CERTIFICATION SYLLABUS

ISO/IEC 27001: Information Security Risk Manager

Exam Code: CSRM™



A complete preparation guide covering exam objectives, core competencies, domain weightage, and topics to prepare.

©2026 Certaining, Inc. All rights reserved.

Table of Contents

1. **Exam Name & Code** 1
2. **Table of Contents** 2
3. **Objective of the Certification** 3
4. **Core Competencies** 4-5
5. **Who Should Take This Certification** 6
6. **Exam Information** 6
7. **Examination Domain & Weightage** 7
8. **Topics to Prepare** 8-9
   - *Risk Management Principles & ISO/IEC 27001 Context*
   - *Risk Identification: Assets, Threats & Vulnerabilities*
   - *Risk Analysis & Evaluation*
   - *Risk Treatment, Controls & Statement of Applicability*
   - *Risk Acceptance, Communication & Governance*
   - *Monitoring, Review & Continual Improvement*
   - *Third-Party, Cloud & Emerging Risk Scenarios*

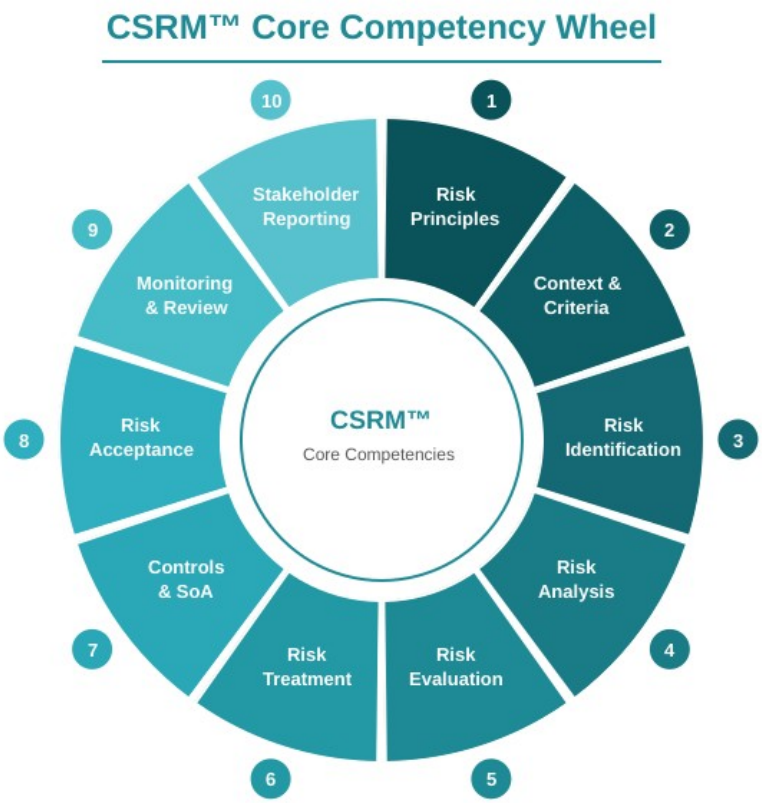
©2026 Certaining, Inc. All rights reserved.

Objective of the Certification

- **Validate risk management competence:** the ability to plan, perform, and manage information security risk assessment and treatment for an ISMS based on ISO/IEC 27001.
- **Apply the standards together:** use ISO/IEC 27001:2022 (clauses 6.1.2, 6.1.3, 8.2, 8.3), ISO/IEC 27005, and ISO 31000 consistently.
- **Establish risk criteria:** define risk acceptance criteria and criteria for performing risk assessments that align with business objectives.
- **Identify risks:** identify assets, threats, vulnerabilities, and risk scenarios, using asset-based and event-based approaches.
- **Analyze and evaluate risks:** estimate likelihood and consequences, determine risk levels, and prioritize risks against the criteria.
- **Select risk treatment options:** choose among modifying, retaining, avoiding, and sharing risk, and justify the choice.
- **Link risk to controls:** determine necessary controls, compare them with ISO/IEC 27001 Annex A, and produce the Statement of Applicability.
- **Manage risk ownership and acceptance:** obtain risk owner approval of treatment plans and acceptance of residual risks.
- **Communicate and report risk:** consult stakeholders and report risks and decisions clearly to management.
- **Monitor and improve:** review risks, indicators, and the risk process to drive continual improvement.

©2026 Certaining, Inc. All rights reserved.

Core Competencies — CSRM™ (ISO/IEC 27001: Information Security Risk Manager)



©2026 Certaining, Inc. All rights reserved.

- **Risk management principles:** explain the principles, framework, and process of ISO 31000 and how they support ISO/IEC 27001 and ISO/IEC 27005.
- **Context and criteria:** establish the scope, context, risk criteria, and risk acceptance criteria for information security risk management.
- **Risk identification:** identify assets, owners, threats, vulnerabilities, and risk scenarios.
- **Risk analysis:** estimate likelihood and consequences using qualitative, semi-quantitative, and quantitative methods.
- **Risk evaluation:** compare risk levels with criteria and prioritize risks for treatment.
- **Risk treatment:** select and justify risk treatment options and prepare a risk treatment plan.
- **Controls and SoA:** determine necessary controls, use ISO/IEC 27001 Annex A, and prepare the Statement of Applicability.
- **Risk acceptance and ownership:** assign risk owners and obtain approval of treatment plans and residual risk acceptance.
- **Monitoring and review:** track risks, indicators, incidents, and changes, and review the effectiveness of treatment.
- **Communication and reporting:** consult stakeholders and keep risk records and reports clear, consistent, and useful.

©2026 Certaining, Inc. All rights reserved.

Who Should Take This Certification

- Information security, ISMS, and risk managers responsible for ISO/IEC 27001 risk assessment and treatment.
- Risk, compliance, and GRC professionals working with information security risk.
- ISMS coordinators, security officers, and IT managers who maintain the risk register and the Statement of Applicability.
- Consultants and implementers supporting organizations preparing for ISO/IEC 27001 certification.
- Internal auditors and security professionals who want to understand and evaluate risk methodologies.
- Professionals who want a career in information security risk management or governance, risk, and compliance.

Exam Information

Exam Name	ISO/IEC 27001: Information Security Risk Manager
Exam Code	CSRM™
Exam Format	Multiple Choice Questions (MCQ), including scenario-based questions
Duration	90 minutes
Number of Questions	60
Passing Score	70%
Mode of Exam	Test Center Based Testing / Online Testing
Language	English
Validity	Lifetime
Open Book	No

©2026 Certaining, Inc. All rights reserved.

Examination Domain & Weightage

Domain	Weightage
Risk Management Principles & ISO/IEC 27001 Context	15%
Risk Identification: Assets, Threats & Vulnerabilities	20%
Risk Analysis & Evaluation	20%
Risk Treatment, Controls & Statement of Applicability	20%
Risk Acceptance, Communication & Governance	10%
Monitoring, Review & Continual Improvement	10%
Third-Party, Cloud & Emerging Risk Scenarios	5%
Total	**100%**

©2026 Certaining, Inc. All rights reserved.

Topics to Prepare — CSRM™ (ISO/IEC 27001: Information Security Risk Manager)

The topics below represent the core areas candidates should focus on for each domain, reflecting the risk management depth expected at the CSRM™ level.

1. Risk Management Principles & ISO/IEC 27001 Context (15%)

- **Risk concepts:** risk, threat, vulnerability, consequence, likelihood, control, residual risk, and risk owner.
- **ISO 31000:** principles, framework, and process, including communication, monitoring, and recording.
- **ISO/IEC 27001 risk requirements:** clauses 6.1.2 (risk assessment), 6.1.3 (risk treatment), 8.2, and 8.3.
- **ISO/IEC 27005:** the guidance on the risk management process, and the asset-based and event-based approaches.
- **Context:** internal and external issues, interested parties, and the scope of the ISMS (clause 4).
- **Roles:** top management, risk owners, asset owners, and the risk manager.

2. Risk Identification: Assets, Threats & Vulnerabilities (20%)

- **Assets:** information, systems, processes, people, and suppliers, and their owners.
- **Threats:** deliberate, accidental, and environmental threats, and sources of threat information.
- **Vulnerabilities:** technical, organizational, physical, and human weaknesses.
- **Risk scenarios:** describing the event, the threat, the vulnerability, and the consequences.
- **Information security properties:** confidentiality, integrity, and availability, and their link to consequences.
- **Change and new initiatives:** identifying risks from projects, remote work, new technology, and organizational change.

3. Risk Analysis & Evaluation (20%)

- **Risk criteria:** scales for likelihood and consequences, and criteria for performing assessments.
- **Methods:** qualitative, semi-quantitative, and quantitative approaches, and their limits.
- **Likelihood and consequences:** factors such as threat capability, exposure, control strength, and impact categories.
- **Quantitative basics:** single loss expectancy, annual rate of occurrence, and annual loss expectancy.

©2026 Certaining, Inc. All rights reserved.

- **Inherent and residual risk:** risk before and after controls, and how each is used.
- **Evaluation:** comparing risk with criteria, prioritizing risks, and consistency of results (clause 6.1.2).

4. Risk Treatment, Controls & Statement of Applicability (20%)

- **Treatment options:** risk modification, retention, avoidance, and sharing.
- **Control selection:** determining necessary controls from any source and comparing them with Annex A.
- **Annex A:** the 93 controls in four themes: organizational, people, physical, and technological.
- **Statement of Applicability:** controls included, implementation status, and justifications for inclusion and exclusion.
- **Risk treatment plan:** owners, actions, resources, and time frames.
- **Control types:** preventive, detective, and corrective controls, and balancing cost and benefit.

5. Risk Acceptance, Communication & Governance (10%)

- **Risk acceptance:** acceptance criteria, authority levels, and documented decisions.
- **Residual risk:** approval by risk owners and acceptance of residual risks.
- **Communication and consultation:** engaging stakeholders throughout the risk process.
- **Risk appetite and tolerance:** how they guide criteria and decisions.
- **Documented information:** retaining results of risk assessment and treatment.

6. Monitoring, Review & Continual Improvement (10%)

- **Monitoring and review:** detecting changes in threats, vulnerabilities, assets, and controls.
- **Key risk indicators:** indicators that signal changes in risk exposure.
- **Reassessment:** performing assessments at planned intervals and when significant changes occur (clause 8.2).
- **Management review and audit:** risk-related inputs and internal audit of the risk process.
- **Lessons learned:** using incidents and audit results to improve methods and criteria.

7. Third-Party, Cloud & Emerging Risk Scenarios (5%)

- **Supplier and cloud risk:** dependency, shared responsibility, contracts, and assurance.
- **Outsourcing:** retained accountability for risks that are outsourced.
- **Emerging risks:** new technology and threats, and how to assess uncertain risks.
- **Business continuity link:** relationship between risk assessment and continuity planning.

©2026 Certaining, Inc. All rights reserved.