{Certible®}
international certification body

Certible® certified

ISO/IEC 27001 Lead Auditor

Candidate Handbook

Version: v2024.1
Status: Released
Release Date: 2024-07-02
Confidentiality: Public
Copyright©2024 Certible GmbH

Table of Contents

i 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.

ii Copyright

© 2024 Certible®. All rights reserved. No part of this publication may be reproduced, distributed, or transmitted in any form or by any means, including photocopying, recording, or other electronic or mechanical methods, without the prior written permission of Certible®, except in the case of brief quotations embodied in critical reviews and certain other non-commercial uses permitted by copyright law. For permission requests, write to Certible® at the address below. Unauthorized use, duplication, or distribution is strictly prohibited and may result in civil and criminal penalties.

iii 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.

iv Trademarks

Certible® the Certible® logo, and all other trademarks, 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.

v Contact

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

1 Certification Path

In our comprehensive certification program, we offer four distinct levels of expertise in ISO/IEC 27001, catering to different roles and depths of knowledge in Information Security Management Systems (ISMS):

1. **ISO/IEC 27001 Foundation:** This entry-level certification provides a solid grounding in the fundamentals of ISO/IEC 27001. It's ideal for those seeking to understand the basic principles and requirements of an ISMS, covering key concepts, terminology, and the structure of the standard.
2. **ISO/IEC 27001 Internal Auditor:** Building on the foundation knowledge, this intermediate certification equips professionals with the skills to conduct internal audits of an ISMS within their organization. It covers audit planning, execution, and reporting, focusing on assessing compliance and effectiveness of ISMS implementation.
3. **ISO/IEC 27001 Implementer:** This specialized certification is designed for professionals responsible for implementing and managing an ISMS in their organization. It focuses on practical skills and knowledge required to successfully plan, implement, and maintain an ISMS that conforms to ISO/IEC 27001 standards, including risk assessment, security controls, and continual improvement processes.
4. **ISO/IEC 27001 Lead Auditor:** Our most advanced certification is designed for professionals aiming to lead ISMS audit teams or manage entire audit programs. This comprehensive exam assesses the candidate's ability to plan, lead, and manage complex ISMS audits, interpret ISO/IEC 27001 requirements in various contexts, and provide valuable insights for continual improvement.

Each level progressively builds upon the previous, offering a clear pathway for professionals to develop their expertise in ISO/IEC 27001 and ISMS auditing, from foundational understanding to leadership in complex audit scenarios.

2 Certification Process

To attain the prestigious Certible® ISO/IEC 27001 Lead Auditor certification, candidates must successfully complete a rigorous two-part qualification process. This process, designed in full compliance with ISO/IEC 17024:2012 standards for personnel certification bodies, thoroughly assesses candidates' theoretical knowledge, practical experience in Information Security Management System (ISMS) auditing, and relevant work experience. By adhering to these internationally recognized standards, Certible® ensures that the certification process is both comprehensive and credible. This approach guarantees that certified professionals possess not only a deep understanding of the standard but also the real-world skills necessary to lead complex ISMS audits effectively, meeting the highest industry benchmarks for competence and reliability.

2.1 Multiple-Choice-Exam:

The exam consists of a series of challenging questions that test not only factual recall but also the application of knowledge in various scenarios an ISMS lead auditor might encounter. Candidates must demonstrate their ability to interpret the standard's requirements and apply auditing principles in complex organizational contexts. Please refer to [3.5 Exam Regulations and Procedures, page 13] and [4 Multiple-Choice Exam, page 15] .

The exam covers the Certible® ISO/IEC 27001 Lead Auditor Syllabus [1] and consists of following areas:

- ISO 27000 Family and Relationship to other Standards
- ISMS as a Management System
- Accreditation, Certification and Legal Context
- Information Security Management 27001 Foundation
- Audit Principles
- Audit Methodologies and their Application
- Process Perspective of an Audit
- Auditor Competencies and Skills

2.2 Documentary Proof of Relevant Audit and Work Experience:

Upon successful completion of the multiple-choice exam, candidates must provide substantial documentary evidence of their practical auditing experience and work experience. This crucial step verifies that the candidate has not only theoretical knowledge but also hands-on experience in conducting ISMS audits.

Candidates for Certible® ISO/IEC 27001 Lead Auditor certification must meet the following experience requirements:

1. A minimum of 5 years of professional experience in Information Technology (IT).
2. At least 2 years of the above experience must be in IT security and/or information security.
3. A minimum of 300 hours of audit-related activities.

Important

All submitted documents must adhere to confidentiality guidelines and be properly anonymized to protect sensitive information, see [2.3 Confidentiality and Data Protection, page 8]

2.2.1 Work experience

To qualify for certification, candidates must demonstrate a minimum of 5 years of professional experience in a relevant IT field, with at least 2 years specifically in IT Security. Candidates should provide comprehensive documentation to verify their work experience, including but not limited to:

- Detailed Curriculum Vitae (CV) or Resume: Highlight relevant positions, projects, and responsibilities. Clearly indicate duration of each role and specific IT security experiences
- Evidence of Professional Experience:
  - Employment certificates or letters of reference from employers
  - Detailed project reports or case studies (with sensitive information redacted, see [2.3 Confidentiality and Data Protection, page 8])
  - Performance evaluations relevant to IT and security roles
  - Contracts or statements of work for relevant consulting assignments
  - Publications, presentations, or research papers in relevant fields
  - Patents or other intellectual property related to IT or security
- Client Testimonials or Recommendations
- Letters from clients or stakeholders (appropriately anonymized, see [2.3 Confidentiality and Data Protection, page 8])
- Feedback on specific IT security projects or initiatives

2.2.2 Audit-related activities

Candidates must submit all required documentation within three years of completing the multiple-choice examination.

Candidates must provide documentation demonstrating their involvement in audit-related activities. This documentation serves as proof of their practical experience and competence in the field. This evidence must be categorized according to the type of audit (1st-, 2nd-, or 3rd-party) and clearly indicate the candidate's role in each. Acceptable forms of evidence include, but are not limited to:

- Documents verifying the candidate's participation in audits
- Testimonials from supervisors, managers or clients
- Proof of experience across various stages of the audit process, including planning, execution, reporting, and follow-up
- Audit planning documents or schedules showing the candidate's involvement
- Certificates of participation in relevant audit activities
- Signed statements from audit team leaders or clients (with sensitive information redacted, see [2.3 Confidentiality and Data Protection, page 8])

Note

If candidates are uncertain about the sufficiency of specific documents as proof, or have questions regarding the relevance of particular experiences, projects, or employments, they are encouraged to contact our support team (see [6 Support, page 17]) for clarification prior to submission.

2.3 Confidentiality and Data Protection

To protect sensitive information and maintain confidentiality, candidates must adhere to the following guidelines when submitting documentation:

1. **Redaction**: All sensitive information must be redacted from the submitted documents. This includes, but is not limited to:
   - Personal identifying information
   - Company-specific confidential data or any other confidential data
   - Client names and identifying details
2. **Sanitization Process**: Candidates are responsible for properly sanitizing their documentation before submission. This process involves:

- Removing or obscuring all confidential information
- Ensuring that redacted information cannot be recovered or deduced from the submitted documents

The certification body

- reserves the right to verify the authenticity of the submitted documentation without compromising confidentiality.
- commits to treating all submitted documentation with strict confidentiality and will not share or disclose any information contained therein.

By following these guidelines, candidates can provide the necessary proof of their work experience while maintaining the confidentiality and integrity of sensitive information.

2.4 Document Evaluation and Verification

All documentation submitted by candidates undergoes a thorough review process conducted by the Certification Board. This process ensures the integrity and validity of the certification program. The review includes:

- **Completeness Check**: The board verifies that all required documents have been submitted and are properly anonymized.
- **Experience Validation**: Each piece of evidence is carefully examined to confirm that it adequately demonstrates the required years of experience in IT and IT Security.
- **Relevance Assessment**: The board evaluates the relevance of the candidate's experience to the certification requirements, ensuring it aligns with the necessary skills and knowledge.
- **Authenticity Verification**: Where necessary, the board may take steps to verify the authenticity of submitted documents, while maintaining strict confidentiality protocols.
- **Consistency Analysis**: The board reviews all submitted materials for consistency across different documents and time periods.

  The Certification Board reserves the right to request additional information or clarification from candidates if needed. Candidates will be notified of the review outcome and any next steps in the certification process.

  This rigorous review process upholds the high standards of the certification, ensuring that only qualified professionals who meet all requirements are granted certification.

  The combination of the rigorous multiple-choice exam and the thorough review of practical experience ensures that Certible® ISO/IEC 27001 Lead Auditor certification holders are truly qualified to lead

ISMS audits at the highest level. This dual-pronged approach validates both the theoretical foundation and practical skills necessary for effective ISMS auditing, maintaining the integrity and value of the certification in the information security industry.

Successful candidates who meet both criteria - passing the examination and providing satisfactory proof of experience - are awarded the Certible® ISO/IEC 27001 Lead Auditor certification, recognizing their comprehensive expertise and readiness to lead complex ISMS audits across various organizational contexts.

2.5 Certification Status Changes: Denial, Suspension, and Withdrawal

Certible® works in accordance to ISO/IEC 17024:2012 and maintains high standards for its certifications and may deny, suspend, or withdraw a certification under certain circumstances:

1. **Denial**: A temporary refusal to grant certification, typically due to examination failure or other issues. Candidates may reapply or retake the exam as per the Certification Scheme document.
2. **Suspension**: A temporary removal of certification, lasting up to six months, usually due to correctable issues. The certified individual:
   - Will be notified of the reason and required corrective actions
   - Must not promote their certification during the suspension period
   - Has the opportunity to resolve the issue and reinstate their certification
3. **Withdrawal**: A permanent cancellation of certification, typically due to serious infractions or failure to resolve a suspension. The individual must cease all claims to certification and use of Certible® marks.

These actions may be initiated by Certible®'s Managing Directors, Certification Committee, or Board. All decisions can be appealed through the Complaints Appeals procedure.

Certible® maintains a central registry of certified individuals, updating it to reflect any status changes. This ensures the integrity and credibility of our certification program.

Certified individuals are bound by Certible®'s terms and conditions, including proper use of certification references and marks. Violations may lead to suspension or withdrawal of certification.

3 Certification Process in Practice

At Certible®, we are committed to providing a comprehensive, flexible, and candidate-friendly certification process. Our aim is to ensure that every step, from initial preparation to final certification, is clear, accessible, and tailored to meet diverse learning needs and schedules. Below, we outline each stage of the certification journey in detail.

3.1 Preparation Options

We recognize that each candidate has unique learning preferences and constraints, therefore we want candidates to have the flexibility to choose their preferred method of preparation.

3.1.1 Self-Study

For those who prefer independent learning or have scheduling constraints, self-study is an excellent option. We provide an extensive array of resources to support the exam preparation:

- **Study Materials**: Access our curated list of recommended textbooks, online resources, practice exams, and study guides. These materials are regularly updated to align with the latest standards and best practices in the field.
- **Practice Tests**: Simulated exam environments to familiarize with the question formats and time management.

Visit our Self-Study page[1] for a comprehensive list of study materials and resources.

3.1.2 Accredited Training Programs

For those who benefit from structured learning environments and direct interaction with instructors, we offer accredited training programs:

- **In-Person Training**: Intensive, instructor-led courses conducted at various locations worldwide.
- **Virtual Live Training**: Real-time online courses allowing for interactive learning from anywhere.
- **Blended Learning**: A combination of self-paced online modules and live instructor-led sessions.

These programs are delivered by our network of accredited trainers, ensuring high-quality, standardized instruction. Find a complete list of upcoming training sessions and accredited trainers on our Training page[2].

[1] Self-Study page: https://www.certible.com/self-study/#CCSI009LA

[2] Training page: https://www.certible.com/trainings/?program=CCSI009LA

3.2 Application and Exam Registration

Once you feel prepared, the next step is to register for the certification exam. We've streamlined this process to make it as convenient as possible and combined the Application for Certification and Exam Registration into one step:

- **Visit the Registration Page**: Navigate to our Registration page[3].
- **Select Exam Date**: Choose from available dates that suit your schedule. We offer multiple time slots to accommodate different time zones and personal preferences.
- **Payment Process**: Complete the secure online payment for your chosen exam slot, or enter the Voucher given to you by your training provider.
- **Confirmation**: Upon successful registration and payment, you'll receive an immediate confirmation email.
- **Access to Self-Service Portal**: Your confirmation email will contain a unique link to our self-service portal, where you can manage various aspects of your exam.

3.3 Self-Service Portal

Our self-service portal is designed to give maximum control over the certification process. Key features include:

3.3.1 Exam Management

- **Rescheduling**: If unforeseen circumstances arise, you can reschedule your exam up to 48 hours before the scheduled time without any additional fee.
- **Cancellation**: Should you need to cancel, you can do so through the portal, subject to our cancellation policy.

3.3.2 Technical Readiness - Self Check

Our **Self Check Tool** allows you to verify if your computer meets all technical requirements for the remote exam. This includes checks for:

- Internet connection stability
- Webcam and microphone functionality
- Screen resolution and display settings

[3] Registration page: https://www.certible.com/register/?cert=CCSI009LA

– Compatible browser versions

3.4 Support and Special Accommodations

We are more than happy to make accommodations for candidates with special requirements, such as offering barrier-free physical access to our exam locations or making adjustments to cater to the visually impaired. Please inform us of any such requirements in advance.

Our remote proctoring software is designed with accessibility in mind and supports screen readers. The software has been tested and verified to work seamlessly with NVDA (NonVisual Desktop Access). If you use a different screen reader or encounter any accessibility issues, please contact our support team for assistance.

3.5 Exam Regulations and Procedures

To ensure the integrity and fairness of the certification process, we have established a comprehensive set of exam regulations. These cover areas such as:

– Identification requirements

– Permitted and prohibited items during the exam

– Breaks and time management

– Proper exam environment setup for remote testing

– Code of conduct during the exam

– Accommodations for candidates with special needs

We strongly recommend thoroughly reviewing these regulations well in advance of the exam date. This will help prepare adequately and avoid any last-minute surprises or disqualifications.

3.5.1 Examination Retake Policy

Candidates have the opportunity to retake the certification exam if they do not pass on their initial attempt. There is no limit to the number of times a candidate may sit for the exam. However, please note that a fee is required for each retake attempt. We strongly encourage thorough preparation for each attempt:

1. **Review**: Carefully analyze your previous exam performance to identify areas for improvement.
2. **Preparation**: Dedicate sufficient time to study and reinforce your understanding of the subject matter before each attempt.

3. **Resources**: Utilize all available study materials, practice exams, and training resources to enhance your knowledge and exam readiness.
4. **Timing**: Allow adequate time between attempts to ensure comprehensive preparation and increased likelihood of success.
5. **Consultation**: Consider seeking guidance from mentors or industry professionals to strengthen your understanding of challenging topics.
6. **Fee Consideration**: Be aware that each retake requires payment of the examination fee. Factor this into your preparation strategy and timeline.

While the option to retake the exam provides flexibility, candidates are advised to approach each attempt with seriousness and dedication to maximize their chances of success and demonstrate true mastery of the subject matter.

3.6 Post-Exam Process

After completing your exam:

- **Immediate Preliminary Results**: You'll receive an preliminary score immediately after finishing the exam.
- **Official Results**: Within 5-7 business days, you'll receive your official results via email.
- **Certificate Issuance**: Once all certification criteria are met and the certification decision is rendered, your certificate will be issued and made available to you.
- **Recertification Information**: Details about maintaining your certification, including any requirements and recertification deadlines, will be provided.

4 Multiple-Choice Exam

4.1 Overview

ISO/IEC 27001 Lead Auditor Exam	
Exam format	Multiple-choice (1 of 4)
Exam duration	150 minutes
Grading method	No malus
Number of questions	75
Pass mark	70%
Exam delivery methods	Remote proctored, Test center, On-site proctored
Materials allowed	ISO standards printed on paper

The certification examination consists of 75 multiple-choice questions, each presenting four options. Each question is assigned a point value that varies depending on its cognitive level, reflecting the complexity and depth of knowledge required. Candidates are allotted 150 minutes to complete the assessment. The exam employs a „no malus" grading method, meaning incorrect answers do not result in point deductions. To successfully pass the exam, candidates must achieve a pass mark of 70% or higher. The duration of the exam is carefully designed to allow candidates ample time to demonstrate their knowledge and skills.

For added flexibility, the exam is available through various delivery methods, including remote proctoring, test center administration, and on-site proctored sessions. Candidates are permitted to reference ISO standards in printed form during the examination. To maintain the highest standards of academic integrity, a qualified invigilator will be present throughout the entire duration of the exam. Their role is to ensure adherence to all examination regulations and to safeguard the overall integrity of the assessment process.

5 Exam Grading and Results

Our examination grading process is entirely automated and has been rigorously verified to ensure accuracy and fairness. The passing score for each exam is predetermined and applied consistently to all candidates. We maintain a strict policy regarding exam results:

- The automated grading system eliminates human error and ensures impartial evaluation of all exam responses.
- The passing score is non-negotiable and applied uniformly to all candidates.
- We do not entertain requests for score adjustments or grade changes, regardless of how close a candidate may be to the passing threshold.
- This policy ensures fairness and maintains the integrity and value of the certification for all participants.

We understand that not achieving a passing score can be disappointing, especially when the margin is small. However, our commitment to maintaining the highest standards of certification integrity necessitates strict adherence to these grading policies. We encourage candidates who do not pass to use their score report to identify areas for improvement and to prepare thoroughly for any subsequent attempts.

5.1 Certification Decision

The certification decision process is initiated only after all requisites are met: mainly, the candidate must successfully pass the multiple-choice examination, and all required documentation must be submitted in full. Once these conditions are satisfied, the certification board commences its comprehensive review of the candidate's qualifications. The final certification decision, including the official exam results, will be completed within 14 business days from the start of this process, ensuring a thorough and timely evaluation.

This thorough review ensures that all aspects of your exam are evaluated accurately and fairly.

We are committed to maintaining a high standard of integrity and fairness in our examination process. Please review this section carefully to understand the regulations and expectations. Should you have any questions or require further clarification, our support team is available to assist you.

6 Support

We strive to provide comprehensive information to ensure a smooth certification process for all candidates. If you have any questions or need assistance, please consider the following resources:

1. **This Candidate Handbook**: Most queries are addressed within this document. We encourage you to review it thoroughly as your primary source of information.
2. **Exam Syllabus**: For detailed information about the content you can expect in the exam, please refer to the Certible® ISO/IEC 27001 Lead Auditor Syllabus [1]. This document outlines the specific topics, skills, and knowledge areas that will be assessed during the examination.
3. **Website**: For additional details and up-to-date information, please visit the Certible® Website[4].
4. **Direct Support**: At Certible®, we're committed to supporting you throughout your certification journey. If you have inquiries not covered in the handbook, syllabus, or on our website, or if you need further clarification, our support team is available to assist with any questions or concerns you may have, from your initial preparation to post-certification guidance.

   support@certible.com

   We aim to respond to all inquiries promptly and comprehensively.

Certification is not just about passing an exam — it's about gaining knowledge and skills that will enhance your professional capabilities. We're here to ensure that your certification experience is rewarding, challenging, and ultimately beneficial to your career growth.

[4] Certible® Website: https://www.certible.com

References

[1] ISO/IEC 27001 Lead Auditor Syllabus. Syllabus, Certible®, 2024. https://www.certible.com/certified/iso-iec-27001-lead-auditor/.

7 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

Copyright:
The contents of this handbook are copyrighted. The reproduction, editing, distribution and any kind of exploitation outside the limits of copyright require the written consent of the respective author or creator.

Last updated: 2024-07-29