ISC2 CISSP Domain #1
Security Governance Through Principles and Policies

Exercise #1
What security controls can be used at each layer of the security model to ensure confidentiality, integrity, and availability are adequately addressed?

Data –
Users –
Application Security –
Endpoint Security –
Network Security –
Perimeter Security –

Question Set #1
Which of the following contains the primary goals and objectives of security?

a) A network's border perimeter
b) The CIA Triad
c) A stand-alone system
d) The internet

Which of the following is not true?

a) Violations of confidentiality include human error
b) Violations of confidentiality include management oversight
c) Violations of confidentiality are limited to direct intentional attacks
d) Violations of confidentiality can occur when a transmission is not properly encrypted

If a security mechanism offers availability, then it offers a high level of assurance that authorized subjects can _____ the data, objects, and resources.

a) Control
b) Audit
c) Access
d) Repudiate

Question Set #2
Which of the following is a principle of the CIA Triad that means authorized subjects are granted timely and uninterrupted access to objects?

a) Identification
b) Availability
c) Encryption
d) Layering

All but which of the following items requires awareness for all individuals affected?

a) Restricting personal email
b) Recording phone conversations
c) Gathering information about surfing habits
d) The backup mechanism used to retain email messages

Data classifications are used to focus security controls over all but which of the following?

a) Storage
b) Processing
c) Layering
d) Transfer

Question Set #3

_____ refers to keeping information confidential that is personally identifiable or that might cause harm, embarrassment, or disgrace to someone if revealed.

a) Seclusion
b) Concealment
c) Privacy
d) Criticality

What element of data categorization management can override all other forms of access control?

a) Classification
b) Physical access
c) Custodian responsibilities
d) Taking ownership

What ensures that the subject of an activity or event cannot deny that the event occurred?

a) CIA Triad
b) Abstraction
c) Nonrepudiation
d) Hash totals

Question Set #4

Which of the following is the most important and distinctive concept in relation to layered security?

a) Multiple
b) Series
c) Parallel
d) Filter

Which NIST Special Publication focuses on security controls for federal information systems

a) NIST SP 800-171
b) NIST SP 800-63
c) NIST SP 800-53
d) NIST SP 800-88

Vulnerabilities and risks are evaluated based on their threats against which of the following?

a) One or more of the CIA Triad principles
b) Data usefulness
c) Due care
d) Extent of liability

What is the primary goal of change management?

a) Maintaining documentation
b) Keeping users informed of changes
c) Allowing rollback of failed changes
d) Preventing security compromises

Question Set #5

If you are writing a document that provides configuration information regarding the minimum level of security that every system in you organization must meet, then what type of document are you preparing?

a) Policy
b) Baseline
c) Guideline
d) Procedure

Which of the following is not considered a violation of confidentiality?

a) Stealing passwords
b) Eavesdropping
c) Hardware destruction
d) Social engineering

Which of the following is not considered an example of data hiding?

a) Preventing an authorized reader of an object from deleting that object
b) Keeping a database from being accessed by unauthorized visitors
c) Restricting a subject at a lower classification level from accessing data at a higher classification level
d) Preventing an application from accessing hardware directly

What is the primary objective of data classification schemes?

a) To control access to objects for authorized subjects
b) To formalize and stratify the process of securing data based on assigned labels of importance and sensitivity
c) To establish a transaction trail for auditing accountability
d) To manipulate access controls to provide for the most efficient means to grant or restrict functionality

Question Set #6

Which of the following is typically not a characteristic considered when classifying data?

a) Value
b) Size of object
c) Useful lifetime
d) National security implications

STRIDE is often used in relation to assess threats against applications or operating systems. Which of the following is not an element of STRIDE?

a) Spoofing
b) Elevation of privilege
c) Repudiation
d) Disclosure

Which commercial business/private sector data classification is used to control information about individuals within an organization?

a) Confidential
b) Private
c) Sensitive
d) Proprietary

What type of Business Impact Assessment tool is most appropriate when attempting to evaluate the impact of failure on customer confidence?

a) Quantitative
b) Qualitative
c) Assessment
d) Reduction

ISC2 CISSP Domain #2
Personnel Security and Risk Management

Question Set #1

Which of the following is the weakest element in any security solution?

a) Software products

b) Internet connections

c) Security policies

d) Humans

When seeking to hire new employees, what is the first step?

a) Create a job description

b) Set position classification

c) Screen candidates

d) Request resumes

Which of the following is a primary purpose of an exit interview?

a) To return the exiting employee's personal belongings

b) To review the nondisclosure agreement

c) To evaluate the exiting employee's performance

d) To cancel the exiting employee's network access accounts

Quantitative Risk Assessment

A cloud provider provides 24 x 7 web solutions to its customers. The organizations revenue is dependent on maximizing server uptime and generates $1M in annual sales. The average server failure based on vendor documentation is 2% and the company current has 5 servers in operation. If server failures do occur, it could cost the company as much as $100,000 due to server downtime. Based on these parameters answer the quantitative risk assessment questions:

What is the AV for this organization?

What is the ARO due to server failures?

What is the companies EF?

What is the SLE for the company?

What is the ALE for the company?

Question Set #2

Which of the following is not specifically or directly related to managing the security function of an organization?

a) Worker job satisfaction

b) Metrics

c) Information security strategies

d) Budget

While performing a risk analysis, you identify a threat of fire and a vulnerability because there are no fire extinguishers. Based on this information, which of the following is a possible risk?

a) Virus infection

b) Damage to equipment

c) System malfunction

d) Unauthorized access to confidential information

You've performed a basic quantitative risk analysis on a specific threat/vulnerability/risk relation. You select a possible countermeasure. When performing the calculations again, which of the following factors will change?

a) Exposure Factor

b) Single Loss Expectancy (SLE)

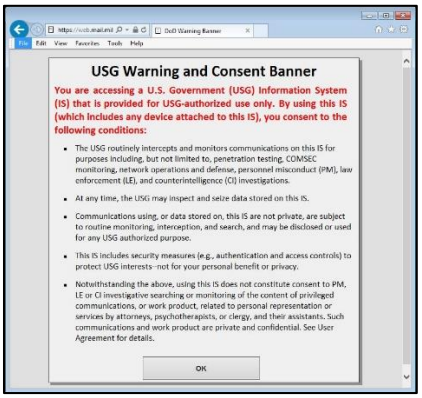
c) Asset Value

d) Annualized Rate of Occurrence (ARO)

Risk Response Exercise

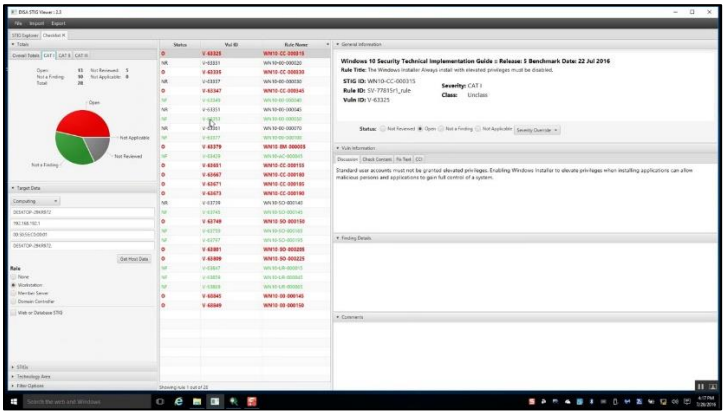
What risk response is shown in each of the following:

a) What kind of risk response is this?



b) What kind of risk response is this?

c) Using a STIG to apply security guidelines for an operating system



Question Set #3

How is the value of a safeguard to a company calculated?

a) ALE before safeguard – ALE after implementing the safeguard – annual cost of safeguard

b) ALE before safeguard ARO of safeguard

c) ALE after implementing safeguard + annual cost of safeguard – controls gap

d) Total risk – controls gap

What security control is directly focused on preventing collusion?

a) Principle of least privilege

b) Job descriptions

c) Separation of duties

d) Qualitative risk analysis

How is single loss expectancy (SLE) calculated?

a) Threat + Vulnerability

b) Asset Value Exposure Factor

c) Annualized Rate of Occurrence Vulnerability

d) Annualized Rate of Occurrence Asset Value Exposure Factor

Security Control Classes Exercise

List as many security controls for each of the security control classes.

a) Technical

b) Physical

c) Administrative

Security Control Identification Exercise

For each control, specify the control class and type:

a) Updating an ACL on a Router

b) Utilizing CCTV to identify personnel entering a facility

c) Conducting a vulnerability assessment scan against a web server

d) Having all employees sign an AUP and NDA during onboarding

e) Reimaging a system after a successful ransomware attack

Question Set #4

When an employee is to be terminated, which of the following should be done?

a) Inform the employee a few hours before they are officially terminated

b) Disable the employee's network access just as they are informed of the termination

c) Send out a broadcast email informing everyone that a specific employee is to be terminated

d) Wait until you and the employee are the only people remaining in the building before announcing the termination

If an organization contracts with outside entities to provide key business functions or services, such as account or technical support, what is the process called that is used to ensure that these entities support sufficient security?

a) Asset identification

b) Third-party governance

c) Exit interview

d) Qualitative analysis

A portion of the _____ is the logical and practical investigation of business processes and organizational policies. This review ensures that the stated and implemented business tasks, systems, and methodologies are practical, efficient, and cost-effective, but most of all that they support security through the reduction of vulnerabilities and the avoidance, reduction, or mitigation of risk.

a) Hybrid assessment

b) Risk aversion process

c) Countermeasure selection

d) Documentation review

Question Set #5

Which of the following statements is not true?

a) IT security can provide protection only against logical or technical attacks

b) The process by which the goals of risk management are achieved is known as risk analysis

c) Risks to an IT infrastructure are all computer based

d) An asset is anything used in a business process or task

Which of the following is not an element of the risk analysis process?

a) Analyzing an environment for risks

b) Creating a cost/benefit report for safeguards to present to upper management

c) Selecting appropriate safeguards and implementing them

d) Evaluating each threat event as to its likelihood of occurring and cost of the resulting damage

What process or event is typically hosted by an organization and is targeted to groups of employees with similar job functions?

a) Education

b) Awareness

c) Training

d) Termination

References

Single Loss Expectancy (SLE)($) – The single event loss due to a risk

SLE ($) = Asset Value ($) Exposure Factor (%)

Annualized Rate of Occurrence (ARO)(%) – Likelihood an event occurs in a year

Annual Loss Expectancy (ALE)($) – Annual loss due to a risk

ALE = SLE ($) ARO (%)

Asset Value (AV)($) – Asset replacement cost

Exposure Factor (EF)(%) – Proportion of asset value destroyed by a risk

No Loss – 0.0, Complete Loss – 1.0

ISC2 CISSP
Business Continuity Planning

Question Set #1

What is the term used to describe the responsibility of a firm's officers and directors to ensure that adequate measures are in place to minimize the effect of a disaster on the organization's continued viability?

a) Corporate responsibility
b) Review and validation of the business organization analysis
c) Due diligence
d) Going concern responsibility

Which one of the following BIA terms identifies the amount of money a business expects to lose to a given risk each year?

a) ARO
b) SLE
c) ALE
d) EF

You are concerned about the risk that an avalanche poses to your $3 million shipping facility. Based on expert opinion, you determine that there is a 5 percent chance that an avalanche will occur each year. Experts advise you that an avalanche would destroy your building and require you to rebuild on the same land. Ninety percent of the $3 million value of the facility is attributed to the building, and 10 percent is attributed to the land itself. What is the single loss expectancy of your shipping facility to avalanches?

a) $3,000,000
b) $2,700,000
c) $270,000
d) $135,000

What BIA metric can be used to express the longest time a business function can be unavailable without causing irreparable harm to the organization?

a) SLE
b) EF
c) MTD
d) ARO

Of the individuals listed, who would provide the best endorsement for a business continuity plan's statement of importance?

a) Vice President of Business Operations
b) Chief Information Officer
c) Chief Executive Officer
d) Business Continuity Manager

Question Set #2

What is the first step that individuals responsible for the development of a business continuity plan should perform?

a) BCP team selection
b) Business organization analysis
c) Resource requirements analysis
d) Legal and regulatory assessment

What will be the major resource consumed by the BCP process during the BCP phase?

a) Hardware
b) Software
c) Processing Time
d) Personnel

What unit of measurement should be used to assign quantitative values to assets in the priority identification phase of the business impact assessment?

a) Monetary
b) Utility
c) Importance
d) Time

You are concerned about the risk that an avalanche poses to your $3 million shipping facility. Based on expert opinion, you determine that there is a 5 percent chance that an avalanche will occur each year. Experts advise you that an avalanche would destroy your building and require you to rebuild on the same land. Ninety percent of the $3 million value of the facility is attributed to the building, and 10 percent is attributed to the land itself. What is the annualized loss expectancy?

a) $3,000,000
b) $2,700,000
c) $270,000
d) $135,000

Martin recently completed a quantitative risk assessment for his organization. Which one of the following risks is least likely to be adequately addressed by his assessment?

a) Downtime from data center flooding
b) Cost of recovery from denial-of-service attack
c) Reputational damage from data breach
d) Remediation costs from ransomware attack

Conduct a Business Impact Analysis

Conduct a Business Impact Analysis for Amazon's online store. Make sure that your BIA addresses the following steps:

- ✓ Identify Business Functions
- ✓ Prioritize Critical Business Functions
- ✓ Identify Organizational Risks
- ✓ Generate a Likelihood Assessment
- ✓ Develop an Impact Assessment
- ✓ Prioritize Resources

Question Set #3

You are concerned about the risk that a hurricane poses to your corporate headquarters in South Florida. The building itself is valued at $15 million. After consulting with the National Weather Service, you determine that there is a 10 percent likelihood that a hurricane will strike over the course of a year. You hired a team of architects and engineers who determined that the average hurricane would destroy approximately 50 percent of the building. What is the annualized loss expectancy (ALE)?

a) $750,000
b) $1.5 million
c) $7.5 million
d) $15 million

Once the BCP team is selected, what should be the first item placed on the team's agenda?

a) Business impact assessment
b) Business organization analysis
c) Resource requirements analysis
d) Legal and regulatory assessment

Which resource should you protect first when designing continuity plan provisions and processes?

a) Physical Plant
b) Infrastructure
c) Financial Resources
d) People

Which one of the following concerns is not suitable for quantitative measurement during the business impact assessment?

a) Loss of a plant
b) Damage to a vehicle
c) Negative publicity
d) Power outage

Lighter Than Air Industries expects that it would lose $10 million if a tornado struck its aircraft operations facility. It expects that a tornado might strike the facility once every 100 years. What is the single loss expectancy for this scenario?

a) 0.01
b) $10,000,000
c) $100,000
d) 0.10

Question Set #4

In which business continuity planning task would you design procedures and mechanisms to mitigate risks deemed unacceptable by the BCP team?

a) Strategy development
b) Business impact assessment
c) Provisions and processes
d) Resource prioritization

What type of mitigation provision is utilized when redundant communications links are installed?

a) Hardening systems
b) Defining systems
c) Reducing systems
d) Alternative systems

What type of plan addresses the technical controls associated with alternate processing facilities, backups, and fault tolerance?

a) Business continuity plan
b) Business impact assessment
c) Disaster recovery plan
d) Vulnerability assessment

Lighter Than Air Industries expects that it would lose $10 million if a tornado struck its aircraft operations facility. It expects that a tornado might strike the facility once every 100 years. What is the single loss expectancy for this scenario? What is the annualized loss expectancy?

a) 0.01
b) $10,000,000
c) $100,000
d) 0.10

What is the formula used to compute the single loss expectancy for a risk scenario?

a) SLE = AV × EF
b) SLE = RO × EF
c) SLE = AV × ARO
d) SLE = EF × ARO

Question Set #1

Richard recently developed a great name for a new product that he plans to begin using immediately. He spoke with his attorney and filed the appropriate application to protect his product name but has not yet received a response from the government regarding his application. He wants to begin using the name immediately. What symbol should he use next to the name to indicate its protected status?

a) ©
b) ®
c) ™
d) †

Which one of the following is not a requirement that Internet service providers must satisfy in order to gain protection under the “transitory activities” clause of the Digital Millennium Copyright Act?

a) The service provider and the originator of the message must be located in different states
b) The transmission, routing, provision of connections, or copying must be carried out by an automated technical process without selection of material by the service provider
c) Any intermediate copies must not ordinarily be accessible to anyone other than anticipated recipients and must not be retained for longer than reasonably necessary
d) The transmission must be originated by a person other than the provider

Which one of the following types of licensing agreements does not require that the user acknowledge that they have read the agreement prior to executing it?

a) Standard license agreement
b) Shrink-wrap agreement
c) Click-wrap agreement
d) Verbal agreement

Which criminal law was the first to implement penalties for the creators of viruses, worms, and other types of malicious code that cause harm to computer systems?

a) Computer Security Act National
b) Infrastructure Protection Act
c) Computer Fraud and Abuse Act
d) Electronic Communications Privacy Act

Which law governs information security operations at federal agencies?

a) FISMA
b) FERPA
c) CFAA
d) ECPA

What type of law does not require an act of Congress to implement at the federal level but rather is enacted by the executive branch in the form of regulations, policies, and procedures?

a) Criminal law
b) Common law
c) Civil law
d) Administrative law

Which federal government agency has responsibility for ensuring the security of government computer systems that are not used to process sensitive and/or classified information?

a) National Security Agency
b) Federal Bureau of Investigation
c) National Institute of Standards and Technology
d) Secret Service

What is the broadest category of computer systems protected by the Computer Fraud and Abuse Act, as amended?

a) Government-owned systems
b) Federal interest systems
c) Systems used in interstate commerce
d) Systems located in the United States

Question Set #2

The Children's Online Privacy Protection Act (COPPA) was designed to protect the privacy of children using the internet. What is the minimum age a child must be before companies can collect personal identifying information from them without parental consent?

a) 13
b) 14
c) 15
d) 16

Which one of the following laws is not designed to protect the privacy rights of consumers and internet users?

a) Health Insurance Portability and Accountability Act
b) Identity Theft Assumption and Deterrence Act
c) USA PATRIOT Act
d) Gramm-Leach-Bliley Act

What industry is most directly impacted by the provisions of the Gramm-Leach-Bliley Act?

a) Healthcare
b) Banking
c) Law enforcement
d) Defense contractors

What is the standard duration of patent protection in the United States?

a) 14 years from the application date
b) 14 years from the date the patent is granted
c) 20 years from the application date
d) 20 years from the date the patent is granted

Which one of the following is the comprehensive EU law that governs data privacy that was passed in 2016 and goes into effect in 2018?

a) DPD
b) GLBA
c) GDPR
d) SOX

What compliance obligation relates to the processing of credit card information?

a) SOX
b) HIPAA
c) PCI DSS
d) FERPA

What act updated the privacy and security requirements of the Health Insurance Portability and Accountability Act (HIPAA)?

a) HITECH
b) CALEA
c) CFAA
d) CCCA

Question Set #3

What law protects the right of citizens to privacy by placing restrictions on the authority granted to government agencies to search private residences and facilities?

a) Privacy Act
b) Fourth Amendment
c) Second Amendment
d) Gramm-Leach-Bliley Act

Matthew recently authored an innovative algorithm for solving a mathematical problem, and he wants to share it with the world. However, prior to publishing the software code in a technical journal, he wants to obtain some sort of intellectual property protection. Which type of protection is best suited to his needs?

a) Copyright
b) Trademark
c) Patent
d) Trade secret

Mary is the cofounder of Acme Widgets, a manufacturing firm. Together with her partner, Joe, she has developed a special oil that will dramatically improve the widget manufacturing process. To keep the formula secret, Mary and Joe plan to make large quantities of the oil by themselves in the plant after the other workers have left. They want to protect this formula for as long as possible. What type of intellectual property protection best suits their needs?

a) Copyright
b) Trademark
c) Patent
d) Trade secret

What law prevents government agencies from disclosing personal information that an individual supplies to the government under protected circumstances?

a) Privacy Act
b) Electronic Communications Privacy Act
c) Health Insurance Portability and Accountability Act
d) Gramm-Leach-Bliley Act

What framework allows U.S. companies to certify compliance with EU privacy laws?

a) COBiT
b) Privacy Shield
c) Privacy Lock
d) EuroLock

ISC2 CISSP
Protecting Security Assets

Question Set #1

Which one of the following identifies the primary purpose of information classification processes?

a) Define the requirements for protecting sensitive data
b) Define the requirements for backing up data
c) Define the requirements for storing data
d) Define the requirements for transmitting data

When determining the classification of data, which one of the following is the most important consideration?

a) Processing system
b) Value
c) Storage media
d) Accessibility

Which of the following answers would not be included as sensitive data?

a) PII
b) PHI
c) Proprietary data
d) Data posted on a website

What is the most important aspect of marking media?

a) Date labeling
b) Content description
c) Electronic labeling
d) Classification

Which would an administrator do to classified media before reusing it in a less secure environment?

a) Erasing
b) Clearing
c) Purging
d) Overwriting

Question Set #2

Which of the following statements correctly identifies a problem with sanitization methods?

a) Methods are not available to remove data ensuring that unauthorized personnel cannot retrieve data
b) Even fully incinerated media can offer extractable data
c) Personnel can perform sanitization steps improperly
d) Stored data is physically etched into the media

Which of the following choices is the most reliable method of destroying data on a solid-state drive (SSD)?

a) Erasing
b) Degaussing
c) Deleting
d) Purging

Which of the following is the most secure method of deleting data on a DVD?

a) Formatting
b) Deleting
c) Destruction
d) Degaussing

Which of the following does not erase data?

a) Clearing
b) Purging
c) Overwriting
d) Remanence

ISC2 CISSP
Cryptography and Symmetric Key Algorithms

Question Set #1

How many possible keys exist in a 4-bit key space?

a) 4
b) 8
c) 16
d) 128

John recently received an email message from Bill. What security principle would need to be met to convince John that Bill was the sender of the message?

a) Nonrepudiation
b) Confidentiality
c) Availability
d) Integrity

What type of cipher relies on changing the location of characters within a message to achieve confidentiality?

a) Stream cipher
b) Transposition cipher
c) Block cipher
d) Substitution cipher

Question Set #2

Dave is developing a key escrow system that requires multiple people to retrieve a key but does not depend on every participant being present. What type of technique is he using?

a) Split knowledge
b) M of N Control
c) Work function
d) Zero-knowledge proof

Many cryptographic algorithms rely on the difficulty of factoring the product of large prime numbers. What characteristic of this problem are they relying on?

a) It contains diffusion
b) It contains confusion
c) It is a one-way function
d) It complies with Kerckhoffs's principle

Which one of the following cannot be achieved by a secret key cryptosystem?

a) Nonrepudiation
b) Confidentiality
c) Authentication
d) Key distribution

What kind of attack makes the Caesar cipher virtually unusable?

a) Meet-in-the-middle attack
b) Escrow attack
c) Frequency analysis attack
d) Transposition attack

Question Set #3

What is the minimum number of cryptographic keys required for secure two-way communications in symmetric key cryptography?

a) One
b) Two
c) Three
d) Four

When correctly implemented, what is the only cryptosystem known to be unbreakable?

a) Transposition cipher
b) Substitution cipher
c) AES
d) OTP

What is the output value of the mathematical function 16 mod 3?

a) 0
b) 1
c) 3
d) 5

What effective key size is used by the DES encryption algorithm?

a) 32 bits
b) 56 bits
c) 64 bits
d) 256 bits

Which one of the following cipher types operates on large pieces of a message rather than individual characters or bits of a message?

a) Stream cipher
b) Caesar cipher
c) Block cipher
d) ROT3 cipher

What block size is used by the Advanced Encryption Standard?

a) 32 bits
b) 64 bits
c) 128 bits
d) Variable

What type of cryptosystem commonly makes use of a passage from a well-known book for the encryption key?

a) Vernam cipher
b) Running key cipher
c) Skipjack cipher
d) Twofish cipher

How many encryption keys are required to fully implement an asymmetric algorithm with 10 participants?

a) 10
b) 20
c) 45
d) 100

ISC2 CISSP
PKI and Cryptographic Applications

Question Set #1

Brian computes the digest of a single sentence of text using a SHA-2 hash function. He then changes a single character of the sentence and computes the hash value again. Which one of the following statements is true about the new hash value?

a) The new hash value will be one character different from the old hash value
b) The new hash value will share at least 50% of the characters of the old hash value
c) The new hash value will be unchanged
d) The new hash value will be completely different from the old hash value

Which cryptographic algorithm forms the basis of the El Gamal cryptosystem?

a) RSA
b) Diffie-Hellman
c) 3DES
d) IDEA

If Richard wants to send an encrypted message to Sue using a public key cryptosystem, which key does he use to encrypt the message?

a) Richard's public key
b) Richard's private key
c) Sue's public key
d) Sue's private key

If a 2,048-bit plaintext message were encrypted with the El Gamal public key cryptosystem, how long would the resulting ciphertext message be?

a) 1,024 bits
b) 2,048 bits
c) 4,096 bits
d) 8,192 bits

Acme Widgets currently uses a 1,024-bit RSA encryption standard companywide. The company plans to convert from RSA to an ECC cryptosystem. If it wants to maintain the same cryptographic strength, what ECC key length should it use?

a) 160 bits
b) 512 bits
c) 1,024 bits
d) 2,048 bits

John wants to produce a message digest of a 2,048-byte message he plans to send to Mary. If he uses the MD5 hashing algorithm, what size will the message digest for this particular message be?

a) 160 bits
b) 256 bits
c) 128 bits
d) 2,048 bits

Which one of the following technologies is considered flawed and should no longer be used?

a) SHA-3
b) PGP
c) WEP
d) TLS

What encryption technique does WPA use to protect wireless communications?

a) TKIP
b) DES
c) 3DES
d) AES

Richard received an encrypted message sent to him from Sue. Which key should he use to decrypt the message?

a) Richard’s public key
b) Richard’s private key
c) Sue’s public key
d) Sue’s private key

Richard wants to digitally sign a message he’s sending to Sue so that Sue can be sure the message came from him without modification while in transit. Which key should he use to encrypt the message digest?

a) Richard’s public key
b) Richard’s private key
c) Sue’s public key
d) Sue’s private key

Question Set #2

Which one of the following algorithms is not supported by the Digital Signature Standard?

a) DSA
b) RSA
c) El Gamal DSA
d) ECDSA

Which International Telecommunications Union (ITU) standard governs the creation and endorsement of digital certificates for secure electronic communication?

a) X.500
b) X.509
c) X.900
d) X.905

What cryptosystem provides the encryption/decryption technology for the commercial version of Phil Zimmerman's Pretty Good Privacy secure email system?

a) ROT13
b) IDEA
c) ECC
d) El Gamal

What TCP/IP communications port is used by TLS traffic?

a) 80
b) 220
c) 443
d) 559

What type of cryptographic attack rendered Double DES (2DES) no more effective than standard DES encryption?

a) Birthday attack
b) Chosen ciphertext attack
c) Meet-in-the-middle attack
d) Man-in-the-middle attack

Question Set #3

Which of the following tools can be used to improve the effectiveness of a brute-force password cracking attack?

a) Rainbow tables
b) Hierarchical screening
c) TKIP
d) Random enhancement

What is the major disadvantage of using certificate revocation lists?

a) Key management
b) Latency
c) Record keeping
d) Vulnerability to brute-force attacks

Which one of the following encryption algorithms is now considered insecure?

a) El Gamal
b) RSA
c) ECC
d) Merkle-Hellman Knapsack

What does IPsec define?

a) All possible security classifications for a specific configuration
b) A framework for setting up a secure communication channel
c) The valid transition states in the Biba model
d) TCSEC security categories

ISC2 CISSP
Principles of Security Models, Design, and Capabilities

Question Set #1

Which security model focuses on data integrity and requires all subjects and objects to have a classification label?

a) Take-Grant Model
b) Biba Model
c) State Machine Model
d) Bell-LaPadula Model

In a Trusted Computing Base what is a proxy that stands between every subject and object and verifies a subject's credentials before processing requests?

a) Security Perimeter
b) Reference Monitor
c) Trusted Path
d) Critical Path System

What is a table of subjects and objects that identifies actions or functions that each subject can perform on each object?

a) Reference Monitor
b) Access Control List
c) Entrance Matrix
d) Acceptance Criteria

Question Set #2

Trusted Computer System Evaluation Criteria category focuses on mandatory protection?

a) A
b) B
c) C
d) D

What common criteria evaluation assurance level applies when developers or users require low to moderate independently assured security, but the complete development record is not readily available?

a) EAL1
b) EAL2
c) EAL4
d) EAL7

What is a technical evaluation of each component of a computing system to determine its alignment with security standards?

a) Authority to Operate
b) Certification
c) Accreditation
d) Vulnerability Assessment

Question Set #3

ISC2 CISSP
Security Vulnerabilities Threats, and Countermeasures

Question Set #1

Many PC operating systems provide functionality that enables them to support the simultaneous execution of multiple applications on single-processor systems. What term is used to describe this capability?

a) Multiprogramming
b) Multithreading
c) Multitasking
d) Multiprocessing

What technology provides an organization with the best control over BYOD equipment?

a) Application whitelisting
b) Mobile device management
c) Encrypted removable storage
d) Geotagging

You have three applications running on a single-core single-processor system that supports multitasking. One of those applications is a word processing program that is managing two threads simultaneously. The other two applications are using only one thread of execution. How many application threads are running on the processor at any given time?

a) One
b) Two
c) Three
d) Four

What type of federal government computing system requires that all individuals accessing the system have a need to know all of the information processed by that system?

a) Dedicated
b) System high
c) Compartmented
d) Multilevel

What is a security risk of an embedded system that is not commonly found in a standard PC?

a) Software flaws
b) Access to the internet
c) Control of a mechanism in the physical world
d) Power loss

Question Set #2

Which of the following describes a community cloud?

a) A cloud environment maintained, used, and paid for by a group of users or organizations for their shared benefit, such as collaboration and data exchange
b) A cloud service within a corporate network and isolated from the internet
c) A cloud service that is accessible to the general public typically over an internet connection

What is the concept of a computer implemented as part of a larger system that is typically designed around a limited set of specific functions (such as management, monitoring, and control) in relation to the larger product of which it's a component?

a) IoT
b) Application appliance
c) SoC
d) Embedded system

Which one of the following types of memory might retain information after being removed from a computer and, therefore, represent a security risk?

a) Static RAM
b) Dynamic RAM
c) Secondary memory
d) Real memory

What type of electrical component serves as the primary building block for dynamic RAM chips?

a) Capacitor
b) Resistor
c) Flip-flop
d) Transistor

Which one of the following storage devices is most likely to require encryption technology in order to maintain data security in a networked environment?

a) Hard disk
b) Backup tape
c) Removable drives
d) RAM

Question Set #3

What form of attack abuses a program's lack of length limitation on the data it receives before storing the input in memory, which can lead to arbitrary code execution?

a) ARP poisoning
b) XSS
c) Domain hijacking
d) Buffer overflow

What security principle helps prevent users from accessing memory spaces assigned to applications being run by other users?

a) Separation of privilege
b) Layering
c) Process isolation
d) Least privilege

Which security principle mandates that only a minimum number of operating system processes should run in supervisory mode?

a) Abstraction
b) Layering
c) Data hiding
d) Least privilege

Which security principle takes the concept of process isolation and implements it using physical controls?

a) Hardware segmentation
b) Data hiding
c) Layering
d) Abstraction

Question Set #4

In which of the following security modes can you be assured that all users have access permissions for all information processed by the system but will not necessarily need to know of all that information?

a) Dedicated
b) System high
c) Compartmented
d) Multilevel

The most commonly overlooked aspect of mobile phone eavesdropping is related to which of the following?

a) Storage device encryption
b) Screen locks
c) Overhearing conversations
d) Wireless networking

What type of memory device is usually used to contain a computer's motherboard BIOS?

a) PROM
b) EEPROM
c) ROM
d) EPROM

What type of memory is directly available to the CPU and is often part of the CPU?

a) RAM
b) ROM
c) Register memory
d) Virtual memory

You are the IT security manager for a retail merchant organization that is just going online with an e-commerce website. You hired several programmers to craft the code that is the backbone of your new web sales system. However, you are concerned that while the new code functions well, it might not be secure. You begin to review the code, the systems design, and the services architecture to track down issues and concerns. Which of the following do you hope to find in order to prevent or protect against XSS? (Select all that apply)

a) Input validation
b) Defensive coding
c) Allowing script input
d) Escaping metacharacters

ISC2 CISSP
Security Vulnerabilities Threats, and Countermeasures

Question Set #1

Which of the following is the most important aspect of security?

a) Physical security
b) Intrusion detection
c) Logical security
d) Awareness training

What method can be used to map out the needs of an organization for a new facility?

a) Log file audit
b) Critical path analysis
c) Risk analysis
d) Inventory

Which of the following is not a security-focused design element of a facility or site?

a) Separation of work and visitor areas
b) Restricted access to areas with higher value or importance
c) Confidential assets located in the heart or center of a facility
d) Equal access to all locations within a facility

Which of the following does not need to be true to maintain the most efficient and secure server room?

a) It must be human compatible
b) It must include the use of nonwater fire suppressants
c) The humidity must be kept between 40 and 60 percent
d) The temperature must be kept between 60 and 75 degrees Fahrenheit

What is the most common and inexpensive form of physical access control device?

a) Lighting
b) Security guard
c) Key locks
d) Fences

Question Set #2

What type of motion detector senses changes in the electrical or magnetic field surrounding a monitored object?

a) Wave
b) Photoelectric
c) Heat
d) Capacitance

Which of the following is a double set of doors that is often protected by a guard and is used to contain a subject until their identity and authentication are verified?

a) Gate
b) Turnstile
c) Mantrap
d) Proximity detector

What is the most common form of perimeter security devices or mechanisms?

a) Security guards
b) Fences
c) CCTV
d) Lighting

Which of the following is not a disadvantage of using security guards?

a) Security guards are usually unaware of the scope of the operations within a facility
b) Not all environments and facilities support security guards
c) Not all security guards are themselves reliable
d) Prescreening, bonding, and training do not guarantee effective and reliable security guards

What is the most common cause of failure for a water-based fire suppression system?

a) Water shortage
b) People
c) Ionization detectors
d) Placement of detectors in drop ceilings

Question Set #3

Which of the following is not a typical security measure implemented in relation to a media storage facility containing reusable removable media?

a) Employing a librarian or custodian
b) Using a check-in/check-out process
c) Hashing
d) Using sanitization tools on returned media

What infrastructure component is often located in the same position across multiple floors in order to provide a convenient means of linking floor-based networks together?

a) Server room
b) Wiring closet
c) Datacenter
d) Media cabinets

Which of the following is not a typical type of alarm that can be triggered for physical security?

a) Preventive
b) Deterrent
c) Repellant
d) Notification

No matter what form of physical access control is used, a security guard or other monitoring system may be deployed to prevent all but which of the following?

a) Piggybacking
b) Espionage
c) Masquerading
d) Abuse

What is the most important goal of all security solutions?

a) Prevention of disclosure
b) Maintaining integrity
c) Human safety
d) Sustaining availability

Question Set #4

What is the ideal humidity range for a computer room?

a) 20–40 percent
b) 40–60 percent
c) 60–75 percent
d) 80–95 percent

Which of the following statements are not true in regards to static electricity?

a) Electrostatic discharge can damage most computing components
b) Static charge accumulation is more prevalent when there is high humidity
c) Static discharge from a person to a metal object can be over 1,000 volts
d) Static electricity is not managed by the deployment of a UPS

A Type B fire extinguisher may use all except which of the following suppression mediums?

a) Water
b) CO2
c) Halon or an acceptable halon substitute
d) Soda acid

What is the best type of water-based fire suppression system for a computer facility?

a) Wet pipe system
b) Dry pipe system
c) Preaction system
d) Deluge system

Which of the following is typically not a culprit in causing damage to computer equipment in the event of a fire and a triggered suppression?

a) Heat
b) Suppression medium
c) Smoke
d) Light