ISACA CISM

ISACA Information Security Manager Certification Questions & Answers

Get Instant Access to Vital Exam Acing Materials | Study Guide | Sample Questions | Practice Test

CISM

ISACA Certified Information Security Manager (CISM)

150 Questions Exam – 450/800 Cut Score – Duration of 240 minutes




EDUSUM

#1 Online Certification Guide

Table of Contents:

Discover More about the CISM Certification

Are you interested in passing the ISACA CISM exam? First discover, who benefits from the CISM certification. The CISM is suitable for a candidate if he wants to learn about IT Security. Passing the CISM exam earns you the ISACA Certified Information Security Manager (CISM) title.

While preparing for the CISM exam, many candidates struggle to get the necessary materials. But do not worry; your struggling days are over. The CISM PDF contains some of the most valuable preparation tips and the details and instant access to useful **CISM study materials just at one click.**

ISACA CISM Information Security Manager Certification Details:

Exam Name	ISACA Certified Information Security Manager (CISM)
Exam Code	CISM
Exam Price ISACA Member	$575 (USD)
Exam Price ISACA Nonmember	$760 (USD)
Duration	240 mins
Number of Questions	150
Passing Score	450/800
Books / Training	**Virtual Instructor-Led Training** **In-Person Training & Conferences** **Customized, On-Site Corporate Training** **CISM Planning Guide**
Schedule Exam	**Exam Registration**
Sample Questions	**ISACA CISM Sample Questions**
Practice Exam	**ISACA CISM Certification Practice Exam**

CISM Syllabus:

Topic	Details	Weights
Information Security Governance	A. Enterprise Governance • Organizational Culture • Legal, Regulatory, and Contractual Requirements • Organizational Structures, Roles, and Responsibilities B. Information Security Strategy • Information Security Strategy Development • Information Governance Frameworks and Standards • Strategic Planning (e.g., budgets, resources, business case).	17%
Information Security Risk Management	A. Information Security Risk Assessment • Emerging Risk and Threat Landscape • Vulnerability and Control Deficiency Analysis • Risk Assessment and Analysis B. Information Security Risk Response • Risk Treatment / Risk Response Options • Risk and Control Ownership • Risk Monitoring and Reporting	20%
Information Security Program	A. Information Security Program Development • Information Security Program Resources (e.g., people, tools, technologies)	33%

Topic	Details	Weights
	• Information Asset Identification and Classification • Industry Standards and Frameworks for Information Security • Information Security Policies, Procedures, and Guidelines • Information Security Program Metrics B. Information Security Program Management • Information Security Control Design and Selection • Information Security Control Implementation and Integrations • Information Security Control Testing and Evaluation • Information Security Awareness and Training/td> • Management of External Services (e.g., providers, suppliers, third parties, fourth parties) • Information Security Program Communications and Reporting	
Incident Management	A. Incident Management Readiness • Incident Response Plan • Business Impact Analysis (BIA) • Business Continuity Plan (BCP) • Disaster Recovery Plan (DRP) • Incident Classification/Categorization • Incident Management Training, Testing, and Evaluation B. Incident Management Operations	30%

Topic	Details	Weights
	• Incident Management Tools and Techniques • Incident Investigation and Evaluation • Incident Containment Methods • Incident Response Communications (e.g., reporting, notification, escalation) • Incident Eradication and Recovery • Post-incident Review Practices	

Broaden Your Knowledge with ISACA CISM Sample Questions:

Question: 1

To determine how a security breach occurred on the corporate network, a security manager looks at the logs of various devices.

Which of the following BEST facilitates the correlation and review of these logs?

a) Database server
b) Domain name server
c) Time server
d) Proxy server

Answer: c

Question: 2

The postincident review of a security incident revealed that there was a process that was not monitored. As a result monitoring functionality has been implemented.

Which of the following may BEST be expected from this remediation?

a) Reduction in total incident duration
b) Increase in risk tolerance
c) Facilitation of escalation
d) Improvement in identification

Answer: d

Question: 3

IT-related risk management activities are MOST effective when they are:

a) treated as a distinct process
b) conducted by the IT department
c) communicated to all employees
d) integrated within business processes

Answer: d

Question: 4

Which of the following BEST illustrates residual risk within an organization?

a) Risk management framework
b) Risk register
c) Business impact analysis
d) Heat map

Answer: a

Question: 5

Abnormal server communication from inside the organization to external parties may be monitored to:

a) record the trace of advanced persistent threats
b) evaluate the process resiliency of server operations
c) verify the effectiveness of an intrusion detection system
d) support a nonrepudiation framework in e-commerce

Answer: a

Question: 6

Which of the following authentication methods prevents authentication replay?

a) Password hash implementation
b) Challenge/response mechanism
c) Wired equivalent privacy encryption usage
d) Hypertext Transfer Protocol basic authentication

Answer: b

Question: 7

A risk assessment and business impact analysis (BIA) have been completed for a major proposed purchase and new process for an organization.

There is disagreement between the information security manager and the business department manager who will be responsible for evaluating the results and identified risk.

Which of the following would be the BEST approach of the information security manager?

a) Acceptance of the business manager's decision on the risk to the corporation
b) Acceptance of the information security manager's decision on the risk to the corporation
c) Review of the risk assessment with executive management for final input
d) Create a new risk assessment and BIA to resolve the disagreement

Answer: c

Question: 8

Which of the following is the BEST way to detect an intruder who successfully penetrates a network before significant damage is inflicted?

a) Perform periodic penetration testing
b) Establish minimum security baselines
c) Implement vendor default settings
d) Install a honeypot on the network

Answer: d

Question: 9

In order to protect a network against unauthorized external connections to corporate systems, the information security manager should BEST implement:

a) a strong authentication.
b) IP antispoofing filtering.
c) network encryption protocol.
d) access lists of trusted devices.

Answer: a

Question: 10

Who is accountable for ensuring that information is categorized and that specific protective measures are taken?

a) The security officer
b) Senior management
c) The end user
d) The custodian

Answer: b

Avail the Study Guide to Pass ISACA CISM Information Security Manager Exam:

- Find out about the CISM syllabus topics. Visiting the official site offers an idea about the exam structure and other important study resources. Going through the syllabus topics help to plan the exam in an organized manner.
- Once you are done exploring the **CISM syllabus**, it is time to plan for studying and covering the syllabus topics from the core. Chalk out the best plan for yourself to cover each part of the syllabus in a hassle-free manner.
- A study schedule helps you to stay calm throughout your exam preparation. It should contain your materials and thoughts like study hours, number of topics for daily studying mentioned on it. The best bet to clear the exam is to follow your schedule rigorously.
- The candidate should not miss out on the scope to learn from the CISM training. Joining the ISACA provided training for CISM exam helps a candidate to strengthen his practical knowledge base from the certification.
- Learning about the probable questions and gaining knowledge regarding the exam structure helps a lot. Go through the **CISM sample questions** and boost your knowledge
- Make yourself a pro through online practicing the syllabus topics. CISM practice tests would guide you on your strengths and weaknesses regarding the syllabus topics. Through rigorous practicing, you can improve the weaker sections too. Learn well about time management during exam and become confident gradually with practice tests.

Career Benefits:

- Passing the CISM exam, helps a candidate to prosper highly in his career. Having the certification on the resume adds to the candidate's benefit and helps to get the best opportunities.