CERTIFICATION SYLLABUS

ISO/IEC 27001: Information Security Executive

Exam Code: CISE™



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
   - *Information Security Governance & Strategy*
   - *ISMS Leadership & Management Responsibilities*
   - *Enterprise Risk Management & Risk Appetite*
   - *Compliance, Legal, Regulatory & Privacy*
   - *Security Programs, Investment & Third-Party Management*
   - *Incident, Crisis & Business Continuity Leadership*
   - *Security Culture, Metrics & Executive Reporting*

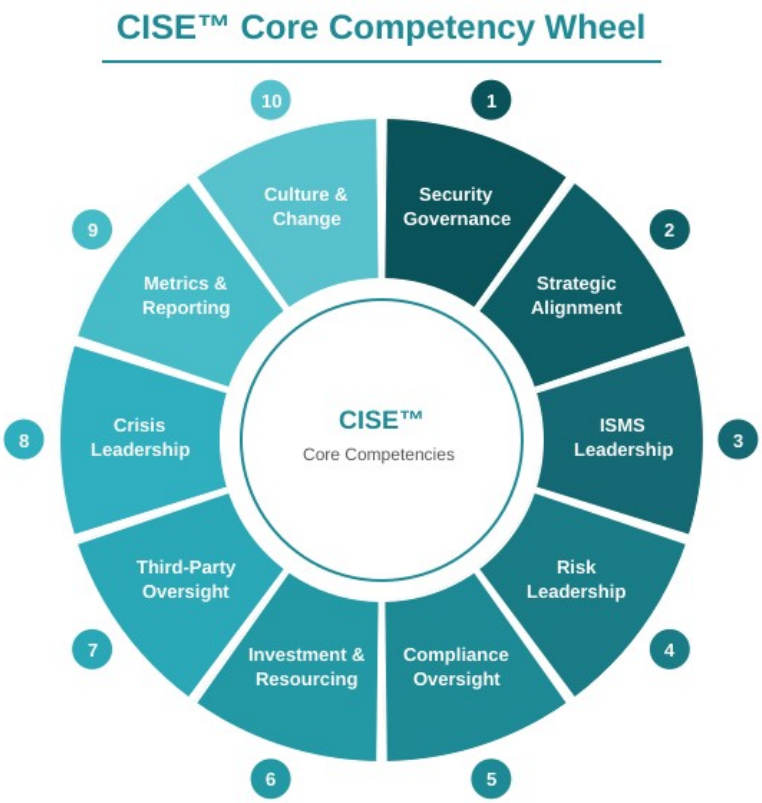
©2026 Certaining, Inc. All rights reserved.

Objective of the Certification

- **Validate executive-level security leadership:** the ability to govern, direct, and be accountable for information security at the senior management and board level.
- **Align security with business strategy:** connect information security objectives to business goals, value creation, and risk appetite.
- **Provide ISMS leadership:** fulfil top management responsibilities under ISO/IEC 27001, including policy, resources, roles, and management review.
- **Govern information security:** apply governance principles, such as those in ISO/IEC 27014, covering accountability, oversight, and decision-making.
- **Lead enterprise risk decisions:** set risk appetite, review risk treatment, and make informed risk acceptance decisions.
- **Oversee compliance and privacy:** understand legal, regulatory, and contractual obligations and how they shape the security program.
- **Direct security investment:** prioritize budgets and resources, evaluate business cases, and manage suppliers and third-party risk.
- **Prepare for crisis leadership:** direct incident response, crisis communication, and business continuity at the executive level.
- **Report with clarity:** use meaningful metrics and communicate security performance and risk to boards and stakeholders.
- **Build a security culture:** lead a culture of accountability, awareness, and continual improvement across the organization.

©2026 Certaining, Inc. All rights reserved.

Core Competencies — CISE™ (ISO/IEC 27001: Information Security Executive)



©2026 Certaining, Inc. All rights reserved.

- **Security governance:** establish governance structures, roles, and accountabilities for information security.
- **Strategic alignment:** link the security strategy to business objectives and communicate its value.
- **ISMS leadership:** carry out top management responsibilities under ISO/IEC 27001, including management review.
- **Risk leadership:** define risk appetite, evaluate risk treatment options, and make or review risk acceptance decisions.
- **Compliance oversight:** monitor legal, regulatory, contractual, and privacy obligations and the evidence of compliance.
- **Investment and resourcing:** build business cases, allocate resources, and assess the return on security investment.
- **Third-party oversight:** manage supplier and cloud risks through governance, contracts, and assurance.
- **Crisis leadership:** lead decision-making during major incidents, and oversee continuity and recovery.
- **Metrics and reporting:** select outcome-based security metrics and report to the board and executive committees.
- **Culture and change:** foster security awareness, accountability, and continual improvement.

©2026 Certaining, Inc. All rights reserved.

Who Should Take This Certification

- Chief Information Security Officers (CISOs) and security directors.
- CIOs, CTOs, and technology and digital leaders accountable for security.
- Board members, executives, and senior managers responsible for risk and governance.
- Heads of risk, compliance, audit, and privacy functions.
- ISMS owners and security managers moving into leadership roles.
- Professionals who have completed credentials such as CSIA™, CSLA™, or a risk management credential and want to advance.

Exam Information

Exam Name	ISO/IEC 27001: Information Security Executive
Exam Code	CISE™
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
Information Security Governance & Strategy	20%
ISMS Leadership & Management Responsibilities	15%
Enterprise Risk Management & Risk Appetite	15%
Compliance, Legal, Regulatory & Privacy	10%
Security Programs, Investment & Third-Party Management	10%
Incident, Crisis & Business Continuity Leadership	15%
Security Culture, Metrics & Executive Reporting	15%
Total	**100%**

©2026 Certaining, Inc. All rights reserved.

Topics to Prepare — CISE™ (ISO/IEC 27001: Information Security Executive)

The topics below represent the core areas candidates should focus on for each domain, reflecting the executive-level depth expected at the CISE™ level.

1. Information Security Governance & Strategy (20%)

- **Governance principles:** accountability, oversight, direction, evaluation, and monitoring.
- **Governance structures:** boards, steering committees, and security roles.
- **Security strategy:** aligning with business strategy, objectives, and risk appetite.
- **Policy framework:** how policies, standards, and procedures are set and approved.
- **Value and outcomes:** demonstrating the contribution of security to the business.
- **Related guidance:** ISO/IEC 27014 on the governance of information security.

2. ISMS Leadership & Management Responsibilities (15%)

- **Top management duties under ISO/IEC 27001:** policy, objectives, resources, and integration of the ISMS into business processes.
- **Roles and responsibilities:** assigning authority for the ISMS and information security.
- **Management review:** inputs, outputs, and decisions.
- **Continual improvement:** driving improvement from audits, incidents, and review results.
- **Certification and assurance:** the executive's role in internal and external audits.

3. Enterprise Risk Management & Risk Appetite (15%)

- **Risk appetite and tolerance:** defining and communicating them.
- **Information security risk assessment:** results, treatment options, and residual risk.
- **Risk acceptance:** authority, criteria, and documentation.
- **Integrating security risk into enterprise risk:** consistent reporting and escalation.
- **Emerging risks:** technology change, threats, and strategic risk scenarios.
- **Related guidance:** ISO/IEC 27005 and ISO 31000.

4. Compliance, Legal, Regulatory & Privacy (10%)

- **Compliance obligations:** legal, regulatory, contractual, and sector-specific requirements.
- **Privacy and data protection:** executive accountability and links to privacy management.
- **Assurance:** audits, certifications, and monitoring evidence of compliance.
- **Breach obligations:** reporting duties and communication with regulators.

©2026 Certaining, Inc. All rights reserved.

- **Related guidance:** the role of ISO/IEC 27701 in privacy management.

5. Security Programs, Investment & Third-Party Management (10%)

- **Business cases:** costs, benefits, and risk reduction for security investments.
- **Prioritization and budgeting:** allocating resources by risk and value.
- **Security program management:** roadmaps, projects, and benefits tracking.
- **Supplier and cloud risk:** due diligence, contracts, and assurance.
- **Resourcing and capability:** teams, skills, and sourcing models.

6. Incident, Crisis & Business Continuity Leadership (15%)

- **Incident management oversight:** readiness, escalation, and executive decision-making.
- **Crisis communication:** messaging for customers, staff, regulators, and media.
- **Business continuity and recovery:** objectives, plans, and testing.
- **Learning from incidents:** post-incident review and organizational improvement.
- **Related guidance:** ISO/IEC 27035 on incident management and ISO 22301 on business continuity.

7. Security Culture, Metrics & Executive Reporting (15%)

- **Security culture:** leadership behaviors, awareness, and accountability.
- **Metrics and KPIs:** outcome-based measures instead of activity counts.
- **Board and executive reporting:** concise, risk-focused reporting.
- **Communicating with non-technical stakeholders:** clear language and decision-ready information.
- **Continuous improvement and maturity:** benchmarking, assessments, and roadmaps.

©2026 Certaining, Inc. All rights reserved.