



ISC2 CC

ISC2 Certified in Cybersecurity Certification Questions & Answers

Exam Summary – Syllabus – Questions

CC

[ISC2 Certified in Cybersecurity](#)

100 Questions Exam - 700 / 1000 Cut Score - Duration of 120 minutes

Table of Contents:

| | |
|--|---|
| Know Your CC Certification Well: | 2 |
| ISC2 CC ISC2 Certified in Cybersecurity Certification Details: | 2 |
| CC Syllabus:..... | 3 |
| Security Principles - 26% | 3 |
| Business Continuity (BC), Disaster Recovery (DR) & Incident Response Concepts - 10% | 3 |
| Access Controls Concepts - 22% | 4 |
| Network Security - 24% | 4 |
| Security Operations - 18% | 5 |
| ISC2 CC Sample Questions: | 5 |
| Study Guide to Crack ISC2 ISC2 Certified in Cybersecurity CC Exam: | 9 |

Know Your CC Certification Well:

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

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

Passing the CC exam makes you ISC2 Certified in Cybersecurity. Having the ISC2 Certified in Cybersecurity 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 CC ISC2 Certified in Cybersecurity Certification Details:

| | |
|---------------------|---|
| Exam Name | ISC2 Certified in Cybersecurity (CC) |
| Exam Code | CC |
| Exam Price | \$199 (USD) |
| Duration | 120 mins |
| Number of Questions | 100 |
| Passing Score | 700 / 1000 |
| Schedule Exam | Pearson VUE |
| Sample Questions | ISC2 CC Sample Questions |
| Practice Exam | ISC2 CC Certification Practice Exam |

CC Syllabus:

| Topic | Details |
|--|---|
| Security Principles - 26% | |
| Understand the security concepts of information assurance | <ul style="list-style-type: none"> - Confidentiality - Integrity - Availability - Authentication (e.g., methods of authentication, multi-factor authentication (MFA)) - Non-repudiation - Privacy |
| Understand the risk management process | <ul style="list-style-type: none"> - Risk management (e.g., risk priorities, risk tolerance) - Risk identification, assessment and treatment |
| Understand security controls | <ul style="list-style-type: none"> - Technical controls - Administrative controls - Physical controls |
| Understand (ISC) ² Code of Ethics | <ul style="list-style-type: none"> - Professional code of conduct |
| Understand governance processes | <ul style="list-style-type: none"> - Policies - Procedures - Standards - Regulations and laws |
| Business Continuity (BC), Disaster Recovery (DR) & Incident Response Concepts - 10% | |
| Understand business continuity (BC) | <ul style="list-style-type: none"> - Purpose - Importance - Components |
| Understand disaster recovery (DR) | <ul style="list-style-type: none"> - Purpose - Importance - Components |
| Understand incident response | <ul style="list-style-type: none"> - Purpose - Importance - Components |

| Topic | Details |
|--|---|
| Access Controls Concepts - 22% | |
| Understand physical access controls | <ul style="list-style-type: none"> - Physical security controls (e.g., badge systems, gate entry, environmental design) - Monitoring (e.g., security guards, closed-circuit television (CCTV), alarm systems, logs) - Authorized versus unauthorized personnel |
| Understand logical access controls | <ul style="list-style-type: none"> - Principle of least privilege - Segregation of duties - Discretionary access control (DAC) - Mandatory access control (MAC) - Role-based access control (RBAC) |
| Network Security - 24% | |
| Understand computer networking | <ul style="list-style-type: none"> - Networks (e.g., Open Systems Interconnection (OSI) model, Transmission Control Protocol/Internet Protocol (TCP/IP) model, Internet Protocol version 4 (IPv4), Internet Protocol version 6 (IPv6), WiFi) - Ports - Applications |
| Understand network threats and attacks | <ul style="list-style-type: none"> - Types of threats (e.g., distributed denial-of-service (DDoS), virus, worm, Trojan, man-in-the-middle (MITM), side-channel) - Identification (e.g., intrusion detection system (IDS), host-based intrusion detection system (HIDS), network intrusion detection system (NIDS)) - Prevention (e.g., antivirus, scans, firewalls, intrusion prevention system (IPS)) |
| Understand network security infrastructure | <ul style="list-style-type: none"> - On-premises (e.g., power, data center/closets, Heating, Ventilation, and Air Conditioning (HVAC), environmental, fire suppression, redundancy, memorandum of understanding (MOU)/memorandum of agreement (MOA)) - Design (e.g., network segmentation (demilitarized zone (DMZ), virtual local area network (VLAN), virtual private network (VPN), micro-segmentation), defense in depth, |

| Topic | Details |
|--|---|
| | Network Access Control (NAC) (segmentation for embedded systems, Internet of Things (IoT)) - Cloud (e.g., service-level agreement (SLA), managed service provider (MSP), Software as a Service (SaaS), Infrastructure as a Service (IaaS), Platform as a Service (PaaS), hybrid) |
| Security Operations - 18% | |
| Understand data security | - Encryption (e.g., symmetric, asymmetric, hashing) - Data handling (e.g., destruction, retention, classification, labeling) - Logging and monitoring security events |
| Understand system hardening | - Configuration management (e.g., baselines, updates, patches) |
| Understand best practice security policies | - Data handling policy - Password policy - Acceptable Use Policy (AUP) - Bring your own device (BYOD) policy - Change management policy (e.g., documentation, approval, rollback) - Privacy policy |
| Understand security awareness training | - Purpose/concepts (e.g., social engineering, password protection) - Importance |

ISC2 CC Sample Questions:

Question: 1

By implementing a layered defense strategy across our organization, what do we improve?

- a) Availability.
- b) Integrity.
- c) Confidentiality.
- d) All of these.

Answer: d

Question: 2

For our authentication, we are looking at knowledge factors. Which is the MOST common knowledge factor in use today?

- a) One-time passwords.
- b) PINs.
- c) Passwords.
- d) Pass phrase.

Answer: c

Question: 3

When an attacker is using a brute force attack to break a password, what are they doing?

- a) Looking at the hash values and comparing it to thousands or millions of pre-calculated hashes.
- b) Trying every possible key to, over time, break any encryption.
- c) Looking at common letter frequency to guess the plaintext.
- d) Trying to recover the key without breaking the encryption.

Answer: b

Question: 4

Our networking department is recommending we use a full duplex solution for an implementation. What is a KEY FEATURE of those?

- a) Both systems can send and receive at the same time.
- b) Only one system on the network can send one signal at a time.
- c) One way communication, one system transmits the other receives, direction can be reversed.
- d) One way communication, one system transmits the other receives, direction can't be reversed.

Answer: a

Question: 5

You can MOST LIKELY be held liable when you display which of these?

- a) Due diligence.
- b) Due care.
- c) Negligence.
- d) Remorse.

Answer: c

Question: 6

Which type of Intrusion Detection Systems (IDS) and Intrusion Prevention System (IPS) are completely vulnerable to 0-day attacks?

- a) Signature based.
- b) Network based.
- c) Heuristic based.
- d) Behavioral based.

Answer: a

Question: 7

As an IT Security professional, you are expected to perform due care. What does this mean?

- a) Continue the security practices of your company.
- b) Researching and acquiring the knowledge to do your job right.
- c) Apply patches annually.
- d) Do what is right in the situation and your job. Act on the knowledge.

Answer: d

Question: 8

You are talking to a new manager of our helpdesk. You are explaining how we do risk analysis. They ask you: "How do you define a vulnerability?"

- a) The total risk after we have implemented our countermeasures.
- b) How bad is it if we are compromised?
- c) A weakness that can possibly be exploited.
- d) A potential harmful incident.

Answer: c

Question: 9

After an attack we have suffered a loss of public confidence, which leg of the CIA was compromised?

- a) Integrity
- b) Confidentiality
- c) Availability
- d) Encryption

Answer: b

Question: 10

Using Mandatory Access Control (MAC), we would use clearance for assigning which of these?

- a) Auditing.
- b) Authorization.
- c) Availability.
- d) Authentication.

Answer: b

Study Guide to Crack ISC2 ISC2 Certified in Cybersecurity CC Exam:

- Getting details of the CC 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 CC 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 CC 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 CC 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 CC practice tests is must. Continuous practice will make you an expert in all syllabus areas.

Reliable Online Practice Test for CC Certification

Make EduSum.com your best friend during your ISC2 Certified in Cybersecurity exam preparation. We provide authentic practice tests for the CC exam. Experts design these online practice tests, so we can offer you an exclusive experience of taking the actual CC 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 CC exam.

Start Online practice of CC Exam by visiting URL

<https://www.edusum.com/isc2/cc-isc2-certified-cybersecurity>