EDUSUM

#1 Online Certification Guide

ISACA CISA

ISACA Information Systems Auditor Certification Questions & Answers

Exam Summary – Syllabus –Questions

CISA

ISACA Certified Information Systems Auditor (CISA)

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

Table of Contents:

Know Your CISA Certification Well:

The CISA is best suitable for candidates who want to gain knowledge in the ISACA IT Audit. Before you start your CISA preparation you may struggle to get all the crucial Information Systems Auditor materials like CISA syllabus, sample questions, study guide.

But don't worry the CISA PDF is here to help you prepare in a stress free manner. The PDF is a combination of all your queries like-

- What is in the CISA syllabus?
- How many questions are there in the CISA exam?
- Which Practice test would help me to pass the CISA exam at the first attempt?

Passing the CISA exam makes you ISACA Certified Information Systems Auditor (CISA). Having the Information Systems Auditor certification opens multiple opportunities for you. You can grab a new job, get a higher salary or simply get recognition within your current organization.

ISACA CISA Information Systems Auditor Certification Details:

Exam Name	ISACA Certified Information Systems Auditor (CISA)
Exam Code	CISA
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** **CISA Planning Guide**
Schedule Exam	**Exam Registration**
Sample Questions	**ISACA CISA Sample Questions**
Practice Exam	**ISACA CISA Certification Practice Exam**

CISA Syllabus:

Topic	Details	Weights
INFORMATION SYSTEMS AUDITING PROCESS	- Providing audit services in accordance with standards to assist organizations in protecting and controlling information systems. Domain 1 affirms your credibility to offer conclusions on the state of an organization's IS/IT security, risk and control solutions. **A. Planning** 1. IS Audit Standards, Guidelines, and Codes of Ethics 2. Business Processes 3. Types of Controls 4. Risk-Based Audit Planning 5. Types of Audits and Assessments **B. Execution** 1. Audit Project Management 2. Sampling Methodology 3. Audit Evidence Collection Techniques 4. Data Analytics 5. Reporting and Communication Techniques 6. Quality Assurance and Improvement of the Audit Process	21%
Governance and Management of IT	- Domain 2 confirms to stakeholders your abilities to identify critical issues and recommend enterprise-specific practices to support and safeguard the governance of information and related technologies. **A. IT Governance** 1. IT Governance and IT Strategy 2. IT-Related Frameworks 3. IT Standards, Policies, and Procedures 4. Organizational Structure 5. Enterprise Architecture 6. Enterprise Risk Management 7. Maturity Models 8. Laws, Regulations, and Industry Standards affecting the Organization **B. IT Management** 1. IT Resource Management 2. IT Service Provider Acquisition and Management	17%

Topic	Details	Weights
	3. IT Performance Monitoring and Reporting 4. Quality Assurance and Quality Management of IT	
Information Systems Acquisition, Development and Implementation	**A. Information Systems Acquisition and Development** 1. Project Governance and Management 2. Business Case and Feasibility Analysis 3. System Development Methodologies 4. Control Identification and Design **B. Information Systems Implementation** 1. Testing Methodologies 2. Configuration and Release Management 3. System Migration, Infrastructure Deployment, and Data Conversion 4. Post-implementation Review	12%
INFORMATION SYSTEMS OPERATIONS AND BUSINESS RESILIENCE	- Domains 3 and 4 offer proof not only of your competency in IT controls, but also your understanding of how IT relates to business. **A. Information Systems Operations** 1. Common Technology Components 2. IT Asset Management 3. Job Scheduling and Production Process Automation 4. System Interfaces 5. End-User Computing 6. Data Governance 7. Systems Performance Management 8. Problem and Incident Management 9. Change, Configuration, Release, and Patch Management 10. IT Service Level Management 11. Database Management **B. Business Resilience** 1. Business Impact Analysis (BIA) 2. System Resiliency 3. Data Backup, Storage, and Restoration 4. Business Continuity Plan (BCP) 5. Disaster Recovery Plans (DRP)	23%

Topic	Details	Weights
Protection of Information Assets	- Cybersecurity now touches virtually every information systems role, and understanding its principles, best practices and pitfalls is a major focus within Domain 5. **A. Information Asset Security and Control** 1. Information Asset Security Frameworks, Standards, and Guidelines 2. Privacy Principles 3. Physical Access and Environmental Controls 4. Identity and Access Management 5. Network and End-Point Security 6. Data Classification 7. Data Encryption and Encryption-Related Techniques 8. Public Key Infrastructure (PKI) 9. Web-Based Communication Techniques 10. Virtualized Environments 11. Mobile, Wireless, and Internet-of-Things (IoT) Devices **B. Security Event Management** 1. Security Awareness Training and Programs 2. Information System Attack Methods and Techniques 3. Security Testing Tools and Techniques 4. Security Monitoring Tools and Techniques 5. Incident Response Management 6. Evidence Collection and Forensics **- Supporting Tasks** 1. Plan audit to determine whether information systems are protected, controlled, and provide value to the organization. 2. Conduct audit in accordance with IS audit standards and a risk-based IS audit strategy. 3. Communicate audit progress, findings, results, and recommendations to stakeholders. 4. Conduct audit follow-up to evaluate whether risks have been sufficiently addressed. 5. Evaluate the IT strategy for alignment with the organization’s strategies and objectives. 6. Evaluate the effectiveness of IT governance structure and IT organizational structure. 7. Evaluate the organization’s management of IT policies and practices.	27%

Topic	Details	Weights
	8. Evaluate the organization’s IT policies and practices for compliance with regulatory and legal requirements. 9. Evaluate IT resource and portfolio management for alignment with the organization’s strategies and objectives. 10. Evaluate the organization's risk management policies and practices. 11. Evaluate IT management and monitoring of controls. 12. Evaluate the monitoring and reporting of IT key performance indicators (KPIs). 13. Evaluate the organization’s ability to continue business operations. 14. Evaluate whether the business case for proposed changes to information systems meet business objectives. 15. Evaluate whether IT supplier selection and contract management processes align with business requirements. 16. Evaluate the organization's project management policies and practices. 17. Evaluate controls at all stages of the information systems development lifecycle. 18. Evaluate the readiness of information systems for implementation and migration into production. 19. Conduct post-implementation review of systems to determine whether project deliverables, controls, and requirements are met. 20. Evaluate whether IT service management practices align with business requirements. 21. Conduct periodic review of information systems and enterprise architecture. 22. Evaluate IT operations to determine whether they are controlled effectively and continue to support the organization’s objectives. 23. Evaluate IT maintenance practices to determine whether they are controlled effectively and continue to support the organization’s objectives. 24. Evaluate database management practices. 25. Evaluate data governance policies and practices. 26. Evaluate problem and incident management policies and practices. 27. Evaluate change, configuration, release, and patch management policies and practices. 28. Evaluate end-user computing to determine whether the processes are effectively controlled.	

Topic	Details	Weights
	29. Evaluate the organization's information security and privacy policies and practices. 30. Evaluate physical and environmental controls to determine whether information assets are adequately safeguarded. 31. Evaluate logical security controls to verify the confidentiality, integrity, and availability of information. 32. Evaluate data classification practices for alignment with the organization's policies and applicable external requirements. 33. Evaluate policies and practices related to asset lifecycle management. 34. Evaluate the information security program to determine its effectiveness and alignment with the organization's strategies and objectives. 35. Perform technical security testing to identify potential threats and vulnerabilities. 36. Utilize data analytics tools to streamline audit processes. 37. Provide consulting services and guidance to the organization in order to improve the quality and control of information systems. 38. Identify opportunities for process improvement in the organization's IT policies and practices. 39. Evaluate potential opportunities and threats associated with emerging technologies, regulations, and industry practices.	

ISACA CISA Sample Questions:

Question: 1

An IS auditor observes that an enterprise has outsourced software development to a third party that is a startup company. To ensure that the enterprise's investment in software is protected, which of the following should be recommended by the IS auditor?

a) Due diligence should be performed on the software vendor.
b) A quarterly audit of the vendor facilities should be performed.
c) There should be a source code escrow agreement in place.
d) A high penalty clause should be included in the contract.

Answer: c

Question: 2

An IS auditor is reviewing the physical security controls of a data center and notices several areas for concern. Which of the following areas is the MOST important?

a) The emergency power off button cover is missing.
b) Scheduled maintenance of the fire suppression system was not performed.
c) There are no security cameras inside the data center.
d) The emergency exit door is blocked.

Answer: d

Question: 3

An IS auditor is assigned to audit a software development project, which is more than 80 percent complete, but has already overrun time by 10 percent and costs by 25 percent. Which of the following actions should the IS auditor take?

a) Report that the organization does not have effective project management.
b) Recommend the project manager be changed.
c) Review the IT governance structure.
d) Review the conduct of the project and the business case.

Answer: d

Question: 4

Which of the following choices BEST helps information owners to properly classify data?

a) Understanding of technical controls that protect data
b) Training on organizational policies and standards
c) Use of an automated data leak prevention (DLP) tool
d) Understanding which people need to access the data

Answer: b

Question: 5

Who is accountable for ensuring relevant controls over IS resources?

a) The system administrator
b) Resource owners
c) Network administration
d) The database administrator

Answer: b

Question: 6

An IS auditor finds a small number of user access requests that had not been authorized by managers through the normal predefined workflow steps and escalation rules. The IS auditor should:

a) recommend that the owner of the identity management (IDM) system fix the workflow issues.
b) report the problem to the audit committee.
c) conduct a security risk assessment.
d) perform an additional analysis.

Answer: d

Question: 7

The primary consideration of an IS auditor when evaluating a fraudulent transaction is:

a) to remain unbiased while evaluating the evidence
b) the independence of the IS auditor
c) to determine the source of the evidence
d) to ensure that the integrity of the evidence is maintained

Answer: d

Question: 8

A test that is conducted when a system is in the development phase is:

a) A sociability test
b) A functionality test
c) A load test
d) A unit test

Answer: d

Question: 9

Responsibility of granting access to data with the help of security officer resides with:

a) The data owners
b) The system developer
c) The library controller
d) The system administrator

Answer: a

Question: 10

An enterprise's risk appetite is BEST established by:

a) the steering committee.
b) security management.
c) the audit committee.
d) the chief legal officer.

Answer: a

Study Guide to Crack ISACA Information Systems Auditor CISA Exam:

- Getting details of the CISA syllabus, is the first step of a study plan. This pdf is going to be of ultimate help. Completion of the syllabus is must to pass the CISA exam.
- Making a schedule is vital. A structured method of preparation leads to success. A candidate must plan his schedule and follow it rigorously to attain success.
- Joining the ISACA provided training for CISA exam could be of much help. If there is specific training for the exam, you can discover it from the link above.
- Read from the CISA sample questions to gain your idea about the actual exam questions. In this PDF useful sample questions are provided to make your exam preparation easy.
- Practicing on CISA practice tests is must. Continuous practice will make you an expert in all syllabus areas.

Reliable Online Practice Test for CISA Certification

Make EduSum.com your best friend during your ISACA Information Systems Auditor exam preparation. We provide authentic practice tests for the CISA exam. Experts design these online practice tests, so we can offer you an exclusive experience of taking the actual CISA exam. We guarantee you 100% success in your first exam attempt if you continue practicing regularly. Don't bother if you don't get 100% marks in initial practice exam attempts. Just utilize the result section to know your strengths and weaknesses and prepare according to that until you get 100% with our practice tests. Our evaluation makes you confident, and you can score high in the CISA exam.

Start Online practice of CISA Exam by visiting URL
https://www.edusum.com/isaca/cisa-isaca-information-systems-auditor