CERTI-TRUST

CERTIFIED ISMS LEAD AUDITOR

Candidate Handbook

CERTITRUST
CONFIDENCE IN THE DIGITAL ERA

CANDIDATE MANUAL

DISTRIBUTION

The content of this document is public.

DISCLAIMER

This document has been prepared by CERTI-TRUST in respect of our policies and procedures for examination and certification activities. The purpose of the document is to present the candidate a fair and right, precise, honest and seamless information about the requirements of the related certification scheme. The content of this document applies to rules and guidelines to obey to in order to get easily certified against the claimed scheme. CERTI-TRUST does not warrant or otherwise comment upon the suitability of the contents of this document or its linked parts for any particular purpose or use. CERTI-TRUST accepts no liability whatsoever for consequences to, or actions taken by, third parties as a result of or in reliance upon information contained in this document.

TABLE OF CONTENT

1. ISO 27001 Lead Auditor Scheme Information

1.1. Scheme information

Scheme name:	ISO 27001 Lead Auditor
Scheme version:	2.1
Main scheme or sub-scheme	Main scheme

1.2. Who we are

Certi-Trust™ is the brand of International Certification Trust Services (ICTS), an international certification body auditing companies, professionals and technology products across a wide range of digital regulations and international standards. As a global supplier of specialized audit and certification services, Certi-Trust provides expertise in supporting digital evolution of enterprises in the field of Information Security, Cybersecurity, Business Continuity and infrastructure resilience, IT service management, critical infrastructure protection, ICT quality and environment management systems, digital risks, protection of citizens' personal and healthcare data with respect to their privacy.

Certi-Trust's main mission is to provide to organizations or individuals and all their interested parties with the assurance that they comply with the new challenges of digital transformation through smart and efficient certification services that bring the necessary confidence to all players of the digital world.

1.3. Introduction

The ISO/IEC 27000 family of standards helps organizations keep information assets secure.

Using this family of standards will help your organization manage the security of assets such as financial information, intellectual property, employee details or information entrusted to you by third parties.

Based on their competence within management systems, the ISO 27001 Lead Auditors are able to initiate, plan, execute and report information security audits and create detailed audit reports in accordance with ISO 27001. The lead auditor managers must be able to execute those activities as a sole lead auditor or as part of an information security audit team.

2. ISMS Lead Auditor

2.1. Why applying to this certification?

Globally recognized and demanded, the ISMS Lead Auditor certification demonstrates to employers, clients and colleagues that a professional possesses information security knowledge, experience and skills to carry out information security audits.
As the demand for skilled Lead Auditors who have an understanding on the importance of audit information security management systems in all types of business activities, the ability to successfully execute an Information Security Audit, create clear and concise audit reports and communicate the findings to management is at a critically urgent level, professionals who hold the ISMS LA certification are well positioned to provide the professional skills necessary to carry out audits related to information security management systems.
This certification recognizes the competence of an individual to perform in the role of an information security Lead Auditor. Year after year, the ISMS certification has garnered global recognition and commanded a higher salary for certified individuals over non-certified individuals.

2.2. Certification Requirements

In this chapter you will find all the requirements necessary to obtain the ISMS Lead Auditor Certificate, please be sure you fulfill them all before applying for certification.

Education

Applicants for certification should have completed at least secondary education (typically all the years full-time schooling prior to university entrance). Documented evidence of the education claimed will be required.

Professional Experience

Applicants for certification shall have at least 5 years full-time (or part time work that totals 4 years) work experience in a technical, professional or management position of accountability involving the exercise of judgement.
Applicants for certification shall provide documentary evidence of work experience; this evidence may be presented in the form of employer or any relevant professional references giving information on work actually carried out and positions held. As an alternative to the documentation requirement, the applicants can provide a signed self-declaration, giving information on work actually carried out and positions held.

Information Security Work Experience

Applicants for certification shall have a minimum of 2 years relevant experience in the implementation, operation, and/or relevant contribution in information security activities and processes, which provides the practical knowledge necessary to effectively perform such risk management activities, audit activities or implementation of an information security management system.

Training

Applicants for certification shall have completed any ISMS Lead Auditor training. Certi-Trust does not require the candidates to complete their own training as an exclusive prerequisite. The training shall cover the competence required for ISMS Lead Auditor in this scheme. A minimum of forty (40) hours training, including up to 15% homework, is required. Training can be performed by in-class courses, e-learning or other suitable learning methods.

Examination

You will need to pass the official Certi-Trust ISMS Lead Auditor exam (composed of two examination: 1 Foundation exam and 1 Auditor exam) and succeed it in order to apply for certification. The exam is based on the Scheme Competency Domains as described in point 2.3 of this chapter. All other considerations for exams can be found in Chapter 5.

Optional – Update to the new version of ISO 27001 (called 'bridge exam')

Optionnally, applicants could also attend the official Certi-Trust ISMS Bridge exam and shall be able to demonstrate the skills necessary for the effective and efficient performance of the information knowledge of an ISMS according to the requirements of ISO/IEC 27001:2022, which is the new version of the standard published on Oct. 31st of 2022, as well as by acknowledging the Certi-Trust Code of Ethics.

Personal Behaviour

Applicants for certification shall be able to demonstrate the personal behavior necessary for the effective and efficient performance of the information Lead Auditor activities as defined in ISO/IEC 27001:2013 - or ISO/IEC 27001:2022 -, as well as by acknowledging the Certi-Trust Code of Ethics.

2.3. ISMS Lead Auditor Scheme Competency Domains

The ISMS Lead Auditor Scheme Competencies are divided in the following 7 main domains:

1. Fundamental principles and concepts in information security
2. Information Security Management System (ISMS)
3. Fundamental Audit Concepts and Principles
4. Preparation of an ISO 27001 audit
5. Conduct of an ISO 27001 audit
6. Closing an ISO 27001 audit
7. Managing an ISO 27001 audit program
8. Optional – for ISO/IEC 27001:2022, knowledge of the gap with version 2013

2.4. Activities to be considered valid for application to this certification

The covered activities could likely include (non exhaustively):

- Conducting security audits to assess compliance with the organization policies, standards and procedures in alignment with the organization's objectives
- Conducting and assessing ongoing technical control validation activities such as application scans, configuration validation and network vulnerability scans
- Documenting security findings, and validates remediation has been completed
- Participating in internal security audits including field audits, foundation audits, service audits, management and process audits, and external audits
- Reporting on metrics to gauge effectiveness of the security policy framework and publishes periodic metrics reports
- Providing input into global security policies and standards to reflect the changing security threat landscape
- Identifying regulatory and technology changes that will affect information security policies, standards, and procedures, and recommend appropriate changes
- Managing the day-to-day security audit activities as required
- Training teams on security policies and standards as well as Information Security processes
- Providing knowledge sharing and technical assistance to other team members
- All other relevant activity that can demonstrated by the candidate to illustrate the knowledge and skills acquired in relation with the setup and the management of an ISMS in the realm of an organization.

3. General Information

3.1. Applying to a certification

Before applying to a certification you will need to pass and succeed the correspondant Certi-Trust exam for that scheme

If you wish to apply for one of Certi-Trust certification you should contact one of our partners, who provide training courses and exam sessions worldwide. To find an examination center in your region, please visit our website: https://www.certi-trust.com

All participants who successfully pass their certification exam will receive an email from examination@certi-trust.com attesting the result of their exam and the next steps they need to follow in order to apply for the correspondent certificate they applied to. The specific requirements mentionned in Chapter 3 need to be fullfilled to get the certificate granted. Candidates are requested to send all required information (incl. three professional references contact details) to certification@certi-trust.com.

In case you need further information you can contact at info.services@certi-trust.com or certification@certi-trust.com.

Once the Certification Manager validates that you fulfil all the certification requirements regarding the scheme you have applied to, your application will be validated. An email will be sent to the email address you provided during your application process to communicate your application status. If approved, you will receive a digital copy of your certificate.

3.2. Specific conditions for Application to this certification

Candidates must first pass the ISMS Foundation exam in order to be eligible for this certification. The Foundation and Auditor exams (leading together to the Lead Auditor designation) can be attended during the same session. However, if a candidate fails the Foundation exam and passes the Auditor, the candidate will not be directly eligible for the ISMS Lead Auditor Certificate and will have to pass the Foundation exam again for getting entitled to request the Lead Auditor professional designation.

If anyone would like to upgrade the certification to any newer versions of the standard (e.g. passing from v2013 to v2022), the candidate must pass an 'ISMS Bridge' exam in order to be eligible for requesting the updated designation. The exam and Auditor exam can be done on the same session, however, if the candidate fails the foundation exam and passes the Auditor the candidate will not be eligible for the ISMS Lead Auditor Certificate.

As per Certi-Trust exam policy, the first retake of any failed exam is free of charge.

4. Exam policies and procedures

4.1. Considerations for Examination

The ISO 27001 Auditor Exam is a 2 hours exam. The exam questions are relevant (covering all domains) and sufficient (100 questions) and cover all domains defined for the “ISO 27001 Lead Auditor” Certification. The exam questions are multiple-choice questions.

Two different sets of questions are available for each of the certification exams of which a different one has to be used at each occasion. A correction key document containing all correct answers of all questions/exams is available.

A minimum score of 60% is required to pass the ISO 27001 Auditor Exam

The evaluation grading will be according to the Control of examination grading process described in the “Exam Management Procedure”.

Education: All CERTI-TRUST certifications require the applicant to minimally hold a high school/secondary education diploma.

The standard method of examination is a paper-based exam presented in an affiliated examination center.

It may take some candidates less than the allowed two (2) hours to complete the examination, in such case the candidate is free to leave the examination center without taking anything outside of the examination area.

There are no scheduled breaks during the exam but candidates can ask for getting out to go to lavatories, one after the other, at invigilator’s discretion.

During the examination there will always be an impartial Invigilator approved by Certi-Trust who will survey the correct development of the exam; the Invigilator will be allowed to answer questions regarding the logistics of the exam but is not entitled neither competent to give explanations about the content of the exam itself.

Certi-Trust examination questions:

- are developed in accordance with ISO/IEC 17024 standard
- are developed and validated by global work groups of certification holders
- are referenced to current information security auditors activities
- are monitored through psychometric analysis

4.2. Content of the exam

Examination questions for ISMS Lead Auditor are divided by domains as follows:

ISMS Lead Auditor – Exam Content	
Questions thematics	Questions weighting
Domain 1	10%
Domain 2	15%
Domain 3	15%
Domain 4	15%
Domain 5	20%
Domain 6	10%
Domain 7	15%
Domain 8 (for ISO 27001 v2022)	Divided into the 7 previous domains

NB: In the 'ISMS bridge' exam, optional Domain 8 (see section 2.3) is not scored in itself. Questions about the addition brung by the new version of the international standard are divided into the 7 other domains, respecting the actual weighting defined for assessing the competences of the candidate towards the ISMS.

4.3. Certi-Trust Examination Security and Confidentiality

The examination, answer sheets, worksheets and/or any other test or test-related materials remain the sole and exclusive property of Certi-Trust. These materials are confidential and are not available for review by any person or agency for any reason, other than those related to accreditation.

Examination results are confidential and will not be disclosed to anyone without candidate consent, unless directed by valid and lawful court order. If you would like your examination results to be released to a third party, you must provide Certi-Trust with a written request that specifically identifies the types of details (e.g., examination date, pass/fail status, etc.) about the examination results that the third-party person or organization should receive.

When you submit an application, you agree to abide by Certi-Trust Certification Application/Renewal Agreement (found in this handbook) and the Code of Ethics

Any discussion of the examination questins would be a potential violation of the Certification Application/Renewal Agreement and thus, could affect the status of your certification, up to and including revocation of your certification or permanent suspension from any Certi-Trust certification examinations.

4.4. Examination Site Requirements & Instructions

In order to be admitted into the examination center, you must bring a valid and current (non-expired) form of government-issued identification. Your identification must include:

- English characters/translation
- your photograph
- your signature

If your government-issued identification does not display a photograph or a signature, a secondary form of identification may be used, which includes a photograph and/or signature (whichever is missing from the government-issued identification), and your name printed on the identification. All identification must be current (non-expired)

All forms of identification being presented at the testing center must match your name exactly as it appears on the scheduling notification. Your identification documents must be in good condition, and cannot be bent, frayed, taped, cracked or otherwise damaged in any way. The identification documents must be the originals, and cannot be photocopies. You will not be permitted to do the test if the name on your identification documents does not exactly match the name on your scheduling notification, or if your identification is damaged

If you do not provide the appropriate and/or matching identification, you will not be permitted to test.

The following are acceptable forms of government-issued identification:

- Valid driver's license
- Valid passport
- Valid national identification card

The following are acceptable forms of secondary identification:

- Valid credit card with signature
- Valid bank (ATM) card

4.5. Check-in procedure

On the day of your examination, please arrive a half hour before your scheduled appointment. You must sign in and present the required identification.

PROHIBITED from the Testing Center:

You may **NOT** bring anything or anyone into the testing area or to the desk where you take the exam. This includes, but is not limited to:

- Food, Drinks
- Coats
- Calculators
- Telephones, Smartphones, Smartwatches, Laptops or any other electronic device.
- Books, Notes, etc. (Unless the escpecific certification allows it).
- Any other personal items.

If you will require any personal items in the testing room due to a medical condition, such as food, beverages or medication, you will need authorization from Certi-Trust prior to scheduling your examination appointment. Please review our Special Accommodations procedure for additional information on obtaining authorization.

As an exeption, computers and laptops may be allowed if the examination center provides an online session of this exam. Conditions for these type of exams will be further notified.

4.6. Examination Results

All examination results are strictly confidential. Upon evaluation of your exam you will receive an email from examination@certi-trust.com stating whether you succeeded or failed the exam. In case the result is "fail", you could request for further information regarding the total percentage obtained and the percentage obtained for each domain, to better prepare for the retake of the examination.

If further information is required regarding your exam results, please contact us on: examination@certi-trust.com.

4.7. Retake Policy

Certi-Trust guarantees that, after a failure to the exam, it may be retaken within one year (year to date) after the reception of the results, free of charge. In case of any further retake, an examination fee could be applied.

To manage exam retakes (date, time, location, administrative cost by the evaluation center), candidate shall contact the Certi-Trust evaluation center with which the initial session has been organized.

5. Certification Rules

5.1. References & Experience Requirements

After a success to the related exam, Cert-Trust will issue an email to the candidate, requiring the following:

- The reference number attached to the exam completion attest.
- A professional resume, summarizing your experience in the field of risk management (minimum professional experience required is 3 years, including at least 1 year in the field of risk management for the designation of "Provisional Risk Manager", 5 years of professional experience including 2 years of experience in risk management for the designation of "Certified ISO 27001 Lead Auditor"
- Three contacts for professional references (email and phone numbers) that we will contact soon to counter check the skills, competences and experience you claimed for.

5.2. Certification Maintainance

This certification is non-transferable and valid for a period of three years from the date indicated on each individual certificate.

> NB: In case the candidate will have successfully passed an 'ISMS bridge' exam to update the version of the standard the candidate would like to be certified against, this will not extend the duration of the initial certificate previously obtained by the candidate. New certificate will be emitted with the same validity date than the one mentioned on the previously emitted certificate. Candidate will have therefore to maintain the certification the same way as it should have been done for the initial certification.

In order to maintain this certification over time, the candidate must however respect the following rules:

- To agree to comply with the professional code of ethics issued by Certi-Trust and available on our website at https://www.certi-trust.com/ethics.
- Record at least 120 continuing professional education (CPE) credits over the three years cycle of the certificate with a minimum of 20 annual credits. Following the passing of one or more Certi-Trust exams, the candidate receive a certain number of valid points for this program (for example, for a Foundation exam - 16 credits, for an Auditor exam - 24 credits).
- Send, at least 2 months before the end of your initial certification or on any request from our certification department, proofs of your continued training.

- If the candidate fails to fulfill one or more of these obligations, his/her certification may be downgraded, suspended or even canceled, as the case may be.

Please refer to our certification policy available on the Certi-Trust website.

Note, however, that unlike other certification bodies, **Certi-Trust does not currently charge any annual fees for maintaining certification.** This is one of the guarantees that we offer to the public in order to make certification democratic and accessible to all professionals, worldwide.

5.3. Certification issuance, suspension, withdrawal and renewal

For all information regarding Certi-Trust procedure for Certification issuance, suspension, withdrawal and renewal, please visit our website: www.certi-trust.com

5.4. Certification Updates & Upgrades

When any change occurs in the certification scheme which requires additional assessment, Certi-Trust will document it and publish the changes on our website, including the specific methods and mechanism required to verify that certified persons comply with changed requirements.

6. Appendices:

6.1. Our Code of Ethics

Ethics is about making the best possible decisions concerning people, resources and the environment. Ethical choices diminish risk, advance positive results, increase trust, determine long term success and build reputations. Leadership is absolutely dependent on ethical choices.

Certi-Trust members have determined that honesty, responsibility, respect and fairness are the values that drive ethical conduct for the Risk Manager. Certi-Trust's Code of Ethics applies those values to the real-life practice, where the best outcome is the most ethical one.

All Certi-Trust members, volunteers, certification holders and certification applicants must comply with this Code.

The full version of our Code of Ethics can be downloaded from this link:

https://www.certi-trust.com/ethics

7. General information

7.1. Contact

For information about the application process, examination or certification process, please contact us at:

info.services@certi-trust.com

7.1. Website

You can find additional information on our website:

www.certi-trust.com