D. A business impact analysis (BIA)

Correct Answer: C
Explanation:
A risk assessment will identify- the business impact of such vulnerability being exploited and is, thus, the correct process. A penetration test or a security baseline review may identify the vulnerability but not the remedy. A business impact analysis (BIA) will more likely identify the impact of the loss of the mail server.

QUESTION 186
Which of the following roles is PRIMARILY responsible for determining the information classification levels for a given information asset?

A. Manager
B. Custodian
C. User
D. Owner

Correct Answer: D
Explanation:
Although the information owner may be in a management position and is also considered a user, the information owner role has the responsibility for determining information classification levels. Management is responsible for higher-level issues such as providing and approving budget, supporting activities, etc. The information custodian is responsible for day-to-day security tasks such as protecting information, backing up information, etc. Users are the lowest level. They use the data, but do not classify the data. The owner classifies the data.

QUESTION 187
The decision as to whether a risk has been reduced to an acceptable level should be determined by:

A. organizational requirements.
B. information systems requirements.
C. information security requirements.
D. international standards.

Correct Answer: A
Explanation:
Organizational requirements should determine when a risk has been reduced to an acceptable level. Information systems and information security should not make the ultimate determination. Since each organization is unique, international standards of best practice do not represent the best solution.

QUESTION 188
All risk management activities are PRIMARILY designed to reduce impacts to:

A. a level defined by the security manager.
B. an acceptable level based on organizational risk tolerance.
C. a minimum level consistent with regulatory requirements.
D. the minimum level possible.

Correct Answer: B

Explanation:
The aim of risk management is to reduce impacts to an acceptable level. "Acceptable" or "reasonable" are relative terms that can vary based on environment and circumstances. A minimum level that is consistent with regulatory requirements may not be consistent with business objectives, and regulators typically do not assign risk levels. The minimum level possible may not be aligned with business requirements.

QUESTION 189
Which of the following is the BEST method to ensure the overall effectiveness of a risk management program?

A. User assessments of changes
B. Comparison of the program results with industry standards
C. Assignment of risk within the organization
D. Participation by all members of the organization

Correct Answer: D
Explanation:
Effective risk management requires participation, support and acceptance by all applicable members of the organization, beginning with the executive levels. Personnel must understand their responsibilities and be trained on how to fulfill their roles.

QUESTION 190
A successful information security management program should use which of the following to determine the amount of resources devoted to mitigating exposures?

A. Risk analysis results
B. Audit report findings
C. Penetration test results
D. Amount of IT budget available

Correct Answer: A
Explanation:
Risk analysis results are the most useful and complete source of information for determining the amount of resources to devote to mitigating exposures. Audit report findings may not address all risks and do not address annual loss frequency. Penetration test results provide only a limited view of exposures, while the IT budget is not tied to the exposures faced by the organization.

QUESTION 191
It is important to classify and determine relative sensitivity of assets to ensure that:

A. cost of protection is in proportion to sensitivity.
B. highly sensitive assets are protected.
C. cost of controls is minimized.
D. countermeasures are proportional to risk.

Correct Answer: D
Explanation:
Classification of assets needs to be undertaken to determine sensitivity of assets in terms of risk to the business operation so that proportional countermeasures can be effectively implemented. While higher costs are allowable to protect sensitive assets, and it is always reasonable to minimize the costs of controls, it is most important that the controls and countermeasures are

commensurate to the risk since this will justify the costs. Choice B is important but it is an incomplete answer because it does not factor in risk. Therefore, choice D is the most important.

QUESTION 192
The MOST important reason for conducting periodic risk assessments is because:

A. risk assessments are not always precise.
B. security risks are subject to frequent change.
C. reviewers can optimize and reduce the cost of controls.
D. it demonstrates to senior management that the security function can add value.

Correct Answer: B
Explanation:
Risks are constantly changing. A previously conducted risk assessment may not include measured risks that have been introduced since the last assessment. Although an assessment can never be perfect and invariably contains some errors, this is not the most important reason for periodic reassessment. The fact that controls can be made more efficient to reduce costs is not sufficient. Finally, risk assessments should not be performed merely to justify the existence of the security function.

QUESTION 193
Who is responsible for ensuring that information is classified?

A. Senior management
B. Security manager
C. Data owner
D. Custodian

Correct Answer: C
Explanation:
The data owner is responsible for applying the proper classification to the data. Senior management is ultimately responsible for the organization. The security officer is responsible for applying security protection relative to the level of classification specified by the owner. The technology group is delegated the custody of the data by the data owner, but the group does not classify the information.

QUESTION 194
An information security manager has been assigned to implement more restrictive preventive controls. By doing so, the net effect will be to PRIMARILY reduce the:

A. threat.
B. loss.
C. vulnerability.
D. probability.

Correct Answer: C
Explanation:
Implementing more restrictive preventive controls mitigates vulnerabilities but not the threats. Losses and probability of occurrence may not be primarily or directly affected.

QUESTION 195

Which of the following measures would be MOST effective against insider threats to confidential information?

A. Role-based access control
B. Audit trail monitoring
C. Privacy policy
D. Defense-in-depth

Correct Answer: A
Explanation:
Role-based access control provides access according to business needs; therefore, it reduces unnecessary- access rights and enforces accountability. Audit trail monitoring is a detective control, which is 'after the fact.' Privacy policy is not relevant to this risk. Defense- in-depth primarily focuses on external threats

QUESTION 196
An organization has decided to implement additional security controls to treat the risks of a new process. This is an example of:

A. eliminating the risk.
B. transferring the risk.
C. mitigating the risk.
D. accepting the risk.

Correct Answer: C
Explanation:
Risk can never be eliminated entirely. Transferring the risk gives it away such as buying insurance so the insurance company can take the risk. Implementing additional controls is an example of mitigating risk. Doing nothing to mitigate the risk would be an example of accepting risk.

QUESTION 197
Which of the following would generally have the GREATEST negative impact on an organization?

A. Theft of computer software
B. Interruption of utility services
C. Loss of customer confidence
D. Internal fraud resulting in monetary loss

Correct Answer: C
Explanation:
Although the theft of software, interruption of utility services and internal frauds are all significant, the loss of customer confidence is the most damaging and could cause the business to fail.

QUESTION 198
Which of the following results from the risk assessment process would BEST assist risk management decision making?

A. Control risk
B. Inherent risk
C. Risk exposure
D. Residual risk

Correct Answer: D
Explanation:
Residual risk provides management with sufficient information to decide to the level of risk that an organization is willing to accept. Control risk is the risk that a control may not succeed in preventing an undesirable event. Risk exposure is the likelihood of an undesirable event occurring. Inherent risk is an important factor to be considered during the risk assessment.

QUESTION 199
Risk management programs are designed to reduce risk to:

A. a level that is too small to be measurable.
B. the point at which the benefit exceeds the expense.
C. a level that the organization is willing to accept.
D. a rate of return that equals the current cost of capital.

Correct Answer: C
Explanation:
Risk should be reduced to a level that an organization is willing to accept. Reducing risk to a level too small to measure is impractical and is often cost-prohibitive. To tie risk to a specific rate of return ignores the qualitative aspects of risk that must also be considered. Depending on the risk preference of an organization, it may or may not choose to pursue risk mitigation to the point at which the benefit equals or exceeds the expense. Therefore, choice C is a more precise answer.

QUESTION 200
Which of the following steps should be performed FIRST in the risk assessment process?

A. Staff interviews
B. Threat identification
C. Asset identification and valuation
D. Determination of the likelihood of identified risks

Correct Answer: C
Explanation:
The first step in the risk assessment methodology is a system characterization, or identification and valuation, of all of the enterprise's assets to define the boundaries of the assessment. Interviewing is a valuable tool to determine qualitative information about an organization's objectives and tolerance for risk. Interviews are used in subsequent steps. Identification of threats comes later in the process and should not be performed prior to an inventory since many possible threats will not be applicable if there is no asset at risk. Determination of likelihood comes later in the risk assessment process.

QUESTION 201
A risk management program should reduce risk to:

A. zero.
B. an acceptable level.
C. an acceptable percent of revenue.
D. an acceptable probability of occurrence.

Correct Answer: B
Explanation: