(ISC)²® CISSP® Examination Preparation Clinic

Sponsored by: University of Fairfax — *Secure Your Future™*

Presented by: Eric Handy, CISSP, CISM, PMP, CIPP/G, MBA

Agenda

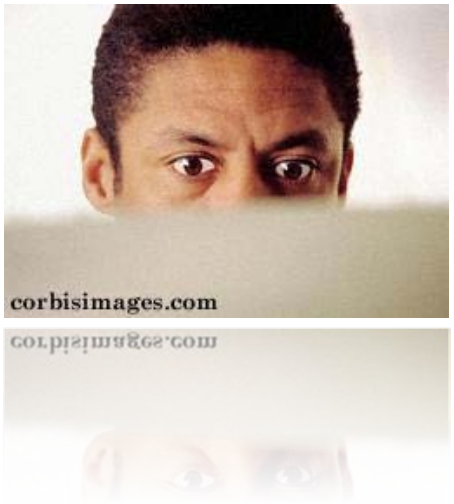
- Preparation
  - Weeks prior - study tips
  - 3 days prior - mental and physical
  - Day of - documents and materials
- Examination
  - Candidate information bulletin (CIB)
  - Format
  - FAQs
- Examination items (i.e., the questions)
  - Psychometrician terminology
  - Acceptable item formats
- Practice items

Agenda

- **Preparation**
  - Weeks prior - study tips
  - 3 days prior - mental and physical
  - Day of - documents and materials
- Examination
  - Candidate information bulletin (CIB)
  - Format
  - FAQs
- Examination items (i.e., the questions)
  - Psychometrician terminology
  - Acceptable item formats
- Practice items

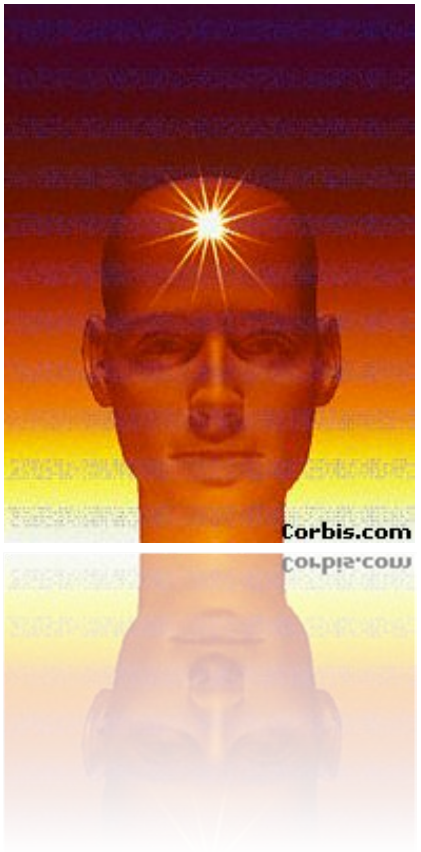
Preparation – Weeks Prior - Study Tips

- Don’t wait until the last minute
  - Study a little at a time
  - Space out your sessions
- Take frequent short breaks
  - Memory retention better at beginning and end
  - Retention not as productive in the middle
- Make sure you understand the material well
  - Don’t just read through the material - underline
  - Memorization is only a short term solution
- Test yourself to find your weak areas
  - Self-assessments (e.g., (ISC)² studISCope)
  - Practice questions (e.g., “Official (ISC)² Guide to the CISSP CBK”)
- Don’t study past your usual bedtime
  - Afternoons and early evenings more productive
  - Listen to relaxing music on low volume to relieve boredom
- Think outside the box
  - Link subjects together



Preparation – 3 Days Prior - Mental and Physical

- Ensure that you are mentally and physically prepared
  - Rested
  - Relaxed
  - Focused
- Both before and during the examination



Preparation – Day of - Documents and Materials

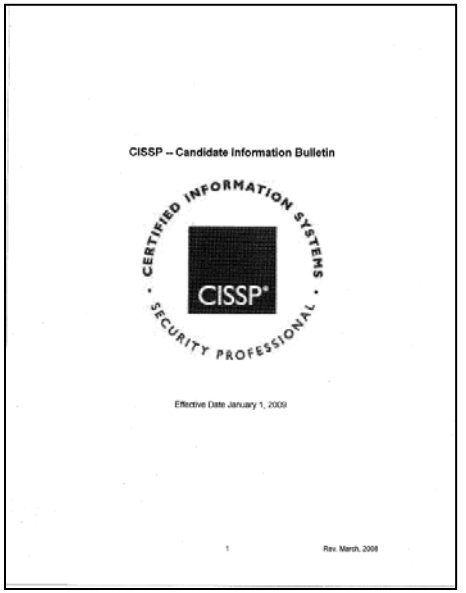
- Be on time
  - 0800 - Examination room doors open
  - 0830 - Examination instructions reviewed
  - 0900 - Examination begins (ends at 1500)
- Admittance
  - Admission letter
  - Government-issued photo ID
- Reference material
  - Not allowed in the examination room
  - Hard copy language translation dictionaries are permitted
  - No electronic language translation dictionaries
- Materials
  - Bring pencils and eraser
  - Water, coffee, lunch, and snacks are permitted in “snack area”
  - Mobile phones, beepers, and headphones are prohibited
  - Ear plugs are allowed
- Dress – business casual (neat…but, comfortable!)

Agenda

- Preparation
  - Weeks prior - study tips
  - 3 days prior - mental and physical
  - Day of - documents and materials
- **Examination**
  - **Candidate information bulletin (CIB)**
  - **Format**
  - **FAQs**
- Examination items (i.e., the questions)
  - Psychometrician terminology
  - Acceptable item formats
- Practice items

Examination – Candidate Information Bulletin (CIB)

- Examination blueprint to a limited level of detail
- Outlines major topics and sub-topics within each domain
- Suggested reference list
- Professional experience requirements
- Description of the format of the items on the examination
- Basic registration and admission policies
- Download at www.isc2.org



Examination – Format

- 250 multiple choice questions with four (4) choices each
  - 225 are marked
  - 25 are for “research purposes” only
- Scenario-based items with more than one multiple choice question associated with it
- Paper/pencil format
- Six (6) hours to complete
- Several forms (i.e., versions) of the examination
- Breaks are permitted
- Passing score: 700 of 1000 points

Examination – FAQs (1 of 2)

- **What is the passing score?**
  - 70% (700 out of 1000 points)
- **What is the pass rate?**
  - Approximately 70%
- **When can I expect the results?**
  - Approximately four (4) to six (6) weeks (official (ISC)² answer)
  - Approximately two (2) to three (3) weeks via email (current practice)
- **What if I fail?**
  - Retake the examination as soon as you are prepared

Examination – FAQs (2 of 2)

- **Must I subscribe to the (ISC)² Code of Ethics?**
  - Yes, it's a prerequisite for certification
- **What are the most difficult domains?**
  - Traditionally, Physical Security; Business Continuity and Disaster Recovery Planning; and Architecture Security and Design
- **Are all domains equally weighted?**
  - Yes
- **Where do the questions come from?**
  - Subject matter experts participate in periodic item writing workshops to create the items under the supervision of psychometricians

Agenda

- Preparation
  - Weeks prior - study tips
  - 3 days prior - mental and physical
  - Day of - documents and materials
- Examination
  - Candidate information bulletin (CIB)
  - Format
  - FAQs
- Examination items (i.e., the questions)
  - Psychometrician terminology
  - Acceptable item formats
- Practice items

Psychometrician Terminology

- **Items** - Multiple-choice questions that make up an examination
- **Stem** - Portion of the item that provides the stimulus to which candidates respond
- **Options** - Responses to the question or problem
- **Candidate** - the individual being tested for professional competency
- **Multiple-choice item** - A style of question that tests a specific knowledge, skill, or ability and offers multiple options; out of these options only one is the correct or best answer
- **Key** - Option that represents the correct solution to the question or problem presented in the stem
- **Distracters** - The incorrect answers to the question or problem presented in the stem

Sample Item

Stem → Which of the following **BEST** describes an El Gamal encryption algorithm?

Options

Distracters

A. It is patented.

B. It is a signature scheme.

C. It is a symmetric algorithm.

Key → D. It is a public key algorithm.

Source : (ISC)² Guidelines for Item Writers and Reviewers

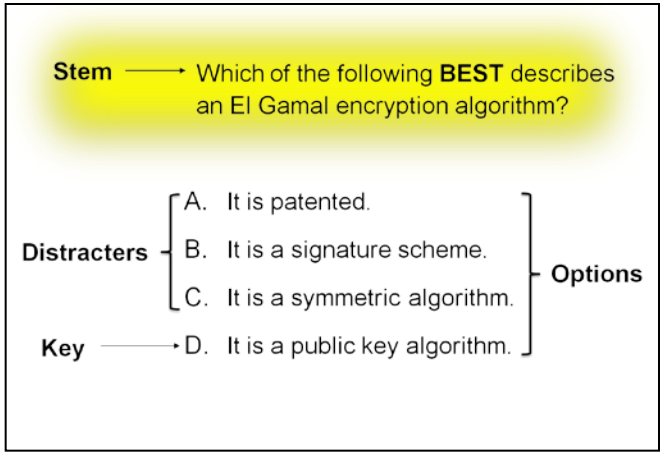
Global Considerations

- Item
  - Ask a question or present a complete statement that requires a response
  - No true/false items
- Question
  - Linked to the content outline
  - Clear and unambiguous - not tricky
- Key
  - Accurate
  - Valid reference

Source : (ISC)² Guidelines for Item Writers and Reviewers

Stem

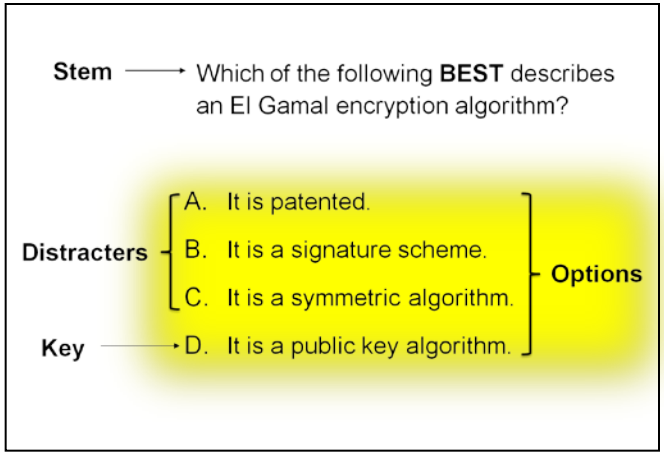
- States the question clearly (i.e., the candidate should not have to read the options to understand what is being asked)
- Free of excess words
- Clear and focused on the problem presented in the question
- Written at an appropriate reading level
- Correct grammar and punctuation
- Does not have "fill-in-the-blanks" within it
- Does not provide clues to the key



Source : (ISC)² Guidelines for Item Writers and Reviewers

Options

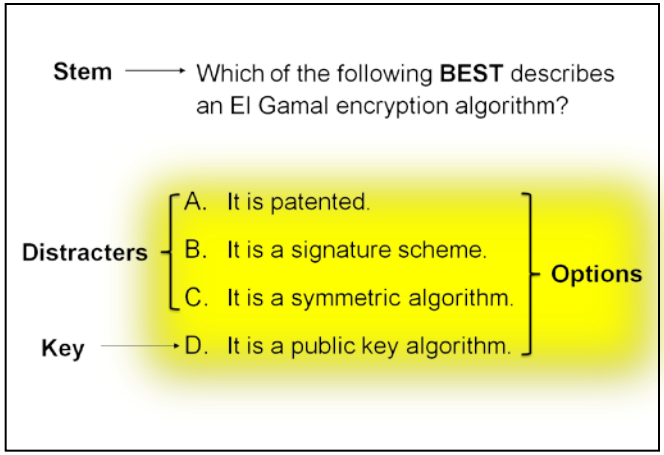
- All items have four options - A, B, C, and D
- Incorrect options are called distracters (attractive to uninformed candidates)
- No two options should have the same meaning
- “All of the above” or “none of the above” are not used as options
- Each option is distinct and unique
- Combinations of two options, such as “A and B”; or “B and C”, are not used



Source : (ISC)² Guidelines for Item Writers and Reviewers

Options (cont.)

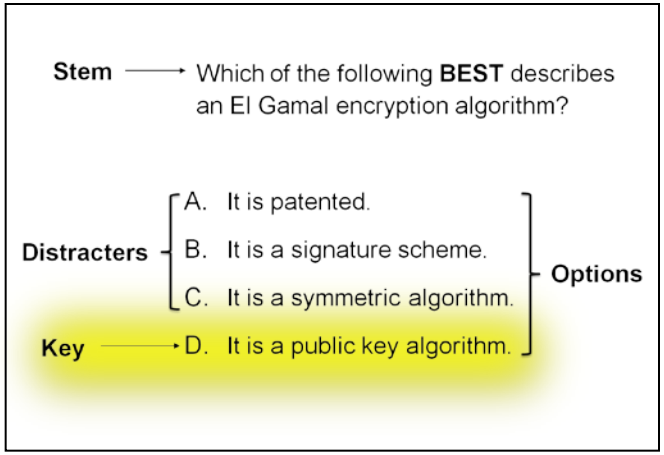
- Options should:
  - Flow with the stem
  - Be real and plausible
  - Be free of absolute qualifiers (e.g., never, always)
  - Be similar in length, if possible
  - Be phrased positively
  - Be concise yet complete
  - Be ordered logically
  - Be free of humor



Source : (ISC)² Guidelines for Item Writers and Reviewers

Key

- Key is the correct or single best answer
- Information from the stem is not used in the key
- Key is varied (i.e., key is assigned to A, B, C, and D alternately)



Source : (ISC)² Guidelines for Item Writers and Reviewers

General Guidelines - Items

- Be relevant to the examination specifications
  - Each item must be linked to one area of the detailed content outline (DCO)
  - The examination measures concepts relevant to the role of the security professional
  - Content objectives found on the DCO reflect day-to-day practice and establish what is fair for assessment
- Have valid references
  - The use of approved references serves to support the validity of the examination
- Be free of bias
  - Examination should be free from all forms of racial, ethnic, religious, regional, age, and gender bias
  - To avoid gender bias, the title of the individual is used
  - Avoid writing items specific to a region or a country.

Source : (ISC)² Guidelines for Item Writers and Reviewers

Style Guidelines

- Write at an acceptable reading level, and avoid wordiness
- Use titles instead of proper names (e.g., “The security professional” instead of “Patty Smith”)
- Do not write in the 1st person (i.e., “I”) or 2nd person (i.e., “You”)
- Do not use teaching statements or humor

Source : (ISC)² Guidelines for Item Writers and Reviewers

Grammar and Syntax Considerations

- Standard rules of grammar are applied to item writing (i.e., correct parts of speech and punctuation, and proper sentence structure)
- The use of absolute qualifiers (e.g., never, always, all, none, only, etc.) which indicate there are no exceptions are avoided

Source : (ISC)² Guidelines for Item Writers and Reviewers

Acceptable Item Formats

- Each item consists of a stem and four options
- An item may be written as a complete question or as a partial phrase with the options completing the sentence
- Punctuation is used to support readability

Complete Question Format

Which of the following describes the concept of non-repudiation?

A. The receiver can verify that the sender's public key is not compromised.

B. The receiver can prove that the sender sent the message.

C. The sender can verify that the receiver read the message.

D. The sender can verify the receiver's private key.

Partial Phrase Format

Non-repudiation means that the

A. receiver can verify that the sender's public key is not compromised.

B. receiver can prove that the sender sent the message.

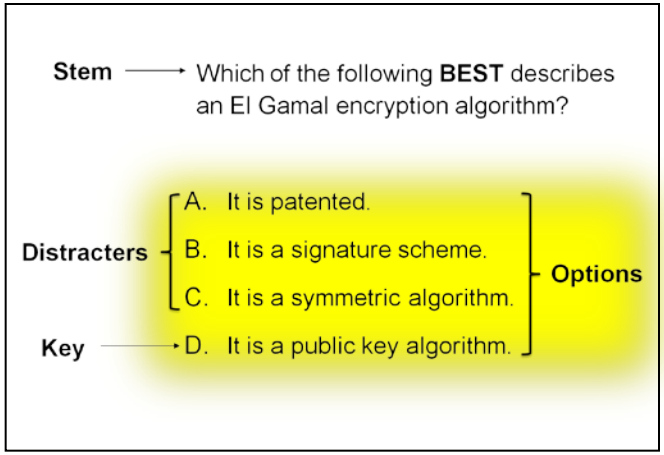
C. sender can verify that the receiver read the message.

D. sender can verify the receiver's private key.

Source : (ISC)² Guidelines for Item Writers and Reviewers

Parallel Options

- Options should be similar and parallel in regards to:
  - Complexity
  - Length
  - Subject
  - Grammar
- To be parallel, all four options must deal with the same issue and answer the same problem or question



Source : (ISC)² Guidelines for Item Writers and Reviewers

Parallel Options

Options that **ARE NOT** parallel

Which of the following groups is the leading source of computer crime losses?

(A) Employees
(B) Weak keys
(C) Hackers
(D) Viruses

Options that **ARE** parallel

Which of the following groups is the leading source of computer crime losses?

(A) Employees
(B) Foreign agents
(C) Hackers
(D) Industrial saboteurs

Source : (ISC)² Guidelines for Item Writers and Reviewers

Numeric Considerations

- Numeric options should be in ascending or descending order
- When using ranges of numbers in the options, there should be no overlap
- The same standard of measurement should be used throughout the item (i.e., either US standard or metric, not both)
- Rational numbers between zero (0) and twelve (12) should be written out in the stem

Source : (ISC)² Guidelines for Item Writers and Reviewers

Clueing

- Do not repeat words in the key that already appear in the stem.

Item which **DOES** contain clueing.

What kind of attack exhausts all possible solutions?

(A) Trojan horse
(B) Trap door
(C) Clone
(D) Exhaustive*

Item which **DOES NOT** contains clueing.

What kind of attack tries all possible solutions?

(A) Trojan horse
(B) Trap door
(C) Clone
(D) Exhaustive*

Source : (ISC)² Guidelines for Item Writers and Reviewers

Negatively Stated Items

- Do not write negative stems using **NOT** or **EXCEPT**
  - Creates undue cognitive burden
  - May provide information to answer other questions

Source : (ISC)² Guidelines for Item Writers and Reviewers

Cognitive Classifications

- Multiple-choice items are written to cover several cognitive domains based on Bloom's taxonomy:
  - Knowledge/comprehension
  - Application
  - Analysis/evaluation

Source : (ISC)² Guidelines for Item Writers and Reviewers

Cognitive Classification (Knowledge)

- A **knowledge/comprehension** item tests the understanding of a fact and asks the candidate to recall data or information
- Example: “Which of the following identifies an objective of the (ISC)² Code of Ethics?”
- Key words: define, describe, identify, etc.

Source : (ISC)² Guidelines for Item Writers and Reviewers

Cognitive Classification (Application)

- An **application** item tests the candidate's ability to apply knowledge to the process of solving a problem in the workplace.
- Example: "How would implementing separation of duties change the number of security incidences within an organization?"
- Key Words: applies, changes, demonstrates, modifies, produces, etc.

Source : (ISC)² Guidelines for Item Writers and Reviewers

Cognitive Classification (Analysis/Evaluation)

- An **analysis/evaluation** item tests the candidate's ability to recognize relationships among elements of knowledge, to distinguish between facts and inferences
- Example: "A security practitioner suspects that an employee is accessing sensitive data from the human resources department. What is the **FIRST** step to take in investigating this incident?"
- Key Words: analyze, differentiate, compare, illustrate, contrast, distinguish, classify, prioritize, etc.

Source : (ISC)² Guidelines for Item Writers and Reviewers

Scenario-Based Items

- A scenario set of items are two or more items related to the same situation or problem
- Each item must be independent of the other items in the set
- One item should not provide clues for answering another item in the set
- Each item in the set must be clearly linked to the scenario

Source : (ISC)² Guidelines for Item Writers and Reviewers

Example of a Scenario-Based Item

- **Scenario**: A security practitioner is implementing a campus-wide network for a university, which is opening a new campus in six months. Over a thousand students have already enrolled. Running cable in conduit is not a possibility due to the historical significance of the buildings on campus. Students need to be able to use this network both for intra- and extra- campus communications.

Source : (ISC)² Guidelines for Item Writers and Reviewers

Example of a Scenario-Based Item (cont.)

Question #1:

1. Which of the following physical issues is the **GREATEST** concern with implementing this new network?

A. The distance between the new campus and the main campus
B. The materials used in the foundation of the buildings and parking lot
C. The amount of metal in the ceilings and walls in the administration building
D. The number of trees and foliage surrounding the campus parking lot

Source : (ISC)² Guidelines for Item Writers and Reviewers

Example of a Scenario-Based Item

Question #2:

2. The campus president's laptop has a wireless card which connects to several different wireless networks both on and off campus. Because others on campus also have network cards, which of the following options would provide comprehensive security for that laptop?

A. Use password access for access to all files and emails
B. Use 256 bit encryption on all outgoing emails and sensitive files
C. Use a proxy server that only allows access to school-approved sites
D. Use a virtual private network (VPN) with secure sockets layer (SSL)

Source : (ISC)² Guidelines for Item Writers and Reviewers

Agenda

- Preparation
  - Weeks prior - study tips
  - 3 days prior - mental and physical
  - Day of - documents and materials
- Examination
  - Candidate information bulletin (CIB)
  - Format
  - FAQs
- Examination items (i.e., the questions)
  - Psychometrician terminology
  - Acceptable item formats
- Practice items

Examination Taking Techniques

- Read the question carefully
- Find the key words in the question
- Determine what is the item writer is trying to ask
- Read all the answers before making a decision
- Choose the best answer of those given
- Keep the "big picture" in mind!
  - Don't let one, two, ten, or even twenty questions, that are confusing, fluster you
  - A successful candidate can miss 60+ items and still achieve a 70%

Practice Items – Access Control

1. The three types of access controls are administrative, physical, and

A. preventive.
B. deterrent.
C. technical.
D. directive.

Practice Items – Access Control

1. The three types of access controls are administrative, physical, and

A. preventive.
B. deterrent.
C. **technical**.
D. directive.

Practice Items – Access Control

2. The basic requirements of access controls include security, reliability, transparency, scalability, maintainability, auditability, integrity, and

A. separation of duties.
B. need to know.
C. least privilege.
D. authenticity.

Practice Items – Access Control

2. The basic requirements of access controls include security, reliability, transparency, scalability, maintainability, auditability, integrity, and

A. separation of duties.
B. need to know.
C. least privilege.
D. **authenticity.**

Practice Items – Access Control

3. Audit logs should include data about user-level events, application-level events, system-level events, and

A. architecture-level events.
B. framework-level events.
C. network-level events.
D. blueprint-level events.

Practice Items – Access Control

3. Audit logs should include data about user-level events, application-level events, system-level events, and

A. architecture-level events.
B. framework-level events.
C. **network-level events.**
D. blueprint-level events.

Practice Items – Access Control

4. An eye retinal scan biometric device measures what physical characteristics?

A. The amount of light reaching the retina
B. The amount of light reflected by the retina
C. The size, curvature, and shape of the retina
D. The pattern of blood vessels on the retina

Practice Items – Access Control

4. An eye retinal scan biometric device measures what physical characteristics?

A. The amount of light reaching the retina
B. The amount of light reflected by the retina
C. The size, curvature, and shape of the retina
D. **The pattern of blood vessels on the retina**

Practice Items – Access Control

5. In discretionary access control (DAC), who has authority to grant access to information?

- User
- Network security administrator
- System administrator
- Information owner

Practice Items – Access Control

5. In discretionary access control (DAC), who has authority to grant access to information?

- User
- Network security administrator
- System administrator
- **Information owner**

Practice Items – Applications Development Security

1. The best practice to prevent logging clutter in application security is to

A. Log an exception when it is wrapped with another exception and propagate.
B. Catch and log exceptions at every level in the software.
C. Catch and log exceptions only at points at which exceptions are actually handled.
D. Disable debug level logging in a production environment.

Practice Items – Applications Development Security

1. The best practice to prevent logging clutter in application security is to

A. Log an exception when it is wrapped with another exception and propagate.
B. Catch and log exceptions at every level in the software.
C. **Catch and log exceptions only at points at which exceptions are actually handled.**
D. Disable debug level logging in a production environment.

Practice Items – Applications Development Security

2. Which of the following database models places the data in tables where the rows represent records and the columns represent attributes?

A. Hierarchical database management system
B. Relational database management system
C. Network database management system
D. Divergent database management system

Practice Items – Applications Development Security

2. Which of the following database models places the data in tables where the rows represent records and the columns represent attributes?

A. Hierarchical database management system
B. **Relational database management system**
C. Network database management system
D. Divergent database management system

Practice Items – Applications Development Security

3. When the results of “Process A” depend on the behavior of other processes on the system, Process A may be vulnerable to

A. shared memory corruption.
B. a poorly designed locking strategy.
C. poor data validation.
D. a race condition.

Practice Items – Applications Development Security

3. When the results of “Process A” depend on the behavior of other processes on the system, Process A may be vulnerable to

A. shared memory corruption.
B. a poorly designed locking strategy.
C. poor data validation.
D. **a race condition.**

Practice Items – Applications Development Security

4. The **PRIMARY** advantage of content-dependent access control of information is that it

A. prevents data locking.
B. limits the user's individual address space.
C. provides highly granular control.
D. confines access to authorized users of the system.

Practice Items – Applications Development Security

4. The **PRIMARY** advantage of content-dependent access control of information is that it

A. prevents data locking.
B. limits the user's individual address space.
C. **provides highly granular control.**
D. confines access to authorized users of the system.

Practice Items – Applications Development Security

5. What type of subsystem is an application program that operates outside the operating system, carries out functions for a group of users, maintains some common data for all users in the group, and protects the data from improper access by users in the group?

A. Prevented subsystem
B. Protected subsystem
C. File subsystem
D. Directory subsystem

Practice Items – Applications Development Security

5. What type of subsystem is an application program that operates outside the operating system, carries out functions for a group of users, maintains some common data for all users in the group, and protects the data from improper access by users in the group?

A. Prevented subsystem
B. **Protected subsystem**
C. File subsystem
D. Directory subsystem

Practice Items – Business Continuity and Disaster Recovery Planning

1. What specifies the number of the most recent transactions which are allowed to be lost during the recovery process following a disaster?

A. Recovery point objective (RPO)
B. Recovery time objective (RTO)
C. Service delivery objective (SDO)
D. Maximum tolerable downtime (MTD)

Practice Items – Business Continuity and Disaster Recovery Planning

1. What specifies the number of the most recent transactions which are allowed to be lost during the recovery process following a disaster?

A. **Recovery point objective (RPO)**
B. Recovery time objective (RTO)
C. Service delivery objective (SDO)
D. Maximum tolerable downtime (MTD)

Practice Items – Business Continuity and Disaster Recovery Planning

2. What is the **MAIN** purpose of periodically testing the incident response plan (IRP)?

A. To identify shortfalls in the plan and make it comprehensive over time by updating it
B. To satisfy auditors requirements for test reports for compliance purposes
C. To assist system administrators in identifying weaknesses in their applications
D. To help prevent the occurrence of future security incidents

Practice Items – Business Continuity and Disaster Recovery Planning

2. What is the **MAIN** purpose of periodically testing the incident response plan (IRP)?

A. **To identify shortfalls in the plan and make it comprehensive over time by updating it**
B. To satisfy auditors requirements for test reports for compliance purposes
C. To assist system administrators in identifying weaknesses in their applications
D. To help prevent the occurrence of future security incidents

Practice Items – Business Continuity and Disaster Recovery Planning

3. The **MAIN** reason for validating a vendor's cyber security policies and procedures is to verify that the vendor

A. uses approved operating systems and specific computer hardware.
B. is not a liability to the company's information technology operations.
C. is financially stable and viable.
D. has implemented a corporate strategy and vision statement.

Practice Items – Business Continuity and Disaster Recovery Planning

3. The **MAIN** reason for validating a vendor's cyber security policies and procedures is to verify that the vendor

A. uses approved operating systems and specific computer hardware.
B. **is not a liability to the company's information technology operations.**
C. is financially stable and viable.
D. has implemented a corporate strategy and vision statement.

Practice Items – Business Continuity and Disaster Recovery Planning

4. In the event of a disaster, in what order should an organization's business functions be recovered?

A. Increasing complexity of restoration
B. Highest to lowest business impact
C. Lowest to highest business impact
D. Decreasing complexity of restoration

Practice Items – Business Continuity and Disaster Recovery Planning

4. In the event of a disaster, in what order should an organization's business functions be recovered?

A. Increasing complexity of restoration
B. **Highest to lowest business impact**
C. Lowest to highest business impact
D. Decreasing complexity of restoration

Practice Items – Business Continuity and Disaster Recovery Planning

5. What is the correct order to accomplish business continuity planning phases?

A. Design, scope, business impact analysis, recovery strategy, implementation, restoration, and management
B. Scope, business impact analysis, recovery strategy, design, implementation, restoration, and management
C. Management, design, business impact analysis, scope, recovery strategy, implementation, and restoration
D. Business impact analysis, scope, recovery strategy, design, implementation, restoration, and management

Practice Items – Business Continuity and Disaster Recovery Planning

5. What is the correct order to accomplish business continuity planning phases?

A. Design, scope, business impact analysis, recovery strategy, implementation, restoration, and management

B. **Scope, business impact analysis, recovery strategy, design, implementation, restoration, and management**

C. Management, design, business impact analysis, scope, recovery strategy, implementation, and restoration

D. Business impact analysis, scope, recovery strategy, design, implementation, restoration, and management

Practice Items – Cryptography

1. Wired equivalent privacy (WEP) uses which cipher?

A. Rivest cipher 5 (RC5)
B. Data encryption standard (DES)
C. Advanced encryption standard (AES)
D. Rivest cipher 4 (RC4)

Practice Items – Cryptography

1. Wired equivalent privacy (WEP) uses which cipher?

A. Rivest cipher 5 (RC5)
B. Data encryption standard (DES)
C. Advanced encryption standard (AES)
D. **Rivest cipher 4 (RC4)**

Practice Items – Cryptography

2. What technique uses a digest-producing function in conjunction with a cryptovariable to increase its cryptographic strength?

A. Internet security association and key management protocol (ISAKMP)
B. Keyed-hash message authentication code (HMAC)
C. Hash function
D. Checksum

Practice Items – Cryptography

2. What technique uses a digest-producing function in conjunction with a cryptovariable to increase its cryptographic strength?

A. Internet security association and key management protocol (ISAKMP)

B. Keyed-hash message authentication code (HMAC)

C. Hash function

D. Checksum

Practice Items – Cryptography

3. What is an industry standard for Internet protocol security (IPSec) remote access virtual private networks (VPN) key exchange?

A. Internet key exchange (IKE) extended authentication
B. Internet security association and key management protocol (ISAKMP)/oakley
C. Transport layer security (TLS)
D. Interior gateway routing protocol (IGRP)

Practice Items – Cryptography

3. What is an industry standard for Internet protocol security (IPSec) remote access virtual private networks (VPN) key exchange?

A. **Internet key exchange (IKE) extended authentication**
B. Internet security association and key management protocol (ISAKMP)/oakley
C. Transport layer security (TLS)
D. Interior gateway routing protocol (IGRP)

Practice Items – Cryptography

4. What is used to provide authentication and confidentiality for electronic mail (email)?

A. Digital signatures
B. Digital certificates
C. Message integrity checks
D. Hash functions

Practice Items – Cryptography

4. What is used to provide authentication and confidentiality for electronic mail (email)?

A. Digital signatures
B. **Digital certificates**
C. Message integrity checks
D. Hash functions

Practice Items – Cryptography

5. What functionality is provided by the Diffie-Hellman protocol?

A. Key agreement or negotiation
B. Digital signatures for integrity and non-repudiation
C. Encrypting e-mail messages for confidentiality
D. Creating a message authentication code (MAC)

Practice Items – Cryptography

5. What functionality is provided by the Diffie-Hellman protocol?

A. **Key agreement or negotiation**
B. Digital signatures for integrity and non-repudiation
C. Encrypting e-mail messages for confidentiality
D. Creating a message authentication code (MAC)

Practice Items – Information Security Governance and Risk Management

1. According to the $(ISC)^2$ Code of Ethics, in which order of priority should ethical conflicts be resolved?

A. Duty to principals, profession, public safety, and individuals
B. Duty to public safety, principals, individuals, and profession
C. Duty to profession, public safety, individuals, and principals
D. Duty to public safety, profession, individuals, and principals

Practice Items – Information Security Governance and Risk Management

1. According to the (ISC)^2 Code of Ethics, in which order of priority should ethical conflicts be resolved?

A. Duty to principals, profession, public safety, and individuals
B. **Duty to public safety, principals, individuals, and profession**
C. Duty to profession, public safety, individuals, and principals
D. Duty to public safety, profession, individuals, and principals

Practice Items – Information Security Governance and Risk Management

2. An unusual number of approved waivers to a specific organizational policy may indicate that the

A. policy is too general.
B. policy is being enforced.
C. policy is inappropriate for the organization or specific situation.
D. waiver process is not properly processing the waivers.

Practice Items – Information Security Governance and Risk Management

2. An unusual number of approved waivers to a specific organizational policy may indicate that the

A. policy is too general.
B. policy is being enforced.
C. **policy is inappropriate for the organization or specific situation.**
D. waiver process is not properly processing the waivers.

Practice Items – Information Security Governance and Risk Management

3. Which risk management methodology uses the exposure factor (EV) multiplied by the asset value (AV) to determine its outcome?

A. Annualized loss expectancy (ALE)
B. Single loss expectancy (SLE)
C. Annualized rate of occurrence (ARO)
D. Information security risk management (ISRM)

Practice Items – Information Security Governance and Risk Management

3. Which risk management methodology uses the exposure factor (EV) multiplied by the asset value (AV) to determine its outcome?

A. Annualized loss expectancy (ALE)
B. **Single loss expectancy (SLE)**
C. Annualized rate of occurrence (ARO)
D. Information security risk management (ISRM)

Practice Items – Information Security Governance and Risk Management

4. Non-binding statements on how to achieve compliance with standards are called

A. policies.
B. standards.
C. guidelines.
D. procedures.

Practice Items – Information Security Governance and Risk Management

4. Non-binding statements on how to achieve compliance with standards are called

A. policies.
B. standards.
C. **guidelines.**
D. procedures.

Practice Items – Information Security Governance and Risk Management

5. What risk analysis term characterizes the absence or weakness of a risk-reducing safeguard?

A. Threat
B. Probability
C. Vulnerability
D. Loss expectancy

Practice Items – Information Security Governance and Risk Management

5. What risk analysis term characterizes the absence or weakness of a risk-reducing safeguard?

A. Threat
B. Probability
C. **Vulnerability**
D. Loss expectancy

Practice Items – Legal, Regulations, Compliance, and Investigations

1. When dealing with intellectual property rights for software between nations, the **PRIMARY** consideration is

A. information concerning the foreign trade agreements between the two nations.
B. the governing law in the agreements between the two nations.
C. foreign corrupt trading practices in the agreement between the two nations.
D. information about the specific software product liabilities.

Practice Items – Legal, Regulations, Compliance, and Investigations

1. When dealing with intellectual property rights for software between nations, the **PRIMARY** consideration is

A. information concerning the foreign trade agreements between the two nations.

B. the governing law in the agreements between the two nations.

C. foreign corrupt trading practices in the agreement between the two nations.

D. information about the specific software product liabilities.

Practice Items – Legal, Regulations, Compliance, and Investigations

2. During an investigation of an incident, a security administrator discovers a document written to a competitor containing proprietary information about the security administrator's company. Based on the $(ISC)^2$ Code of Ethics, what is the **FIRST** action the security administrator should take?

A. Delete the document to ensure no one else sees it
B. Contact the author of the document to let the author know of the discovery
C. Immediately inform the company's management of the security administrator's findings and the potential risk
D. Launch a training program outlining the need for protection of intellectual property

Practice Items – Legal, Regulations, Compliance, and Investigations

2. During an investigation of an incident, a security administrator discovers a document written to a competitor containing proprietary information about the security administrator's company. Based on the (ISC)^2 Code of Ethics, what is the **FIRST** action the security administrator should take?

A. Delete the document to ensure no one else sees it
B. Contact the author of the document to let the author know of the discovery
C. **Immediately inform the company's management of the security administrator's findings and the potential risk**
D. Launch a training program outlining the need for protection of intellectual property

Practice Items – Legal, Regulations, Compliance, and Investigations

3. What is the **MOST** critical link in the cyber security chain?

A. Technology
B. People
C. Management
D. Awareness programs

Practice Items – Legal, Regulations, Compliance, and Investigations

3. What is the **MOST** critical link in the cyber security chain?

A. Technology
B. **People**
C. Management
D. Awareness programs

Practice Items – Legal, Regulations, Compliance, and Investigations

4. What is the **PRIMARY** benefit of capturing all network traffic during an attack, as opposed to only capturing alerts?

A. Attacks can be stopped before they occur.
B. Attack captures can be easily compressed.
C. Attacks using proxies can be easily traced.
D. Attacks can be recreated later in laboratory environments for analysis.

Practice Items – Legal, Regulations, Compliance, and Investigations

4. What is the **PRIMARY** benefit of capturing all network traffic during an attack, as opposed to only capturing alerts?

A. Attacks can be stopped before they occur.
B. Attack captures can be easily compressed.
C. Attacks using proxies can be easily traced.
D. **Attacks can be recreated later in laboratory environments for analysis.**

Practice Items – Legal, Regulations, Compliance, and Investigations

5. When establishing a process to analyze violations, what is often used to keep the quantity of data to manageable levels?

A. Quantity baseline
B. Maximum log size
C. Circular logging
D. Clipping levels

Practice Items – Legal, Regulations, Compliance, and Investigations

5. When establishing a process to analyze violations, what is often used to keep the quantity of data to manageable levels?

A. Quantity baseline
B. Maximum log size
C. Circular logging
D. **Clipping levels**

Practice Items – Operations Security

1. The **MAIN** goal of implementing change management processes in a data center is to

A. ensure that the entire environment is safe and free of problems and errors.
B. help prepare for documentation for the auditors.
C. help provide the statistics of changes to senior management for cost-benefit analysis.
D. provide feedback to the information technology staff to improve their technical skills.

Practice Items – Operations Security

1. The **MAIN** goal of implementing change management processes in a data center is to

A. **ensure that the entire environment is safe and free of problems and errors.**
B. help prepare for documentation for the auditors.
C. help provide the statistics of changes to senior management for cost-benefit analysis.
D. provide feedback to the information technology staff to improve their technical skills.

Practice Items – Operations Security

2. What is the **MOST** secure way to dispose of information on a compact disk-read only memory (CD-ROM)?

A. Overwrite the CD-ROM using multiple passes with a standardized, evaluated software utility.
B. Re-format the CD-ROM.
C. Degauss the CD-ROM.
D. Physically destroy the CD-ROM.

Practice Items – Operations Security

2. What is the **MOST** secure way to dispose of information on a compact disk-read only memory (CD-ROM)?

A. Overwrite the CD-ROM using multiple passes with a standardized, evaluated software utility.
B. Re-format the CD-ROM.
C. Degauss the CD-ROM.
D. **Physically destroy the CD-ROM.**

Practice Items – Operations Security

3. Personnel background investigations should be conducted in coordination with which organizational specialists?

A. Physical security
B. Facilities management
C. Accounting
D. Human resources

Practice Items – Operations Security

3. Personnel background investigations should be conducted in coordination with which organizational specialists?

A. Physical security
B. Facilities management
C. Accounting
D. **Human resources**

Practice Items – Operations Security

4. A periodic review of a processing facility's operator shift logs is an example of what control category:

A. Directive
B. Detective
C. Recovery
D. Deterrent

Practice Items – Operations Security

4. A periodic review of a processing facility's operator shift logs is an example of what control category:

A. Directive
B. **Detective**
C. Recovery
D. Deterrent

Practice Items – Operations Security

5. Non-scheduled reviews of physical access controls to the data center should be done

A. on a periodic, frequent basis.
B. when a privileged employee leaves the organization.
C. when a new employee starts with the organization.
D. as requested.

Practice Items – Operations Security

5. Non-scheduled reviews of physical access controls to the data center should be done

A. on a periodic, frequent basis.
B. **when a privileged employee leaves the organization.**
C. when a new employee starts with the organization.
D. as requested.

Practice Items – Physical Security

1. What is the **MOST** effective method for reducing vulnerabilities associated with building entrances?

A. Minimize the total number of entrances.
B. Use solid metal doors and frames.
C. Brightly illuminate the entrances.
D. Install tamperproof hinges and glass.

Practice Items – Physical Security

1. What is the **MOST** effective method for reducing vulnerabilities associated with building entrances?

A. **Minimize the total number of entrances.**
B. Use solid metal doors and frames.
C. Brightly illuminate the entrances.
D. Install tamperproof hinges and glass.

Practice Items – Physical Security

2. Why is glare lighting mounted at the same height as the barbed wire “top dress” of a fence?

A. It makes it easier to observe an attacker climbing over the fence.
B. It increases the field of view for observing the area.
C. It reduces the height and cost of guard towers.
D. It blinds the approaching attacker’s view of the area.

Practice Items – Physical Security

2. Why is glare lighting mounted at the same height as the barbed wire “top dress” of a fence?

A. It makes it easier to observe an attacker climbing over the fence.

B. It increases the field of view for observing the area.

C. It reduces the height and cost of guard towers.

D. **It blinds the approaching attacker’s view of the area.**

Practice Items – Physical Security

- Questions 3 and 4 refer to the following scenario.

A company is constructing a new processing facility and is installing a multi-factor access control system consisting of proximity badges and biometric devices. The chief information security officer (CISO) is tasked with acquiring the access control systems. The only requirements are to keep cost as low as possible and minimize system down time.

Practice Items – Physical Security

3. During the evaluation of the effectiveness of several new biometric devices, the CISO should expect that a biometric device becomes more sensitive when

A. both the false acceptance rate (FAR) and the false rejection rate (FRR) increase.
B. the FAR increases while the FRR decreases.
C. the FAR decreases while the FRR increases.
D. both the FAR and FRR decrease.

Practice Items – Physical Security

3. During the evaluation of the effectiveness of several new biometric devices, the CISO should expect that a biometric device becomes more sensitive when

A. both the false acceptance rate (FAR) and the false rejection rate (FRR) increase.
B. the FAR increases while the FRR decreases.
C. **the FAR decreases while the FRR increases.**
D. both the FAR and FRR decrease.

Practice Items – Physical Security

4. The point where the false acceptance rate (FAR) and the false rejection rate (FRR) is balanced is known as the

A. Crossover error rate (CER).
B. Crossover acceptance rate (CAR).
C. Equal crossover rate (EQR).
D. Equal acceptance rate (EAR).

Practice Items – Physical Security

4. The point where the false acceptance rate (FAR) and the false rejection rate (FRR) is balanced is known as the

A. **Crossover error rate (CER).**
B. Crossover acceptance rate (CAR).
C. Equal crossover rate (EQR).
D. Equal acceptance rate (EAR).

Practice Items – Physical Security

5. What is the **GREATEST** vulnerability associated with relying solely on proximity cards for access control to a secure facility?

A. A lost or stolen card may allow an unauthorized person to gain access.
B. A proximity card is too easy to duplicate or forge.
C. A proximity card does not record time of departure.
D. An electrical power failure may deny access to all users.

Practice Items – Physical Security

5. What is the **GREATEST** vulnerability associated with relying solely on proximity cards for access control to a secure facility?

A. **A lost or stolen card may allow an unauthorized person to gain access.**
B. A proximity card is too easy to duplicate or forge.
C. A proximity card does not record time of departure.
D. An electrical power failure may deny access to all users.

Practice Items – Security Architecture and Design

1. The collection of protection mechanisms within a computer system is called the

A. Trusted security infrastructure
B. Reference monitor
C. Security kernel
D. Trusted computing base

Practice Items – Security Architecture and Design

1. The collection of protection mechanisms within a computer system is called the

A. Trusted security infrastructure
B. Reference monitor
C. Security kernel
D. **Trusted computing base**

Practice Items – Security Architecture and Design

2. When basic standards for software development are implemented within an organization and are in common use (defined, established, and documented), the organization has reached what level of the capability maturity model (CMM) for software engineering?

A. Level 1
B. Level 2
C. Level 3
D. Level 4

Practice Items – Security Architecture and Design

2. When basic standards for software development are implemented within an organization and are in common use (defined, established, and documented), the organization has reached what level of the capability maturity model (CMM) for software engineering?

A. Level 1
B. Level 2
C. **Level 3**
D. Level 4

Practice Items – Security Architecture and Design

3. What is the main purpose of the Common Criteria (International Standards Organization (ISO) 15408)?

A. To provide an international standard version of the United States Trusted Computer Security Evaluation Criteria (TCSEC).
B. To provide an international standard version of the European Information Technology Security Evaluation Criteria (ITSEC).
C. To independently measure how well a vendor's products meet a company's business requirements.
D. To independently measure how well a vendor's products meet the vendor's claims and promises.

Practice Items – Security Architecture and Design

3. What is the main purpose of the Common Criteria (International Standards Organization (ISO) 15408)?

A. To provide an international standard version of the United States Trusted Computer Security Evaluation Criteria (TCSEC).

B. To provide an international standard version of the European Information Technology Security Evaluation Criteria (ITSEC).

C. To independently measure how well a vendor's products meet a company's business requirements.

D. To independently measure how well a vendor's products meet the vendor's claims and promises.

Practice Items – Security Architecture and Design

4. Data remanence occurs when

A. residual data remains on a storage media following erasure.
B. data resists accidental deletion.
C. data exceeds the boundaries of its memory buffers.
D. No data remains on the storage media following an overwrite process.

Practice Items – Security Architecture and Design

4. Data remanence occurs when

A. **residual data remains on a storage media following erasure.**
B. data resists accidental deletion.
C. data exceeds the boundaries of its memory buffers.
D. No data remains on the storage media following an overwrite process.

Practice Items – Security Architecture and Design

5. What is the **PRIMARY** weakness of the Bell-LaPadula model?

A. Enforcing separation of duties
B. Defining job roles and functions
C. Addressing need-to-know requirements
D. Creating well-formed transactions

Practice Items – Security Architecture and Design

5. What is the **PRIMARY** weakness of the Bell-LaPadula model?

A. Enforcing separation of duties
B. Defining job roles and functions
C. **Addressing need-to-know requirements**
D. Creating well-formed transactions

Practice Items – Telecommunications and Network Security

1. What is the **BEST** method for storing user passwords in an information system?

A. Password-protected file
B. File restricted to one individual
C. One-way encrypted hash
D. Two-way encrypted cipher

Practice Items – Telecommunications and Network Security

1. What is the **BEST** method for storing user passwords in an information system?

A. Password-protected file
B. File restricted to one individual
C. **One-way encrypted hash**
D. Two-way encrypted cipher

Practice Items – Telecommunications and Network Security

2. What is a series of characters used to verify a user's identity?

A. Token serial number
B. UserID
C. Password
D. Security ticket

Practice Items – Telecommunications and Network Security

2. What is a series of characters used to verify a user's identity?

A. Token serial number
B. UserID
C. **Password**
D. Security ticket

Practice Items – Telecommunications and Network Security

3. Removing unnecessary processes, segregating inter-process communications, and reducing executing privileges to increase system security is referred to as

A. hardening.
B. segmenting.
C. aggregating.
D. kerneling.

Practice Items – Telecommunications and Network Security

3. Removing unnecessary processes, segregating inter-process communications, and reducing executing privileges to increase system security is referred to as

A. **hardening.**
B. segmenting.
C. aggregating.
D. kerneling.

Practice Items – Telecommunications and Network Security

4. How can a user of digital signatures ensure non-repudiation of delivery of the correct message?

A. Sender encrypts the message with the recipient's public key and signs it with their own private key.
B. Sender computes a digest of the message and sends it to a trusted third party who signs it and stores it for later reference.
C. Sender signs the message and sends it to the recipient and requests "return receipt" of the e-mail.
D. Sender gets a digitally signed acknowledgement from the recipient containing a copy or digest of the message.

Practice Items – Telecommunications and Network Security

4. How can a user of digital signatures ensure non-repudiation of delivery of the correct message?

A. Sender encrypts the message with the recipient's public key and signs it with their own private key.

B. Sender computes a digest of the message and sends it to a trusted third party who signs it and stores it for later reference.

C. Sender signs the message and sends it to the recipient and requests "return receipt" of the e-mail.

D. Sender gets a digitally signed acknowledgement from the recipient containing a copy or digest of the message.

Practice Items – Telecommunications and Network Security

5. An Internet worm that causes many information systems to become unresponsive is seeking to affect which leg of the information security TRIAD?

A. Availability
B. Integrity
C. Confidentiality
D. Denial of service (DoS)

Practice Items – Telecommunications and Network Security

5. An Internet worm that causes many information systems to become unresponsive is seeking to affect which leg of the information security TRIAD?

A. **Availability**
B. Integrity
C. Confidentiality
D. Denial of service (DoS)

MORE CISSP HELP!

- The University of Fairfax provides you with additional learning tools to help you pass your CISSP examination.

- To find out more information
  - www.ufairfax.net
  - email Juliette Goldman, Associate Dean of Continuing Professional Education at jgoldman@ufairfax.net.