GRC CAREERS

GRC CAREERS · REFERENCE LIBRARY

CISM

Certified Information Security Manager

Certification Reference & Study Guide

VOLUME I

ISACA · Senior-Level Certification · Verified 2026-07-28

OVERVIEW

What CISM Is

CISM is a management-focused cybersecurity credential for professionals responsible for security governance, enterprise risk, security programs and incident management. It is especially relevant for security managers, GRC leaders and professionals preparing for director or CISO-level responsibilities.

CISM certifies that you can build, lead and defend an enterprise information security program. The exam is written from the point of view of the manager who owns the outcome rather than the engineer who implements a single control, so most questions ask what a responsible leader should evaluate, decide or escalate first.

The credential sits at the governance and program layer of security work. It assumes you already understand the technology and asks whether you can align it with business objectives, fund it, staff it, measure it and answer for it when something goes wrong.

Exam at a Glance

Questions	**150 (Multiple choice. ISACA exams are made up of scored items plus unscored pretest items, so not every question counts toward your result.)**
Duration	**4 hours**
Format	**Multiple choice**
Passing scale	**450 on a scaled range of 200 to 800 — The scaled score is not a percentage of correct answers. Domain-level results on your score report are informational only and are not used to decide whether you pass.**
Exam fee	**Member USD575 · Non-member USD760**
Application fee	**USD50 — A one-time certification application fee, paid by members and nonmembers alike when you apply for certification after passing. It is not part of the exam fee.**
Eligibility window	**Registration opens a 12-month window in which to sit the exam. Retakes carry waiting periods of 30 days after the first attempt and 90 days after each attempt that follows.**
Delivery	**Computer-based, at an authorized PSI test center or remotely proctored online**
Experience required	**Five years of information security management work experience, across at least three of the four CISM domains.**
Maintenance	**20 CPE/yr, 120 over 3 yrs**
Annual fee	**Member USD45 · Non-member USD85**

EXAM CONTENT

The Four Domains

1 Information Security Governance — 17%

Establishes the authority, direction and accountability that a security program runs on. This domain is about who decides, on what basis, and how that direction reaches the rest of the organization.

- Governance frameworks and operating models
- Information security strategy and its alignment to business objectives
- Organizational roles, responsibilities and accountability
- Policies, standards and supporting documentation
- Legal, regulatory and contractual requirements
- Risk appetite and risk tolerance
- Executive and board reporting

2 Information Security Risk Management — 20%

Covers how risk is found, sized, treated and monitored over time. The management emphasis is on ownership and defensible decisions rather than on producing the most elaborate calculation.

- Risk identification and threat and vulnerability analysis
- Risk assessment and risk analysis methods
- Risk treatment options and selection
- Risk ownership and accountability
- Risk acceptance and formal exceptions
- Inherent risk and residual risk
- Risk monitoring, reporting and escalation

3 Information Security Program — 33%

The largest domain. It covers building and running the program itself: the roadmap, the resources, the controls, the third parties and the evidence that any of it is working.

- Program development and operating structure
- Program roadmaps and prioritization
- Resource, budget and staffing management
- Security control selection and implementation
- Metrics, measurement and management reporting
- Third-party and supply-chain risk
- Security awareness and training
- Cloud and emerging-technology considerations
- Program maturity and continuous improvement

4 Incident Management 30%

Covers readiness, response and recovery. Expect questions that test sequencing and priority under pressure, and that separate the manager's job from the responder's job.

- Incident-management planning and readiness
- Detection and analysis
- Classification and escalation
- Containment, eradication and recovery
- Crisis communication and stakeholder notification
- Business continuity planning
- Disaster recovery
- Post-incident review and lessons learned

STUDY GUIDE

Core Concepts to Master

The CISM exam is designed to test management judgment. Candidates should evaluate questions from the perspective of the person responsible for governing risk, directing a security program and protecting the organization's business objectives.

Governance

[object Object]

Risk Management

[object Object]

Frameworks

- {"name":"NIST Cybersecurity Framework","managementUse":"A common language for describing security outcomes and reporting maturity to non-specialists."}
- {"name":"NIST Risk Management Framework","managementUse":"A structured process for categorizing systems, selecting controls and authorizing them for operation."}
- {"name":"ISO/IEC 27001","managementUse":"A certifiable management-system standard, useful where customers or regulators want independent assurance."}
- {"name":"COBIT","managementUse":"Governance and management of enterprise IT, including how objectives cascade into accountability."}
- {"name":"ITIL","managementUse":"Service-management practice, relevant where security depends on change, incident and problem processes."}
- {"name":"COSO","managementUse":"Internal control and enterprise risk management, the language finance and audit committees already use."}
- {"name":"FAIR","managementUse":"Quantitative risk analysis, useful for expressing risk in financial terms for comparison."}

You do not need to memorize every clause of every framework. Understand what each one is for, what management problem it solves, and how they relate to each other. A frequent exam pattern gives you a business need and asks which kind of framework fits it.

Incident Response Lifecycle

- {"step":1,"name":"Preparation","detail":"Plans, roles, tooling, contacts and exercises are in place before anything happens."}
- {"step":2,"name":"Detection","detail":"The event is noticed and recorded through monitoring, reporting or a third party."}
- {"step":3,"name":"Analysis","detail":"Scope, severity and business impact are established well enough to decide."}
- {"step":4,"name":"Containment","detail":"Spread is limited while evidence and critical operations are protected."}
- {"step":5,"name":"Eradication","detail":"The cause is removed rather than the symptom suppressed."}
- {"step":6,"name":"Recovery","detail":"Services are restored and validated, with monitoring for recurrence."}
- {"step":7,"name":"Lessons learned","detail":"Findings are turned into changes to the program, not filed and forgotten."}

Incident Priorities

- Protect people
- Protect critical business operations
- Limit damage
- Preserve evidence
- Communicate through approved channels
- Restore services
- Improve the program after the incident

This ordering is GRC Careers' study aid, not a sequence published by ISACA. It reflects how CISM questions tend to reward management judgment: when several technical actions are all defensible, safety outranks operations, operations outrank convenience, and nothing is communicated outside approved channels.

Metrics

[object Object]

Leadership

- {"principle":"Align security with business objectives","detail":"Security that cannot explain which objective it protects will lose the budget argument."}
- {"principle":"Manage risk rather than promise zero risk","detail":"Promising that nothing will happen destroys credibility the first time something does."}
- {"principle":"Communicate clearly with executives","detail":"Lead with the decision you need and the business consequence, not with the control detail."}
- {"principle":"Build a sustainable security culture","detail":"Controls people work around are not controls. Design for how the organization actually operates."}

CAREERS

Roles CISM Supports

- **Information Security Manager** — Owns the day-to-day security function, its people and its delivery against the roadmap.

- **Cybersecurity Program Manager** — Runs the multi-year program across workstreams, budgets and dependencies.
- **GRC Manager** — Joins governance, risk and compliance activity to what the security team actually does.
- **Security Governance Lead** — Owns policy, standards, exceptions and the reporting line into executives.
- **Cyber Risk Manager** — Runs assessment, treatment and reporting, and keeps risk ownership honest.
- **Director of Information Security** — Sets direction across several teams and answers for the program at executive level.
- **Security Consultant** — Advises client organizations on program design, maturity and remediation priorities.
- **Chief Information Security Officer** — Carries enterprise accountability for information security and its risk position.

CISM supports these roles, but it does not by itself qualify anyone for them. Hiring for security leadership weighs demonstrated program ownership, incident experience and executive communication alongside credentials.

GO DEEPER

Official Resources

- **CISM certification page** — The overview page, with current exam fees and registration.
  https://www.isaca.org/credentialing/cism
- **CISM exam content outline** — The authoritative list of domains, weightings and supporting tasks.
  https://www.isaca.org/credentialing/cism/cism-exam-content-outline
- **ISACA exam candidate guide** — Scheduling, identification, testing rules and scoring.
  https://www.isaca.org/credentialing/exam-candidate-guide
- **CISM certification application information** — How to apply once you pass, and how experience is verified.
  https://www.isaca.org/credentialing/cism/get-cism-certified
- **CISM maintenance requirements** — CPE hours, reporting cycle and annual maintenance fees.
  https://www.isaca.org/credentialing/cism/maintain-cism-certification