CERTI-TRUST

CERTIFIED ISO 27005 RISK MANAGER

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 27005 Risk Manager Scheme Information

1.1. Scheme information

Scheme name:	ISO 27005 Risk Manager
Scheme version:	1.0
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 27005 Risk Managers are able to initiate, plan, execute and report risk assessments and risk treatment activities within an information security management system in accordance with ISO 27005. The risk managers must be able to execute those activities as a sole risk manager or as a member of risk management team.

2. Certification Overview and pricing

2.1. Pricing

Certi-Trust offers several global certifications that cover a variety of practitionner, implementer and audit specialties, including public information security management, risk management, personal data protection and others. Information and pricing for the ISO 27001 & ISO 27005 schemes is provided in the table below:

Certification	Price Zone A[1]	Price Zone B[2]
ISO 270001 Foundation	300 EUR	200 EUR
ISO 270001 Lead Implementer	500 EUR	350 EUR
ISO 270001 Lead Auditor	500 EUR	350 EUR
ISO 270005 Risk Manager	350 EUR	240 EUR

[1] Zone A: Economic European Area, United States of America, Canada, Australia, Ukraine, Russia, Saudi Arabia, South Africa, Japan
[2] Zone B: All other countries

2.2. Eligibility Requirements

To obtain and maintain a Certi-Trust certification, you must meet all program requirements: meet eligibility requirements, maintain exam confidentiality, adhere to Certi-Trust Code of Ethics, obtain the required continuing professional education (CPE), and meet all other conditions of the program. Proof of identification (ID) is also required.

Familiarize yourself with the eligibility requirements for your selected program to ensure you qualify and agree to the program's terms and conditions. Eligibility requirements cover the following four areas:

- Education.
- Ethics.
- Examinations.
- Experience.

Education

Generally, post-secondary education is required for Certi-Trust certification programs. However, if you do not meet the minimum education requirements, Certi-Trust offers an alternate pathway for experienced professionals on the domain of certification to become eligible for certification programs. Please refer to Chapter 3 for the specific requirements for this certification.

Ethics

To obtain a Certi-Trust certification, you must exhibit high moral and professional character and agree to abide by Certi-Trust's Code of Ethics. A character reference form signed by your supervisor, teacher or colleague might be required.

Examination

You must successfully complete all examinations for your certification program before earning a certified status.

Experience

Although work experience is required to become certified, you may apply to the certification program and sit for exams prior to obtaining the requisite work experience. However, you will not be certified until all program requirements have been met. Additionally, you must meet the experience requirement within the program eligibility period of three years in order to receive your certification. Work experience for Certi-Trust's certification programs is based on the maximum level of education achieved, as indicated in Chapter 3.

3. ISO 27005 Risk Manager

3.1. Why applying to this certification?

Globally recognized and demanded, the ISO 27005 Risk Manager certification demonstrates to employers, clients and colleagues that professional possesses information security knowledge, experience and skills to carry out information security audits.

As the demand for skilled Risk Managers who have an understanding on the importance of managing Information related risks in all types of business activities, the ability to successfully execute an Information Security risk assessment, create clear and concise risk reports and communicate the findings management is at a critically urgent level, professionals who hold the ISO 27005 RM certification are well positioned to provide the professional skills necessary to mangerisks related to information security.

This certification recognizes the competence of an individual to perform in the role of an information security Risk Manager. Year after year, the ISO 27005 certification has garnered global recognition and commanded a higher salary for certified individuals over non-certified individuals.

3.2. Certification Requirements

In this chapter you will find all the requirements necessary to obtain the ISO 27005 Risk Manager 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. As an alternative, applicants may be considered for certification if they can document 10 years full time work experience and satisfy the PCB that they have achieved a satisfactory level of knowledge relevant to Information Security Risk Management Systems.

Professional Experience

Applicants for certification for all grades with post-secondary education degree shall have at least 4 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. This period shall be increased to 5 years for applicants with secondary education. 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.

Risk Management 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 risk management activities and processes, which provides the practical knowledge necessary to effectively perform such risk management activities.

Training

Applicants for certification shall have completed ISO 27005 Practitioner 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 ISO 27005 Risk Manager in this scheme. A minimum of forty (40) hours training 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 ISO 27005 Risk Manager exam and succeed it in order to apply for certification. The exam is based on the Scheme Competency Domains as described in point 3.3 of this chapter.

All other considerations for exams can be found in Chapter 5.

Personal Behaviour

Applicants for certification shall be able to demonstrate the personal behavior necessary for the effective and efficient performance of the information security risk management activities as defined in ISO/IEC 27005:2018 as well as by acknowledging the Certi-Trust Code of Ethics.

3.3. Scheme Competencies Domains

The ISO 27005 Risk Manager Scheme Competencies are divided in the following three main domains:

1. Concepts, methods and information security risk management techniques
2. Information security risk identification, analysis, evaluation and reporting based on ISO 27005
3. Setup, deployment, maintenance and correction of a corporate information security risk management framework

In the section below you will find a detailed explanation of which competencies are required to master and the knowledge statements needed to pass the exam and apply to a certification.

Domain 1: Concepts, methods and information security risk management techniques

Main objective: The ISO 27005 Risk Manager applicant will understand, adequately manipulate and know how to handle basic concepts and guidelines articulated on a risk management approach based on ISO 27005.

Competencies	Knowledge statements
1. Understanding and explaining the different risk management standards, methods and approaches	1. Knowledge of the application of ISO management principles to information security risk management
2. Being skilled in illustrating the basic concepts in information security risk management	2. Knowledge of the different issues and sources of risk management in an organization: legal, regulatory, normative, contractual, competitional, internal
3. Being able to identify, analyze and evaluate information security risks in any organization	3. Knowledge of the different standards, methods and approaches in risk management
4. Mastering the relationships between the concepts of informational asset, threat, vulnerability, consequences and security controls from ISO 27005 - Appendix A	4. Knowledge of the main information security concepts and terminology as described in Guide 73 and other glossary of terms, like ISO 27000
5. Being able to know and to explain differences between information and data protection	5. Knowledge of the concept of risk and its application in information security
6. Being able to discriminate, with examples, the differences between ISO 27005 and ISO 31000 or ISO 27005.	6. Knowledge of the relationship between the concepts of informational asset, threat, vulnerability, consequences and security controls from ISO 27005
	7. Knowledge of relationship and main differences between ISO 27005, ISO 31000 and ISO 27005.

Domain 2: Information security risk identification, analysis, evaluation and reporting based on ISO 27005

Main objective: The ISO 27005 Risk Manager applicant will be able to perform the different actions required in a risk assessment based on the guidance of ISO 27005.

Competencies	Knowledge statements
1. Being able to manage Information Security Risk Management processes in relation with ISO 27005 2. Being able to identify and select appropriate risk assessment methodologies for different purposes 3. Being able to select the right risk assessment approach in a specific organizational context 4. Being able to design and schedule risk assessment activities and integrate them appropriately into a risk management strategy 5. Being able to control risk assessment projects and to lead a risk assessment team	1. Knowledge of the risk management guidelines and common processes used into an ISO 27005 risk management approach 2. Knowledge of the main information security risk assessment methods. 3. Ability to plan risk assessment projects and inclusion of relevant stakeholders throughout the whole assessment process 4. Knowledge of the guidelines and best practices to design and schedule risk assessment activities and integrate them appropriately into a risk management strategy 5. Knowledge of the best practices on how to manage a risk-based project 6. Ability to run multidisciplinary risk-based projects and team leading.

Domain 3: Setup, deployment, maintenance and correction of a corporate information security risk management framework

Main objective: The ISO 27005 Risk Manager applicant will be able to master the several processes included in an information security risk management program based on ISO 27005.

Competencies	Knowledge statements
1. Dealing with roles and responsibilities designation while setting up and managing a risk management program	1. Knowledge of the roles and responsibilities of the key actors during the implementation of an risk management framework and in its operation after the end of the implementation project
2. Being able to define the necessary documentation to support the setup and the daily operations of a risk management program	2. Knowledge of the main organizational structures applicable for an organization to manage its risk
3. Being able to create adequate policies and procedures for risk management and assessment	3. Knowledge of the best practices on document and record management processes and the document management life cycle
4. Being able to design controls & processes and to document them adequately	4. Knowledge of the characteristics and the differences between the different documents related to policy, procedure, guideline, standard, baseline, worksheet, etc.
5. Being able to set the right information security risk processes up	5. Knowledge of model-building controls and processes techniques and best practices
6. Being able to operationalize a risk framework and to manage its related changes	6. Knowledge of controls and processes deployment techniques and best practices
7. Being able to identify educational needs and to deploy adequate training, awareness and education plans	7. Knowledge of techniques and best practices to write policies, procedures and others types of documents
8. Being able to seamlessly communicate about the assessed and treated risks	8. Knowledge of the characteristics and the best practices to implement risk management training, awareness and communication plans
9. Being able to design and to appropriately follow up on information security incidents as sources of risks	9. Knowledge of the characteristics and main processes of an information security risk management incident management process based on best practices
	10. Knowledge of change management techniques best practices

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

The covered activities could likely include (non exhaustively):

- planning, designing and implementing an overall risk management process for the organisation
- risk assessment, which involves analysing risks as well as identifying, describing and estimating the risks affecting the information security
- risk evaluation, which involves comparing estimated risks with criteria established by the organisation such as costs, legal requirements and environmental factors, and evaluating previous handling of risks
- establishing and quantifying the organisation's 'risk appetite', i.e. the level of risk they are prepared to accept
- risk reporting in an appropriate way for different audiences, for example, to the board of directors so they understand the most significant risks, to business heads to ensure they are aware of risks relevant to their parts of the business and to individuals to understand their accountability for individual risks
- information security governance involving external risk reporting to stakeholders
- carrying out processes such as advising for the purchase of insurance, implementing security measures or physical security measures and making business continuity plans to limit risks and prepare for if things go wrong
- conducting assessments of policy and compliance to standards, including liaison with internal and external auditors
- providing support, education and training to staff to build risk awareness within the organisation.

4. General Information

4.1. 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.

4.2. Specific conditions for Application to this certification

Out of the certification conditions presented in Chapter 3.2, there's no additional conditions for applicants to have any prerequisite to apply to this certification.

5. Exam policies and procedures

5.1. Considerations for Examination

The ISO 27005 Risk Manager examination is comprised of short-essay questionnaires. Questions are based on situational cases asking for an argumented answer (no “yes-no” answer) with development.

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

The time allowed to complete the examination is two (2) hours.

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 risk managers activities
- are monitored through psychometric analysis

5.2. Content of the exam

Examination questions for ISO 27005 Risk Manager are divided by domains as follows:

ISO 27005 Risk Manager – Exam Content	
Questions thematics	Questions weighting
1. Information security risk management governance	10%
2. Information security measures against risks	15%

3. Assets, threats, vulnerabilities, consequences, controls + risk treatment	30%
4. Risk assessment activities	15%
5. Risk treatment option selection	20%
6. Risk surveillance and communication	10%

5.3. 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 Certu-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.

5.4. 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

5.5. 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.

5.6. 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.

5.7. 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.

6. Certification Rules

6.1. 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 27005 Risk Manager"
- 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.

6.2. 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

6.3. 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.

7. Appendices:

7.1. 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

7.2. Other certifications

	List of recognized certifications at CERTI-TRUST
27K1FD	Certified ISO 27001 Foundation[1]
27K1LI	Certified ISO 27001 Lead Implementer[1]
27K1LA	Certified ISO 27001 Lead Auditor[1]
BCMSFD	Certified ISO 22301 Foundation3
BCMSLI	Certified ISO 22301 Lead Implementer[3]
BCMSLA	Certified ISO 22301 Lead Auditor[3]
27K5RM	Certified ISO 27005 Risk Manager[1]
31KERM	Certified ISO 31000 Risk Manager
GDPRFD	Certified GDPR Foundation[2]
CERDPO	Certified Data Protection Officer[2]
CYBMGR	Certified Cybersecurity Manager
PENMGR	Certified Pentest Manager[3]
CLOMGR	Certified Cloud Security Manager[3]
CAPSLI	Certified Application Security Lead Implementer[3]

[1] *Examinations and certifications under review for an international accreditation.*
[2] *Examinations and certifications under review for a European accreditation.*
[3] *Examinations and certifications issued by ICTS with InterDigicert Alliance.*

8. General information

8.1. Contact

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

info.services@certi-trust.com

8.1. Website

You can find additional information on our website:

www.certi-trust.com