EDUSUM

#1 Online Certification Guide

ISC2 CISSP-ISSAP

ISC2 ISSAP Certification Questions & Answers

Exam Summary – Syllabus –Questions

CISSP-ISSAP

ISC2 Information Systems Security Architecture Professional (CISSP-ISSAP)

125 Questions Exam – 700/1000 Cut Score – Duration of 180 minutes

Table of Contents:

Know Your CISSP-ISSAP Certification Well:

The CISSP-ISSAP is best suitable for candidates who want to gain knowledge in the ISC2 Cybersecurity. Before you start your CISSP-ISSAP preparation you may struggle to get all the crucial ISSAP materials like CISSP-ISSAP syllabus, sample questions, study guide.

But don't worry the CISSP-ISSAP 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 CISSP-ISSAP syllabus?
- How many questions are there in the CISSP-ISSAP exam?
- Which Practice test would help me to pass the CISSP-ISSAP exam at the first attempt?

Passing the CISSP-ISSAP exam makes you ISC2 Information Systems Security Architecture Professional (CISSP-ISSAP). Having the ISSAP certification opens multiple opportunities for you. You can grab a new job, get a higher salary or simply get recognition within your current organization.

ISC2 CISSP-ISSAP Certification Details:

Exam Name	ISC2 Information Systems Security Architecture Professional (CISSP-ISSAP)
Exam Code	CISSP-ISSAP
Exam Price	$599 (USD)
Duration	180 mins
Number of Questions	125
Passing Score	700/1000
Schedule Exam	**Pearson VUE**
Sample Questions	**ISC2 CISSP-ISSAP Sample Questions**
Practice Exam	**ISC2 CISSP-ISSAP Certification Practice Exam**

CISSP-ISSAP Syllabus:

Topic	Details
Architect for Governance, Compliance and Risk Management - 17%	
Determine legal, regulatory, organizational and industry requirements	- Determine applicable information security standards and guidelines - Identify third-party and contractual obligations (e.g., supply chain, outsourcing, partners) - Determine applicable sensitive/personal data standards, guidelines and privacy regulations - Design for auditability (e.g., determine regulatory, legislative, forensic requirements, segregation, high assurance systems) - Coordinate with external entities (e.g., law enforcement, public relations, independent assessor)
Manage Risk	- Identify and classify risks - Assess risk - Recommend risk treatment (e.g., mitigate, transfer, accept, avoid) - Risk monitoring and reporting
Security Architecture Modeling - 15%	
Identify security architecture approach	- Types and scope (e.g., enterprise, network, Service-Oriented Architecture (SOA), cloud, Internet of Things (IoT), Industrial Control Systems (ICS)/Supervisory Control and Data Acquisition (SCADA)) - Frameworks (e.g., Sherwood Applied Business Security Architecture (SABSA), Service-Oriented Modeling Framework (SOMF)) - Reference architectures and blueprints - Security configuration (e.g., baselines, benchmarks, profiles) - Network configuration (e.g., physical, logical, high availability, segmentation, zones)
Verify and validate design (e.g., Functional Acceptance Testing (FAT), regression)	- Validate results of threat modeling (e.g., threat vectors, impact, probability) - Identify gaps and alternative solutions - Independent Verification and Validation (IV&V)

Topic	Details
	(e.g., tabletop exercises, modeling and simulation, manual review of functions)
Infrastructure Security Architecture - 21%	
Develop infrastructure security requirements	- On-premise, cloud-based, hybrid - Internet of Things (IoT), zero trust
Design defense-in-depth architecture	- Management networks - Industrial Control Systems (ICS) security - Network security - Operating systems (OS) security - Database security - Container security - Cloud workload security - Firmware security - User security awareness considerations
Secure shared services (e.g., wireless, e-mail, Voice over Internet Protocol (VoIP), Unified Communications (UC), Domain Name System (DNS), Network Time Protocol (NTP))	
Integrate technical security controls	- Design boundary protection (e.g., firewalls, Virtual Private Network (VPN), airgaps, software defined perimeters, wireless, cloud-native) - Secure device management (e.g., Bring Your Own Device (BYOD), mobile, server, endpoint, cloud instance, storage)
Design and integrate infrastructure monitoring	- Network visibility (e.g., sensor placement, time reconciliation, span of control, record compatibility) - Active/Passive collection solutions (e.g., span port, port mirroring, tap, inline, flow logs) - Security analytics (e.g., Security Information and Event Management (SIEM), log collection, machine learning, User Behavior Analytics (UBA))
Design infrastructure cryptographic solutions	- Determine cryptographic design considerations and constraints - Determine cryptographic implementation (e.g., in-transit, in-use, at-rest) - Plan key management lifecycle (e.g., generation, storage, distribution)

Topic	Details
Design secure network and communication infrastructure (e.g., Virtual Private Network (VPN), Internet Protocol Security (IPsec), Transport Layer Security (TLS))	
Evaluate physical and environmental security requirements	- Map physical security requirements to organizational needs (e.g., perimeter protection and internal zoning, fire suppression) - Validate physical security controls
Identity and Access Management (IAM) Architecture - 16%	
Design identity management and lifecycle	- Establish and verify identity - Assign identifiers (e.g., to users, services, processes, devices) - Identity provisioning and de-provisioning - Define trust relationships (e.g., federated, standalone) - Define authentication methods (e.g., Multi-Factor Authentication (MFA), risk-based, location-based, knowledge-based, object-based, characteristics-based) - Authentication protocols and technologies (e.g., Security Assertion Markup Language (SAML), Remote Authentication Dial-In User Service (RADIUS), Kerberos)
Design access control management and lifecycle	- Access control concepts and principles (e.g., discretionary/mandatory, segregation/Separation of Duties (SoD), least privilege) - Access control configurations (e.g., physical, logical, administrative) - Authorization process and workflow (e.g., governance, issuance, periodic review, revocation) - Roles, rights, and responsibilities related to system, application, and data access control (e.g., groups, Digital Rights Management (DRM), trust relationships) - Management of privileged accounts - Authorization (e.g., Single Sign-On (SSO), rule-based, role-based, attribute- based)

Topic	Details
Design identity and access solutions	- Access control protocols and technologies (e.g., eXtensible Access Control Markup Language (XACML), Lightweight Directory Access Protocol (LDAP)) - Credential management technologies (e.g., password management, certificates, smart cards) - Centralized Identity and Access Management (IAM) architecture (e.g., cloud-based, on-premise, hybrid) - Decentralized Identity and Access Management (IAM) architecture (e.g., cloud-based, on-premise, hybrid) - Privileged Access Management (PAM) implementation (for users with elevated privileges - Accounting (e.g., logging, tracking, auditing)
Architect for Application Security - 13%	
Integrate Software Development Life Cycle (SDLC) with application security architecture (e.g., Requirements Traceability Matrix (RTM), security architecture documentation, secure coding)	- Assess code review methodology (e.g., dynamic, manual, static) - Assess the need for application protection (e.g., Web Application Firewall (WAF), anti-malware, secure Application Programming Interface (API), secure Security Assertion Markup Language (SAML)) - Determine encryption requirements (e.g., at-rest, in-transit, in-use) - Assess the need for secure communications between applications and databases or other endpoints - Leverage secure code repository
Determine application security capability requirements and strategy (e.g., open source, Cloud Service Providers (CSP), Software as a Service (SaaS)/Infrastructure as a Service (IaaS)/ Platform as a Service (PaaS) environments)	- Review security of applications (e.g., custom, Commercial Off-the-Shelf (COTS), in-house, cloud) - Determine application cryptographic solutions (e.g., cryptographic Application Programming Interface (API), Pseudo Random Number Generator (PRNG), key management) - Evaluate applicability of security controls for system components (e.g., mobile and web client applications; proxy, application, and database services)

Topic	Details
Identify common proactive controls for applications (e.g., Open Web Application Security Project (OWASP))	
Security Operations Architecture - 18%	
Gather security operations requirements (e.g., legal, compliance, organizational, and business requirements)	
Design information security monitoring (e.g., Security Information and Event Management (SIEM), insider threat, threat intelligence, user behavior analytics, Incident Response (IR) procedures)	- Detection and analysis - Proactive and automated security monitoring and remediation (e.g., vulnerability management, compliance audit, penetration testing)
Design Business Continuity (BC) and resiliency solutions	- Incorporate Business Impact Analysis (BIA) - Determine recovery and survivability strategy - Identify continuity and availability solutions (e.g., cold, warm, hot, cloud backup) - Define processing agreement requirements (e.g., provider, reciprocal, mutual, cloud, virtualization) - Establish Recovery Time Objectives (RTO) and Recovery Point Objectives (RPO) - Design secure contingency communication for operations (e.g., backup communication channels, Out-of-Band (OOB))
Validate Business Continuity Plan (BCP)/Disaster Recovery Plan (DRP) architecture	
Design Incident Response (IR) management	- Preparation (e.g., communication plan, Incident Response Plan (IRP), training) - Identification - Containment - Eradication - Recovery - Review lessons learned

ISC2 CISSP-ISSAP Sample Questions:

Question: 1

Which of the following statements about Discretionary Access Control List (DACL) is true?

a) It specifies whether an audit activity should be performed when an object attempts to access a resource.
b) It is a unique number that identifies a user, group, and computer account.
c) It is a list containing user accounts, groups, and computers that are allowed (or denied) access to the object.
d) It is a rule list containing access control entries.

Answer: c

Question: 2

Which of the following protocols uses public-key cryptography to authenticate the remote computer?

a) SSH
b) Telnet
c) SCP
d) SSL

Answer: a

Question: 3

Which of the following describes the acceptable amount of data loss measured in time?

a) Recovery Consistency Objective (RCO)
b) Recovery Time Objective (RTO)
c) Recovery Point Objective (RPO)
d) Recovery Time Actual (RTA)

Answer: c

Question: 4

In which of the following access control models, owner of an object decides who is allowed to access the object and what privileges they have?

a) Access Control List (ACL)
b) Mandatory Access Control (MAC)
c) Role Based Access Control (RBAC)
d) Discretionary Access Control (DAC)

Answer: d

Question: 5

Which of the following are the countermeasures against a man-in-the-middle attack?
Each correct answer represents a complete solution. Choose all that apply.

a) Using public key infrastructure authentication.
b) Using basic authentication.
c) Using Secret keys for authentication.
d) Using Off-channel verification.

Answer: a, c, d

Question: 6

Which of the following types of firewall functions at the Session layer of OSI model?

a) Circuit-level firewall
b) Application-level firewall
c) Packet filtering firewall
d) Switch-level firewall

Answer: a

Question: 7

In which of the following network topologies does the data travel around a loop in a single direction and pass through each device?

a) Ring topology
b) Tree topology
c) Star topology
d) Mesh topology

Answer: a

Question: 8

Which of the following attacks can be overcome by applying cryptography?

a) Web ripping
b) DoS
c) Sniffing
d) Buffer overflow

Answer: c

Question: 9

The network you administer allows owners of objects to manage the access to those objects via access control lists. This is an example of what type of access control?

a) RBAC
b) MAC
c) CIA
d) DAC

Answer: d

Question: 10

You work as a Network Administrator of a TCP/IP network. You are having DNS resolution problem. Which of the following utilities will you use to diagnose the problem?

a) TRACERT
b) PING
c) IPCONFIG
d) NSLOOKUP

Answer: d

Study Guide to Crack ISC2 CISSP-ISSAP Exam:

- Getting details of the CISSP-ISSAP 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 CISSP-ISSAP 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 ISC2 provided training for CISSP-ISSAP 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 CISSP-ISSAP 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 CISSP-ISSAP practice tests is must. Continuous practice will make you an expert in all syllabus areas.