Exam

CISSP

CISSP Certified Information Systems Security Professional

Free demo	100 sample questions
Full exam	1485 questions with answers and explanations
Contents	Questions with answers and explanations

Exam domains

Domain	Exam weight	Questions
D1 Security and Risk Management		29
D2 Asset Security		5
D3 Security Architecture and Engineering		14
D4 Communication and Network Security		10
D5 Identity and Access Management (IAM)		13
D6 Security Assessment and Testing		9
D7 Security Operations		13
D8 Software Development Security		6

This is a free demo from Dumpsgate: 100 of the exam's 1485 questions. **Get the full CISSP exam** with every question, answer and explanation.

Question 1

Single choice · Domain: D1 Security and Risk Management › Perform risk assessment for cyber-physical systems

When designing a Cyber-Physical System (CPS), which of the following should be a security practitioner's first consideration?

A. Resiliency of the system
B. Detection of sophisticated attackers
C. Risk assessment of the system
D. Topology of the network used for the system

Answer: C. Risk assessment of the system

Explanation

The question asks what a security practitioner should consider first when designing a CPS; the CISSP body of knowledge states that risk assessment is the initial step in the security engineering process.

✗ **A** Resiliency of the system
Resiliency is important but it is addressed after the risk assessment identifies threats and impacts.
https://www.isc2.org/Certifications/CISSP

✗ **B** Detection of sophisticated attackers
Detecting attackers is a later security operation activity; the first step is to assess risk.
https://www.isc2.org/Certifications/CISSP

✓ **C** Risk assessment of the system
Risk assessment is the foundational activity when designing any system, including CPS, to identify threats, vulnerabilities, and impacts before other design decisions.
https://www.isc2.org/Certifications/CISSP

✗ **D** Topology of the network used for the system
Network topology is a design detail that follows the initial risk assessment and threat modeling phases.
https://www.isc2.org/Certifications/CISSP

Question 2

Single choice · Domain: D1 Security and Risk Management › Identify legal and regulatory requirements before establishing a data retention policy

Which of the following is the FIRST requirement a data owner should consider before implementing a data retention policy?

A. Training
B. Legal
C. Business
D. Storage

Free demo · full exam: 1485 questions

Answer: B. Legal

Explanation

The question assesses the candidate's understanding that compliance with legal and regulatory obligations is the primary consideration for a data owner when creating a retention policy.

✗ **A** Training
Training is important but follows after legal compliance requirements are identified.
https://www.isc2.org/Certifications/CISSP

✓ **B** Legal
Legal and regulatory requirements are the first factor a data owner must evaluate before implementing a data retention policy.
https://www.isc2.org/Certifications/CISSP

✗ **C** Business
Business considerations are secondary to legal obligations in the initial assessment of a retention policy.
https://www.isc2.org/Certifications/CISSP

✗ **D** Storage
Storage capacity is a technical factor that is addressed after legal requirements are satisfied.
https://www.isc2.org/Certifications/CISSP

Question 3

Single choice · Domain: D1 Security and Risk Management › Conduct a Business Impact Analysis to assess impact of information system failures on business processes

What is the MAIN purpose of conducting a business impact analysis (BIA)?

A. To determine the critical resources required to recover from an incident within a specified time period
B. To determine the effect of mission-critical information system failures on core business processes
C. To determine the cost for restoration of damaged information system
D. To determine the controls required to return to business critical operations

Answer: B. To determine the effect of mission-critical information system failures on core business processes

Explanation

The question asks for the main purpose of a BIA, which is a risk management activity covered under the Security and Risk Management domain of the CISSP CBK.

✗ **A** To determine the critical resources required to recover from an incident within a specified time period
Incorrect. Determining recovery resources and time frames relates to Recovery Time Objectives (RTO) and recovery planning, not the primary purpose of a BIA.
https://www.isc2.org/Certifications/CISSP

Free demo · full exam: 1485 questions

✓ **B** To determine the effect of mission-critical information system failures on core business processes
Correct. The main purpose of a BIA is to assess the impact of disruptions to mission-critical information systems on core business processes.
https://www.isc2.org/Certifications/CISSP

✗ **C** To determine the cost for restoration of damaged information system
Incorrect. Estimating restoration costs is part of cost-benefit analysis or recovery budgeting, not the primary focus of a BIA.
https://www.isc2.org/Certifications/CISSP

✗ **D** To determine the controls required to return to business critical operations
Incorrect. Identifying required controls is addressed in the risk treatment and control selection phases, not the core purpose of a BIA.
https://www.isc2.org/Certifications/CISSP

Question 4

Single choice · Domain: D1 Security and Risk Management › Understand legal and regulatory issues related to privacy and data protection

If traveling abroad and a customs official demands to examine a personal computer, which of the following should be assumed?

A. The hard drive has been stolen.
B. The Internet Protocol (IP) address has been copied.
C. The hard drive has been copied.
D. The Media Access Control (MAC) address was stolen

Answer: C. The hard drive has been copied.

Explanation

The question assesses knowledge of how customs officials may handle electronic devices and the assumption that data can be duplicated during inspection.

✗ **A** The hard drive has been stolen.
Incorrect. Customs officials may copy data but theft of the physical drive is not assumed.
https://www.isc2.org/Certifications/CISSP

✗ **B** The Internet Protocol (IP) address has been copied.
Incorrect. An IP address is not stored on the computer and cannot be "copied" from the device.
https://www.isc2.org/Certifications/CISSP

✓ **C** The hard drive has been copied.
Correct. When a customs official examines a computer, they can make a forensic image of the hard drive, so the assumption is that the drive's contents have been copied.
https://www.isc2.org/Certifications/CISSP

✗ **D** The Media Access Control (MAC) address was stolen
Incorrect. A MAC address is a hardware identifier that can be observed but is not typically "stolen" in this context.
https://www.isc2.org/Certifications/CISSP

Free demo · full exam: 1485 questions

Question 5

Single choice · Domain: D1 Security and Risk Management › Identify jurisdictional challenges in enforcing criminal law for cybercrime

What is the P R IM A R Y reason criminal law is difficult to enforce when dealing with cyber-crime?

A. Extradition treaties are rarely enforced.
B. Numerous language barriers exist.
C. Law enforcement agencies are understaffed.
D. Jurisdiction is hard to define.

Answer: D. Jurisdiction is hard to define.

Explanation

The question assesses knowledge of legal and regulatory issues, specifically why jurisdiction complicates cybercrime enforcement.

✗ **A** Extradition treaties are rarely enforced.
Incorrect. While extradition can be complex, CISSP material identifies jurisdictional ambiguity as the primary legal obstacle, not treaty enforcement.
https://www.isc2.org/Certifications/CISSP

✗ **B** Numerous language barriers exist.
Incorrect. Language barriers are not highlighted in the CISSP domain as the main reason criminal law is hard to enforce in cybercrime.
https://www.isc2.org/Certifications/CISSP

✗ **C** Law enforcement agencies are understaffed.
Incorrect. Staffing issues are operational concerns; the CISSP framework points to jurisdictional challenges as the primary legal difficulty.
https://www.isc2.org/Certifications/CISSP

✓ **D** Jurisdiction is hard to define.
Correct. CISSP emphasizes that defining jurisdiction is the primary reason criminal law is difficult to enforce in cyber-crime cases.
https://www.isc2.org/Certifications/CISSP

Dumpsgate

Question 6

Single choice · Domain: D1 Security and Risk Management › Calculate Maximum Tolerable Downtime (MTD) using the appropriate BCP formula

When designing a business continuity plan (BCP), what is the formula to determine the Maximum Tolerable Downtime (MTD)?

A. Annual Loss Expectancy (ALE) + Work Recovery Time (WRT)
B. Business impact analysis (BIA) + Recovery Point Objective (RPO)
C. Recovery Time Objective (RTO) + Work Recovery Time (WRT)
D. Estimated Maximum Loss (EML) + Recovery Time Objective (RTO)

Answer: C. Recovery Time Objective (RTO) + Work Recovery Time (WRT)

Explanation

The question assesses the candidate's understanding of business continuity planning concepts, specifically the relationship between MTD, RTO, and WRT.

✗ **A** Annual Loss Expectancy (ALE) + Work Recovery Time (WRT)
Incorrect. ALE is a risk-based loss metric and is not part of the MTD calculation.
https://www.isc2.org/Certifications/CISSP

✗ **B** Business impact analysis (BIA) + Recovery Point Objective (RPO)
Incorrect. BIA and RPO are inputs to the BCP process but do not directly sum to MTD.
https://www.isc2.org/Certifications/CISSP

✓ **C** Recovery Time Objective (RTO) + Work Recovery Time (WRT)
Correct. MTD is calculated as the sum of the Recovery Time Objective and the Work Recovery Time, representing the total allowable downtime before unacceptable impact.
https://www.isc2.org/Certifications/CISSP

✗ **D** Estimated Maximum Loss (EML) + Recovery Time Objective (RTO)
Incorrect. Estimated Maximum Loss is a financial metric and is not combined with RTO to determine MTD.
https://www.isc2.org/Certifications/CISSP

Question 7

Single choice · Domain: D1 Security and Risk Management › Apply the (ISC)² Code of Ethics canons

Which of the (ISC)? Code of Ethics canons is MOST reflected when preserving the value of systems, applications, and entrusted information while avoiding conflicts of interest?

A. Act honorably, honestly, justly, responsibly, and legally.
B. Protect society, the commonwealth, and the infrastructure.
C. Provide diligent and competent service to principles.
D. Advance and protect the profession.

Answer: C. Provide diligent and competent service to principles.

Explanation

The question assesses knowledge of which canon of the (ISC)² Code of Ethics aligns with preserving system value and avoiding conflicts of interest.

✗ **A** Act honorably, honestly, justly, responsibly, and legally.

✗ **B** Protect society, the commonwealth, and the infrastructure.
Incorrect. Canon 1 focuses on protecting society and infrastructure, not specifically on preserving system value or conflict of interest.

https://www.isc2.org/Ethics

✓ **C** Provide diligent and competent service to principles.
Provide diligent and competent service to principals. This is the third ISC2 Code of Ethics canon.

✗ **D** Advance and protect the profession.
Incorrect. Canon 4 deals with advancing the profession, not directly with preserving system value or avoiding conflicts of interest.

https://www.isc2.org/Ethics

Dumpsgate

Question 8

Single choice · Domain: D1 Security and Risk Management › Conduct third-party risk assessments and evaluate service provider assurance reports

When conducting a third-party risk assessment of a new supplier, which of the following reports should be reviewed to confirm the operating effectiveness of the security, availability, confidentiality, and privacy trust principles?

A. Service Organization Control (SOC) 1, Type 2
B. Service Organization Control (SOC) 2, Type 2
C. International Organization for Standardization (ISO) 27001
D. International Organization for Standardization (ISO) 27002

Answer: B. Service Organization Control (SOC) 2, Type 2

Explanation

The question tests the candidate's ability to identify the appropriate assurance report (SOC 2 Type 2) that demonstrates a supplier's operating effectiveness across the security, availability, confidentiality, and privacy trust principles.

✗ **A** Service Organization Control (SOC) 1, Type 2
Incorrect. SOC 1 reports focus on controls relevant to financial reporting, not on the security, availability, confidentiality, or privacy principles.

https://www.isc2.org/News-and-Events/Blog/What-is-a-SOC-1-Report

✓ **B** Service Organization Control (SOC) 2, Type 2

Free demo · full exam: 1485 questions

Correct. SOC 2 Type 2 reports assess the operating effectiveness of controls related to the Trust Services Criteria: security, availability, processing integrity, confidentiality, and privacy.

https://www.isc2.org/News-and-Events/Blog/What-is-a-SOC-2-Report

✗ **C** International Organization for Standardization (ISO) 27001
Incorrect. ISO 27001 is a certification of an information security management system, not a report that provides evidence of operating effectiveness for specific trust principles.

https://www.isc2.org/News-and-Events/Blog/ISO-27001-Overview

✗ **D** International Organization for Standardization (ISO) 27002
Incorrect. ISO 27002 is a code of practice providing guidelines for controls, not an assurance report demonstrating their effectiveness.

https://www.isc2.org/News-and-Events/Blog/ISO-27002-Guide

Question 9

Multiple choice · Domain: D1 Security and Risk Management › Identify the mandatory canons of the (ISC)² Code of Ethics

Which of the following are mandatory canons for the (ISC)* Code of Ethics?

A. Develop comprehensive security strategies for the organization.
B. Perform is, honestly, fairly, responsibly, and lawfully for the organization.
C. Create secure data protection policies to principals.
D. Provide diligent and competent service to principals.

Answer

- B. **Perform is, honestly, fairly, responsibly, and lawfully for the organization.**
- D. **Provide diligent and competent service to principals.**

Explanation

This question assesses knowledge of the four required canons in the (ISC)² Code of Ethics, which are covered under the Security and Risk Management domain.

✗ **A** Develop comprehensive security strategies for the organization.
Incorrect. This statement is not one of the four mandatory canons of the (ISC)² Code of Ethics. See the official canons list.

https://www.isc2.org/Ethics

✓ **B** Perform is, honestly, fairly, responsibly, and lawfully for the organization.
Correct. This aligns with Canon 2: "Act honorably, honestly, justly, responsibly, and legally.".

https://www.isc2.org/Ethics

✗ **C** Create secure data protection policies to principals.
Incorrect. While important, this is not one of the mandatory canons. The official canons are listed at.

https://www.isc2.org/Ethics

✓ **D** Provide diligent and competent service to principals.
Correct. This matches Canon 3: "Provide diligent and competent service to principals.".

https://www.isc2.org/Ethics

Free demo · full exam: 1485 questions

Question 10

Single choice · Domain: D1 Security and Risk Management › Select appropriate data protection controls to achieve regulatory compliance

An organization is preparing to achieve General Data Protection Regulation (GDPR) compliance. The Chief Information Security Officer (CISO) is reviewing data protection methods.

Which of the following is the BEST data protection method?

A. Encryption
B. Backups
C. Data obfuscation
D. Strong authentication

Answer: A. Encryption

Explanation

The question asks for the best method to protect personal data for GDPR compliance, testing the candidate's ability to choose the most effective control.

✓ **A** Encryption
Correct. Encryption provides confidentiality for personal data both at rest and in transit, which is a core requirement of GDPR's data protection principle.
https://www.isc2.org/News-and-Events/Blog/2020/05/06/Encryption-and-Data-Protection

✗ **B** Backups
Incorrect. Backups ensure data availability and recovery but do not inherently protect the confidentiality of personal data, which is the primary GDPR requirement.
https://www.isc2.org/News-and-Events/Blog/2020/05/06/Encryption-and-Data-Protection

✗ **C** Data obfuscation
Incorrect. Data obfuscation (e.g., masking) can reduce exposure but is not as comprehensive as encryption for protecting all personal data in scope of GDPR.
https://www.isc2.org/News-and-Events/Blog/2020/05/06/Encryption-and-Data-Protection

✗ **D** Strong authentication
Incorrect. Strong authentication controls access but does not protect the data itself; encryption directly safeguards the data's confidentiality, which is the best method for GDPR compliance.
https://www.isc2.org/News-and-Events/Blog/2020/05/06/Encryption-and-Data-Protection

Free demo · full exam: 1485 questions

Question 11

Single choice · Domain: D1 Security and Risk Management › Recognize and apply security awareness principles for reporting suspicious activity

A new employee formally reported suspicious behavior to the organization security team. The report claims that someone not affiliated with the organization was inquiring about the member's work location, length of employment, and building access controls. The employee's reporting is MOST likely the result of which of the following?

A. Risk avoidance
B. Security engineering
C. security awareness
D. Phishing

Answer: C. security awareness

Explanation

The question evaluates the candidate's understanding that employee reporting of suspicious behavior is driven by security awareness training, a key component of the Security and Risk Management domain.

✗ **A** Risk avoidance
Incorrect. Risk avoidance is a risk response strategy, not related to employee reporting.
https://www.isc2.org/Certifications/CISSP/Domain-1-Security-and-Risk-Management

✗ **B** Security engineering
Incorrect. Security engineering focuses on designing secure systems, not on awareness reporting.
https://www.isc2.org/Certifications/CISSP/Domain-3-Security-Architecture-and-Engineering

✓ **C** security awareness
Correct. The employee reported due to security awareness training that encourages reporting of suspicious activity.
https://www.isc2.org/Certifications/CISSP/Domain-1-Security-and-Risk-Management

✗ **D** Phishing
Incorrect. Phishing is an attack technique, not the reason for reporting.
https://www.isc2.org/Certifications/CISSP/Domain-7-Security-Operations

Free demo · full exam: 1485 questions

Question 12

Multiple choice · Domain: D1 Security and Risk Management › Identify appropriate SOC reporting type for security and availability assurance

The Chief Information Security Officer (CISO) of an organization has requested that a Service Organization Control (SOC) report be created to outline the security and availability of a particular system over a 12-month period. Which type of SOC report should be utilized?

A. SOC 1 Type 1
B. SOC 2 Type 2
C. SOC 2 Type 2
D. SOC 3 Type 1

Answer

- B. **SOC 2 Type 2**
- C. **SOC 2 Type 2**

Explanation

The question tests the candidate's knowledge of SOC audit reports and the ability to select the report that provides security and availability coverage over a defined period.

✗ **A** SOC 1 Type 1
Incorrect. SOC 1 reports address internal controls over financial reporting, and a Type 1 report provides a point-in-time description, not a 12-month security/availability assessment.
https://www.isc2.org/Certifications/CISSP

✓ **B** SOC 2 Type 2
Correct. SOC 2 Type 2 reports evaluate the Trust Services Criteria—including security and availability—over a reporting period (typically 12 months).
https://www.isc2.org/Certifications/CISSP

✓ **C** SOC 2 Type 2
Correct. As above, SOC 2 Type 2 is the appropriate report for ongoing security and availability assurance.
https://www.isc2.org/Certifications/CISSP

✗ **D** SOC 3 Type 1
Incorrect. SOC 3 provides a general-use summary without the detailed criteria needed for security and availability, and a Type 1 report is only a point-in-time snapshot.
https://www.isc2.org/Certifications/CISSP

Dumpsgate

Question 13

Single choice · Domain: D1 Security and Risk Management › Classify security measures as administrative, technical, or physical controls

employee training, risk management, and data handling procedures and policies could be characterized as which type of security measure?

A. Non-essential
B. Management
C. Preventative
D. Administrative

Answer: D. Administrative

Explanation

The question asks the candidate to identify the category of security measures that include training, risk management, and policies, which are administrative controls—a core concept in the Security and Risk Management domain.

✗ **A** Non-essential
Incorrect. Employee training, risk management, and policies are essential controls, not non-essential.
https://www.isc2.org/News-and-Events/Blog?tag=security+controls

✗ **B** Management
Incorrect. While related to management, the specific classification used in CISSP is "administrative" controls.
https://www.isc2.org/News-and-Events/Blog?tag=security+controls

✗ **C** Preventative
Incorrect. Preventative describes the purpose of a control, but the question seeks the type of control; these are administrative controls.
https://www.isc2.org/News-and-Events/Blog?tag=security+controls

✓ **D** Administrative
Correct. Training, risk management, and policies are examples of administrative security measures.
https://www.isc2.org/News-and-Events/Blog?tag=security+controls

Dumpsgate

Free demo · full exam: 1485 questions

Question 14

Single choice · Domain: D1 Security and Risk Management › Identify and differentiate service level documentation (SLR vs SLA, etc.)

Which of the following documents specifies services from the client's viewpoint?

A. Service level report
B. Business impact analysis (BIA)
C. Service level agreement (SLA)
D. Service Level Requirement (SLR)

Answer: D. Service Level Requirement (SLR)

Explanation

The question assesses the candidate's understanding of service level management artifacts, specifically the document that captures client-viewpoint service requirements.

✗ **A** Service level report
A service level report summarizes performance against agreed levels; it does not define services from the client perspective.

https://www.isc2.org/News-and-Events/Blog/Service-Level-Agreements

✗ **B** Business impact analysis (BIA)
A BIA identifies critical business functions and impacts of disruption, not service specifications from the client view.

https://www.isc2.org/News-and-Events/Blog/Service-Level-Agreements

✗ **C** Service level agreement (SLA)
An SLA is a contract that records the agreed service levels between provider and client, but the client-viewpoint requirements are captured earlier in the Service Level Requirement document.

https://www.isc2.org/News-and-Events/Blog/Service-Level-Agreements

✓ **D** Service Level Requirement (SLR)
The SLR specifies the services and performance levels required from the client's perspective before an SLA is negotiated.

https://www.isc2.org/News-and-Events/Blog/Service-Level-Agreements

Free demo · full exam: 1485 questions

Question 15

Single choice · Domain: D1 Security and Risk Management › Identify elements of a disaster recovery plan

Which of the following are all elements of a disaster recovery plan (DRP)?

A. Document the actual location of the ORP, developing an incident notification procedure, evaluating costs of critical components

B. Document the actual location of the ORP, developing an incident notification procedure, establishing recovery locations

C. Maintain proper documentation of all server logs, developing an incident notification procedure, establishing recovery locations

D. Document the actual location of the ORP, recording minutes at all ORP planning sessions, establishing recovery locations

Answer: B. Document the actual location of the ORP, developing an incident notification procedure, establishing recovery locations

Explanation

The question assesses knowledge of the components that must be included in a DRP, which is a core topic within the Security and Risk Management domain.

✗ **A** Document the actual location of the ORP, developing an incident notification procedure, evaluating costs of critical components
Incorrect. While documenting the ORP location and an incident notification procedure are DRP elements, evaluating costs of critical components is not a standard DRP element.

https://www.isc2.org/Domain-Descriptions

✓ **B** Document the actual location of the ORP, developing an incident notification procedure, establishing recovery locations
Correct. A disaster recovery plan includes documenting the Operations Recovery Plan (ORP) location, an incident notification procedure, and establishing recovery locations.

https://www.isc2.org/Domain-Descriptions

✗ **C** Maintain proper documentation of all server logs, developing an incident notification procedure, establishing recovery locations
Incorrect. Maintaining server logs is an operational activity, not a core element of a DRP. The other two items are correct DRP components.

https://www.isc2.org/Domain-Descriptions

✗ **D** Document the actual location of the ORP, recording minutes at all ORP planning sessions, establishing recovery locations
Incorrect. Recording minutes of planning sessions is a documentation practice, not a required DRP element. The essential DRP elements are ORP location, incident notification, and recovery locations.

https://www.isc2.org/Domain-Descriptions

Free demo · full exam: 1485 questions

Question 16

Single choice · Domain: D1 Security and Risk Management › Develop an information security budget aligned with risk assessment

When developing an organization's information security budget, it is important that the

A. expected risk can be managed appropriately with the funds allocated.
B. requested funds are at an equal amount to the expected cost of breaches.
C. requested funds are part of a shared funding pool with other areas.
D. expected risk to the organization does not exceed the funds allocated.

Answer: A. expected risk can be managed appropriately with the funds allocated.

Explanation

The question tests the candidate's ability to link budgeting decisions to risk management, a core skill in the Security and Risk Management domain.

✓ **A** expected risk can be managed appropriately with the funds allocated.
Correct. A budget must provide sufficient resources to manage the identified risk to an acceptable level.
https://www.isc2.org/Certifications/CISSP/Domain-1

✗ **B** requested funds are at an equal amount to the expected cost of breaches.
Incorrect. Budgets are not set to match the projected cost of breaches; they are based on risk mitigation strategies, not on covering breach costs.
https://www.isc2.org/Certifications/CISSP/Domain-1

✗ **C** requested funds are part of a shared funding pool with other areas.
Incorrect. While shared funding may occur, the primary concern is that the allocated budget addresses the specific information security risk, not merely being part of a pooled budget.
https://www.isc2.org/Certifications/CISSP/Domain-1

✗ **D** expected risk to the organization does not exceed the funds allocated.
Incorrect. Comparing risk magnitude directly to monetary funds is misleading; the budget must enable appropriate controls to reduce risk, not simply ensure risk value is less than the budget amount.
https://www.isc2.org/Certifications/CISSP/Domain-1

Free demo · full exam: 1485 questions

Question 17

Single choice · Domain: D1 Security and Risk Management › Identify high-risk application types that can introduce malware into a network

Which application type is considered high risk and provides a common way for malware and viruses to enter a network?

A. Instant messaging or chat applications
B. E-mail applications
C. Peer-to-Peer (P2P) file sharing applications
D. End-to-end applications

Answer: B. E-mail applications

Explanation

The question assesses the candidate's ability to recognize application vectors that pose a high risk for malware infection, a key aspect of risk management.

✗ **A** Instant messaging or chat applications
Instant messaging can be a vector for social engineering, but it is not the primary application type cited for widespread malware entry.

https://www.isc2.org/

✓ **B** E-mail applications
E-mail applications are widely recognized as the most common high-risk vector for malware and viruses entering a network.

https://www.isc2.org/

✗ **C** Peer-to-Peer (P2P) file sharing applications
P2P file sharing can expose systems to malicious files, yet it is less prevalent than e-mail as a primary malware delivery method.

https://www.isc2.org/

✗ **D** End-to-end applications
End-to-end applications focus on secure communication and are not typically identified as the main conduit for malware spread.

https://www.isc2.org/

Free demo · full exam: 1485 questions

Question 18

Single choice · Domain: D1 Security and Risk Management › Identify common attack vectors that lead to Remote Desktop Protocol (RDP) compromise

What is the MOST common cause of Remote Desktop Protocol (RDP) compromise?

A. Port scan
B. Brute force attack
C. Remote exploit
D. Social engineering

Answer: B. Brute force attack

Explanation

The question tests the candidate's knowledge of the most frequent threat vector used to compromise RDP services, a key aspect of risk assessment and threat modeling.

✗ **A** Port scan
Port scanning discovers open RDP ports but does not directly compromise the service. The most common compromise method is credential guessing.
https://www.isc2.org/News-and-Events/Blog/2020/06/Remote-Desktop-Protocol-RDP-Exploits

✓ **B** Brute force attack
Brute-force credential attacks are the leading cause of RDP compromise, exploiting weak or reused passwords.
https://www.isc2.org/News-and-Events/Blog/2020/06/Remote-Desktop-Protocol-RDP-Exploits

✗ **C** Remote exploit
While remote code exploits exist, they are less common than credential-guessing attacks for RDP.
https://www.isc2.org/News-and-Events/Blog/2020/06/Remote-Desktop-Protocol-RDP-Exploits

✗ **D** Social engineering
Social engineering can lead to credential theft, but the most frequent direct technical method is brute-force attacks.
https://www.isc2.org/News-and-Events/Blog/2020/06/Remote-Desktop-Protocol-RDP-Exploits

Question 19

Single choice · Domain: D1 Security and Risk Management › Identify risks associated with using commercial off-the-shelf (COTS) products

What Is a risk of using commercial off-the-shelf (COTS) products?

A. COTS products may not map directly to an organization’s security requirements.
B. COTS products are typically more expensive than developing software in-house.
C. Cost to implement COTS products is difficult to predict.
D. Vendors are often hesitant to share their source code.

Free demo · full exam: 1485 questions

Answer: A. COTS products may not map directly to an organization’s security requirements.

Explanation

The question tests the candidate's ability to recognize security risks that arise when adopting COTS solutions, which is a core competency in the Security and Risk Management domain.

✓ **A** COTS products may not map directly to an organization’s security requirements.
Correct. COTS solutions often cannot be customized to fully satisfy an organization’s specific security controls, creating a risk.

https://www.isc2.org/Certifications/CISSP

✗ **B** COTS products are typically more expensive than developing software in-house.
Incorrect. Cost is generally a benefit of COTS, not a primary security risk.

https://www.isc2.org/Certifications/CISSP

✗ **C** Cost to implement COTS products is difficult to predict.
Incorrect. While budgeting can be a concern, it is not the main security risk highlighted for COTS adoption.

https://www.isc2.org/Certifications/CISSP

✗ **D** Vendors are often hesitant to share their source code.
Incorrect. Lack of source code visibility is a concern, but the primary risk emphasized in CISSP material is the mismatch with security requirements.

https://www.isc2.org/Certifications/CISSP

Question 20

Single choice · Domain: D1 Security and Risk Management › Apply risk management concepts to security architecture design

A systems engineer is designing a wide area network (WAN) environment for a new organization. The WAN will connect sites holding information at various levels of sensitivity, from publicly available to highly confidential. The organization requires a high degree of interconnectedness to support existing business processes. What is the BEST design approach to securing this environment?

A. Place firewalls around critical devices, isolating them from the rest of the environment.
B. Layer multiple detective and preventative technologies at the environment perimeter.
C. Use reverse proxies to create a secondary "shadow" environment for critical systems.
D. Align risk across all interconnected elements to ensure critical threats are detected and handled.

Answer: D. Align risk across all interconnected elements to ensure critical threats are detected and handled.

Explanation

The question requires selecting a design approach that balances security with high interconnectedness across a WAN, testing the candidate's ability to align risk and controls across all network elements.

Free demo · full exam: 1485 questions

✗ **A** Place firewalls around critical devices, isolating them from the rest of the environment.
Incorrect. Isolating critical devices with firewalls would impede the required high degree of interconnectedness. Security and risk management guidance emphasizes balancing segmentation with business needs.

https://www.isc2.org/Certifications/CISSP/Domain-1-Security-and-Risk-Management

✗ **B** Layer multiple detective and preventative technologies at the environment perimeter.
Incorrect. Focusing solely on perimeter defenses does not address risks within the WAN itself; a comprehensive, risk-based approach is needed across all elements. See the defense-in-depth discussion in the Security Architecture and Engineering domain.

https://www.isc2.org/Certifications/CISSP/Domain-3-Security-Architecture-and-Engineering

✗ **C** Use reverse proxies to create a secondary "shadow" environment for critical systems.
Incorrect. Reverse proxies are primarily used for web traffic and do not provide a holistic security solution for a WAN spanning multiple sites with varying data sensitivity. Refer to network security controls in the Communication and Network Security domain.

https://www.isc2.org/Certifications/CISSP/Domain-4-Communication-and-Network-Security

✓ **D** Align risk across all interconnected elements to ensure critical threats are detected and handled.
Correct. A risk-based design that aligns security controls with the sensitivity of data across all interconnected WAN elements ensures both protection and the required level of connectivity. This reflects the core principle of Security and Risk Management.

https://www.isc2.org/Certifications/CISSP/Domain-1-Security-and-Risk-Management

Dumpsgate

Question 21

Single choice · Domain: D1 Security and Risk Management › Identify the scope of GDPR and apply its privacy requirements

An organization with divisions in the United States (US) and the United Kingdom (UK) processes data comprised of personal information belonging to subjects living in the European Union (EU) and in the US. Which data MUST be handled according to the privacy protections of General Data Protection Regulation (GDPR)?

A. Only the EU citizens' data
B. Only the EU residents' data
C. Only the UK citizens' data
D. Only data processed in the UK

Answer: B. Only the EU residents' data

Explanation

The question tests the candidate's knowledge of GDPR applicability to personal data of individuals located in the EU, regardless of citizenship or processing location.

✗ **A** Only the EU citizens' data
Incorrect. GDPR applies based on the data subject's location, not citizenship.

https://www.isc2.org/News-and-Events/Blog/2018/05/25/What-is-the-GDPR

✓ **B** Only the EU residents' data
Correct. GDPR protects personal data of individuals residing in the EU, irrespective of their nationality or

Free demo · full exam: 1485 questions

where the data is processed.

https://www.isc2.org/News-and-Events/Blog/2018/05/25/What-is-the-GDPR

✗ **C** Only the UK citizens' data
Incorrect. Post-Brexit, the UK is no longer covered by GDPR for its citizens; GDPR scope is limited to the EU.

https://www.isc2.org/News-and-Events/Blog/2018/05/25/What-is-the-GDPR

✗ **D** Only data processed in the UK
Incorrect. GDPR applies to data of EU-located subjects, not merely where processing occurs, and the UK is outside the EU jurisdiction.

https://www.isc2.org/News-and-Events/Blog/2018/05/25/What-is-the-GDPR

Question 22

Single choice · Domain: D1 Security and Risk Management › Identify traits of crisis management in disaster recovery testing

In a disaster recovery (DR) test, which of the following would be a trait of crisis management?

A. Wide focus
B. Strategic
C. Anticipate
D. Process

Answer: A. Wide focus

Explanation

The question assesses knowledge of crisis management characteristics, which are part of Business Continuity and Disaster Recovery concepts within the Security and Risk Management domain.

✓ **A** Wide focus
Correct. Crisis management requires a wide focus across the organization to coordinate response efforts.

https://www.isc2.org/Certifications/CISSP/Domain-1

✗ **B** Strategic
Incorrect. While strategic planning is part of business continuity, crisis management is more tactical and operational during an incident.

https://www.isc2.org/Certifications/CISSP/Domain-1

✗ **C** Anticipate
Incorrect. Anticipation relates to risk assessment and prevention, not the immediate traits of crisis management.

https://www.isc2.org/Certifications/CISSP/Domain-1

✗ **D** Process
Incorrect. Process describes procedures, whereas crisis management emphasizes a broad, coordinated focus during an emergency.

https://www.isc2.org/Certifications/CISSP/Domain-1

Free demo · full exam: 1485 questions

Question 23

Single choice · Domain: D1 Security and Risk Management › Explain the CIA triad

What BEST describes the confidentiality, integrity, availability triad?

A. A tool used to assist in understanding how to protect the organization's data
B. The three-step approach to determine the risk level of an organization
C. The implementation of security systems to protect the organization's data
D. A vulnerability assessment to see how well the organization's data is protected

Answer: A. A tool used to assist in understanding how to protect the organization's data

Explanation

The question asks for the best description of the confidentiality, integrity, and availability (CIA) triad, which is a fundamental concept in security and risk management.

✓ **A** A tool used to assist in understanding how to protect the organization's data
Correct. The CIA triad is a conceptual model (a tool) that helps organizations understand and protect data by focusing on confidentiality, integrity, and availability.
https://www.isc2.org/Blog/2020/03/03/What-is-the-CIA-Triad

✗ **B** The three-step approach to determine the risk level of an organization
Incorrect. Determining risk level involves risk assessment processes, not the CIA triad. The CIA triad defines security goals, not a risk calculation method.
https://www.isc2.org/Blog/2020/03/03/What-is-the-CIA-Triad

✗ **C** The implementation of security systems to protect the organization's data
Incorrect. Implementing security systems are controls that address the CIA objectives, but the triad itself is not the implementation.
https://www.isc2.org/Blog/2020/03/03/What-is-the-CIA-Triad

✗ **D** A vulnerability assessment to see how well the organization's data is protected
Incorrect. A vulnerability assessment is a testing activity, whereas the CIA triad is a model describing core security principles.
https://www.isc2.org/Blog/2020/03/03/What-is-the-CIA-Triad

Question 24

Single choice · Domain: D1 Security and Risk Management › Define security program objectives and scope

Which of the following is the FIRST step an organization's security professional performs when defining a cyber-security program based upon industry standards?

A. Map the organization's current security practices to industry standards and frameworks.
B. Define the organization's objectives regarding security and risk mitigation.
C. Select from a choice of security best practices.
D. Review the past security assessments.

Free demo · full exam: 1485 questions

Answer: B. Define the organization's objectives regarding security and risk mitigation.

Explanation

The question tests the candidate's ability to initiate a cybersecurity program by first establishing the organization's security and risk mitigation objectives, which is a core skill in security governance.

✗ **A** Map the organization's current security practices to industry standards and frameworks.
Mapping current practices is performed after objectives are set, not as the first step.
https://www.isc2.org/Certifications/CISSP

✓ **B** Define the organization's objectives regarding security and risk mitigation.
Establishing security and risk mitigation objectives is the initial activity when creating a cyber-security program based on standards.
https://www.isc2.org/Certifications/CISSP

✗ **C** Select from a choice of security best practices.
Choosing best practices follows the definition of objectives and the mapping of current controls.
https://www.isc2.org/Certifications/CISSP

✗ **D** Review the past security assessments.
Reviewing past assessments informs gaps after objectives are defined; it is not the first step.
https://www.isc2.org/Certifications/CISSP

Question 25

Single choice · Domain: D1 Security and Risk Management › Select and apply appropriate risk response strategies, such as compensating controls, when patches cannot be deployed

A scan report returned multiple vulnerabilities affecting several production servers that are mission critical. Attempts to apply the patches in the development environment have caused the servers to crash. What is the BEST course of action?

A. Upgrade the software affected by the vulnerability.
B. Inform management of possible risks.
C. Mitigate the risks with compensating controls.
D. Remove the affected software from the servers.

Answer: C. Mitigate the risks with compensating controls.

Explanation

The question tests the candidate's ability to choose the proper risk mitigation approach for mission-critical systems when patching is not feasible.

✗ **A** Upgrade the software affected by the vulnerability.
Upgrading may not be possible if patches cause crashes; the immediate step is to mitigate risk rather than attempt another upgrade.
https://www.isc2.org/Certifications/CISSP/Domain-1

Free demo · full exam: 1485 questions

✗ **B** Inform management of possible risks.
While informing management is required, it does not address the immediate risk to the production servers.

https://www.isc2.org/Certifications/CISSP/Domain-1

✓ **C** Mitigate the risks with compensating controls.
When patches cannot be applied, the best action is to implement compensating controls to reduce risk until a safe fix is available.

https://www.isc2.org/Certifications/CISSP/Domain-1

✗ **D** Remove the affected software from the servers.
Removing mission-critical software would likely disrupt business operations and is not the preferred first response.

https://www.isc2.org/Certifications/CISSP/Domain-1

Question 26

Single choice · Domain: D1 Security and Risk Management › Develop baseline security standards for third-party suppliers

An enterprise is developing a baseline cybersecurity standard its suppliers must meet before being awarded a contract. Which of the following statements is TRUE about the baseline cybersecurity standard?

A. It should be expressed as general requirements.
B. It should be expressed in legal terminology.
C. It should be expressed in business terminology.
D. It should be expressed as technical requirements.

Answer: C. It should be expressed in business terminology.

Explanation

The question tests the candidate's ability to define how a baseline cybersecurity standard should be expressed, which is a governance activity within the Security and Risk Management domain.

✗ **A** It should be expressed as general requirements.
Incorrect. Baseline standards need to be tied to business objectives, not merely vague general requirements.

https://www.isc2.org/Certifications/CISSP/Domain-1

✗ **B** It should be expressed in legal terminology.
Incorrect. While legal considerations are important, the baseline standard should be understandable to business stakeholders, not written in legal jargon.

https://www.isc2.org/Certifications/CISSP/Domain-1

✓ **C** It should be expressed in business terminology.
Correct. Baseline cybersecurity standards are typically expressed in business terms to align with organizational risk appetite and to be clear to suppliers.

https://www.isc2.org/Certifications/CISSP/Domain-1

✗ **D** It should be expressed as technical requirements.
Incorrect. Technical details are too granular for a baseline standard; the standard should focus on

Free demo · full exam: 1485 questions

business-level requirements.
https://www.isc2.org/Certifications/CISSP/Domain-1

Question 27

Single choice · Domain: D1 Security and Risk Management › Identify modern NIST risk management goals

Which of the following goals represents a modern shift in risk management according to National Institute of Standards and Technology (NIST)?

A. Focus on operating environments that are changing, evolving, and full of emerging threats.
B. Secure information technology (IT) systems that store, process, or transmit organizational information.
C. Enable management to make well-informed risk-based decisions justifying security expenditure.
D. Provide an improved mission accomplishment approach.

Answer: A. Focus on operating environments that are changing, evolving, and full of emerging threats.

Explanation

The question tests knowledge of the updated NIST approach to risk management, which emphasizes adapting to changing operating environments and emerging threats.

✓ **A** Focus on operating environments that are changing, evolving, and full of emerging threats.
Correct. NIST's modern risk management guidance highlights the need to address dynamic, evolving environments and emerging threats.
https://www.isc2.org/Certifications/CISSP

✗ **B** Secure information technology (IT) systems that store, process, or transmit organizational information.
Incorrect. This reflects a traditional focus on protecting IT assets rather than the newer emphasis on changing environments.
https://www.isc2.org/Certifications/CISSP

✗ **C** Enable management to make well-informed risk-based decisions justifying security expenditure.
Incorrect. While important, this goal aligns with classic risk-based decision making, not the modern shift described by NIST.
https://www.isc2.org/Certifications/CISSP

✗ **D** Provide an improved mission accomplishment approach.
Incorrect. This option does not capture the specific NIST focus on evolving operating environments and emerging threats.
https://www.isc2.org/Certifications/CISSP

Free demo · full exam: 1485 questions

Question 28

Single choice · Domain: D1 Security and Risk Management › Identify applicable laws, regulations, and standards

Which of the following regulations dictates how data breaches are handled?

A. Sarbanes-Oxley (SOX)
B. National Institute of Standards and Technology (NIST)
C. Payment Card Industry Data Security Standard (PCI-DSS)
D. General Data Protection Regulation (GDPR)

Answer: D. General Data Protection Regulation (GDPR)

Explanation

The question assesses the candidate's ability to recognize which regulation specifically mandates breach handling and notification procedures.

✗ **A** Sarbanes-Oxley (SOX)
Incorrect. SOX focuses on financial reporting and internal controls, not on data breach handling.
https://www.isc2.org/News-and-Events/Blog/2018/05/25/What-is-the-GDPR

✗ **B** National Institute of Standards and Technology (NIST)
Incorrect. NIST provides frameworks and guidelines, but it is not a regulation that dictates breach handling requirements.
https://www.isc2.org/News-and-Events/Blog/2018/05/25/What-is-the-GDPR

✗ **C** Payment Card Industry Data Security Standard (PCI-DSS)
Incorrect. PCI-DSS includes breach reporting for cardholder data, but the question asks for a regulation, and PCI-DSS is an industry standard, not a legal regulation.
https://www.isc2.org/News-and-Events/Blog/2018/05/25/What-is-the-GDPR

✓ **D** General Data Protection Regulation (GDPR)
Correct. GDPR mandates specific breach notification timelines and procedures for personal data breaches.
https://www.isc2.org/News-and-Events/Blog/2018/05/25/What-is-the-GDPR

Question 29

Single choice · Domain: D1 Security and Risk Management › Identify change management roles and responsibilities

Which change management role is responsible for the overall success of the project and supporting the change throughout the organization?

A. Change driver
B. Change implementer
C. Program sponsor
D. Project manager

Free demo · full exam: 1485 questions

Answer: C. Program sponsor

Explanation

The question tests knowledge of organizational change management structures, a key component of security governance covered in the Security and Risk Management domain.

✗ **A** Change driver
Incorrect. The change driver initiates the need for change but is not accountable for overall project success.

https://www.isc2.org/News-and-Events/Blog/Change-Management

✗ **B** Change implementer
Incorrect. The change implementer executes specific change activities; responsibility for overall success lies elsewhere.

https://www.isc2.org/News-and-Events/Blog/Change-Management

✓ **C** Program sponsor
Correct. The program sponsor provides executive support, ensures resources, and is accountable for the overall success of the change initiative across the organization.

https://www.isc2.org/News-and-Events/Blog/Change-Management

✗ **D** Project manager
Incorrect. The project manager manages day-to-day project tasks but does not carry the ultimate responsibility for organization-wide change adoption.

https://www.isc2.org/News-and-Events/Blog/Change-Management

Question 30

Single choice · Domain: D2 Asset Security › Identify and classify information assets

Which of the fallowing statements is MOST accurate regarding information assets?

A. International Organization for Standardization (ISO) 27001 compliance specifies which information assets must be included in asset inventory.
B. S3 Information assets include any information that is valuable to the organization,
C. Building an information assets register is a resource-intensive job.
D. Information assets inventory is not required for risk assessment.

Answer: B. S3 Information assets include any information that is valuable to the organization,

Explanation

The question tests the candidate's understanding of what constitutes an information asset and the need for an asset inventory in risk management.

✗ **A** International Organization for Standardization (ISO) 27001 compliance specifies which information assets must be included in asset inventory.
Incorrect. ISO/IEC 27001 requires an asset inventory but does not dictate which specific assets must be

Free demo · full exam: 1485 questions

listed.
https://www.isc2.org/Certifications/CISSP

✓ **B** S3 Information assets include any information that is valuable to the organization,
Correct. An information asset is any data or information that holds value to the organization.
https://www.isc2.org/Certifications/CISSP

✗ **C** Building an information assets register is a resource-intensive job.
While creating a register may require effort, this statement does not accurately define information assets.
https://www.isc2.org/Certifications/CISSP

✗ **D** Information assets inventory is not required for risk assessment.
Incorrect. An asset inventory is a prerequisite for conducting a risk assessment.
https://www.isc2.org/Certifications/CISSP

Question 31

Single choice · Domain: D2 Asset Security › Identify inference attacks on databases

What type of database attack would allow a customer service employee to determine quarterly sales results before they are publically announced?

A. Polyinstantiation
B. Inference
C. Aggregation
D. Data mining

Answer: B. Inference

Explanation

The question tests knowledge of database attacks, specifically the inference attack that allows deduction of confidential information such as quarterly sales results.

✗ **A** Polyinstantiation
Incorrect. Polyinstantiation is a technique to store multiple versions of data at different classification levels, not a method for deducing confidential information.
https://www.isc2.org/News-and-Events/Blog

✓ **B** Inference
Correct. An inference attack allows a user to deduce sensitive data (e.g., quarterly sales) from seemingly non-sensitive data.
https://www.isc2.org/News-and-Events/Blog

✗ **C** Aggregation
Incorrect. Aggregation combines data from multiple sources but does not specifically describe the deduction of confidential results before release.
https://www.isc2.org/News-and-Events/Blog

✗ **D** Data mining
Incorrect. Data mining involves analyzing large datasets for patterns; it is not the specific attack type that infers confidential sales results.
https://www.isc2.org/News-and-Events/Blog

Free demo · full exam: 1485 questions

Question 32

Single choice · Domain: D2 Asset Security › Identify common components of big data architectures

When determining data and information asset handling, regardless of the specific toolset being used, which of the following is one of the common components of big data?

A. Consolidated data collection
B. Distributed storage locations
C. Distributed data collection
D. Centralized processing location

Answer: B. Distributed storage locations

Explanation

The question tests knowledge of data handling concepts, specifically recognizing architectural elements of big data, which falls under asset security and data protection.

✗ **A** Consolidated data collection
Incorrect. Big data typically relies on distributed collection rather than a single consolidated source.
https://www.isc2.org/News/Big-Data-Analytics

✓ **B** Distributed storage locations
Correct. Distributed storage locations are a fundamental component of big data architectures, enabling horizontal scaling and fault tolerance.
https://www.isc2.org/News/Big-Data-Analytics

✗ **C** Distributed data collection
Incorrect. While data collection can be distributed, the more distinctive component highlighted in big data design is distributed storage.
https://www.isc2.org/News/Big-Data-Analytics

✗ **D** Centralized processing location
Incorrect. Big data processing is typically performed in a distributed manner (e.g., MapReduce), not centralized.
https://www.isc2.org/News/Big-Data-Analytics

Question 33

Single choice · Domain: D2 Asset Security › Identify appropriate reference architecture tier for asset tracking

An organization is looking to include mobile devices in its asset management system for better tracking. In which system tier of the reference architecture would mobile devices be tracked?

A. 0
B. 1
C. 2
D. 3

Free demo · full exam: 1485 questions

Answer: A. 0

Explanation

The question tests knowledge of the CISSP reference architecture tiers and where physical assets such as mobile devices are classified.

✓ **A** 0
Correct. Mobile devices are physical hardware assets and are tracked in Tier 0 of the CISSP reference architecture, which covers physical assets.
https://www.isc2.org/News-and-Events/Reference-Architecture

✗ **B** 1
Incorrect. Tier 1 represents the network layer, which includes routers, switches, and other networking components, not individual mobile devices.
https://www.isc2.org/News-and-Events/Reference-Architecture

✗ **C** 2
Incorrect. Tier 2 corresponds to the system layer (servers, operating systems). Mobile devices are not classified at this tier.
https://www.isc2.org/News-and-Events/Reference-Architecture

✗ **D** 3
Incorrect. Tier 3 is the application layer, which includes software applications and services, not hardware assets like mobile devices.
https://www.isc2.org/News-and-Events/Reference-Architecture

Question 34

Single choice · Domain: D2 Asset Security › Implement whole-device encryption and key management for mobile devices

Which of the following features is MOST effective in mitigating against theft of data on a corporate mobile device which has been stolen?

A. Mobile Device Management (MDM) with device wipe
B. Whole device encryption with key escrow
C. Virtual private network (VPN) with traffic encryption
D. Mobile device tracking with geolocation

Answer: B. Whole device encryption with key escrow

Explanation

The question assesses the candidate's ability to select the most effective data protection control for mobile devices, which is covered under the Asset Security domain of the CISSP CBK.

✗ **A** Mobile Device Management (MDM) with device wipe
Incorrect. Remote wipe can delete data only when the device is reachable and does not protect data that

Free demo · full exam: 1485 questions

may be accessed before the wipe occurs.

https://www.isc2.org/Certifications/CISSP

✓ **B** Whole device encryption with key escrow
Correct. Whole-device encryption safeguards data at rest on a stolen device; key escrow allows the organization to recover encrypted data if needed.

https://www.isc2.org/Certifications/CISSP

✗ **C** Virtual private network (VPN) with traffic encryption
Incorrect. VPN encrypts network traffic but does not protect data stored on the device itself, so it does not mitigate data theft from a stolen device.

https://www.isc2.org/Certifications/CISSP

✗ **D** Mobile device tracking with geolocation
Incorrect. Geolocation helps locate a lost or stolen device but does not provide any protection for the data stored on it.

https://www.isc2.org/Certifications/CISSP

Question 35

Single choice · Domain: D3 Security Architecture and Engineering › Design physical security controls such as mantraps

Which of the following is an important design feature for the outer door o f a mantrap?

A. Allow it to be opened by an alarmed emergency button.
B. Do not allow anyone to enter it alone.
C. Do not allow it to be observed by dosed-circuit television (CCTV) cameras.
D. Allow it be opened when the inner door of the mantrap is also open

Answer: A. Allow it to be opened by an alarmed emergency button.

Explanation

The question tests knowledge of physical security design principles for a mantrap, which falls under the Security Architecture and Engineering domain.

✓ **A** Allow it to be opened by an alarmed emergency button.
Correct. The outer door of a mantrap must provide a means of emergency egress, typically via an alarmed emergency release button, to meet fire and life-safety requirements.

https://www.isc2.org/Certifications/CISSP

✗ **B** Do not allow anyone to enter it alone.
Incorrect. Mantraps are designed to isolate a single individual for authentication; restricting entry to groups defeats the purpose.

https://www.isc2.org/Certifications/CISSP

✗ **C** Do not allow it to be observed by dosed-circuit television (CCTV) cameras.
Incorrect. CCTV monitoring is a recommended security measure for mantraps, not a design restriction.

https://www.isc2.org/Certifications/CISSP

✗ **D** Allow it be opened when the inner door of the mantrap is also open
Incorrect. The outer door must not be operable while the inner door is open to prevent tailgating and maintain the security function of the mantrap.

https://www.isc2.org/Certifications/CISSP

Question 36

Single choice · Domain: D3 Security Architecture and Engineering › Design network segmentation and DMZ monitoring to protect mobile device VPN access

Which of the following BEST describes the use of network architecture in reducing corporate risks associated with mobile devices?

A. Maintaining a "closed applications model on all mobile devices depends on demilitarized 2one (DM2) servers

B. Split tunneling enabled for mobile devices improves demilitarized zone (DMZ) security posture

C. Segmentation and demilitarized zone (DMZ) monitoring are implemented to secure a virtual private network (VPN) access for mobile devices

D. Applications that manage mobile devices are located in an Internet demilitarized zone (DMZ)

Answer: C. Segmentation and demilitarized zone (DMZ) monitoring are implemented to secure a virtual private network (VPN) access for mobile devices

Explanation

The question assesses the candidate's ability to apply network architecture concepts, such as segmentation and DMZ monitoring, to mitigate risks associated with mobile devices.

✗ **A** Maintaining a "closed applications model on all mobile devices depends on demilitarized 2one (DM2) servers
Incorrect. A closed applications model relies on application control, not on DMZ servers; network architecture for mobile risk reduction focuses on segmentation and secure VPN access.

https://www.isc2.org/Certifications/CISSP

✗ **B** Split tunneling enabled for mobile devices improves demilitarized zone (DMZ) security posture
Incorrect. Split tunneling can expose the corporate network to external threats and is generally discouraged for mobile devices.

https://www.isc2.org/Certifications/CISSP

✓ **C** Segmentation and demilitarized zone (DMZ) monitoring are implemented to secure a virtual private network (VPN) access for mobile devices
Correct. Using network segmentation and DMZ monitoring to protect VPN connections is a best practice for reducing corporate risk from mobile devices.

https://www.isc2.org/Certifications/CISSP

✗ **D** Applications that manage mobile devices are located in an Internet demilitarized zone (DMZ)
Incorrect. Placing mobile device management applications in an Internet-facing DMZ increases exposure rather than reducing risk.

https://www.isc2.org/Certifications/CISSP

Free demo · full exam: 1485 questions

Question 37

Single choice · Domain: D3 Security Architecture and Engineering › Apply threat modeling to evaluate secure design principles of network and software architectures

Which of the following techniques evaluates the secure design principles of network OF software architectures?

A. Risk modeling
B. Threat modeling
C. Fuzzing
D. Waterfall method

Answer: B. Threat modeling

Explanation

The question asks which technique assesses secure design principles, which is a core skill in the Security Architecture and Engineering domain.

✗ **A** Risk modeling
Risk modeling focuses on identifying and quantifying risks, not on evaluating design principles.
https://www.isc2.org/News-and-Events/Blog/2020/Threat-Modeling

✓ **B** Threat modeling
Threat modeling is used to analyze and evaluate the security of design architectures, matching the question.
https://www.isc2.org/News-and-Events/Blog/2020/Threat-Modeling

✗ **C** Fuzzing
Fuzzing is a testing technique that discovers implementation bugs, not a design evaluation method.
https://www.isc2.org/News-and-Events/Blog/2020/Threat-Modeling

✗ **D** Waterfall method
The waterfall method is a software development lifecycle model, not a technique for evaluating secure design.
https://www.isc2.org/News-and-Events/Blog/2020/Threat-Modeling

Free demo · full exam: 1485 questions

Question 38

Single choice · Domain: D3 Security Architecture and Engineering › Identify key management challenges associated with symmetric key distribution

Which of the following is the MOST significant key management problem due to the number of keys created?

A. Keys are more difficult to provision and
B. Storage of the keys require increased security
C. Exponential growth when using asymmetric keys
D. Exponential growth when using symmetric keys

Answer: D. Exponential growth when using symmetric keys

Explanation

The question tests knowledge of how the number of keys required grows with different cryptographic schemes, a core concept in cryptography within the Security Architecture and Engineering domain.

✗ **A** Keys are more difficult to provision and
Provisioning difficulty is a concern but not the most significant issue related to the sheer number of keys.
https://www.isc2.org/News-and-Events/Blog/Key-Management-Considerations

✗ **B** Storage of the keys require increased security
While secure storage is important, it does not represent the primary problem caused by the volume of keys.
https://www.isc2.org/News-and-Events/Blog/Key-Management-Considerations

✗ **C** Exponential growth when using asymmetric keys
Asymmetric key pairs grow linearly with the number of entities, not exponentially.
https://www.isc2.org/News-and-Events/Blog/Key-Management-Considerations

✓ **D** Exponential growth when using symmetric keys
Symmetric key distribution requires a unique key for each pair of entities, leading to O(n^2) exponential growth as the number of users increases.
https://www.isc2.org/News-and-Events/Blog/Key-Management-Considerations

Free demo · full exam: 1485 questions

Question 39

Single choice · Domain: D3 Security Architecture and Engineering › Identify cloud service models (IaaS, PaaS, SaaS) and their responsibility boundaries

An organization is considering partnering with a third-party supplier of cloud services. The organization will only be providing the data and the third-party supplier will be providing the security controls. Which of the following BEST describes this service offering?

A. Platform as a Service (PaaS)
B. Infrastructure as a Service (IaaS)
C. Software as a Service (SaaS)
D. Anything as a Service (XaaS)

Answer: C. Software as a Service (SaaS)

Explanation

The question tests knowledge of cloud service delivery models and which party is responsible for security controls, a key concept in security architecture.

✗ **A** Platform as a Service (PaaS)
Incorrect. In PaaS the provider supplies the platform and underlying security, but the organization still manages its applications and data.
https://www.isc2.org/Certifications/CISSP

✗ **B** Infrastructure as a Service (IaaS)
Incorrect. IaaS provides virtualized compute, storage, and networking; the organization is responsible for operating systems, applications, and data security.
https://www.isc2.org/Certifications/CISSP

✓ **C** Software as a Service (SaaS)
Correct. SaaS delivers fully managed software where the provider handles security controls and the customer only supplies data.
https://www.isc2.org/Certifications/CISSP

✗ **D** Anything as a Service (XaaS)
Incorrect. XaaS is a generic term for various service models and does not specifically describe the scenario where the provider handles all security controls.
https://www.isc2.org/Certifications/CISSP

Dumpsgate

Question 40

Single choice · Domain: D3 Security Architecture and Engineering › Apply cryptographic and emerging technologies to ensure data integrity and authenticity of transactions

Which of the following BEST ensures the integrity of transactions to intended recipients?

A. Public key infrastructure (PKI)
B. Blockchain technology
C. Pre-shared key (PSK)
D. Web of trust

Answer: B. Blockchain technology

Explanation

The question tests knowledge of mechanisms that protect the integrity of transactional data, a core skill in security architecture and engineering.

✗ **A** Public key infrastructure (PKI)
PKI provides digital signatures for integrity and authentication, but it does not inherently guarantee the integrity of a sequence of transactions across multiple parties.
https://www.isc2.org/News-and-Events/Blog/Blockchain-and-Cybersecurity

✓ **B** Blockchain technology
Blockchain creates an immutable ledger where each transaction is cryptographically linked to the previous one, ensuring integrity of transactions to intended recipients.
https://www.isc2.org/News-and-Events/Blog/Blockchain-and-Cybersecurity

✗ **C** Pre-shared key (PSK)
A PSK is a symmetric secret used for authentication and encryption; it does not provide the distributed, tamper-evident properties needed to ensure transaction integrity across recipients.
https://www.isc2.org/News-and-Events/Blog/Blockchain-and-Cybersecurity

✗ **D** Web of trust
Web of trust is a decentralized model for verifying identities, primarily used for authenticity, not for guaranteeing the integrity of transaction records.
https://www.isc2.org/News-and-Events/Blog/Blockchain-and-Cybersecurity

Free demo · full exam: 1485 questions

Question 41

Single choice · Domain: D3 Security Architecture and Engineering › Identify firewall types and their inspection methods

Which of the following types of firewall only examines the “handshaking” between packets before forwarding traffic?

A. Proxy firewalls
B. Host-based firewalls
C. Circuit-level firewalls
D. Network Address Translation (NAT) firewalls

Answer: C. Circuit-level firewalls

Explanation

The question tests knowledge of firewall categories, specifically the inspection level of circuit-level firewalls.

✗ **A** Proxy firewalls
Proxy firewalls operate at the application layer and inspect the content of traffic, not just handshaking.
https://www.isc2.org/News-and-Events/Blog?search=firewall

✗ **B** Host-based firewalls
Host-based firewalls run on individual devices and filter traffic based on rules, not limited to handshaking.
https://www.isc2.org/News-and-Events/Blog?search=firewall

✓ **C** Circuit-level firewalls
Circuit-level firewalls monitor the TCP/UDP handshaking process and allow packets through once a session is established, without inspecting payload.
https://www.isc2.org/News-and-Events/Blog?search=firewall

✗ **D** Network Address Translation (NAT) firewalls
NAT firewalls translate IP addresses but do not specifically examine handshaking; they operate at the network layer.
https://www.isc2.org/News-and-Events/Blog?search=firewall

Question 42

Single choice · Domain: D3 Security Architecture and Engineering › Identify key exchange algorithms based on the discrete logarithm problem

Which algorithm gets its security from the difficulty of calculating discrete logarithms in a finite field and is used to distribute keys, but cannot be used to encrypt or decrypt messages?

A. Diffie-Hellman
B. Digital Signature Algorithm (DSA)
C. Rivest-Shamir-Adleman (RSA)
D. Kerberos

Free demo · full exam: 1485 questions

Answer: A. Diffie-Hellman

Explanation

The question tests knowledge of cryptographic algorithms that rely on discrete logarithms for security and are used for key distribution rather than encryption/decryption.

✓ **A** Diffie-Hellman
Correct. Diffie-Hellman is a key-exchange algorithm whose security is based on the difficulty of solving discrete logarithms in a finite field and is not used for encrypting or decrypting messages.
https://www.isc2.org/Certifications/CISSP/CBK

✗ **B** Digital Signature Algorithm (DSA)
Incorrect. DSA is a digital signature algorithm that also relies on discrete logarithms, but it is used for signing, not for key distribution.
https://www.isc2.org/Certifications/CISSP/CBK

✗ **C** Rivest-Shamir-Adleman (RSA)
Incorrect. RSA is based on the difficulty of factoring large integers, not on discrete logarithms, and it can be used for both encryption/decryption and digital signatures.
https://www.isc2.org/Certifications/CISSP/CBK

✗ **D** Kerberos
Incorrect. Kerberos is an authentication protocol that uses symmetric key cryptography; it does not rely on discrete logarithms for its security.
https://www.isc2.org/Certifications/CISSP/CBK

Question 43

Single choice · Domain: D3 Security Architecture and Engineering › Apply system hardening techniques to reduce the attack surface

Which of the following is the BEST option to reduce the network attack surface of a system?

A. Ensuring that there are no group accounts on the system
B. Removing unnecessary system user accounts
C. Disabling unnecessary ports and services
D. Uninstalling default software on the system

Answer: C. Disabling unnecessary ports and services

Explanation

The question assesses the candidate's ability to identify the most effective hardening measure for minimizing a system's network attack surface.

✗ **A** Ensuring that there are no group accounts on the system
Group accounts affect privilege management but do not directly reduce the network attack surface.
https://www.isc2.org/Certifications/CISSP

Free demo · full exam: 1485 questions

✗ **B** Removing unnecessary system user accounts
Removing unused user accounts improves account management, yet it does not primarily address exposed network ports or services.
https://www.isc2.org/Certifications/CISSP

✓ **C** Disabling unnecessary ports and services
Disabling unused ports and services directly reduces the number of entry points an attacker can exploit, which is the most effective way to shrink the network attack surface.
https://www.isc2.org/Certifications/CISSP

✗ **D** Uninstalling default software on the system
While removing default software can reduce vulnerabilities, it is less directly tied to minimizing exposed network interfaces compared to disabling ports/services.
https://www.isc2.org/Certifications/CISSP

Question 44

Single choice · Domain: D3 Security Architecture and Engineering › Apply HTTP security headers to mitigate client-side attacks

What Hypertext Transfer Protocol (HTTP) response header can be used to disable the execution of inline JavaScript and the execution of eval()-type functions?

A. Strict-Transport-Security
B. X-XSS-Protection
C. X-Frame-Options
D. Content-Security-Policy

Answer: D. Content-Security-Policy

Explanation

The question tests knowledge of web security controls, specifically which HTTP response header can be used to prevent execution of inline JavaScript and eval functions.

✗ **A** Strict-Transport-Security
Incorrect. HSTS forces HTTPS connections but does not control script execution.
https://www.isc2.org/Certifications/CISSP

✗ **B** X-XSS-Protection
Incorrect. X-XSS-Protection enables the browser's XSS filter but does not block inline scripts or eval().
https://www.isc2.org/Certifications/CISSP

✗ **C** X-Frame-Options
Incorrect. X-Frame-Options mitigates clickjacking by controlling framing, not script execution.
https://www.isc2.org/Certifications/CISSP

✓ **D** Content-Security-Policy
Correct. CSP can restrict script sources and disallow 'unsafe-inline' and 'unsafe-eval', thereby preventing inline JavaScript and eval() execution.
https://www.isc2.org/News-and-Events/Blog/Content-Security-Policy

Free demo · full exam: 1485 questions

Question 45

Single choice · Domain: D3 Security Architecture and Engineering › Identify limitations of the Bell-LaPadula confidentiality model

Which of the following is a limitation of the Bell-LaPadula model?

A. Segregation of duties (SoD) is difficult to implement as the "no read-up" rule limits the ability of an object to access information with a higher classification.

B. Mandatory access control (MAC) is enforced at all levels making discretionary access control (DAC) impossible to implement.

C. It contains no provision or policy for changing data access control and works well only with access systems that are static in nature.

D. It prioritizes integrity over confidentiality which can lead to inadvertent information disclosure.

Answer: C. It contains no provision or policy for changing data access control and works well only with access systems that are static in nature.

Explanation

The question tests knowledge of the Bell-LaPadula model, which is covered under the Security Architecture and Engineering domain of the CISSP CBK.

✗ **A** Segregation of duties (SoD) is difficult to implement as the "no read-up" rule limits the ability of an object to access information with a higher classification.
Bell-LaPadula focuses on confidentiality and does not address segregation of duties; SoD is not a limitation of the model.

https://www.isc2.org/Certifications/CISSP/Domain-3

✗ **B** Mandatory access control (MAC) is enforced at all levels making discretionary access control (DAC) impossible to implement.
While Bell-LaPadula is a MAC model, it does not preclude the use of DAC overlays; this is not a stated limitation.

https://www.isc2.org/Certifications/CISSP/Domain-3

✓ **C** It contains no provision or policy for changing data access control and works well only with access systems that are static in nature.
A known limitation of Bell-LaPadula is that it assumes a static access environment and provides no mechanism for dynamic changes to access rights.

https://www.isc2.org/Certifications/CISSP/Domain-3

✗ **D** It prioritizes integrity over confidentiality which can lead to inadvertent information disclosure.
Bell-LaPadula actually prioritizes confidentiality over integrity; the statement reverses the model's focus and is therefore incorrect.

https://www.isc2.org/Certifications/CISSP/Domain-3

Free demo · full exam: 1485 questions

Question 46

Single choice · Domain: D3 Security Architecture and Engineering › Apply memory protection techniques such as ASLR to mitigate buffer overflow attacks

A security architect is developing an information system for a client. One of the requirements is to deliver a platform that mitigates against common vulnerabilities and attacks, What is the MOST efficient option used to prevent buffer overflow attacks?

A. Process isolation
B. Address Space Layout Randomization (ASLR)
C. Processor states
D. Access control mechanisms

Answer: B. Address Space Layout Randomization (ASLR)

Explanation

The question assesses the candidate's knowledge of architectural controls that reduce the risk of software vulnerabilities, specifically the use of ASLR to prevent exploitation of buffer overflows.

✗ **A** Process isolation
Process isolation limits the impact of a compromised process but does not directly prevent buffer overflow exploitation.
https://www.isc2.org/News-and-Events/Blog

✓ **B** Address Space Layout Randomization (ASLR)
ASLR randomizes the memory address space, making it difficult for an attacker to predict the location of injected code, thus effectively mitigating buffer overflow attacks.
https://www.isc2.org/News-and-Events/Blog

✗ **C** Processor states
Processor states relate to CPU operation modes and are not a primary mitigation technique for buffer overflows.
https://www.isc2.org/News-and-Events/Blog

✗ **D** Access control mechanisms
Access control restricts resource usage but does not address the memory layout vulnerabilities exploited by buffer overflows.
https://www.isc2.org/News-and-Events/Blog

Dumpsgate

Question 47

Single choice · Domain: D3 Security Architecture and Engineering › Implement input validation and data sanitization controls to prevent data tampering

A database server for a financial application is scheduled for production deployment. Which of the following controls will BEST prevent tampering?

A. Service accounts removal
B. Data validation
C. Logging and monitoring
D. Data sanitization

Answer: B. Data validation

Explanation

The question assesses the candidate's ability to select the most effective control for preventing tampering of data on a database server, which is a core concept in the Security Architecture and Engineering domain.

✗ **A** Service accounts removal
Removing service accounts reduces privileged access but does not directly prevent data tampering.
https://www.isc2.org/Domain-3-Security-Architecture-and-Engineering

✓ **B** Data validation
Data validation ensures that only properly formatted and authorized data is processed, which is the most effective control to prevent tampering at the input level.
https://www.isc2.org/Domain-3-Security-Architecture-and-Engineering

✗ **C** Logging and monitoring
Logging and monitoring detect tampering after it occurs but do not prevent it.
https://www.isc2.org/Domain-3-Security-Architecture-and-Engineering

✗ **D** Data sanitization
Data sanitization cleans data for safe use but is less comprehensive than validation for preventing tampering.
https://www.isc2.org/Domain-3-Security-Architecture-and-Engineering

Dumpsgate

Question 48

Single choice · Domain: D3 Security Architecture and Engineering › Select appropriate technical controls for VoIP phone security

An organization recently upgraded to a Voice over Internet Protocol (VoIP) phone system.

Management is concerned with unauthorized phone usage. Security consultant is responsible for putting together a plan to secure these phones. Administrators have assigned unique personal identification number codes for each person in the organization. What is the BEST solution?

A. Use phone locking software to enforce usage and PIN policies.

B. Inform the user to change the PIN regularly. Implement call detail records (CDR) reports to track usage.

C. Have the administrator enforce a policy to change the PIN regularly. Implement call detail records (CDR) reports to track usage.

D. Have the administrator change the PIN regularly. Implement call detail records (CDR) reports to track usage.

Answer: A. Use phone locking software to enforce usage and PIN policies.

Explanation

The question evaluates the candidate's ability to choose a technical control (phone locking software) to enforce PIN policies on VoIP devices, which falls under the Security Architecture and Engineering domain covering telecommunications security.

✓ **A** Use phone locking software to enforce usage and PIN policies.
Correct. Implementing phone locking software provides a technical control that enforces PIN usage and prevents unauthorized calls, aligning with telecommunications security controls described in the CISSP Security Architecture and Engineering domain.

https://www.isc2.org/Portals/0/Domain%20Exam%20Outline.pdf

✗ **B** Inform the user to change the PIN regularly. Implement call detail records (CDR) reports to track usage.
Incorrect. Relying on users to change PINs and only tracking usage with CDR reports does not provide proactive technical enforcement of security policies, which is required for VoIP device protection.

https://www.isc2.org/Portals/0/Domain%20Exam%20Outline.pdf

✗ **C** Have the administrator enforce a policy to change the PIN regularly. Implement call detail records (CDR) reports to track usage.
Incorrect. Administrative policy alone without technical enforcement (e.g., phone locking) is insufficient to prevent unauthorized usage of VoIP phones.

https://www.isc2.org/Portals/0/Domain%20Exam%20Outline.pdf

✗ **D** Have the administrator change the PIN regularly. Implement call detail records (CDR) reports to track usage.
Incorrect. Having an administrator manually change PINs is impractical and does not enforce consistent security controls; it lacks the automated enforcement needed for VoIP security.

https://www.isc2.org/Portals/0/Domain%20Exam%20Outline.pdf

Free demo · full exam: 1485 questions

Question 49

Single choice · Domain: D4 Communication and Network Security › Identify attacks that compromise data integrity during transmission

Which of the following attack types can be used to compromise the integrity of data during transmission?

A. Keylogging
B. Packet sniffing
C. Synchronization flooding
D. Session hijacking

Answer: D. Session hijacking

Explanation

The question asks which attack type can affect the integrity of data while it is being transmitted, which is a core concept in the Communication and Network Security domain.

✗ **A** Keylogging
Keylogging captures keystrokes locally and does not alter data in transit, so it does not compromise integrity of transmitted data.
https://www.isc2.org/Resources/Glossary

✗ **B** Packet sniffing
Packet sniffing is a passive eavesdropping technique that threatens confidentiality, not integrity, of data in transmission.
https://www.isc2.org/Resources/Glossary

✗ **C** Synchronization flooding
Synchronization flooding is a denial-of-service style attack that disrupts availability, not the integrity of data being transmitted.
https://www.isc2.org/Resources/Glossary

✓ **D** Session hijacking
Session hijacking allows an attacker to take over an active communication session and modify the data exchanged, thereby compromising its integrity.
https://www.isc2.org/Resources/Glossary

Dumpsgate

Question 50

Single choice · Domain: D4 Communication and Network Security › Identify the role of the control plane in determining traffic flow based on infrastructure status

Which of the following determines how traffic should flow based on the status of the infrastructure true?

A. Application plane
B. Data plane
C. Control plane
D. Traffic plane

Answer: C. Control plane

Explanation

The question tests knowledge of network architecture planes, specifically the control plane's function in directing traffic.

✗ **A** Application plane
Incorrect. The application plane deals with application-level functions, not traffic routing decisions.
https://www.isc2.org/CBK

✗ **B** Data plane
Incorrect. The data plane forwards packets based on decisions made by the control plane, but does not determine traffic flow.
https://www.isc2.org/CBK

✓ **C** Control plane
Correct. The control plane determines how traffic should flow based on the status of the infrastructure.
https://www.isc2.org/CBK

✗ **D** Traffic plane
Incorrect. 'Traffic plane' is not a standard term; traffic flow decisions are made by the control plane.
https://www.isc2.org/CBK

Dumpsgate

Question 51

Single choice · Domain: D4 Communication and Network Security › Identify security benefits of software-defined networking (SDN)

Compared to a traditional network, which of the following is a security-related benefit that software-defined networking (SDN) provides?

A. Centralized network provisioning
B. Centralized network administrator control
C. Reduced network latency when scaled
D. Reduced hardware footprint and cost

Free demo · full exam: 1485 questions

Answer: B. Centralized network administrator control

Explanation

The question assesses the candidate's understanding of how SDN improves security posture compared to traditional networks, which falls under the Communication and Network Security domain.

✗ **A** Centralized network provisioning
Provisioning is an operational benefit, not a security-specific advantage.
https://www.isc2.org/News-and-Events/Blog/Software-Defined-Networking

✓ **B** Centralized network administrator control
SDN centralizes control, enabling consistent policy enforcement, rapid threat response, and improved visibility, which are key security benefits.
https://www.isc2.org/News-and-Events/Blog/Software-Defined-Networking

✗ **C** Reduced network latency when scaled
Reduced latency is a performance benefit, not directly related to security.
https://www.isc2.org/News-and-Events/Blog/Software-Defined-Networking

✗ **D** Reduced hardware footprint and cost
Lower hardware costs are financial advantages, not security-specific.
https://www.isc2.org/News-and-Events/Blog/Software-Defined-Networking

Question 52

Single choice · Domain: D4 Communication and Network Security › Map OSI model layers to the TCP/IP model

Which Open Systems Interconnection (OSI) layer(s) BEST corresponds to the network access layer in the Transmission Control Protocol/Internet Protocol (TCP/IP) model?

A. Transport Layer
B. Data Link and Physical Layers
C. Application, Presentation, and Session Layers
D. Session and Network Layers

Answer: B. Data Link and Physical Layers

Explanation

The question assesses the candidate's knowledge of network architecture by requiring identification of which OSI layer(s) correspond to the TCP/IP network access layer.

✗ **A** Transport Layer
Incorrect. The Transport layer in the OSI model maps to the Transport layer of the TCP/IP model, not the Network Access layer.
https://www.isc2.org/Certifications/CISSP

✓ **B** Data Link and Physical Layers
Correct. The TCP/IP Network Access layer encompasses the OSI Data Link and Physical layers.

Free demo · full exam: 1485 questions

https://www.isc2.org/Certifications/CISSP

✗ **C** Application, Presentation, and Session Layers
Incorrect. These OSI layers correspond to the Application layer of the TCP/IP model, not the Network Access layer.

https://www.isc2.org/Certifications/CISSP

✗ **D** Session and Network Layers
Incorrect. The Session layer maps to the Application layer, and the Network layer maps to the Internet layer of TCP/IP, not the Network Access layer.

https://www.isc2.org/Certifications/CISSP

Question 53

Single choice · Domain: D4 Communication and Network Security › Apply transport layer security to protect VoIP communications

Which of the following would be the BEST mitigation practice for man-in-the-middle (MITM) Voice over Internet Protocol (VoIP) attacks?

A. Use Media Gateway Control Protocol (MGCP)
B. Use Transport Layer Security (TLS) protocol
C. Use File Transfer Protocol (FTP)
D. Use Secure Shell (SSH) protocol

Answer: B. Use Transport Layer Security (TLS) protocol

Explanation

The question tests knowledge of securing VoIP against man-in-the-middle attacks, which falls under the Communication and Network Security domain of the CISSP exam.

✗ **A** Use Media Gateway Control Protocol (MGCP)
MGCP is a signaling protocol for controlling media gateways and does not provide encryption or authentication to prevent MITM attacks.

https://www.isc2.org/Certifications/CISSP

✓ **B** Use Transport Layer Security (TLS) protocol
TLS encrypts SIP signaling (SIPS) and can be combined with SRTP to protect media streams, effectively mitigating MITM VoIP attacks.

https://www.isc2.org/Certifications/CISSP

✗ **C** Use File Transfer Protocol (FTP)
FTP is a file-transfer protocol and provides no security for VoIP signaling or media, making it unsuitable for MITM mitigation.

https://www.isc2.org/Certifications/CISSP

✗ **D** Use Secure Shell (SSH) protocol
SSH secures remote command-line sessions but does not protect VoIP signaling or media traffic, so it is not the best mitigation for MITM VoIP attacks.

https://www.isc2.org/Certifications/CISSP

Free demo · full exam: 1485 questions

Question 54

Single choice · Domain: D4 Communication and Network Security › Design and implement content delivery network caching strategies

A software architect has been asked to build a platform to distribute music to thousands of users on a global scale. The architect has been reading about content delivery networks (CDN). Which of the following is a principal task to undertake?

A. Establish a service-oriented architecture (SOA).
B. Establish a media caching methodology.
C. Establish relationships with hundreds of Internet service providers (ISP).
D. Establish a low-latency wide area network (WAN).

Answer: B. Establish a media caching methodology.

Explanation

The question tests the candidate's ability to apply network security architecture principles by selecting the primary task for a CDN, which is establishing a media caching methodology.

✗ **A** Establish a service-oriented architecture (SOA).
Incorrect. While SOA is an architectural approach, it is not the principal task specific to CDN implementation.

https://www.isc2.org/Certifications/CISSP

✓ **B** Establish a media caching methodology.
Correct. The core function of a CDN is to cache media content at edge locations to improve delivery performance.

https://www.isc2.org/Certifications/CISSP

✗ **C** Establish relationships with hundreds of Internet service providers (ISP).
Incorrect. While ISP relationships can be beneficial, they are not the primary task when designing a CDN.

https://www.isc2.org/Certifications/CISSP

✗ **D** Establish a low-latency wide area network (WAN).
Incorrect. A low-latency WAN supports network performance but does not address the essential CDN function of caching content.

https://www.isc2.org/Certifications/CISSP

Dumpsgate

Question 55

Single choice · Domain: D4 Communication and Network Security › Select and implement appropriate Network Access Control (NAC) mechanisms

In an environment where there is not full administrative control over all network connected endpoints, such as a university where non-corporate devices are used, what is the BEST way to restrict access to the network?

A. Use switch port security to limit devices connected to a particular switch port.
B. Use of virtual local area networks (VLAN) to segregate users.
C. Use a client-based Network Access Control (NAC) solution.
D. Use a clientless Network Access Control (NAC) solution

Answer: D. Use a clientless Network Access Control (NAC) solution

Explanation

The question tests the candidate's ability to choose the most suitable NAC approach for environments where endpoint control is limited, a key skill in the Communication and Network Security domain.

✗ **A** Use switch port security to limit devices connected to a particular switch port.
Switch port security restricts MAC addresses per port but does not prevent unauthorized devices from connecting to other ports; it is less effective when endpoint control is limited.

https://www.isc2.org/Certifications/CISSP

✗ **B** Use of virtual local area networks (VLAN) to segregate users.
VLAN segmentation isolates traffic but still allows any device to join a VLAN if it can connect to the network; it does not enforce authentication of unmanaged devices.

https://www.isc2.org/Certifications/CISSP

✗ **C** Use a client-based Network Access Control (NAC) solution.
Client-based NAC requires installing an agent on each endpoint, which is not feasible when the organization lacks administrative control over devices.

https://www.isc2.org/Certifications/CISSP

✓ **D** Use a clientless Network Access Control (NAC) solution
Clientless NAC (e.g., captive-portal or 802.1X with web authentication) can enforce access policies without requiring software on the endpoint, making it the best choice for environments with unmanaged devices.

https://www.isc2.org/Certifications/CISSP

Free demo · full exam: 1485 questions

Question 56

Single choice · Domain: D4 Communication and Network Security › Validate endpoint security posture using Network Admission Control

What is the benefit of using Network Admission Control (NAC)?

A. Operating system (OS) versions can be validated prior to allowing network access.

B. NAC supports validation of the endpoint's security posture prior to allowing the session to go into an authorized state.

C. NAC can require the use of certificates, passwords, or a combination of both before allowing network admission.

D. NAC only supports Windows operating systems (OS).

Answer: B. NAC supports validation of the endpoint's security posture prior to allowing the session to go into an authorized state.

Explanation

The question assesses understanding of NAC benefits, which are part of communication and network security controls.

✗ **A** Operating system (OS) versions can be validated prior to allowing network access.
While NAC can check OS versions, the primary benefit is broader security-posture validation.

https://www.isc2.org/Certifications/CISSP/Domain-4

✓ **B** NAC supports validation of the endpoint's security posture prior to allowing the session to go into an authorized state.
Correct. NAC evaluates the endpoint's security posture (antivirus status, patches, OS version, etc.) before granting network access.

https://www.isc2.org/Certifications/CISSP/Domain-4

✗ **C** NAC can require the use of certificates, passwords, or a combination of both before allowing network admission.
Authentication methods may be used, but they are not the core benefit of NAC; the key advantage is posture validation.

https://www.isc2.org/Certifications/CISSP/Domain-4

✗ **D** NAC only supports Windows operating systems (OS).
Incorrect. NAC solutions are platform-agnostic and can enforce policies on multiple operating systems.

https://www.isc2.org/Certifications/CISSP/Domain-4

Dumpsgate

Free demo · full exam: 1485 questions

Question 57

Single choice · Domain: D4 Communication and Network Security › Apply network filtering techniques to mitigate protocol-based attacks

What is the FIRST step in reducing the exposure of a network to Internet Control Message Protocol (ICMP) based attacks?

A. Implement egress filtering at the organization's network boundary.
B. Implement network access control lists (ACL).
C. Implement a web application firewall (WAF).
D. Implement an intrusion prevention system (IPS).

Answer: B. Implement network access control lists (ACL).

Explanation

The question tests the candidate's ability to identify the initial network control (ACL) used to reduce exposure to ICMP attacks.

✗ **A** Implement egress filtering at the organization's network boundary.
Incorrect. Egress filtering controls outbound traffic and does not address inbound ICMP exposure.
https://www.isc2.org/Certifications/CISSP

✓ **B** Implement network access control lists (ACL).
Correct. ACLs at the perimeter can block inbound ICMP traffic, providing the first line of defense against ICMP-based attacks.
https://www.isc2.org/Certifications/CISSP

✗ **C** Implement a web application firewall (WAF).
Incorrect. A WAF protects web applications, not network-layer protocols like ICMP.
https://www.isc2.org/Certifications/CISSP

✗ **D** Implement an intrusion prevention system (IPS).
Incorrect. While an IPS can detect ICMP attacks, the first step is to block the traffic with ACLs.
https://www.isc2.org/Certifications/CISSP

Dumpsgate

Question 58

Single choice · Domain: D4 Communication and Network Security › Identify the OSI layer that must be inspected to control application-level traffic

An information security administrator wishes to block peer-to-peer (P2P) traffic over Hypertext Transfer Protocol (HTTP) tunnels. Which of the following layers of the Open Systems Interconnection (OSI) model requires inspection?

A. Presentation
B. Transport
C. Session
D. Application

Answer: D. Application

Explanation

The question tests the candidate's ability to map a security control (blocking P2P over HTTP tunnels) to the appropriate OSI layer, which is a core skill in the Communication and Network Security domain.

✗ **A** Presentation
Incorrect. The Presentation layer handles data formatting and encryption, not the inspection of HTTP traffic.

https://www.isc2.org/Certifications/CISSP

✗ **B** Transport
Incorrect. The Transport layer manages end-to-end communication (e.g., TCP/UDP) but does not interpret HTTP payloads.

https://www.isc2.org/Certifications/CISSP

✗ **C** Session
Incorrect. The Session layer establishes, manages, and terminates sessions; it does not inspect the content of HTTP tunnels.

https://www.isc2.org/Certifications/CISSP

✓ **D** Application
Correct. HTTP operates at the Application layer; to block P2P traffic encapsulated in HTTP tunnels, inspection must occur at this layer.

https://www.isc2.org/Certifications/CISSP

Dumpsgate

Free demo · full exam: 1485 questions

Question 59

Single choice · Domain: D5 Identity and Access Management (IAM) › Identify open standards for authentication and authorization data exchange

Which of the following is an open standard for exchanging authentication and authorization data between parties?

A. Wired markup language
B. Hypertext Markup Language (HTML)
C. Extensible Markup Language (XML)
D. Security Assertion Markup Language (SAML)

Answer: D. Security Assertion Markup Language (SAML)

Explanation

The question assesses knowledge of authentication/authorization standards, specifically the open standard SAML used for exchanging security assertions between parties.

✗ **A** Wired markup language
Wired markup language is not a recognized standard for authentication or authorization data exchange.
https://www.isc2.org/News-and-Events/Blog/2020/09/01/SAML-Authentication-Standard

✗ **B** Hypertext Markup Language (HTML)
HTML is a markup language for structuring web content, not an authentication/authorization protocol.
https://www.isc2.org/News-and-Events/Blog/2020/09/01/SAML-Authentication-Standard

✗ **C** Extensible Markup Language (XML)
XML is a generic data format; while SAML is expressed in XML, XML itself is not an authentication/authorization standard.
https://www.isc2.org/News-and-Events/Blog/2020/09/01/SAML-Authentication-Standard

✓ **D** Security Assertion Markup Language (SAML)
SAML is an open standard for exchanging authentication and authorization data between parties.
https://www.isc2.org/News-and-Events/Blog/2020/09/01/SAML-Authentication-Standard

Free demo · full exam: 1485 questions

Question 60

Single choice · Domain: D5 Identity and Access Management (IAM) › Implement multi-factor authentication mechanisms

An information security professional is reviewing user access controls on a customer-facing application. The application must have multi-factor authentication (MFA) in place. The application currently requires a username and password to login. Which of the following options would BEST implement MFA?

A. Geolocate the user and compare to previous logins
B. Require a pre-selected number as part of the login
C. Have the user answer a secret question that is known to them
D. Enter an automatically generated number from a hardware token

Answer: D. Enter an automatically generated number from a hardware token

Explanation

The question tests the candidate's ability to identify a solution that combines two independent authentication factors, fulfilling MFA requirements.

✗ **A** Geolocate the user and compare to previous logins
Geolocation is a risk-based control, not a separate authentication factor, so it does not satisfy MFA.
https://www.isc2.org/Certifications/CISSP

✗ **B** Require a pre-selected number as part of the login
A pre-selected number is another knowledge-based factor, still only one factor when used with password.
https://www.isc2.org/Certifications/CISSP

✗ **C** Have the user answer a secret question that is known to them
Secret questions are also knowledge-based and do not add a distinct factor to the password.
https://www.isc2.org/Certifications/CISSP

✓ **D** Enter an automatically generated number from a hardware token
A hardware token provides a possession factor combined with the password (knowledge factor), meeting MFA requirements.
https://www.isc2.org/Certifications/CISSP

Free demo · full exam: 1485 questions

Question 61

Single choice · Domain: D5 Identity and Access Management (IAM) › Identify the fundamental components of logical access control

What are the first two components of logical access control?

A. Confidentiality and authentication
B. Authentication and identification
C. Identification and confidentiality
D. Authentication and availability

Answer: B. Authentication and identification

Explanation

The question assesses knowledge of the first two logical access control components (identification and authentication) which are core concepts in the IAM domain.

✗ **A** Confidentiality and authentication
Incorrect. Confidentiality is not one of the first two logical access control components; the correct pair is identification and authentication.

https://www.isc2.org/Blog/Identity-and-Access-Management

✓ **B** Authentication and identification
Correct. Logical access control begins with identification followed by authentication; this option includes both components (order is not critical).

https://www.isc2.org/Blog/Identity-and-Access-Management

✗ **C** Identification and confidentiality
Incorrect. While identification is correct, confidentiality is not part of the first two logical access control components.

https://www.isc2.org/Blog/Identity-and-Access-Management

✗ **D** Authentication and availability
Incorrect. Availability is a CIA triad element, not one of the initial logical access control steps.

https://www.isc2.org/Blog/Identity-and-Access-Management

Dumpsgate

Question 62

Single choice · Domain: D5 Identity and Access Management (IAM) › Explain biometric authentication performance metrics (FRR, FAR, Equal Error Rate)

a large organization uses biometrics to allow access to its facilities. It adjusts the biometric value for incorrectly granting or denying access so that the two numbers are the same.

What is this value called?

A. False Rejection Rate (FRR)
B. Accuracy acceptance threshold
C. Equal error rate
D. False Acceptance Rate (FAR)

Answer: C. Equal error rate

Explanation

The question assesses understanding of biometric system error rates, which are part of authentication concepts within the IAM domain.

✗ **A** False Rejection Rate (FRR)
FRR measures the proportion of legitimate users incorrectly denied access; it is not the point where false acceptance and false rejection rates are equal.

https://www.isc2.org/Glossary

✗ **B** Accuracy acceptance threshold
This term is not a standard biometric performance metric in the (ISC)² body of knowledge.

https://www.isc2.org/Glossary

✓ **C** Equal error rate
Equal Error Rate (EER) is the point at which the false acceptance rate and false rejection rate are equal, matching the described adjustment.

https://www.isc2.org/Glossary

✗ **D** False Acceptance Rate (FAR)
FAR measures the proportion of impostors incorrectly granted access; it alone does not represent the balance point described.

https://www.isc2.org/Glossary

Free demo · full exam: 1485 questions

Question 63

Single choice · Domain: D5 Identity and Access Management (IAM) › Identify authentication mechanisms that use challenge-response

After the INITIAL input o f a user identification (ID) and password, what is an authentication system that prompts the user for a different response each time the user logs on?

A. Persons Identification Number (PIN)
B. Secondary password
C. Challenge response
D. Voice authentication

Answer: C. Challenge response

Explanation

The question tests knowledge of authentication methods, specifically the challenge-response technique, which falls under the IAM domain of the CISSP CBK.

✗ **A** Persons Identification Number (PIN)
A PIN is a static secret, not a dynamic challenge-response mechanism.
https://www.isc2.org/Certifications/CISSP/Exam-Outline

✗ **B** Secondary password
A secondary password is another static credential; it does not change per login session.
https://www.isc2.org/Certifications/CISSP/Exam-Outline

✓ **C** Challenge response
Correct. Challenge-response authentication presents a new challenge each login and requires a corresponding response, satisfying the described behavior.
https://www.isc2.org/Certifications/CISSP/Exam-Outline

✗ **D** Voice authentication
Voice authentication is a biometric factor; it does not inherently provide a different challenge each login.
https://www.isc2.org/Certifications/CISSP/Exam-Outline

Question 64

Single choice · Domain: D5 Identity and Access Management (IAM) › Identify and describe single sign-on (SSO) mechanisms

Which of the following terms BEST describes a system which allows a user to log in and access multiple related servers and applications?

A. Remote Desktop Protocol (RDP)
B. Federated identity management (FIM)
C. Single sign-on (SSO)
D. Multi-factor authentication (MFA)

Free demo · full exam: 1485 questions

Answer: C. Single sign-on (SSO)

Explanation

The question tests knowledge of authentication and identity federation concepts, specifically the ability to recognize a system that provides seamless access to multiple applications after one login.

✗ **A** Remote Desktop Protocol (RDP)
RDP is a protocol for remote desktop access, not a mechanism that provides a single login for multiple applications.

https://www.isc2.org/

✗ **B** Federated identity management (FIM)
Federated identity management enables identity sharing across domains but does not itself provide the single login experience described; SSO is the specific term.

https://www.isc2.org/

✓ **C** Single sign-on (SSO)
SSO allows a user to authenticate once and gain access to multiple related servers and applications without re-entering credentials.

https://www.isc2.org/Certifications/CISSP

✗ **D** Multi-factor authentication (MFA)
MFA adds additional verification factors to a login process but does not inherently provide access to multiple systems after a single login.

https://www.isc2.org/

Question 65

Single choice · Domain: D5 Identity and Access Management (IAM) › Implement multi-factor authentication for mobile device access

A recent information security risk assessment identified weak system access controls on mobile devices as a high me In order to address this risk and ensure only authorized staff access company information, which of the following should the organization implement?

A. Intrusion prevention system (IPS)
B. Multi-factor authentication (MFA)
C. Data loss protection (DLP)
D. Data at rest encryption

Answer: B. Multi-factor authentication (MFA)

Explanation

The question tests the candidate's ability to select appropriate controls to strengthen access controls on mobile devices, which falls under the IAM domain.

✗ **A** Intrusion prevention system (IPS)

Free demo · full exam: 1485 questions

IPS monitors network traffic for threats but does not verify user identity for mobile device access.
https://www.isc2.org/Certifications/CISSP

✓ **B** Multi-factor authentication (MFA)
MFA adds additional verification factors, ensuring only authorized staff can access company information on mobile devices.
https://www.isc2.org/Certifications/CISSP

✗ **C** Data loss protection (DLP)
DLP focuses on preventing data exfiltration, not on authenticating users to mobile devices.
https://www.isc2.org/Certifications/CISSP

✗ **D** Data at rest encryption
Encryption protects stored data but does not control who can access the device.
https://www.isc2.org/Certifications/CISSP

Question 66

Single choice · Domain: D5 Identity and Access Management (IAM) › Establish trust relationships for federated identity

Which of the following is TRUE for an organization that is using a third-party federated identity service?

A. The organization enforces the rules to other organization's user provisioning
B. The organization establishes a trust relationship with the other organizations
C. The organization defines internal standard for overall user identification
D. The organization specifies alone how to authenticate other organization's users

Answer: B. The organization establishes a trust relationship with the other organizations

Explanation

The question tests knowledge of federated identity concepts, specifically the need to establish a trust relationship with external identity providers.

✗ **A** The organization enforces the rules to other organization's user provisioning
Incorrect. In federated identity, the organization does not enforce provisioning rules on the external provider.
https://www.isc2.org/Certifications/CISSP/CBK

✓ **B** The organization establishes a trust relationship with the other organizations
Correct. Federated identity requires establishing a trust relationship with the external identity provider.
https://www.isc2.org/Certifications/CISSP/CBK

✗ **C** The organization defines internal standard for overall user identification
Incorrect. Standards are defined internally but federated identity relies on external provider's identifiers.
https://www.isc2.org/Certifications/CISSP/CBK

✗ **D** The organization specifies alone how to authenticate other organization's users
Incorrect. Authentication is performed by the third-party federated service, not solely by the organization.
https://www.isc2.org/Certifications/CISSP/CBK

Free demo · full exam: 1485 questions

Question 67

Single choice · Domain: D5 Identity and Access Management (IAM) › Implement unique user accounts and enforce individual authentication

An internal audit for an organization recently identified malicious actions by a user account. Upon further investigation, it was determined the offending user account was used by multiple people at multiple locations simultaneously for various services and applications. What is the BEST method to prevent this problem in the future?

A. Ensure the security information and event management (SIEM) is set to alert.
B. Inform users only one user should be using the account at a time.
C. Ensure each user has their own unique account,
D. Allow several users to share a generic account.

Answer: C. Ensure each user has their own unique account,

Explanation

The question assesses the candidate's ability to apply IAM principles by ensuring each individual has a distinct account, preventing credential sharing.

✗ **A** Ensure the security information and event management (SIEM) is set to alert.
SIEM alerts detect suspicious activity but do not prevent shared accounts. Prevention requires unique credentials.

https://www.isc2.org/Certifications/CISSP/Domain-5-Identity-and-Access-Management

✗ **B** Inform users only one user should be using the account at a time.
User education alone cannot enforce exclusive use; technical controls are needed.

https://www.isc2.org/Certifications/CISSP/Domain-5-Identity-and-Access-Management

✓ **C** Ensure each user has their own unique account,
Providing individual accounts enforces accountability and prevents credential sharing, which is a core IAM best practice.

https://www.isc2.org/Certifications/CISSP/Domain-5-Identity-and-Access-Management

✗ **D** Allow several users to share a generic account.
Sharing generic accounts violates IAM principles and creates audit and security risks.

https://www.isc2.org/Certifications/CISSP/Domain-5-Identity-and-Access-Management

Dumpsgate

Free demo · full exam: 1485 questions

Question 68

Single choice · Domain: D5 Identity and Access Management (IAM) › Implement and manage session controls

An attacker is able to remain indefinitely logged into a exploiting to remain on the web service?

A. Alert management
B. Password management
C. Session management
D. Identity management (IM)

Answer: C. Session management

Explanation

The question assesses the candidate's understanding of session management, a core component of the Identity and Access Management domain.

✗ **A** Alert management
Alert management relates to monitoring and does not address persistent login issues.
https://www.isc2.org/Certifications/CISSP

✗ **B** Password management
Password management concerns credential creation and storage, not the ability to stay logged in indefinitely.
https://www.isc2.org/Certifications/CISSP

✓ **C** Session management
Session management controls protect session tokens and enforce timeouts; a failure allows an attacker to remain logged in indefinitely.
https://www.isc2.org/Certifications/CISSP

✗ **D** Identity management (IM)
Identity management deals with establishing user identities, not maintaining an active session after authentication.
https://www.isc2.org/Certifications/CISSP

Dumpsgate

Question 69

Single choice · Domain: D5 Identity and Access Management (IAM) › Select and implement multi-factor authentication mechanisms

A company wants to implement two-factor authentication (2FA) to protect their computers from unauthorized users. Which solution provides the MOST secure means of authentication and meets the criteria they have set?

A. Username and personal identification number (PIN)
B. Fingerprint and retinal scanners
C. Short Message Services (SMS) and smartphone authenticator
D. Hardware token and password

Answer: D. Hardware token and password

Explanation

The question evaluates the candidate's ability to differentiate authentication factors and choose the most secure two-factor solution.

✗ **A** Username and personal identification number (PIN)
Both elements are knowledge factors, not two separate factors, so this does not satisfy true two-factor authentication.

https://www.isc2.org/Certifications/CISSP/Domain-5-Identity-and-Access-Management

✗ **B** Fingerprint and retinal scanners
Both are biometric (something you are) factors; using two of the same factor type does not constitute two-factor authentication.

https://www.isc2.org/Certifications/CISSP/Domain-5-Identity-and-Access-Management

✗ **C** Short Message Services (SMS) and smartphone authenticator
SMS OTP and a smartphone authenticator both rely on possession of the same device and are vulnerable to interception or malware, making them less secure than a hardware token combined with a password.

https://www.isc2.org/Certifications/CISSP/Domain-5-Identity-and-Access-Management

✓ **D** Hardware token and password
A hardware token (something you have) paired with a password (something you know) provides true two-factor authentication and is considered the most secure among the options.

https://www.isc2.org/Certifications/CISSP/Domain-5-Identity-and-Access-Management

Free demo · full exam: 1485 questions

Question 70

Single choice · Domain: D5 Identity and Access Management (IAM) › Perform user access review and adjust permissions when a role change occurs

If an employee transfers from one role to another, which of the following actions should this trigger within the identity and access management (IAM) lifecycle?

A. New account creation
B. User access review and adjustment
C. Deprovisioning
D. System account access review and adjustment

Answer: B. User access review and adjustment

Explanation

The question tests the candidate's knowledge of the IAM lifecycle step required when an employee transfers roles, which is to review and adjust the user's access rights.

✗ **A** New account creation
Incorrect. Role changes typically do not require a new account; the existing account is retained and permissions are modified.

https://www.isc2.org/Certifications/CISSP

✓ **B** User access review and adjustment
Correct. When an employee moves to a new role, the IAM lifecycle mandates a review of current permissions and adjustment to align with the new job responsibilities.

https://www.isc2.org/Certifications/CISSP

✗ **C** Deprovisioning
Incorrect. Deprovisioning is performed when an employee leaves the organization, not when they change roles.

https://www.isc2.org/Certifications/CISSP

✗ **D** System account access review and adjustment
Incorrect. System account reviews are separate from regular user role changes; the appropriate action is a user access review.

https://www.isc2.org/Certifications/CISSP

Dumpsgate

Question 71

Single choice · Domain: D5 Identity and Access Management (IAM) › Explain centralized identity management concepts

Which of the following BEST describes centralized identity management?

A. Service providers rely on a trusted third party (TTP) to provide requestors with both credentials and identifiers.
B. Service providers agree to integrate identity system recognition across organizational boundaries.
C. Service providers identify an entity by behavior analysis versus an identification factor.
D. Service providers perform as both the credential and identity provider (IdP).

Answer: A. Service providers rely on a trusted third party (TTP) to provide requestors with both credentials and identifiers.

Explanation

The question assesses the candidate's understanding of identity management models, specifically the definition of centralized identity management versus federated or decentralized approaches.

✓ **A** Service providers rely on a trusted third party (TTP) to provide requestors with both credentials and identifiers.
Correct. Centralized identity management uses a single trusted third-party IdP that issues both credentials and identifiers to service providers.

https://www.isc2.org/Certifications/CISSP/CBK

✗ **B** Service providers agree to integrate identity system recognition across organizational boundaries.
Incorrect. This describes federated identity management, where multiple domains recognize each other's identities, not a centralized model.

https://www.isc2.org/Certifications/CISSP/CBK

✗ **C** Service providers identify an entity by behavior analysis versus an identification factor.
Incorrect. Behavior-based identification is a risk-based or adaptive authentication technique, not a definition of centralized identity management.

https://www.isc2.org/Certifications/CISSP/CBK

✗ **D** Service providers perform as both the credential and identity provider (IdP).
Incorrect. When service providers act as their own IdP, identity management is decentralized or self-asserted, not centralized.

https://www.isc2.org/Certifications/CISSP/CBK

Dumpsgate

Question 72

Single choice · Domain: D6 Security Assessment and Testing › Explain the limitations and scope of security testing results

In setting expectations when reviewing the results of a security test, which of the following statements is MOST important to convey to reviewers?

A. The target's security posture cannot be further compromised.
B. The results of the tests represent a point-in-time assessment of the target(s).
C. The accuracy of testing results can be greatly improved if the target(s) are properly hardened.
D. The deficiencies identified can be corrected immediately

Answer: B. The results of the tests represent a point-in-time assessment of the target(s).

Explanation

The question assesses understanding of how to set realistic expectations for test results, emphasizing that they are point-in-time assessments.

✗ **A** The target's security posture cannot be further compromised.
Incorrect. Security testing cannot guarantee that the target cannot be further compromised; tests provide evidence of current weaknesses, not absolute security.
https://www.isc2.org/News-and-Events/Blog/2020/06/03/Understanding-Penetration-Testing

✓ **B** The results of the tests represent a point-in-time assessment of the target(s).
Correct. Test results are snapshots of the environment at the time of testing and may change as configurations evolve. This limitation must be communicated to reviewers.
https://www.isc2.org/News-and-Events/Blog/2020/06/03/Understanding-Penetration-Testing

✗ **C** The accuracy of testing results can be greatly improved if the target(s) are properly hardened.
Incorrect. While hardening can reduce findings, it does not fundamentally improve the accuracy of test results; the primary expectation is about the temporal nature of the assessment.
https://www.isc2.org/News-and-Events/Blog/2020/06/03/Understanding-Penetration-Testing

✗ **D** The deficiencies identified can be corrected immediately
Incorrect. Remediation may require planning, resources, and time; it is not guaranteed to be immediate.
https://www.isc2.org/News-and-Events/Blog/2020/06/03/Understanding-Penetration-Testing

Free demo · full exam: 1485 questions

Question 73

Single choice · Domain: D6 Security Assessment and Testing › Define the purpose and components of a security assessment plan

What is the MAIN purpose of a security assessment plan?

A. Provide guidance on security requirements, to ensure the identified security risks are properly addressed based on the recommendation

B. Provide the objectives for the security and privacy control assessments and a detailed roadmap of how to conduct such assessments.

C. Provide technical information to executives to help them understand information security postures and secure funding.

D. Provide education to employees on security and privacy, to ensure their awareness on policies and procedures

Answer: B. Provide the objectives for the security and privacy control assessments and a detailed roadmap of how to conduct such assessments.

Explanation

The question evaluates the candidate's understanding of the primary goal of a security assessment plan, which is to outline objectives and a roadmap for conducting security and privacy control assessments.

✗ **A** Provide guidance on security requirements, to ensure the identified security risks are properly addressed based on the recommendation
Incorrect. This describes a requirements-driven approach, not the main purpose of a security assessment plan.

https://www.isc2.org/Certifications/CISSP/Domain-6

✓ **B** Provide the objectives for the security and privacy control assessments and a detailed roadmap of how to conduct such assessments.
Correct. The primary purpose of a security assessment plan is to define assessment objectives and outline a detailed roadmap for executing security and privacy control assessments.

https://www.isc2.org/Certifications/CISSP/Domain-6

✗ **C** Provide technical information to executives to help them understand information security postures and secure funding.
Incorrect. Supplying executive-level technical briefings is a reporting activity, not the core purpose of the assessment plan.

https://www.isc2.org/Certifications/CISSP/Domain-6

✗ **D** Provide education to employees on security and privacy, to ensure their awareness on policies and procedures
Incorrect. Employee education falls under security awareness training, not the main function of a security assessment plan.

https://www.isc2.org/Certifications/CISSP/Domain-6

Free demo · full exam: 1485 questions

Question 74

Single choice · Domain: D6 Security Assessment and Testing › Identify characteristics of effective security metrics

Which of the following are the B EST characteristics of security metrics?

A. They are generalized and provide a broad overview
B. They use acronyms and abbreviations to be concise
C. They use bar charts and Venn diagrams
D. They are consistently measured and quantitatively expressed

Answer: D. They are consistently measured and quantitatively expressed

Explanation

The question assesses knowledge of what makes security metrics useful, a topic covered in the Security Assessment and Testing domain of the CISSP CBK.

✗ **A** They are generalized and provide a broad overview
Security metrics should be specific and measurable, not merely generalized overviews.
https://www.isc2.org/News-and-Events/Blog/2020/09/01/Security-Metrics-Why-They-Matter

✗ **B** They use acronyms and abbreviations to be concise
Use of acronyms does not define a good metric; clarity and quantifiability are required.
https://www.isc2.org/News-and-Events/Blog/2020/09/01/Security-Metrics-Why-They-Matter

✗ **C** They use bar charts and Venn diagrams
Presentation format (charts, diagrams) is a reporting choice, not a core characteristic of a metric itself.
https://www.isc2.org/News-and-Events/Blog/2020/09/01/Security-Metrics-Why-They-Matter

✓ **D** They are consistently measured and quantitatively expressed
Effective security metrics are consistently measured and expressed in quantitative terms to allow comparison and trend analysis.
https://www.isc2.org/News-and-Events/Blog/2020/09/01/Security-Metrics-Why-They-Matter

Question 75

Single choice · Domain: D6 Security Assessment and Testing › Identify security assessment requirements for software acquisition

Which of the following addresses requirements of security assessment during software acquisition?

A. Software assurance policy
B. Continuous monitoring
C. Software configuration management (SCM)
D. Data loss prevention (DLP) policy

Answer: A. Software assurance policy

Free demo · full exam: 1485 questions

Dumpsgate

Question 76

Single choice · Domain: D6 Security Assessment and Testing › Plan and scope a security audit

Which of the following is the MOST important first step in preparing for a security audit?

A. Identify team members.
B. Define the scope.
C. Notify system administrators.
D. Collect evidence.

Answer: B. Define the scope.

Explanation

The question tests the candidate's ability to identify the initial step in audit preparation, which is defining the audit scope, a core activity within the Security Assessment and Testing domain.

✗ **A** Identify team members.
While team identification is important, it follows establishing the audit scope. (ISC)² guidance places scope definition first.

https://www.isc2.org/Certifications/CISSP

✓ **B** Define the scope.
Defining the audit scope is the primary first step in audit planning, ensuring objectives, boundaries, and criteria are set before any other activities.

https://www.isc2.org/Certifications/CISSP

✗ **C** Notify system administrators.

Free demo · full exam: 1485 questions

Notifying administrators is a later step after the scope and audit plan are established. (ISC)² audit preparation sequence lists notification after scope definition.

https://www.isc2.org/Certifications/CISSP

✗ **D** Collect evidence.
Evidence collection occurs during the audit execution phase, not as the initial preparatory activity.

https://www.isc2.org/Certifications/CISSP

Question 77

Single choice · Domain: D6 Security Assessment and Testing › Assess security impact of acquired software

What is the BEST method to use for assessing the security impact of acquired software?

A. Common vulnerability review
B. Software security compliance validation
C. Threat modeling
D. Vendor assessment

Answer: B. Software security compliance validation

Explanation

The question evaluates the candidate's ability to select the most appropriate assessment technique for determining the security impact of software that has been purchased, which is a core skill within the Security Assessment and Testing domain.

✗ **A** Common vulnerability review
Incorrect. A common vulnerability review focuses on known flaws but does not provide a comprehensive assessment of the overall security impact of newly acquired software.

https://www.isc2.org/Certifications/CISSP

✓ **B** Software security compliance validation
Correct. Validating that the acquired software complies with organizational security policies and standards is the most effective way to assess its security impact.

https://www.isc2.org/Certifications/CISSP

✗ **C** Threat modeling
Incorrect. Threat modeling is primarily used during design and development to identify potential threats, not to evaluate the security impact of already built, acquired software.

https://www.isc2.org/Certifications/CISSP

✗ **D** Vendor assessment
Incorrect. Vendor assessment evaluates the supplier's security posture, not the specific security impact of the software product itself.

https://www.isc2.org/Certifications/CISSP

Free demo · full exam: 1485 questions

Question 78

Single choice · Domain: D6 Security Assessment and Testing › Identify stages of penetration testing methodology

Dumpster diving is a technique used in which stage of penetration testing methodology?

A. Attack
B. Discovery
C. Reporting
D. Planning

Answer: B. Discovery

Explanation

The question assesses knowledge of the penetration testing phases, specifically which phase involves information gathering techniques such as dumpster diving.

✗ **A** Attack
Attack (exploitation) follows the discovery phase; dumpster diving is not performed during exploitation.
https://www.isc2.org/News-and-Events/Blog/2020/09/01/Penetration-Testing-Methodology

✓ **B** Discovery
Dumpster diving is an information-gathering technique used to collect data from discarded materials, which belongs to the discovery (reconnaissance) phase of penetration testing.
https://www.isc2.org/News-and-Events/Blog/2020/09/01/Penetration-Testing-Methodology

✗ **C** Reporting
Reporting documents findings after testing; it does not involve data collection techniques like dumpster diving.
https://www.isc2.org/News-and-Events/Blog/2020/09/01/Penetration-Testing-Methodology

✗ **D** Planning
Planning defines scope and rules of engagement; dumpster diving occurs later during discovery, not during planning.
https://www.isc2.org/News-and-Events/Blog/2020/09/01/Penetration-Testing-Methodology

Question 79

Single choice · Domain: D6 Security Assessment and Testing › Select appropriate industry-recognized baseline documents for security assessments

What industry-recognized document could be used as a baseline reference that is related to data security and business operations for conducting a security assessment?

A. Service Organization Control (SOC) 1 Type 2
B. Service Organization Control (SOC) 2 Type 1
C. Service Organization Control (SOC) 1 Type 1
D. Service Organization Control (SOC) 2 Type 2

Free demo · full exam: 1485 questions

Answer: D. Service Organization Control (SOC) 2 Type 2

Explanation

The question asks which SOC report can serve as a baseline reference for data security and business operations when performing a security assessment, testing the candidate's knowledge of assessment frameworks.

✗ **A** Service Organization Control (SOC) 1 Type 2
SOC 1 focuses on controls over financial reporting, not on data security or operational controls needed for a security assessment.

https://www.isc2.org/News-and-Events/Blog/What-is-a-SOC-1-Report

✗ **B** Service Organization Control (SOC) 2 Type 1
SOC 2 Type 1 describes the design of security-related controls at a point in time but does not provide evidence of operating effectiveness, making it less suitable as a baseline for an assessment.

https://www.isc2.org/News-and-Events/Blog/What-is-a-SOC-2-Report

✗ **C** Service Organization Control (SOC) 1 Type 1
SOC 1 Type 1, like SOC 1 Type 2, is limited to financial reporting controls and does not address the security criteria required for a baseline security assessment.

https://www.isc2.org/News-and-Events/Blog/What-is-a-SOC-1-Report

✓ **D** Service Organization Control (SOC) 2 Type 2
SOC 2 Type 2 provides an independent assessment of the design and operating effectiveness of security, availability, processing integrity, confidentiality, and privacy controls over a period of time, making it an industry-recognized baseline for data security and business-operations assessments.

https://www.isc2.org/News-and-Events/Blog/What-is-a-SOC-2-Report

Question 80

Single choice · Domain: D6 Security Assessment and Testing › Identify and apply vulnerability scoring frameworks such as CVSS

Which of the following frameworks provides vulnerability metrics and characteristics to support the National Vulnerability Database (NVD)?

A. Center for Internet Security (CIS)
B. Common Vulnerabilities and Exposures (CVE)
C. Open Web Application Security Project (OWASP)
D. Common Vulnerability Scoring System (CVSS)

Answer: D. Common Vulnerability Scoring System (CVSS)

Explanation

The question tests knowledge of frameworks that provide vulnerability metrics used by the NVD, which is part of security assessment and testing.

Free demo · full exam: 1485 questions

✗ **A** Center for Internet Security (CIS)
CIS provides security benchmarks, not vulnerability metrics for the NVD.
https://www.isc2.org/Certifications/CISSP

✗ **B** Common Vulnerabilities and Exposures (CVE)
CVE supplies unique identifiers for vulnerabilities but does not define metrics or characteristics.
https://www.isc2.org/Certifications/CISSP

✗ **C** Open Web Application Security Project (OWASP)
OWASP offers project resources like the Top Ten, not a scoring framework for the NVD.
https://www.isc2.org/Certifications/CISSP

✓ **D** Common Vulnerability Scoring System (CVSS)
CVSS provides standardized vulnerability metrics and severity scores used by the NVD.
https://www.isc2.org/Certifications/CISSP

Question 81

Single choice · Domain: D7 Security Operations › Develop an Information Security Continuous Monitoring (ISCM) strategy

Information Security Continuous Monitoring (1SCM) is defined as maintaining ongoing awareness of information security, vulnerabilities, and threats to support organizational risk management decisions. Which of the following is the FIRST step in developing an ISCM strategy and implementing an ISCM program?

A. Define a strategy based on risk tolerance that maintains clear visibility into assets, awareness of vulnerabilities, up-to-date threat information, and mission/business impacts.

B. Conduct a vulnerability assessment to discover current threats against the environment and incorporate them into the program.

C. Respond to findings with technical management, and operational mitigating activities or acceptance, transference/sharing, or avoidance/rejection.

D. Analyze the data collected and report findings, determining the appropriate response. It may be necessary to collect additional information to clarify or supplement existing monitoring data.

Answer: A. Define a strategy based on risk tolerance that maintains clear visibility into assets, awareness of vulnerabilities, up-to-date threat information, and mission/business impacts.

Explanation

The question tests the candidate's ability to identify the initial activity when creating an ISCM program, which is to define a strategy aligned with risk tolerance and asset visibility, a core task in Security Operations.

✓ **A** Define a strategy based on risk tolerance that maintains clear visibility into assets, awareness of vulnerabilities, up-to-date threat information, and mission/business impacts.
Correct. The first step in an ISCM program is to establish a strategy that aligns with the organization's risk tolerance and defines the scope of monitoring.
https://www.isc2.org/News-and-Events/Blog/2020/06/02/Information-Security-Continuous-Monitoring

✗ **B** Conduct a vulnerability assessment to discover current threats against the environment and incorporate them into the program.

Free demo · full exam: 1485 questions

Incorrect. Vulnerability assessment is a subsequent activity that provides data for the monitoring process, not the initial strategic definition.

https://www.isc2.org/News-and-Events/Blog/2020/06/02/Information-Security-Continuous-Monitoring

✗ **C** Respond to findings with technical management, and operational mitigating activities or acceptance, transference/sharing, or avoidance/rejection.
Incorrect. Response actions occur after data collection and analysis; they are not the first step in developing the ISCM strategy.

https://www.isc2.org/News-and-Events/Blog/2020/06/02/Information-Security-Continuous-Monitoring

✗ **D** Analyze the data collected and report findings, determining the appropriate response. It may be necessary to collect additional information to clarify or supplement existing monitoring data.
Incorrect. Data analysis and reporting are later phases of the ISCM lifecycle, following the establishment of the monitoring strategy.

https://www.isc2.org/News-and-Events/Blog/2020/06/02/Information-Security-Continuous-Monitoring

Question 82

Single choice · Domain: D7 Security Operations › Identify and describe types of malicious software, specifically spyware

Spyware is BEST described as

A. data mining for advertising.
B. a form of cyber-terrorism,
C. an information gathering technique,
D. a web-based attack.

Answer: C. an information gathering technique,

Explanation

The question tests the candidate's ability to correctly define spyware, a form of malware that covertly gathers information about a user.

✗ **A** data mining for advertising.
Incorrect. Spyware is not merely data mining for advertising; it operates without user consent to collect data.

https://www.isc2.org/News-and-Events/Blog/What-is-Malware

✗ **B** a form of cyber-terrorism,
Incorrect. While spyware can be used in malicious campaigns, it is not defined as cyber-terrorism.

https://www.isc2.org/News-and-Events/Blog/What-is-Malware

✓ **C** an information gathering technique,
Correct. Spyware is software designed to gather information about a user or system without their knowledge.

https://www.isc2.org/News-and-Events/Blog/What-is-Malware

✗ **D** a web-based attack.
Incorrect. Spyware is not limited to web-based attacks; it can be installed via various vectors.

https://www.isc2.org/News-and-Events/Blog/What-is-Malware

Dumpsgate

Question 83

Single choice · Domain: D7 Security Operations › Identify and classify security incidents reported by a SIEM system

Which of the following would be considered an incident if reported by a security information and event management (SIEM) system?

A. An administrator is logging in on a server through a virtual private network (VPN).

B. A log source has stopped sending data.

C. A web resource has reported a 404 error.

D. A firewall logs a connection between a client on the Internet and a web server using Transmission Control Protocol (TCP) on port 80.

Answer: B. A log source has stopped sending data.

Explanation

The question tests the candidate's ability to distinguish between routine log events and true security incidents as defined in the Security Operations domain of the CISSP CBK.

✗ **A** An administrator is logging in on a server through a virtual private network (VPN).
Normal administrative activity is not inherently an incident; incidents involve violations or threats.

https://www.isc2.org/Certifications/CISSP/Domain-7

✓ **B** A log source has stopped sending data.
Loss of a log source is treated as a security incident because it may indicate tampering, failure, or a gap in monitoring that requires investigation.

https://www.isc2.org/Certifications/CISSP/Domain-7

✗ **C** A web resource has reported a 404 error.
A 404 error is a standard client-side response for a missing page and does not constitute a security incident.

https://www.isc2.org/Certifications/CISSP/Domain-7

✗ **D** A firewall logs a connection between a client on the Internet and a web server using Transmission Control Protocol (TCP) on port 80.
Logging normal HTTP traffic is routine monitoring, not an incident unless anomalous behavior is detected.

https://www.isc2.org/Certifications/CISSP/Domain-7

Free demo · full exam: 1485 questions

Question 84

Single choice · Domain: D7 Security Operations › Ensure log sources are synchronized to a common time reference for accurate event correlation

Which of the following MUST the administrator of a security information and event management (SIEM) system ensure?

A. All sources are reporting in the exact same Extensible Markup Language (XML) format.
B. Data sources do not contain information infringing upon privacy regulations.
C. All sources are synchronized with a common time reference.
D. Each source uses the same Internet Protocol (IP) address for reporting.

Answer: C. All sources are synchronized with a common time reference.

Explanation

The question tests the candidate's knowledge of essential SIEM requirements, specifically the need for time synchronization across all data sources.

✗ **A** All sources are reporting in the exact same Extensible Markup Language (XML) format.
Incorrect. SIEM solutions can ingest multiple log formats (XML, JSON, syslog, etc.); uniform format is not mandatory.

https://www.isc2.org/Portals/0/CBK/Domain%20VIII%20-%20Security%20Operations.pdf

✗ **B** Data sources do not contain information infringing upon privacy regulations.
Incorrect. While privacy compliance is important, the SIEM administrator is not required to guarantee that sources contain no privacy-infringing data; that is a broader organizational compliance issue.

https://www.isc2.org/Portals/0/CBK/Domain%20VIII%20-%20Security%20Operations.pdf

✓ **C** All sources are synchronized with a common time reference.
Correct. Accurate correlation of events across multiple sources depends on consistent timestamps, which requires all sources to be synchronized to a common time reference (e.g., NTP).

https://www.isc2.org/Portals/0/CBK/Domain%20VIII%20-%20Security%20Operations.pdf

✗ **D** Each source uses the same Internet Protocol (IP) address for reporting.
Incorrect. SIEM collectors can receive logs from many different IP addresses; using a single IP address is not a requirement.

https://www.isc2.org/Portals/0/CBK/Domain%20VIII%20-%20Security%20Operations.pdf

Free demo · full exam: 1485 questions

Question 85

Single choice · Domain: D7 Security Operations › Select and implement technologies to detect successful network breaches

The security organization is loading for a solution that could help them determine with a strong level of confident that attackers have breached their network. Which solution is MOST effective at discovering successful network breach?

A. Installing an intrusion prevention system (IPS)
B. Deploying a honeypot
C. Installing an intrusion detection system (IDS)
D. Developing a sandbox

Answer: B. Deploying a honeypot

Explanation

The question tests the candidate's ability to choose the most effective detection mechanism for confirming a network compromise.

✗ **A** Installing an intrusion prevention system (IPS)
Incorrect. An IPS blocks malicious traffic but does not provide strong confidence that a breach has already occurred.

https://www.isc2.org/Certifications/CISSP

✓ **B** Deploying a honeypot
Correct. A honeypot is a decoy system that, when accessed, gives high confidence that an attacker has breached the network.

https://www.isc2.org/Certifications/CISSP

✗ **C** Installing an intrusion detection system (IDS)
Incorrect. An IDS can generate alerts but may produce false positives and does not guarantee confirmation of a breach.

https://www.isc2.org/Certifications/CISSP

✗ **D** Developing a sandbox
Incorrect. A sandbox isolates and analyzes suspicious code but is not primarily used to detect a network breach.

https://www.isc2.org/Certifications/CISSP

Free demo · full exam: 1485 questions

Question 86

Single choice · Domain: D7 Security Operations › Describe the standard digital forensic process steps

Which of the following describes the order in which a digital forensic process is usually conducted?

A. Ascertain legal authority, agree upon examination strategy, conduct examination, and report results

B. Ascertain legal authority, conduct investigation, report results, and agree upon examination strategy

C. Agree upon examination strategy, ascertain legal authority, conduct examination, and report results

D. Agree upon examination strategy, ascertain legal authority, report results, and conduct examination

Answer: A. Ascertain legal authority, agree upon examination strategy, conduct examination, and report results

Explanation

The question tests knowledge of the correct sequence of activities in a digital forensic investigation, which falls under the Security Operations domain.

✓ **A** Ascertain legal authority, agree upon examination strategy, conduct examination, and report results Correct. The typical digital forensic workflow begins with establishing legal authority, then planning the examination strategy, followed by the actual examination, and finally reporting the findings.

https://www.isc2.org/Certifications/CISSP

✗ **B** Ascertain legal authority, conduct investigation, report results, and agree upon examination strategy Incorrect. The examination strategy must be agreed upon before the investigation begins, and reporting occurs after the examination, not before.

https://www.isc2.org/Certifications/CISSP

✗ **C** Agree upon examination strategy, ascertain legal authority, conduct examination, and report results Incorrect. Legal authority must be established prior to planning the examination strategy to ensure compliance with laws and regulations.

https://www.isc2.org/Certifications/CISSP

✗ **D** Agree upon examination strategy, ascertain legal authority, report results, and conduct examination Incorrect. Reporting cannot be completed before the examination is performed; the proper order places reporting after the examination.

https://www.isc2.org/Certifications/CISSP

Free demo · full exam: 1485 questions

Question 87

Single choice · Domain: D7 Security Operations › Identify the purpose of physical security controls such as tamper seals

The MAIN purpose of placing a tamper seal on a computer system's case is to:

A. raise security awareness.
B. detect efforts to open the case.
C. expedite physical auditing.
D. make it difficult to steal internal components.

Answer: B. detect efforts to open the case.

Explanation

The question assesses knowledge of physical security measures used to detect unauthorized access to equipment.

✗ **A** raise security awareness.
Incorrect. Tamper seals are not primarily for awareness; they provide evidence of case opening.
https://www.isc2.org/Certifications/CISSP

✓ **B** detect efforts to open the case.
Correct. The main purpose of a tamper seal is to indicate if the case has been opened, providing detection of unauthorized access.
https://www.isc2.org/Certifications/CISSP

✗ **C** expedite physical auditing.
Incorrect. While tamper seals may aid audits, their primary purpose is detection, not expediting audits.
https://www.isc2.org/Certifications/CISSP

✗ **D** make it difficult to steal internal components.
Incorrect. Tamper seals do not primarily deter theft; they signal case opening.
https://www.isc2.org/Certifications/CISSP

Question 88

Single choice · Domain: D7 Security Operations › Identify the department responsible for initiating request, approval, and provisioning processes

Which of the following departments initiates the request, approval, and provisioning business process?

A. Operations
B. Human resources (HR)
C. Information technology (IT)
D. Security

Answer: C. Information technology (IT)

Free demo · full exam: 1485 questions

Dumpsgate

Question 89

Single choice · Domain: D7 Security Operations › Identify appropriate security controls for incident response and recovery

While dealing with the consequences of a security incident, which of the following security controls are MOST appropriate?

A. Detective and recovery controls
B. Corrective and recovery controls
C. Preventative and corrective controls
D. Recovery and proactive controls

Answer: B. Corrective and recovery controls

Explanation

The question asks which controls are most suitable when handling the consequences of a security incident, which is a core topic of incident response within the Security Operations domain.

✗ **A** Detective and recovery controls
Detective controls are used to identify events, not to address consequences. Recovery alone is insufficient without corrective actions.

https://www.isc2.org/News-and-Events/Blog/Incident-Response-The-6-Phases

✓ **B** Corrective and recovery controls
Corrective controls remediate the effects of an incident, and recovery controls restore normal operations, making them the most appropriate for dealing with consequences.

Free demo · full exam: 1485 questions

https://www.isc2.org/News-and-Events/Blog/Incident-Response-The-6-Phases

✗ **C** Preventative and corrective controls
Preventative controls aim to stop incidents before they occur; they are not focused on post-incident consequences. Corrective is relevant, but the pair is not optimal.

https://www.isc2.org/News-and-Events/Blog/Incident-Response-The-6-Phases

✗ **D** Recovery and proactive controls
Proactive controls are forward-looking measures, not intended for handling incident aftermath. Recovery alone does not address remediation.

https://www.isc2.org/News-and-Events/Blog/Incident-Response-The-6-Phases

Question 90

Single choice · Domain: D7 Security Operations › Identify primary responsibilities of security operations for incident handling and reporting

What are the PRIMARY responsibilities of security operations for handling and reporting violations and incidents?

A. Monitoring and identifying system failures, documenting incidents for future analysis, and scheduling patches for systems
B. Scheduling patches for systems, notifying the help desk, and alerting key personnel
C. Monitoring and identifying system failures, alerting key personnel, and containing events
D. Documenting incidents for future analysis, notifying end users, and containing events

Answer: C. Monitoring and identifying system failures, alerting key personnel, and containing events

Explanation

The question asks about the core duties of a security operations function when dealing with violations and incidents, which is covered in the Security Operations domain of the CISSP CBK.

✗ **A** Monitoring and identifying system failures, documenting incidents for future analysis, and scheduling patches for systems
Incorrect. While monitoring and documentation are relevant, scheduling patches is a vulnerability-management activity, not a primary incident-handling responsibility.

https://www.isc2.org/Certifications/CISSP/Domain-5

✗ **B** Scheduling patches for systems, notifying the help desk, and alerting key personnel
Incorrect. This option omits monitoring and containment, which are essential to security operations incident response.

https://www.isc2.org/Certifications/CISSP/Domain-5

✓ **C** Monitoring and identifying system failures, alerting key personnel, and containing events
Correct. Security operations' primary responsibilities include continuous monitoring, alerting appropriate stakeholders, and containing incidents to limit impact.

https://www.isc2.org/Certifications/CISSP/Domain-5

✗ **D** Documenting incidents for future analysis, notifying end users, and containing events
Incorrect. Although documentation and containment are relevant, the lack of monitoring and immediate alerting makes this option incomplete for primary responsibilities.

Free demo · full exam: 1485 questions

https://www.isc2.org/Certifications/CISSP/Domain-5

Question 91

Single choice · Domain: D7 Security Operations › Identify and evaluate disaster recovery plan testing methods and associated operational risks

Which type of disaster recovery plan (DRP) testing carries the MOST operational risk?

A. Cutover
B. Walkthrough
C. Tabletop
D. Parallel

Answer: A. Cutover

Explanation

The question assesses the candidate's knowledge of different DRP testing types and which carries the greatest operational risk, a key skill in security operations and business continuity planning.

✓ **A** Cutover
Correct. Cutover testing involves fully activating the disaster recovery site and shutting down the primary production environment, exposing the organization to the highest operational risk.

https://www.isc2.org/Certifications/CISSP/Exam-Outline

✗ **B** Walkthrough
Incorrect. A walkthrough is a review of the DR plan without executing any actual changes, presenting minimal operational risk.

https://www.isc2.org/Certifications/CISSP/Exam-Outline

✗ **C** Tabletop
Incorrect. Tabletop exercises are discussion-based simulations that do not affect live systems, thus they carry low operational risk.

https://www.isc2.org/Certifications/CISSP/Exam-Outline

✗ **D** Parallel
Incorrect. Parallel testing runs the DR site alongside the production environment, allowing verification without disrupting operations, so its operational risk is lower than cutover testing.

https://www.isc2.org/Certifications/CISSP/Exam-Outline

Free demo · full exam: 1485 questions

Question 92

Single choice · Domain: D7 Security Operations › Select appropriate level of detail for audit record generation

Which of the following is the PRIMARY reason for selecting the appropriate level of detail for audit record generation?

A. Lower costs throughout the System Development Life Cycle (SDLC)
B. Facilitate a root cause analysis (RCA)
C. Enable generation of corrective action reports
D. Avoid lengthy audit reports

Answer: B. Facilitate a root cause analysis (RCA)

Explanation

The question assesses the candidate's ability to determine the primary purpose of audit log detail, which is to support effective root cause analysis during investigations.

✗ **A** Lower costs throughout the System Development Life Cycle (SDLC)
Incorrect. While cost considerations are important, they are not the primary reason for choosing audit detail level.

https://www.isc2.org/Certifications/CISSP/Domain-7

✓ **B** Facilitate a root cause analysis (RCA)
Correct. Selecting the appropriate level of detail ensures sufficient information is available to perform effective root cause analysis of security events.

https://www.isc2.org/Certifications/CISSP/Domain-7

✗ **C** Enable generation of corrective action reports
Incorrect. Generating corrective action reports is a downstream activity; the primary driver for audit detail is to support RCA.

https://www.isc2.org/Certifications/CISSP/Domain-7

✗ **D** Avoid lengthy audit reports
Incorrect. While brevity is a consideration, the main purpose of audit detail selection is to provide enough data for root cause analysis, not merely to shorten reports.

https://www.isc2.org/Certifications/CISSP/Domain-7

Free demo · full exam: 1485 questions

Question 93

Single choice · Domain: D7 Security Operations › Implement media sanitization and disposal techniques

Which of the following is the MOST appropriate technique for destroying magnetic platter style hard disk drives (HDD) containing data with a "HIGH" security categorization?

A. Drill through the device and platters.
B. Mechanically shred the entire HDD.
C. Remove the control electronics.
D. HP iProcess the HDD through a degaussing device.

Answer: B. Mechanically shred the entire HDD.

Explanation

The question tests knowledge of appropriate data destruction methods for high-security classification media, a key skill in security operations.

✗ **A** Drill through the device and platters.
Drilling may damage the platters but does not guarantee complete data destruction and is not the recommended method for high-security media.
https://www.isc2.org/News-and-Events/Blog/2019/09/12/Data-Destruction

✓ **B** Mechanically shred the entire HDD.
Physical shredding of the whole drive meets the high-security requirement for media sanitization, ensuring data cannot be recovered.
https://www.isc2.org/News-and-Events/Blog/2019/09/12/Data-Destruction

✗ **C** Remove the control electronics.
Removing electronics leaves the magnetic platters intact, allowing data recovery; it is insufficient for high-security classification.
https://www.isc2.org/News-and-Events/Blog/2019/09/12/Data-Destruction

✗ **D** HP iProcess the HDD through a degaussing device.
Degaussing is ineffective for modern HDDs due to high coercivity; it is not the preferred method for high-security media destruction.
https://www.isc2.org/News-and-Events/Blog/2019/09/12/Data-Destruction

Question 94

Single choice · Domain: D8 Software Development Security › Explain the primary purpose of software security testing

What is the overall goal of software security testing?

A. Identifying the key security features of the software
B. Ensuring all software functions perform as specified
C. Reducing vulnerabilities within a software system
D. Making software development more agile

Free demo · full exam: 1485 questions

Answer: C. Reducing vulnerabilities within a software system

Explanation

The question asks for the overall goal of software security testing, which is a core concept in the Software Development Security domain of the CISSP CBK.

✗ **A** Identifying the key security features of the software
Incorrect. Identifying security features is part of security design, not the primary goal of testing.
https://www.isc2.org/Certifications/CISSP

✗ **B** Ensuring all software functions perform as specified
Incorrect. This describes functional testing, whereas security testing focuses on vulnerabilities.
https://www.isc2.org/Certifications/CISSP

✓ **C** Reducing vulnerabilities within a software system
Correct. The overall goal of software security testing is to discover and mitigate vulnerabilities to improve the security posture.
https://www.isc2.org/Certifications/CISSP

✗ **D** Making software development more agile
Incorrect. Agility relates to development processes, not the primary aim of security testing.
https://www.isc2.org/Certifications/CISSP

Question 95

Single choice · Domain: D8 Software Development Security › Identify the appropriate phase in the software assurance life cycle for recognizing risks related to software acquisition strategies

At which phase of the software assurance life cycle should risks associated with software acquisition strategies be identified?

A. Follow-on phase
B. Planning phase
C. Monitoring and acceptance phase
D. Contracting phase

Answer: B. Planning phase

Explanation

The question assesses knowledge of the software assurance life cycle phases and where risk identification for acquisition activities belongs.

✗ **A** Follow-on phase
The follow-on phase occurs after implementation and is not the point at which acquisition-related risks are identified.
https://www.isc2.org/Certifications/CISSP

✓ **B** Planning phase

Free demo · full exam: 1485 questions

During the planning phase of the software assurance life cycle, security requirements, acquisition strategies, and associated risks are defined and evaluated.

https://www.isc2.org/Certifications/CISSP

✗ **C** Monitoring and acceptance phase
Monitoring and acceptance focus on post-implementation performance and compliance, not on initial acquisition risk identification.

https://www.isc2.org/Certifications/CISSP

✗ **D** Contracting phase
While contracts address terms, the identification of acquisition-related risks is performed earlier during planning to inform contract negotiations.

https://www.isc2.org/Certifications/CISSP

Question 96

Single choice · Domain: D8 Software Development Security › Apply secure design principles using object-oriented programming concepts

Which of the following should be included in a good defense-in-depth strategy provided by object-oriented programming for software deployment?

A. Polyinstantiation
B. Polymorphism
C. Encapsulation
D. Inheritance

Answer: C. Encapsulation

Explanation

The question assesses knowledge of OOP mechanisms that contribute to defense-in-depth, a key topic in the Software Development Security domain.

✗ **A** Polyinstantiation
Polyinstantiation is a database security technique, not an OOP concept for defense-in-depth.

https://www.isc2.org/Certifications/CISSP/Domain-8

✗ **B** Polymorphism
Polymorphism allows objects to be treated as instances of their parent type but does not directly provide encapsulation or defense-in-depth.

https://www.isc2.org/Certifications/CISSP/Domain-8

✓ **C** Encapsulation
Encapsulation hides internal object state and enforces access controls, supporting defense-in-depth in software design.

https://www.isc2.org/Certifications/CISSP/Domain-8

✗ **D** Inheritance
Inheritance promotes code reuse but does not inherently provide the layered security controls characteristic of defense-in-depth.

https://www.isc2.org/Certifications/CISSP/Domain-8

Free demo · full exam: 1485 questions

Question 97

Single choice · Domain: D8 Software Development Security › Identify appropriate SDLC phase for static code analysis

A software engineer uses automated tools to review application code and search for application flaws, back doors, or other malicious code. Which of the following is the FIRST Software Development Life Cycle (SDLC) phase where this takes place?

A. Design
B. Test
C. Development
D. Deployment

Answer: C. Development

Explanation

The question assesses knowledge of where security activities like automated code review occur within the SDLC.

✗ **A** Design
Code review is not typically performed during design; design focuses on architecture.
https://www.isc2.org/News-and-Events/Blog/2020/09/03/Software-Development-Life-Cycle-SDLC-Phases

✗ **B** Test
Testing includes dynamic testing, but static code analysis occurs earlier, during development.
https://www.isc2.org/News-and-Events/Blog/2020/09/03/Software-Development-Life-Cycle-SDLC-Phases

✓ **C** Development
Static code analysis and automated code review are performed during the development phase, the first SDLC phase where this occurs.
https://www.isc2.org/News-and-Events/Blog/2020/09/03/Software-Development-Life-Cycle-SDLC-Phases

✗ **D** Deployment
Deployment occurs after testing; code review is done earlier.
https://www.isc2.org/News-and-Events/Blog/2020/09/03/Software-Development-Life-Cycle-SDLC-Phases

Question 98

Single choice · Domain: D8 Software Development Security › Identify high-level audit phases of the Software Development Life Cycle

When auditing the Software Development Life Cycle (SDLC) which of the following is one of the high-level audit phases?

A. Requirements
B. Risk assessment
C. Due diligence
D. Planning

Free demo · full exam: 1485 questions

Answer: D. Planning

Explanation

The question asks which option represents a high-level audit phase within the SDLC, testing the candidate's knowledge of SDLC audit structure.

✗ **A** Requirements
Requirements is an SDLC activity but not listed as a high-level audit phase in the official (ISC)² guidance.
https://www.isc2.org/Certifications/CISSP

✗ **B** Risk assessment
Risk assessment is a security activity performed during planning, not a distinct high-level audit phase of the SDLC.
https://www.isc2.org/Certifications/CISSP

✗ **C** Due diligence
Due diligence relates to vendor or compliance reviews, not to the defined high-level audit phases of the SDLC.
https://www.isc2.org/Certifications/CISSP

✓ **D** Planning
Planning is recognized as one of the high-level audit phases in the SDLC audit process.
https://www.isc2.org/Certifications/CISSP

Question 99

Single choice · Domain: D8 Software Development Security › Identify security risks associated with software supply chain components

Which element of software supply chain management has the GREATEST security risk to organizations?

A. New software development skills are hard to acquire.
B. Unsupported libraries are often used.
C. Applications with multiple contributors are difficult to evaluate.
D. Vulnerabilities are difficult to detect.

Answer: B. Unsupported libraries are often used.

Explanation

The question evaluates the candidate's ability to recognize which aspect of software supply chain management presents the highest security risk, a key competency within the Software Development Security domain.

✗ **A** New software development skills are hard to acquire.
While talent shortages are a concern, they are not the greatest security risk in the software supply chain.
https://www.isc2.org/Certifications/CISSP/Domain-8-Software-Development-Security

Free demo · full exam: 1485 questions

✓ **B** Unsupported libraries are often used.
Using unsupported or outdated third-party libraries introduces known vulnerabilities into applications, representing the greatest security risk in the software supply chain.
https://www.isc2.org/Certifications/CISSP/Domain-8-Software-Development-Security

✗ **C** Applications with multiple contributors are difficult to evaluate.
Multiple contributors increase complexity, but the primary risk stems from vulnerable components such as unsupported libraries.
https://www.isc2.org/Certifications/CISSP/Domain-8-Software-Development-Security

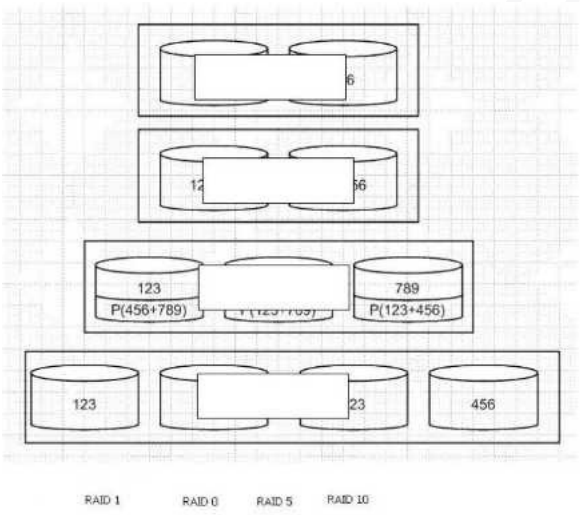
✗ **D** Vulnerabilities are difficult to detect.
Detecting vulnerabilities is a challenge, yet the root cause is often the inclusion of insecure, unsupported libraries, making option B the greater risk.
https://www.isc2.org/Certifications/CISSP/Domain-8-Software-Development-Security

Question 100

Domain: UNKNOWN › Interpret visual RAID level representations

Given a file containing ordered number, i.e. “123456789,” match each of the following redundant Array of independent Disks (RAID) levels to the corresponding visual representation visual representation. Note: P() = parity.

Drag each level to the appropriate place on the diagram.



Answer: Cannot determine the RAID level placements because the diagram is not included.

Explanation

The question asks you to match RAID levels to visual patterns, but the diagram that contains those patterns is not available here. The sequence “123456789” and the note that P() denotes parity do not specify which visual representation corresponds to each RAID level. Therefore, the placements cannot be determined from the provided material.

✓ **Answer** Cannot determine the RAID level placements because the diagram is not included.
The diagram is essential to identify the visual layouts being matched. Without it, there is no way to assign

Free demo · full exam: 1485 questions

RAID levels to the representations based only on the sequence and parity notation shown.

Dumpsgate