Risk should be reduced to an acceptable level based on the risk preference of the organization. Reducing risk to zero is impractical and could be cost-prohibitive. Tying risk to a percentage of revenue is inadvisable since there is no direct correlation between the two. Reducing the probability of risk occurrence may not always be possible, as in the ease of natural disasters. The focus should be on reducing the impact to an acceptable level to the organization, not reducing the probability of the risk.

QUESTION 202
When implementing security controls, an information security manager must PRIMARILY focus on:

A. minimizing operational impacts.
B. eliminating all vulnerabilities.
C. usage by similar organizations.
D. certification from a third party.

Correct Answer: A
Explanation:
Security controls must be compatible with business needs. It is not feasible to eliminate all vulnerabilities. Usage by similar organizations does not guarantee that controls are adequate. Certification by a third party is important, but not a primary concern.

QUESTION 203
Which of the following is the PRIMARY prerequisite to implementing data classification within an organization?

A. Defining job roles
B. Performing a risk assessment
C. Identifying data owners
D. Establishing data retention policies

Correct Answer: C
Explanation:
Identifying the data owners is the first step, and is essential to implementing data classification. Defining job roles is not relevant. Performing a risk assessment is important, but will require the participation of data owners (who must first be identified). Establishing data retention policies may occur after data have been classified.

QUESTION 204
Which of the following would be of GREATEST importance to the security manager in determining whether to accept residual risk?

A. Historical cost of the asset
B. Acceptable level of potential business impacts
C. Cost versus benefit of additional mitigating controls
D. Annualized loss expectancy (ALE)

Correct Answer: C
Explanation:
The security manager would be most concerned with whether residual risk would be reduced by a greater amount than the cost of adding additional controls. The other choices, although relevant, would not be as important.

QUESTION 205
The systems administrator did not immediately notify the security officer about a malicious attack. An information security manager could prevent this situation by:

A. periodically testing the incident response plans.
B. regularly testing the intrusion detection system (IDS).
C. establishing mandatory training of all personnel.
D. periodically reviewing incident response procedures.

Correct Answer: A
Explanation:
Security incident response plans should be tested to find any deficiencies and improve existing processes. Testing the intrusion detection system (IDS) is a good practice but would not have prevented this situation. All personnel need to go through formal training to ensure that they understand the process, tools and methodology involved in handling security incidents. However, testing of the actual plans is more effective in ensuring the process works as intended. Reviewing the response procedures is not enough; the security response plan needs to be tested on a regular basis.

QUESTION 206
Before conducting a formal risk assessment of an organization's information resources, an information security manager should FIRST:

A. map the major threats to business objectives.
B. review available sources of risk information.
C. identify the value of the critical assets.
D. determine the financial impact if threats materialize.

Correct Answer: A
Explanation:
Risk mapping or a macro assessment of the major threats to the organization is a simple first step before performing a risk assessment. Compiling all available sources of risk information is part of the risk assessment. Choices C and D are also components of the risk assessment process, which are performed subsequent to the threats-business mapping.

QUESTION 207
The PRIMARY reason for initiating a policy exception process is when:

A. operations are too busy to comply.
B. the risk is justified by the benefit.
C. policy compliance would be difficult to enforce.
D. users may initially be inconvenienced.

Correct Answer: B
Explanation:
Exceptions to policy are warranted in circumstances where compliance may be difficult or impossible and the risk of noncompliance is outweighed by the benefits. Being busy is not a justification for policy exceptions, nor is the fact that compliance cannot be enforced. User inconvenience is not a reason to automatically grant exception to a policy.

QUESTION 208
The recovery point objective (RPO) requires which of the following?

A. Disaster declaration
B. Before-image restoration
C. System restoration
D. After-image processing

Correct Answer: B
Explanation:
The recovery point objective (RPO) is the point in the processing flow at which system recovery should occur. This is the predetermined state of the application processing and data used to restore the system and to continue the processing flow. Disaster declaration is independent of this processing checkpoint. Restoration of the system can occur at a later date, as does the return to normal, after-image processing.

QUESTION 209
Previously accepted risk should be:

A. re-assessed periodically since the risk can be escalated to an unacceptable level due to revised conditions.
B. accepted permanently since management has already spent resources (time and labor) to conclude that the risk level is acceptable.
C. avoided next time since risk avoidance provides the best protection to the company.
D. removed from the risk log once it is accepted.

Correct Answer: A
Explanation:
Acceptance of risk should be regularly reviewed to ensure that the rationale for the initial risk acceptance is still valid within the current business context. The rationale for initial risk acceptance may no longer be valid due to change(s) and. hence, risk cannot be accepted permanently. Risk is an inherent part of business and it is impractical and costly to eliminate all risk. Even risks that have been accepted should be monitored for changing conditions that could alter the original decision.

QUESTION 210
When performing a qualitative risk analysis, which of the following will BEST produce reliable results?

A. Estimated productivity losses
B. Possible scenarios with threats and impacts
C. Value of information assets
D. Vulnerability assessment

Correct Answer: B
Explanation:
Listing all possible scenarios that could occur, along with threats and impacts, will better frame the range of risks and facilitate a more informed discussion and decision. Estimated productivity losses, value of information assets and vulnerability assessments would not be sufficient on their own.

QUESTION 211
Identification and prioritization of business risk enables project managers to:

A. establish implementation milestones.
B. reduce the overall amount of slack time.
C. address areas with most significance.
D. accelerate completion of critical paths.

Correct Answer: C
Explanation:
Identification and prioritization of risk allows project managers to focus more attention on areas of greater importance and impact. It will not reduce the overall amount of slack time, facilitate establishing implementation milestones or allow a critical path to be completed any sooner.

QUESTION 212
Which of the following will BEST prevent external security attacks?

A. Static IP addressing
B. Network address translation
C. Background checks for temporary employees
D. Securing and analyzing system access logs

Correct Answer: B
Explanation:
Network address translation is helpful by having internal addresses that are nonroutable. Background checks of temporary employees are more likely to prevent an attack launched from within the enterprise. Static IP addressing does little to prevent an attack. Writing all computer logs to removable media does not help in preventing an attack.

QUESTION 213
An organization has to comply with recently published industry regulatory requirements--compliance that potentially has high implementation costs. What should the information security manager do FIRST?

A. Implement a security committee.
B. Perform a gap analysis.
C. Implement compensating controls.
D. Demand immediate compliance.

Correct Answer: B
Explanation:
Since they are regulatory requirements, a gap analysis would be the first step to determine the level of compliance already in place. Implementing a security committee or compensating controls would not be the first step. Demanding immediate compliance would not assess the situation.

QUESTION 214
The PRIMARY benefit of performing an information asset classification is to:

A. link security requirements to business objectives.
B. identify controls commensurate to risk.
C. define access rights.

D. establish ownership.

Correct Answer: B
Explanation:
All choices are benefits of information classification. However, identifying controls that are proportional to the risk in all cases is the primary benefit of the process.

QUESTION 215
Which of the following would a security manager establish to determine the target for restoration of normal processing?

A. Recover)' time objective (RTO)
B. Maximum tolerable outage (MTO)
C. Recovery point objectives (RPOs)
D. Services delivery objectives (SDOs)

Correct Answer: A
Explanation:
Recovery time objective (RTO) is the length of time from the moment of an interruption until the time the process must be functioning at a service level sufficient to limit financial and operational impacts to an acceptable level. Maximum tolerable outage (MTO) is the maximum time for which an organization can operate in a reduced mode. Recovery point objectives (RPOs) relate to the age of the data required for recovery. Services delivery objectives (SDOs) are the levels of service required in reduced mode.

QUESTION 216
One way to determine control effectiveness is by determining:

A. whether it is preventive, detective or compensatory.
B. the capability of providing notification of failure.
C. the test results of intended objectives.
D. the evaluation and analysis of reliability.

Correct Answer: C
Explanation:
Control effectiveness requires a process to verify that the control process worked as intended. Examples such as dual-control or dual-entry bookkeeping provide verification and assurance that the process operated as intended. The type of control is not relevant, and notification of failure is not determinative of control strength. Reliability is not an indication of control strength; weak controls can be highly reliable, even if they are ineffective controls.

QUESTION 217
When residual risk is minimized:

A. acceptable risk is probable.
B. transferred risk is acceptable.
C. control risk is reduced.
D. risk is transferable.

Correct Answer: A
Explanation:
Since residual risk is the risk that remains after putting into place an effective risk management