Certified Information Security Manager (CISM)

Paul Phillips, CISA, CISM, CDPSE, CPT, MBA

Director, Event Content Development

ISACA®

CISM Job Practice

The primary focus areas of the job practice are the current tasks performed and the knowledge used by CISMs. By gathering evidence of the current work practice of CISMs, ISACA ensures that the CISM program continues to meet the high standards set for the certification of professionals throughout the world.

CISM Job Practice

- An international job practice analysis is conducted periodically to maintain the validity of the CISM certification program.
- Beginning in 2022, the Certified Information Security Manager® exam will test the new CISM job practice.
- The findings of the CISM job practice analysis are carefully considered and directly influence the development of new test specifications to ensure that the CISM exam reflects the most current best practices.
- The new job practice reflects the areas of study to be tested. The complete CISM job practice can be found at www.isaca.org/credentialing/CISM

CISM Job Practices

- Information Security Governance (17%)
- Information Security Risk Management (20%)
- Information Security Program (33%)
- Incident Management (30%)

CISM Review Content

Job Practice = Domain = Chapter

CISM Review Content

- **Information Security Governance (17%)**
  - **Part A: Enterprise Governance**
    - Importance of Information Security Governance
    - Organizational Culture
    - Legal, Regulatory and Contractual Requirements
    - Organizational Structures, Roles and Responsibilities
  - **Part B: Information Security Strategy**
    - Information Security Strategy Development
    - Information Governance Frameworks and Standards
    - Strategic Planning

CISM Review Content

- **Information Security Risk Management (20%)**
  - **Part A: Information Risk Assessment**
    - Emerging Risk and Threat Landscape
    - Vulnerability and Control Deficiency Analysis.
    - Risk Analysis, Evaluation and Assessment
  - **Part B: Information Risk Response**
    - Risk Treatment/Risk Response Options
    - Risk and Control Ownership
    - Risk Monitoring and Reporting

CISM Review Content

- **Information Security Program (33%)**
  - Part A: Information Security Program Development
    - Information Security Program Overview
    - Information Security Program Resources
    - Information Asset Identification and Classification
    - Industry Standards and Frameworks for Information Security
    - Information Security Policies, Procedures and Guidelines
    - Defining an Information Security Program Road Map
    - Information Security Program Metrics

CISM Review Content

- **Information Security Program (33%)**
  - **Part B: Information Security Program Management**
    - Information Security Control Design and Selection
    - Information Security Control Implementation and Integration
    - Information Security Control Testing and Evaluation
    - Information Security Awareness and Training
    - Integration of the Security Program With IT Operations
    - Management of External Services and Relationships
    - Information Security Program Communications and Reporting

CISM Review Content

- **Incident Management (30%)**
  - Part A: Incident Management Readiness
    - Incident Management and Incident Response Overview
    - Incident Management and Incident Response Plans
    - Business Impact Analysis
    - Business Continuity Plan
    - Disaster Recovery Plan
    - Incident Classification/Categorization.
    - Incident Management Training, Testing and Evaluation

CISM Review Content

- **Incident Management (30%)**
  - Incident Management Tools and Technologies
  - Incident Investigation and Evaluation
  - Incident Containment Methods
  - Incident Response Communications
  - Incident Eradication and Recovery
  - Post-Incident Review Practices

Things to Keep In Mind

- Roles & Responsibilities
- Wholistic Security Program
- Maturity of Program
- Cross-Functional Collaboration

Closing

Questions?

Closing

THANK YOU