1)A risk assessment and business impact analysis (BIA) have been completed for a major proposed purchase and new process for an organization. There is disagreement between the information security manager and the business department manager who will be responsible for evaluating the results and identified risk. Which of the following would be the BEST approach of the information security manager?

A: Acceptance of the business manager’s decision on the risk to the corporation

B: Acceptance of the information security manager’s decision on the risk to the corporation

C: Review of the risk assessment with executive management for final input

D: Create a new risk assessment and BIA to resolve the disagreement

2) Who is accountable for ensuring that information is categorized and that specific protective measures are taken?

A: The security officer

B: Senior management

C: The end user

D: The custodian

3)Abnormal server communication from inside the organization to external parties may be monitored to:

A: record the trace of advanced persistent threats

B: evaluate the process resiliency of server operations

C: verify the effectiveness of an intrusion detection system

D: support a nonrepudiation framework in e-commerce

4)Which of the following authentication methods prevents authentication replay?

A: Password hash implementation

B: Challenge/response mechanism

C: Wired equivalent privacy encryption usage

D: Hypertext Transfer Protocol basic authentication

5)IT-related risk management activities are MOST effective when they are:

A: treated as a distinct process

B: conducted by the IT department

C: integrated within business processes

D: communicated to all employees

6) Which of the following is the BEST way to detect an intruder who successfully penetrates a network before significant damage is inflicted?

A: Perform periodic penetration testing

B: Establish minimum security baselines

C: Implement vendor default settings

D: Install a honeypot on the network

7) Which of the following presents the GREATEST threat to the security of an enterprise resource planning (ERP) system?

A: User ad hoc reporting is not logged

B: Network traffic is through a single switch

C: Operating system security patches have not been applied

D: Database security defaults to ERP settings

8)In a social engineering scenario, which of the following will MOST likely reduce the likelihood of an unauthorized individual gaining access to computing resources?

A: Implementing on-screen masking of passwords

B: Conducting periodic security awareness programs

C: Increasing the frequency of password changes

D: Requiring that passwords be kept strictly confidential

9) The postincident review of a security incident revealed that there was a process that was not monitored. As a result monitoring functionality has been implemented. Which of the following may BEST be expected from this remediation?

A: Reduction in total incident duration

B: Increase in risk tolerance

C: Improvement in identific

D: Facilitation of escalation

10)To determine how a security breach occurred on the corporate network, a security manager looks at the logs of various devices. Which of the following BEST facilitates the correlation and review of these logs?

A: Database server

B: Domain name server

C: Time server

D: Proxy server