**QUESTION 265**
Risk assessment is MOST effective when performed:

A. at the beginning of security program development.
B. on a continuous basis.
C. while developing the business case for the security program.
D. during the business change process.

**Correct Answer:** B
**Explanation:**
Risk assessment needs to be performed on a continuous basis because of organizational and technical changes. Risk assessment must take into account all significant changes in order to be effective.

**QUESTION 266**
In a business impact analysis, the value of an information system should be based on the overall cost:

A. of recovery.
B. to recreate.
C. if unavailable.
D. of emergency operations.

**Correct Answer:** C
**Explanation:**
The value of an information system should be based on the cost incurred if the system were to become unavailable. The cost to design or recreate the system is not as relevant since a business impact analysis measures the impact that would occur if an information system were to become unavailable. Similarly, the cost of emergency operations is not as relevant.

**QUESTION 267**
After obtaining commitment from senior management, which of the following should be completed NEXT when establishing an information security program?

A. Define security metrics
B. Conduct a risk assessment
C. Perform a gap analysis
D. Procure security tools

**Correct Answer:** B
**Explanation:**
When establishing an information security program, conducting a risk assessment is key to identifying the needs of the organization and developing a security strategy. Defining security metrics, performing a gap analysis and procuring security tools are all subsequent considerations.

**QUESTION 268**
Attackers who exploit cross-site scripting vulnerabilities take advantage of:

A. a lack of proper input validation controls.

B. weak authentication controls in the web application layer.
C. flawed cryptographic secure sockets layer (SSL) implementations and short key lengths.
D. implicit web application trust relationships.

**Correct Answer:** A
**Explanation:**
Cross-site scripting attacks inject malformed input. Attackers who exploit weak application authentication controls can gain unauthorized access to applications and this has little to do with cross-site scripting vulnerabilities. Attackers who exploit flawed cryptographic secure sockets layer (SSI.) implementations and short key lengths can sniff network traffic and crack keys to gain unauthorized access to information. This has little to do with cross-site scripting vulnerabilities. Web application trust relationships do not relate directly to the attack.

**QUESTION 269**
The purpose of a corrective control is to:

A. reduce adverse events.
B. indicate compromise.
C. mitigate impact.
D. ensure compliance.

**Correct Answer:** C
**Explanation:**
Corrective controls serve to reduce or mitigate impacts, such as providing recovery capabilities. Preventive controls reduce adverse events, such as firewalls. Compromise can be detected by detective controls, such as intrusion detection systems (IDSs). Compliance could be ensured by preventive controls, such as access controls.

**QUESTION 270**
After a risk assessment study, a bank with global operations decided to continue doing business in certain regions of the world where identity theft is rampant. The information security manager should encourage the business to:

A. increase its customer awareness efforts in those regions.
B. implement monitoring techniques to detect and react to potential fraud.
C. outsource credit card processing to a third party.
D. make the customer liable for losses if they fail to follow the bank's advice.

**Correct Answer:** B
**Explanation:**
While customer awareness will help mitigate the risks, this is insufficient on its own to control fraud risk. Implementing monitoring techniques which will detect and deal with potential fraud cases is the most effective way to deal with this risk. If the bank outsources its processing, the bank still retains liability. While making the customer liable for losses is a possible approach, nevertheless, the bank needs to be seen to be proactive in managing its risks.

**QUESTION 271**
When the computer incident response team (CIRT) finds clear evidence that a hacker has penetrated the corporate network and modified customer information, an information security

manager should FIRST notify:

A. the information security steering committee.
B. customers who may be impacted.
C. data owners who may be impacted.
D. regulatory- agencies overseeing privacy.

**Correct Answer:** C
**Explanation:**
The data owners should be notified first so they can take steps to determine the extent of the damage and coordinate a plan for corrective action with the computer incident response team. Other parties will be notified later as required by corporate policy and regulatory requirements.

**QUESTION 272**
Risk acceptance is a component of which of the following?

A. Assessment
B. Mitigation
C. Evaluation
D. Monitoring

**Correct Answer:** B
**Explanation:**
Risk acceptance is one of the alternatives to be considered in the risk mitigation process. Assessment and evaluation are components of the risk analysis process. Risk acceptance is not a component of monitoring.

**QUESTION 273**
Which of (lie following would be the MOST relevant factor when defining the information classification policy?

A. Quantity of information
B. Available IT infrastructure
C. Benchmarking
D. Requirements of data owners

**Correct Answer:** D
**Explanation:**
When defining the information classification policy, the requirements of the data owners need to be identified. The quantity of information, availability of IT infrastructure and benchmarking may be part of the scheme after the fact and would be less relevant.

**QUESTION 274**
The security responsibility of data custodians in an organization will include:

A. assuming overall protection of information assets.
B. determining data classification levels.
C. implementing security controls in products they install.
D. ensuring security measures are consistent with policy.

**Correct Answer:** D
**Explanation:**
Security responsibilities of data custodians within an organization include ensuring that appropriate security measures are maintained and are consistent with organizational policy. Executive management holds overall responsibility for protection of the information assets. Data owners determine data classification levels for information assets so that appropriate levels of controls can be provided to meet the requirements relating to confidentiality, integrity and availability. Implementation of information security in products is the responsibility of the IT developers.

**QUESTION 275**
Which of the following is MOST important to the success of an information security program?

A. Security' awareness training
B. Achievable goals and objectives
C. Senior management sponsorship
D. Adequate start-up budget and staffing

**Correct Answer:** C
**Explanation:**
Sufficient senior management support is the most important factor for the success of an information security program. Security awareness training, although important, is secondary. Achievable goals and objectives as well as having adequate budgeting and staffing are important factors, but they will not ensure success if senior management support is not present.

**QUESTION 276**
In an organization, information systems security is the responsibility of:

A. all personnel.
B. information systems personnel.
C. information systems security personnel.
D. functional personnel.

**Correct Answer:** A
**Explanation:**
All personnel of the organization have the responsibility of ensuring information systems security-this can include indirect personnel such as physical security personnel. Information systems security cannot be the responsibility of information systems personnel alone since they cannot ensure security. Information systems security cannot be the responsibility of information systems security personnel alone since they cannot ensure security. Information systems security cannot be the responsibility of functional personnel alone since they cannot ensure security.

**QUESTION 277**
Which of the following tools is MOST appropriate for determining how long a security project will take to implement?

A. Gantt chart
B. Waterfall chart
C. Critical path
D. Rapid Application Development (RAD)

**Correct Answer:** C

**Explanation:**
The critical path method is most effective for determining how long a project will take. A waterfall chart is used to understand the flow of one process into another. A Gantt chart facilitates the proper estimation and allocation of resources. The Rapid Application Development (RAD) method is used as an aid to facilitate and expedite systems development.

**QUESTION 278**
Priority should be given to which of the following to ensure effective implementation of information security governance?

A. Consultation
B. Negotiation
C. Facilitation
D. Planning

**Correct Answer:** D
**Explanation:**
Planning is the key to effective implementation of information security governance. Consultation, negotiation and facilitation come after planning.

**QUESTION 279**
At what stage of the applications development process would encryption key management initially be addressed?

A. Requirements development
B. Deployment
C. Systems testing
D. Code reviews

**Correct Answer:** A
**Explanation:**
Encryption key management has to be integrated into the requirements of the application's design. During systems testing and deployment would be too late since the requirements have already been agreed upon. Code reviews are part of the final quality assurance (QA) process and would also be too late in the process.

**QUESTION 280**
A risk assessment study carried out by an organization noted that there is no segmentation of the local area network (LAN). Network segmentation would reduce the potential impact of which of the following?

A. Denial of service (DoS) attacks
B. Traffic sniffing
C. Virus infections
D. IP address spoofing

**Correct Answer:** B
**Explanation:**
Network segmentation reduces the impact of traffic sniffing by limiting the amount of traffic that may be visible on any one network segment. Network segmentation would not mitigate the risk posed by denial of service (DoS) attacks, virus infections or IP address spoofing since each of these would be able to traverse network segments.