**Chapter 3 – InfoSec and Risk Management Answers**

Multiple choice

1. What is the main purpose of a security policy?
   1. to transfer the responsibility for the information security to all users of the organization
   2. **to provide the management direction and support for information security**
   3. to provide detailed steps for performing specific actions
   4. to provide a common framework for all development activities

Answer: b Pg.103

1. One purpose of a security awareness program is to modify:
   1. **employee's attitudes and behaviors.**
   2. management's approach.
   3. attitudes of employees with sensitive data.
   4. corporate attitudes about safeguarding data.

Answer: a Pg.134

1. Related to information security, confidentiality is the opposite of which of the following?
   1. closure
   2. **disclosure**
   3. disposal
   4. disaster

Answer: b Pg.53

1. Which of the following would best relate to resources being used only for intended purposes?
   1. Confidentiality
   2. **Availability**
   3. Integrity
   4. Reliability

Answer: b Pg.51

1. A deviation from an organization-wide security policy requires which of the following?
   1. **risk acceptance**
   2. risk assignment
   3. risk reduction
   4. risk containment

Answer: a Pg.101

1. Which of the following should NOT be a role of the Security Administrator?
   1. **Authorizing access rights**
   2. Implementing security rules
   3. Ensuring that local policies have been authorized by management
   4. Allocating access rights

Answer: a Pg.126

1. All risks must be:
   1. Transferred
   2. Eliminated
   3. **Identified**
   4. Insured for

Answer: c Pg.76

1. Computer security should be first and foremost which of the following:
   1. Cover all identified risks.
   2. **Be cost-effective.**
   3. Be examined in both monetary and non-monetary terms.
   4. Be proportionate to the value of IT systems.

Answer: b Pg.68

1. Which of the following is not a goal of integrity?
   1. Prevention of the modification of information by unauthorized users.
   2. Prevention of the unauthorized or unintentional modification of information by authorized users.
   3. Preservation of the internal and external consistency.
   4. **Prevention of the modification of information by authorized users.**

Answer: d Pg.392

1. Which of the following questions would not help in assessing personnel security controls?
   1. Are all positions reviewed for sensitivity level?
   2. Are sensitive functions divided among different individuals?
   3. Is there a process for requesting, establishing, issuing, and closing user accounts?
   4. **Is access to facilities by personnel controlled through the use of guards, identification badges, or entry devices such as key cards or biometrics?**

Answer: d Pg.447

1. Which of the following would violate the Due Care concept?
   1. Security policy being outdated
   2. **Data owners not laying out the foundation of data protection**
   3. Network administrator not taking mandatory two-week vacation as planned
   4. Latest security patches for servers only being installed once a week

Answer: b Pg.49

1. Which of the following is not a component of a Operations Security "triples"?
   1. Asset
   2. Threat
   3. Vulnerability
   4. **Risk**

Answer: d Pg.1050

1. What is a difference between Quantitative and Qualitative Risk Analysis?
   1. qualitative uses strong mathematical formulas and quantitative not
   2. fully qualitative analysis if not possible, while quantitative is
   3. **quantitative provides formal cost/benefit analysis and qualitative not**
   4. there is no difference between qualitative and quantitative analysis

Answer: c Pg.86

1. Three key things that must be considered for the planning and implementation of access control mechanisms do not include:
   1. threats to the system
   2. the system's vulnerability to threats to the system
   3. **the system's vulnerability to viruses**
   4. the risk that the threat may materialize

Answer: c Pg.95

1. What is called the probability that a threat to an information system will materialize?
   1. Threat
   2. **Risk**
   3. Vulnerability
   4. Hole

Answer: b Pg.73

1. Which of the following provides a minimum level of security acceptable for an environment?
   1. **A baseline**
   2. A standard
   3. A procedure
   4. A guideline

Answer: a Pg.107

1. ISO 17799 is a standard for:
   1. **Information Security Management**
   2. Implementation and certification of basic security measures
   3. Evaluation criteria for the validation of cryptographic algorithms
   4. Certification of public key infrastructures

Answer: a Pg.63

1. What is called an event or activity that has the potential to cause harm to the information systems or networks?
   1. Vulnerability
   2. Threat agent
   3. Weakness
   4. **Threat**

Answer: d Pg.54

1. Which of the following best allows risk management results to be used knowledgeably?
   1. A vulnerability analysis
   2. A likelihood assessment
   3. **An uncertainty analysis**
   4. A threat identification

Answer: c Pg.79

1. The major objective of system configuration management is which of the following?
   1. system maintenance
   2. **system stability**
   3. system operations
   4. system tracking

Answer: b Pg.317

1. Who of the following is responsible for ensuring that proper controls are in place to address integrity, confidentiality, and availability of IT systems and data?
   1. Business and functional managers
   2. IT Security practitioners
   3. **System and information owners**
   4. Chief information officer

Answer: c Pg.49

1. In the CIA triad, what does the letter A stand for?
   1. Auditability
   2. Accountability
   3. **Availability**
   4. Authentication

Answer: c Pg.51

1. Related to information security, availability is the opposite of which of the following?
   1. delegation
   2. distribution
   3. documentation
   4. **destruction**

Answer: d Pg.51

1. Making sure that only those who are supposed to access the data can access is which of the following?
   1. **confidentiality.**
   2. capability.
   3. integrity.
   4. availability.

Answer: a Pg.53

1. Which of the following choices is NOT part of a security policy?
   1. definition of overall steps of information security and the importance of security
   2. statement of management intend, supporting the goals and principles of information security
   3. definition of general and specific responsibilities for information security management
   4. **description of specific technologies used in the field of information security**

Answer: d Pg.104

1. Which must bear the primary responsibility for determining the level of protection needed for information systems resources?
   1. IS security specialists
   2. **Senior Management**
   3. Seniors security analysts
   4. systems auditors

Answer: b P.103

1. The absence or weakness in a system that may possibly be exploited is called a(n)?
   1. Threat
   2. Exposure
   3. **Vulnerability**
   4. Risk

Answer: c Pg.139

1. How is Annualized Loss Expectancy (ALE) derived from a treat?
   1. ARO x (SLE - EF)
   2. **SLE x ARO**
   3. SLE/EF
   4. AV x EF

Answer: b Pg.90

1. What is called a weakness or lack of a safeguard, which may be exploited by a threat, causing harm to the information systems or networks?
   1. **Vulnerability**
   2. Risk
   3. Threat
   4. Weakness

Answer: a Pg.54

1. Which of the following is the weakest link in a security system?
   1. **People**
   2. Software
   3. Communications
   4. Hardware

Answer: a Pg.130

1. Security of computer-based information systems is which of the following?
   1. technical issue
   2. operational issue
   3. **management issue**
   4. training issue

Answer: c Pg.37

1. Which of the following statements pertaining to a security policy is incorrect?
   1. Its main purpose is to inform the users, administrators and managers of their obligatory requirements for protecting technology and information assets.
   2. **It specifies how hardware and software should be used throughout the organization.**
   3. It needs to have the acceptance and support of all levels of employees within the organization in order for it to be appropriate and effective.
   4. It must be flexible to the changing environment.

Answer: b P.103

1. Which of the following is most likely given the responsibility of the maintenance and protection of the data?
   1. Data owner
   2. **Data custodian**
   3. User
   4. Security administrator

Answer: b Pg.116

1. Related to information security, the guarantee that the message sent is the message received is an example of which of the following?
   1. **integrity**
   2. confidentiality
   3. availability
   4. identity

Answer: a Pg.155

1. Making sure that the data is accessible when and where it is needed is which of the following?
   1. confidentiality
   2. integrity
   3. acceptability
   4. **availability**

Answer: d Pg.51

1. What can be described as a measure of the magnitude of loss or impact on the value of an asset?
   1. Probability
   2. **Exposure factor**
   3. Vulnerability
   4. Threat

Answer: b Pg.89

1. An effective information security policy should not have which of the following characteristic?
   1. Include separation of duties
   2. **Be designed with a short- to mid-term focus**
   3. Be understandable and supported by all stakeholders
   4. Specify areas of responsibility and authority

Answer: b Pg.103

1. According to private sector data classification levels, how would salary levels and medical information be classified?
   1. Public
   2. Sensitive
   3. **Private**
   4. Confidential

Answer: c Pg.213

1. Which of the next are steps of a common development process of creating a security policy, standards and procedures?
   1. design, development, publication, coding, testing
   2. design, evaluation, approval, publication, implementation
   3. **initial and evaluation, development, approval, publication, implementation, maintenance**
   4. feasibility, development, approval, implementation, integration

Answer: c Pg.104

1. If risk is defined as "the potential that a given threat will exploit vulnerabilities of an asset or group of assets to cause loss or damage to the assets" then risk has all of the following elements EXCEPT?
   1. An impact on assets based on threats and vulnerabilities
   2. **Controls addressing the threats**
   3. Threats to and vulnerabilities of processes and/or assets
   4. Probabilities of the threats

Answer: b Pg.54

1. The concept of integrity also contains which of the following?
   1. Identity
   2. **nonrepudiation of a message source**
   3. Availability
   4. Confidentiality

Answer: b Pg.768

1. Which of the following is not a responsibility of an information owner?
   1. Determine what level of classification the information requires.
   2. Periodically review the classification assignments against business needs.
   3. Delegate the responsibility of data protection to data custodians.
   4. **Running regular backups and periodically testing the validity of the backup data.**

Answer: d Pg.125

1. Preservation of confidentiality information systems requires that the information is not disclosed to:
   1. Authorized person
   2. **Unauthorized persons or processes.**
   3. Unauthorized persons.
   4. Authorized persons and processes

Answer: b Pg.53

1. Which approach to a security program makes sure that the people actually responsible for protecting the company's assets are driving the program?
   1. The Delphi approach
   2. **The top-down approach**
   3. The bottom-up approach
   4. The technology approach

Answer: b Pg.786

1. The C.I.A. triad is often represented by a:
   1. **triangle**
   2. circle
   3. ellipse
   4. diagonal

Answer: a Pg.51

1. Which of the following statements pertaining to quantitative risk analysis is false?
   1. It can be automated
   2. It involves complex calculations
   3. It requires a high volume of information
   4. **It involves a lot of guesswork**

Answer: d Pg.86

1. What is reverse to the triple C.I.A. in risk management:
   1. misuse, exposure, destruction
   2. authorization, non-repudiation, integrity
   3. **disclosure, alteration, destruction**
   4. confidentiality, integrity, availability

Answer: c

1. What will be Annualized Rate of Occurrence (ARO) of the threat "user input error", in the case that company employs 100 data entry clerks and every one of them make one input error each month?
   1. 100
   2. 120
   3. 1
   4. **1,200**

Answer: d Pg.89

1. Step-by-step instructions used to satisfy control requirements is called a:
   1. policy
   2. standard
   3. guideline
   4. **procedure**

Answer: d Pg.108

1. Making sure that only those who are supposed to access the data can access is:
   1. **Confidentiality.**
   2. Capability.
   3. Integrity.
   4. Availability.

Answer: a Pg.155

1. Which of the following embodies all the detailed actions that personnel are required to follow?
   1. Standards
   2. Guidelines
   3. **Procedures**
   4. Baselines

Answer: c Pg.108

1. What can be defined as an event that could cause harm to the information systems?
   1. A risk
   2. **A threat**
   3. A vulnerability
   4. A weakness

Answer: b Pg.54

1. What would best define risk management?
   1. The process of eliminating the risk
   2. The process of assessing the risks
   3. **The process of reducing risk to an acceptable level**
   4. The process of transferring risk

Answer: c Pg.73

1. Which of the following would be the first step in establishing an information security program?
   1. **Adoption of a corporate information security policy statement.**
   2. Development and implementation of an information security standards manual.
   3. Development of a security awareness-training program for employees.
   4. Purchase of security access control software.

Answer: a Pg.103

1. Within the realm of IT security, which of the following combinations best defines risk?
   1. Threat coupled with a breach
   2. **Threat coupled with a vulnerability**
   3. Vulnerability coupled with an attack
   4. Threat coupled with a breach of security

Answer: b Pg.54

1. Which of the following is less likely to assist in ensuring availability?
   1. Backups and redundant disk systems
   2. **Regular system and security audits**
   3. Reliable and interoperable security processes and network security mechanisms
   4. Acceptable log-ins and operating process performances

Answer: b Pg.51

1. Related to information security, the prevention of the intentional or unintentional unauthorized disclosure of contents is which of the following?
   1. **Confidentiality**
   2. Integrity
   3. Availability
   4. capability

Answer: a Pg.53

1. Which data classification should apply to commercial trade secrets?
   1. Sensitive
   2. **Confidential**
   3. Private
   4. Secret

Answer: b Pg.53

1. What are the three fundamental principles of security?
   1. Accountability, confidentiality and integrity
   2. **Confidentiality, integrity and availability**
   3. Integrity, availability and accountability
   4. Availability, accountability and confidentiality

Answer: b Pg.51

1. In an organization, an Information Technology security function should:
   1. Be a function within the information systems function of an organization.
   2. Report directly to a specialized business unit such as legal, corporate security or insurance.
   3. **Be lead by a Chief Security Officer and report directly to the CEO.**
   4. Be independent but report to the Information Systems function.

Answer: c Pg.60

1. Which of the following should be given technical security training?
   1. Operators
   2. Security practitioners and information systems auditors
   3. **IT support personnel and system administrators**
   4. Senior managers, functional managers and business unit managers

Answer: c Pg.135

1. What does "residual risk" mean?
   1. **The security risk that remains after controls have been implemented**
   2. Weakness of an assets which can be exploited by a threat
   3. Risk that remains after risk analysis has has been performed
   4. The result of unwanted incident

Answer: a Pg.100

1. Which of the following is the MOST important aspect relating to employee termination?
   1. The details of employee have been removed from active payroll files.
   2. Company property provided to the employee has been returned.
   3. **User ID and passwords of the employee have been deleted.**
   4. The related company staff are notified about the termination.

Answer: c

1. Which of the following is an advantage of a qualitative over a quantitative risk analysis?
   1. **It prioritizes the risks and identifies areas for immediate improvement in addressing the vulnerabilities.**
   2. It provides specific quantifiable measurements of the magnitude of the impacts.
   3. It makes a cost-benefit analysis of recommended controls easier.
   4. It can easily be automated.

Answer: a Pg.91

1. Who should measure the effectiveness of security related controls in an organization?
   1. the local security specialist
   2. the business manager
   3. **the systems auditor**
   4. the central security manager

Answer: c Pg.124

1. Who should provide access authorization to computerized information?
   1. Database administrator
   2. Security administrator
   3. **Data owner**
   4. Network administrator

Answer: c Pg.124

1. Related to information security, integrity is the opposite of which of the following?
   1. abstraction
   2. **alteration**
   3. accreditation
   4. application

Answer: b Pg.52

1. Who should decide how a company should approach security and what security measures should be implemented?
   1. **Senior management**
   2. Data owner
   3. Auditor
   4. The information security specialist

Answer: a Pg.103

1. Which one of the following represents an ALE calculation?
   1. **single loss expectancy x annualized rate of occurrence**
   2. gross loss expectancy x loss frequency
   3. actual replacement cost - proceeds of salvage
   4. asset value x loss expectancy

Answer: a Pg.89

1. Which of the following could be defined as the likelihood of a threat agent taking advantage of a vulnerability?
   1. **A risk**
   2. A residual risk
   3. An exposure
   4. A countermeasure

Answer: a Pg.54

1. Which one of the following individuals has PRIMARY responsibility for determining the classification level of information?
   1. Security manager
   2. User
   3. **Owner**
   4. Auditor

Answer: c Pg.49

1. Which of the following is the best reason for the use of an automated risk analysis tool?
   1. Much of the data gathered during the review cannot be reused for subsequent analysis.
   2. Automated methodologies require minimal training and knowledge of risk analysis.
   3. Most software tools have user interfaces that are easy to use
   4. **Minimal information gathering is required due to the amount of information built into the tool.**

Answer: d Pg.86

1. Why do many organizations require every employee to take a mandatory vacation of a week or more?
   1. **To reduce the opportunity for an employee to commit an improper or illegal act.**
   2. To lead to greater productivity through a better quality of life for the employee.
   3. To provide proper cross training for another employee.
   4. To allow more employees to have a better understanding of the overall system.

Answer: a Pg.141

1. What can best be defined as high-level statements, beliefs, goals and objectives?
   1. Standards
   2. **Policies**
   3. Guidelines
   4. Procedures

Answer: b Pg.104

1. Which of the following is not a common integrity goal?
   1. Prevent unauthorized users from making modifications.
   2. Maintain internal and external consistency.
   3. Prevent authorized users from making improper modifications.
   4. **Prevent paths that could lead to inappropriate disclosure.**

Answer: d Pg.52

1. Which of the following department managers would be best suited to oversee the development of an information security policy?
   1. Information systems
   2. Human resources
   3. **Business operations**
   4. Security administration

Answer: c Pg.103

1. Which of the following would be the first criteria to consider, to determine the classification of an information object?
   1. **Value**
   2. Age
   3. Useful life
   4. Personal association

Answer: a Pg.105

1. Which of the following best defines add-on security?
   1. Physical security complementing logical security measures.
   2. Protection mechanisms implemented as an integral part of an information system.
   3. Layer security.
   4. **Protection mechanisms implemented after an information system has become operational.**

Answer: d Pg.1133

1. Which of the following is not a part of a risk analysis?
   1. Identify risks
   2. Quantify the impact of potential threats
   3. Provide an economic balance between the impact of the risk and the cost of the associated countermeasure
   4. **Choose the best countermeasure**

Answer: d Pg.76

1. According to governmental data classification levels, how would answers to tests and health care information be classified?
   1. Unclassified
   2. **Sensitive but unclassified**
   3. Confidential
   4. Private

Answer: b Pg.112

1. How should a risk be handled when the cost of the countermeasure outweighs the cost of the risk?
   1. Reject the risk
   2. Perform another risk analysis
   3. **Accept the risk**
   4. Reduce the risk

Answer: c Pg.89

1. What is the highest amount a company should spend annually on countermeasures for protecting an asset valued at $1,000,000 from a threat that has an annualized rate of occurrence (ARO) of 5% and an exposure factor (EF) of 30%?
   1. 300,000$
   2. 150,000$
   3. **15,000$**
   4. 1,500$

Answer: c Pg.89

1. Which of the following describe elements that create reliability and stability in networks and systems and which assures that connectivity is accessible when needed?
   1. **Availability**
   2. Acceptability
   3. confidentiality
   4. Integrity

Answer: a Pg.51

1. Which of the following would be defined as an absence or weakness of safeguard that could be exploited?
   1. A threat
   2. **A vulnerability**
   3. A risk
   4. An exposure

Answer: b Pg.54

1. Which of the following represents an ALE calculation?
   1. Gross loss expectancy X loss frequency.
   2. Asset value X loss expectancy.
   3. Total cost of loss + actual replacement value.
   4. **Single loss expectancy X annualized rate of occurrence.**

Answer: d Pg.89

1. Making sure that the data has not been changed unintentionally, due to an accident or malice is:
   1. **Integrity.**
   2. Confidentiality.
   3. Availability.
   4. Auditability.

Answer: a Pg.52