The lack of change management is a severe omission and will greatly increase information security risk. Since procedures are generally nonauthoritative, their lack of enforcement is not a primary concern. Systems that are developed by third-party vendors are becoming commonplace and do not represent an increase in security risk as much as poor change management. Poor capacity management may not necessarily represent a security risk.

QUESTION 153
A successful risk management program should lead to:

A. optimization of risk reduction efforts against cost.
B. containment of losses to an annual budgeted amount.
C. identification and removal of all man-made threats.
D. elimination or transference of all organizational risks.

Correct Answer: A
Explanation:
Successful risk management should lead to a breakeven point of risk reduction and cost. The other options listed are not achievable. Threats cannot be totally removed or transferred, while losses cannot be budgeted in advance with absolute certainty.

QUESTION 154
The PRIMARY purpose of using risk analysis within a security program is to:

A. justify the security expenditure.
B. help businesses prioritize the assets to be protected.
C. inform executive management of residual risk value.
D. assess exposures and plan remediation.

Correct Answer: D
Explanation:
Risk analysis explores the degree to which an asset needs protecting so this can be managed effectively. Risk analysis indirectly supports the security expenditure, but justifying the security expenditure is not its primary purpose. Helping businesses prioritize the assets to be protected is an indirect benefit of risk analysis, but not its primary purpose. Informing executive management of residual risk value is not directly relevant.

QUESTION 155
Which of the following attacks is BEST mitigated by utilizing strong passwords?

A. Man-in-the-middle attack
B. Brute force attack
C. Remote buffer overflow
D. Root kit

Correct Answer: B
Explanation:
A brute force attack is normally successful against weak passwords, whereas strong passwords would not prevent any of the other attacks. Man-in-the-middle attacks intercept network traffic, which could contain passwords, but is not naturally password-protected. Remote buffer overflows rarely require a password to exploit a remote host. Root kits hook into the operating system's kernel and, therefore, operate underneath any authentication mechanism.

QUESTION 156
The MOST important function of a risk management program is to:

A. quantify overall risk.
B. minimize residual risk.
C. eliminate inherent risk.
D. maximize the sum of all annualized loss expectancies (ALEs).

Correct Answer: B
Explanation:
A risk management program should minimize the amount of risk that cannot be otherwise eliminated or transferred; this is the residual risk to the organization. Quantifying overall risk is important but not as critical as the end result. Eliminating inherent risk is virtually impossible. Maximizing the sum of all ALEs is actually the opposite of what is desirable.

QUESTION 157
Which of the following would BEST address the risk of data leakage?

A. File backup procedures
B. Database integrity checks
C. Acceptable use policies
D. Incident response procedures

Correct Answer: C
Explanation:
Acceptable use policies are the best measure for preventing the unauthorized disclosure of confidential information. The other choices do not address confidentiality of information.

QUESTION 158
Which of the following is the MOST usable deliverable of an information security risk analysis?

A. Business impact analysis (BIA) report
B. List of action items to mitigate risk
C. Assignment of risks to process owners
D. Quantification of organizational risk

Correct Answer: B
Explanation:
Although all of these are important, the list of action items is used to reduce or transfer the current level of risk. The other options materially contribute to the way the actions are implemented.

QUESTION 159
Which of the following groups would be in the BEST position to perform a risk analysis for a business?

A. External auditors
B. A peer group within a similar business
C. Process owners
D. A specialized management consultant

Correct Answer: C
Explanation:
Process owners have the most in-depth knowledge of risks and compensating controls within their environment. External parties do not have that level of detailed knowledge on the inner workings of the business. Management consultants are expected to have the necessary skills in risk analysis techniques but are still less effective than a group with intimate knowledge of the business.

QUESTION 160
A risk management program would be expected to:

A. remove all inherent risk.
B. maintain residual risk at an acceptable level.
C. implement preventive controls for every threat.
D. reduce control risk to zero.

Correct Answer: B
Explanation:
The object of risk management is to ensure that all residual risk is maintained at a level acceptable to the business; it is not intended to remove every identified risk or implement controls for every threat since this may not be cost-effective. Control risk, i.e., that a control may not be effective, is a component of the program but is unlikely to be reduced to zero.

QUESTION 161
Which would be one of the BEST metrics an information security manager can employ to effectively evaluate the results of a security program?

A. Number of controls implemented
B. Percent of control objectives accomplished
C. Percent of compliance with the security policy
D. Reduction in the number of reported security incidents

Correct Answer: B
Explanation:
Control objectives are directly related to business objectives; therefore, they would be the best metrics. Number of controls implemented does not have a direct relationship with the results of a security program. Percentage of compliance with the security policy and reduction in the number of security incidents are not as broad as choice B.

QUESTION 162
A business impact analysis (BIA) is the BEST tool for calculating:

A. total cost of ownership.
B. priority of restoration.
C. annualized loss expectancy (ALE).
D. residual risk.

Correct Answer: B
Explanation:
A business impact analysis (BIA) is the best tool for calculating the priority of restoration for applications. It is not used to determine total cost of ownership, annualized loss expectancy (ALE) or residual risk to the organization.

QUESTION 163
When performing an information risk analysis, an information security manager should FIRST:

A. establish the ownership of assets.
B. evaluate the risks to the assets.
C. take an asset inventory.
D. categorize the assets.

Correct Answer: C
Explanation:
Assets must be inventoried before any of the other choices can be performed.

QUESTION 164
The decision on whether new risks should fall under periodic or event-driven reporting should be based on which of the following?

A. Mitigating controls
B. Visibility of impact
C. Likelihood of occurrence
D. Incident frequency

Correct Answer: B
Explanation:
Visibility of impact is the best measure since it manages risks to an organization in the timeliest manner. Likelihood of occurrence and incident frequency are not as relevant. Mitigating controls is not a determining factor on incident reporting.

QUESTION 165
A risk analysis should:

A. include a benchmark of similar companies in its scope.
B. assume an equal degree of protection for all assets.
C. address the potential size and likelihood of loss.
D. give more weight to the likelihood vs. the size of the loss.

Correct Answer: C
Explanation:
A risk analysis should take into account the potential size and likelihood of a loss. It could include comparisons with a group of companies of similar size. It should not assume an equal degree of protection for all assets since assets may have different risk factors. The likelihood of the loss should not receive greater emphasis than the size of the loss; a risk analysis should always address both equally.

QUESTION 166
The PRIMARY goal of a corporate risk management program is to ensure that an organization's:

A. IT assets in key business functions are protected.
B. business risks are addressed by preventive controls.
C. stated objectives are achievable.
D. IT facilities and systems are always available.

Correct Answer: C
Explanation:
Risk management's primary goal is to ensure an organization maintains the ability to achieve its objectives. Protecting IT assets is one possible goal as well as ensuring infrastructure and systems availability. However, these should be put in the perspective of achieving an organization's objectives. Preventive controls are not always possible or necessary; risk management will address issues with an appropriate mix of preventive and corrective controls.

QUESTION 167
A project manager is developing a developer portal and requests that the security manager assign a public IP address so that it can be accessed by in-house staff and by external consultants outside the organization's local area network (LAN). What should the security manager do FIRST?

A. Understand the business requirements of the developer portal
B. Perform a vulnerability assessment of the developer portal
C. Install an intrusion detection system (IDS)
D. Obtain a signed nondisclosure agreement (NDA) from the external consultants before allowing external access to the server

Correct Answer: A
Explanation:
The information security manager cannot make an informed decision about the request without first understanding the business requirements of the developer portal. Performing a vulnerability assessment of developer portal and installing an intrusion detection system (IDS) are best practices but are subsequent to understanding the requirements. Obtaining a signed nondisclosure agreement will not take care of the risks inherent in the organization's application.

QUESTION 168
The impact of losing frame relay network connectivity for 18-24 hours should be calculated using the:

A. hourly billing rate charged by the carrier.
B. value of the data transmitted over the network.
C. aggregate compensation of all affected business users.
D. financial losses incurred by affected business units.

Correct Answer: D
Explanation:
The bottom line on calculating the impact of a loss is what its cost will be to the organization. The other choices are all factors that contribute to the overall monetary impact.

QUESTION 169
A risk assessment should be conducted:

A. once a year for each business process and subprocess.
B. every three to six months for critical business processes.
C. by external parties to maintain objectivity.
D. annually or whenever there is a significant change.

Correct Answer: D