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 — 18%

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.

- Organizational purpose and culture
- Legal, regulatory and contractual requirements
- Organizational structures, roles and responsibilities
- Information security strategy development
- Enterprise architecture (new in the November 2026 outline)
- Information governance frameworks and standards
- Strategic planning, including budgets, resources and the business case

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.

- Emerging risk and threat landscape
- Vulnerability and control deficiency analysis
- Risk assessment and analysis
- Risk treatment and risk response options
- Risk and control ownership
- Risk monitoring and reporting

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.

- Information security architecture (new in the November 2026 outline)
- Program resources: people, process and technology
- Industry standards and frameworks
- Policies, standards, procedures and guidelines
- Information asset identification and classification
- Control design and selection
- Control implementation, integration, testing and evaluation
- Awareness and training
- Management of external services, including suppliers, third parties and nth parties
- Program metrics development, communications and reporting

4 Incident Management 29%

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 response plan
- Business impact analysis (BIA)
- Business continuity plan (BCP) and disaster recovery plan (DRP)
- Incident classification and categorization
- Incident management training, testing and evaluation
- Incident management tools and techniques
- Investigation, evaluation and containment
- Response communications: reporting, notification and escalation
- Eradication, recovery and post-incident review

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

- **Security governance:** The system of direction, accountability and oversight that decides how security is run and who answers for it.
- **Corporate governance:** The wider structure of board and executive control that security governance has to fit inside.
- **Strategic alignment:** Making security objectives serve stated business objectives rather than running in parallel to them.
- **Policy:** A short statement of management direction and intent, approved at executive level.
- **Standard:** A mandatory requirement that gives a policy a measurable, enforceable form.
- **Procedure:** The step-by-step instructions for carrying out a task so that a standard is met.
- **Guideline:** Recommended practice offered as help, not as a requirement.
- **Baseline:** The minimum accepted configuration or control level for a class of systems.
- **Roles and accountability:** The named assignment of who owns, performs and reviews each part of the program.
- **Board oversight:** The board's duty to understand and challenge the organization's risk position.
- **Executive sponsorship:** Senior backing that supplies authority, funding and the ability to resolve conflicts.

Risk Management

- **Asset:** Anything of value to the organization that is worth protecting.
- **Threat:** A potential cause of an unwanted event.
- **Vulnerability:** A weakness that a threat can act on.
- **Likelihood:** How probable it is that a given event occurs in a stated period.
- **Impact:** The business consequence if the event does occur.
- **Exposure:** The extent to which the organization is open to a given loss.

- **Inherent risk:** The risk present before any controls are considered.
- **Residual risk:** The risk that remains after controls are applied.
- **Risk appetite:** The amount and type of risk the organization is willing to pursue.
- **Risk tolerance:** The acceptable variation around that appetite for a specific objective.
- **Risk owner:** The accountable person with authority to accept or fund treatment of a risk.
- **Risk acceptance:** A documented decision to live with a risk as it stands.
- **Risk avoidance:** Stopping or not starting the activity that creates the risk.
- **Risk mitigation:** Applying controls to reduce likelihood or impact.
- **Risk transfer:** Shifting financial consequence to another party, commonly through insurance or contract.

ALE = SLE × ARO

- **SLE (Single Loss Expectancy):** The expected loss from one occurrence of the event.
- **ARO (Annual Rate of Occurrence):** How many times that event is expected in a year.
- **ALE (Annual Loss Expectancy):** The expected annual loss, used to compare against the cost of treatment.

Financial calculations are tools for supporting risk decisions, not substitutes for management judgment. A number helps you compare options and justify spend. It does not tell you who owns the risk, whether the assumptions behind it hold, or whether the organization can survive the tail case.

Frameworks

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

- **Preparation:** Plans, roles, tooling, contacts and exercises are in place before anything happens.
- **Detection:** The event is noticed and recorded through monitoring, reporting or a third party.
- **Analysis:** Scope, severity and business impact are established well enough to decide.
- **Containment:** Spread is limited while evidence and critical operations are protected.
- **Eradication:** The cause is removed rather than the symptom suppressed.
- **Recovery:** Services are restored and validated, with monitoring for recurrence.
- **Lessons learned:** 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

KPIs (Key Performance Indicators): Measure whether the program is doing what it set out to do. Examples: security-awareness completion, patch-compliance rate, mfa adoption, control implementation, incident-response exercise completion.

KRIs (Key Risk Indicators): Signal that risk is building before it becomes a loss. Examples: critical vulnerabilities, high-risk third parties, repeat incidents, unresolved audit findings, mean time to detect, concentration of unsupported systems.

A useful metric supports a decision. Before adding one to an executive report, ask what a reader would do differently depending on the value. Counts of activity with no business context are vanity metrics: they fill a slide and change nothing.

Leadership

- **Align security with business objectives:** Security that cannot explain which objective it protects will lose the budget argument.
- **Manage risk rather than promise zero risk:** Promising that nothing will happen destroys credibility the first time something does.
- **Communicate clearly with executives:** Lead with the decision you need and the business consequence, not with the control detail.
- **Build a sustainable security culture:** 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

Hiring for GRC & AI-governance roles?
Browse hand-reviewed CISM and cybersecurity-management jobs with salaries at **https://www.ai-governance-jobs.com/cism-jobs/**
Full CISM reference: **https://www.ai-governance-jobs.com/certifications/cism/**

CISM and ISACA are trademarks of ISACA. GRC-Careers.org is not affiliated with, endorsed by or accredited by ISACA. This page is an independent study aid and contains no real exam questions.
Exam facts, fees, experience requirements and maintenance requirements on this page were verified against ISACA's published pages on the date shown. Domain weights and subtopics rechecked November 7, 2026 against the CISM Exam Content Outline that applies to exams taken on or after November 3, 2026; exams taken through November 2, 2026 used the previous weights of 17%, 20%, 33% and 30%. Credential level, study priorities and the incident-priority ordering are GRC Careers' editorial classifications rather than ISACA designations. Fees and exam requirements change. Confirm current information with ISACA before you register.
This is an original study aid produced by GRC Careers. It contains no real exam questions. © GRC Careers. Facts verified against ISACA (https://www.isaca.org/).