

CISM: Certified Information Security Manager

Official Body: ISACA | Syllabus: 2024-2026 CISM Job Practice

Free 10-Q Diagnostic ->

Passing Standard: Scaled score of 450 on a 200-800 scale

Format & Timing: 150 multiple-choice questions (4 hours), computer-based testing at PSI (PSI Services)

Testing Windows: Continuous on-demand testing year-round

1. OFFICIAL 2026 BLUEPRINT DOMAINS & WEIGHTINGS

CISM-1: Information Security Governance	Weight: 17%
Enterprise Governance and Strategic Alignment: Aligning Information Security Strategy with Organizational Goals, Business Objectives, and Risk Appetite, Organizational Structure, Roles, and Responsibilities: Board of Directors, Senior Management, CISO, Steering Committee, Data Owners, and Custodians,	
CISM-2: Information Security Risk Management	Weight: 20%
Asset Classification, Valuation, and Risk Ownership: Establishing Business Process Owners as Accountable Risk Owners, Risk Identification and Assessment: Emerging Threats, Vulnerabilities, Likelihood/Impact Analysis, Quantitative (SLE, ARO, ALE) vs. Qualitative Methods, Risk Treatment and Response Options:	
CISM-3: Information Security Program	Weight: 33%
Information Security Program Charter, Scope, Roadmap, and Alignment with Enterprise Architecture and IT Operations, Security Program Resources and Frameworks: Implementing ISO/IEC 27001, NIST CSF, COBIT, Defense-in-Depth, and Control Design, Security Awareness, Training, and Organizational Culture:	
CISM-4: Incident Management	Weight: 30%
Incident Management Readiness: Incident Response Plan (IRP), CSIRT/SOC Structure, Escalation Thresholds, Communication Plans, and Retainer Agreements, Business Impact Analysis (BIA), Business Continuity Planning (BCP), and Disaster Recovery Planning (DRP): RTO, RPO, WRT, MTD, and Recovery Sites,	

2. PRIMARY STATUTORY & REGULATORY AUTHORITIES TESTED

- * **ISACA CISM Job Practice Areas - ISACA CISM Exam Content Outline (Domains 1-4)**
Four-domain official CISM examination blueprint
- * **ISO/IEC 27001 & 27002 - ISO/IEC 27001:2022**
International standards for information security management systems and controls

3. EXAMINER TRAPS & HIGH-YIELD PASS STRATEGY

Key Challenge: Requires answering from an enterprise governance and business-alignment perspective rather than a hands-on technical perspective.