feder

Last updated: 2024-08-14