- **Vendor:** Isaca
- **Exam Code:** CISM
- **Exam Name:** Certified Information Security Manager
- **New Updated Questions from Braindump2go (Updated in April/2022)**

QUESTION 1603
An information security team has been tasked with identifying confidential data within the organization to formalize its asset classification scheme. The MOST relevant input would be provided by:

A. the chief information officer (CIO),
B. the legal department.
C. database administrators (DBAs).
D. business process owners.

Answer: D

QUESTION 1604
Which of the following is MOST important to have in place to effectively manage security incidents that could potentially escalate to disasters?

A. Alignment of incident management activities with business continuity and disaster recovery plans
B. Senior management commitment to funding the disaster recovery program
C. Well-defined disaster recovery time and recovery point objectives (RTOs and RPOs)
D. An incident response team with a clear understanding of their roles and responsibilities

Answer: A

QUESTION 1605
An organization is going through a digital transformation process, which places the IT organization in an unfamiliar risk landscape. The information security manager has been tasked with leading the IT risk management process. Which of the following should be given the HIGHEST priority?

A. Analysis of control gaps
B. Identification of risk
C. Design of key risk indicators (KRIs)
D. Selection of risk treatment options

Answer: B

QUESTION 1606
An information security manager has noticed a large number of security policy exceptions have been approved by business unit leaders. Which of the following would be the BEST course of action to address this situation?

A. Provide security awareness training to business unit leaders more frequently.

B. Ensure that business unit leaders are aware of the relevant risk.
C. Report the exceptions as a security incident.
D. Revise the security policy to accommodate the exceptions

Answer: B

QUESTION 1607
An information security manager has discovered that a business unit is planning on implementing a new application and has not engaged anyone from the information security department. Which of the following is the BEST course of action?

A. Block the application from going into production.
B. Discuss the issue with senior leadership.
C. Recommend involvement with the change manager.
D. Review and update the change management process

Answer: B

QUESTION 1608
Which of the following is the MOST significant advantage of developing a well-defined information security strategy?

A. Support for buy-in from organizational employees
B. Prevention of deviations from risk tolerance thresholds
C. Allocation of resources to highest priorities
D. Increased maturity of incident response processes

Answer: C

QUESTION 1609
Which of the following BEST enables the deployment of consistent security throughout international branches within a multinational organization?

A. Decentralization of security governance
B. Maturity of security processes
C. Establishment of security governance
D. Remediation of audit findings

Answer: C

QUESTION 1610
What is the PRIMARY benefit of effective configuration management?

A. Improved vulnerability management
B. Standardization of system support
C. Decreased risk to the organization's systems
D. Reduced frequency of incidents

Answer: A

QUESTION 1611
An information security manager wants to improve the ability to identify changes in risk levels affecting the organization's systems. Which of the following is the BEST method to achieve this objective?

A. Monitoring key risk indicators (KRIs)

B. Monitoring key goal indicators (KGIs)
C. Updating the risk register
D. Performing business impact analyses (BIA)

Answer: A

QUESTION 1612
Which of the following BEST enables successful identification of a potential IT security incident?

A. Event correlation
B. File integrity monitoring
C. Network intrusion detection systems (NIDS)
D. Configuration management standards

Answer: A

QUESTION 1613
Which of the following architectures for e-business BEST ensures high availability?

A. Availability of an adjacent hot site and a standby server with mirrored copies of critical data
B. A single point of entry allowing transactions to be received and processed quickly
C. Intelligent middleware to direct transactions from a downed system to an alternative
D. Automatic failover to the web site of another e-business that meets the user's needs

Answer: D

QUESTION 1614
Who should be PRIMARILY responsible for defining a security asset classification scheme?

A. Legal counsel
B. Information security manager
C. Network security manager
D. Business unit manager

Answer: A

QUESTION 1615
An information security manager has recently been notified of potential security risks associated with a third-party service provider. What should be done NEXT to address this concern?

A. Conduct a risk analysis
B. Conduct a vulnerability analysis
C. Escalate to the chief risk officer
D. Determine compensating controls

Answer: A

QUESTION 1616
Which of the following is the MOST important issue in a penetration test?

A. Having a defined goal as well as success and failure criteria
B. Performing the test without the benefit of any insider knowledge
C. Obtaining permission from audit
D. Having an independent group perform the test

Answer: A

QUESTION 1617
Which of the following controls would BEST help to detect a targeted attack exploiting a zero-day vulnerability?

A. Vulnerability scanning
B. Antivirus protection
C. Sandbox emulation
D. Intrusion prevention system (IPS)

Answer: A

QUESTION 1618
What is the PRIMARY objective of triage within the incident response process?

A. Timely reporting of incidents
B. Containment of incidents
C. Optimization of resources
D. Determination of incident impact

Answer: C

QUESTION 1619
Who should an information security manager contact FIRST upon discovering that a cloud-based payment system used by the organization may be infected with malware?

A. Cloud service provider
B. The incident response team
C. Affected customers
D. Senior management

Answer: B

QUESTION 1620
Which of the following is the MOST important consideration when presenting objectives and benefits of an information security program to nontechnical stakeholders?

A. Using technical terms
B. Using measurable terms
C. Using financial metrics
D. Using business terms

Answer: D

QUESTION 1621
Which of the following types of controls would be MOST important to implement when digitizing human resource (HR) records?

A. Project management controls
B. Change management controls
C. Software development controls
D. Access management controls

Answer: B

QUESTION 1622
Which of the following is the MOST effective method of determining security priorities?

A. Gap analysis
B. Impact analysis
C. Vulnerability assessment
D. Threat assessment

Answer: B

QUESTION 1623
An email digital signature will:

A. prevent unauthorized modification of an email message.
B. protect the confidentiality of an email message.
C. automatically correct unauthorized modification of an email message.
D. verify to recipients the integrity of an email message.

Answer: A

QUESTION 1624
Which of the following should be established FIRST when implementing an information security governance framework?

A. Security incident management team
B. Security policies
C. Security awareness training program
D. Security architecture

Answer: D

QUESTION 1625
Which of the following is the MOST effective way to protect the authenticity of data in transit?

A. Digital signature
B. Hash value
C. Public key
D. Private key

Answer: B

QUESTION 1626
Information security policies should PRIMARILY reflect:

A. industry best practices.
B. compliance requirements,
C. data security standards.
D. senior management intent.

Answer: D

QUESTION 1627

Which is MOST important to identify when developing an effective information security strategy?

A. Compliance requirements
B. Control gaps that require remediation
C. Potential savings resulting from security governance
D. Business assets to be secured

Answer: B

QUESTION 1628
Which of the following is the MAIN reason for integrating an organization's incident response plan with its business continuity process?

A. Integration of the plan will reduce resource costs to the organization.
B. Incidents will be reported more timely when categorized as a disaster.
C. Recovery time objectives (RTOs) need to be determined.
D. Incidents can escalate into disasters needing proper response.

Answer: D

QUESTION 1629
The business advantage of implementing authentication tokens is that they:

A. reduce overall cost.
B. improve access security.
C. provide nonrepudiation.
D. reduce administrative workload.

Answer: B

QUESTION 1630
An IT department is evaluating a new cloud backup service to support the human resources (HR) department. Which of the following is the information security manager's MOST important action prior to contract execution?

A. Ensure HR data is encrypted prior to sending it to the cloud vendor.
B. Review the risk with HR executives.
C. Evaluate the cloud vendor's information security program.
D. Complete a compliance risk assessment.

Answer: C

QUESTION 1631
The MAIN purpose of incorporating social media monitoring into the information security program is to:

A. gauge public opinion of the company.
B. assess employee adherence to policy.
C. detect potential information disclosure.
D. identify disgruntled employees.

Answer: B

QUESTION 1632
When implementing information security in system development projects, which of the following is the MOST effective approach for an information security manager with limited resources?

A. Reviewing security requirements prior to development
B. Presenting security requirements during project planning
C. Embedding a representative in business projects
D. Assigning resources based on the business impact

Answer: B

QUESTION 1633
Which of the following is the BEST method to protect consumer private information for an online public website?

A. Encrypt consumer's data in transit and at rest.
B. Use secure encrypted transport layer.
C. Apply a masking policy to the consumer data.
D. Apply strong authentication to online account

Answer: A

QUESTION 1634
The MOST useful technique for maintaining management support for the information security program is:

A. identifying the risks and consequences of failure to comply with standards.
B. benchmarking the security programs of comparable organizations.
C. implementing a comprehensive security awareness and training program.
D. informing management about the security of business operations.

Answer: D

QUESTION 1635
The PRIMARY reason for using metrics as part of an information security program is to help management:

A. determine whether objectives are being met.
B. develop an information security baseline.
C. visualize security trends.
D. track financial impact of the program.

Answer: A

QUESTION 1636
Which of the following is the MOST important objective of testing a security incident response plan?

A. Ensure the thoroughness of the response plan.
B. Confirm that systems are recovered in the proper order.
C. Validate the business impact analysis (BIA).
D. Verify the response assumptions are valid

Answer: D

QUESTION 1637
What is the PRIMARY objective of assigning classifications to information assets?

A. Maintain an accurate IT asset inventory.
B. Identify business owners and information custodians.
C. Identify appropriate levels of protection.

D. Demonstrate compliance with regulatory requirements

Answer: C

QUESTION 1638
Which of the following would BEST enable an information security manager to provide monthly status on the health of the information security environment to senior management?

A. Key performance indicators (KPIs)
B. Key risk indicators (KRIs)
C. Internal audits
D. Key control assessments

Answer: A

QUESTION 1639
Which of the following BEST facilitates the monitoring of risk across an organization?

A. Risk appetite trends
B. Penetration testing
C. Key risk indicators (KRIs)
D. Threat assessments

Answer: C

QUESTION 1640
The fundamental purpose of establishing security metrics is to:

A. increase return on investment (ROI).
B. adopt security best practices.
C. provide feedback on control effectiveness,
D. establish security benchmarks

Answer: C

QUESTION 1641
After isolating a system compromised in a security incident, which of the following should be the PRIMARY objective of the information security team?

A. Preserving the integrity of incident-related data
B. Identifying the type of threat that compromised the system
C. Implementing improvements to prevent recurrence of the incident
D. Providing response actions to restore the compromised system

Answer: D

QUESTION 1642
Which of the following is the PRIMARY role of the information security manager in application development? To ensure:

A. enterprise security controls are implemented.
B. compliance with industry best practice.
C. security is integrated into the system development life cycle (SDLC).
D. control procedures address business risk.

Answer: C

QUESTION 1643
Which of the following is MOST important to ensuring an incident response team has the necessary authorization to perform its role?

A. Senior management representation on the team
B. Legal counsel representation on the team
C. Approved job descriptions outlining member responsibilities
D. A charter endorsed by the security steering committee

Answer: D

QUESTION 1644
An information security manager is planning to purchase a mobile device management (MDM) system to manage personal devices used by employees to access corporate email. Which of the following is MOST important to include in the business case?

A. Cost-benefit analysis
B. Industry best practice benchmarking results
C. Identified risks and mitigating controls
D. Information security-related metrics

Answer: A

QUESTION 1645
Which of the following is MOST helpful in securing funding for a commercial vulnerability assessment tool?

A. Presenting a vulnerability scan report for current business systems
B. Developing security metrics linked to business objectives
C. Explaining the business value of vulnerability remediation
D. Identifying applicable legal and regulatory requirements

Answer: C

QUESTION 1646
Which of the following is an information security manager's BEST course of action to gain approval for investment in a technical control?

A. Conduct a business impact analysis (BIA).
B. Calculate the exposure factor.
C. Perform a cost-benefit analysis.
D. Conduct a risk assessment.

Answer: C

QUESTION 1647
Which of the following is the MOST important reason to involve external forensics experts in evidence collection when responding to a major security breach?

A. To validate the incident response process
B. To prevent evidence from being disclosed to any internal staff members
C. To ensure evidence is handled by qualified resources
D. To provide the response team with expert training on evidence handling

Answer: C

QUESTION 1648
Which of the following BEST indicates that an organization can respond to incidents in a timely manner?

A. The organization conducts walk-through exercises for incident response.
B. The incident response plan has been endorsed by management.
C. Adequate financial resources are available for the response team.
D. No audit issues were identified with the incident response plan.

Answer: A

QUESTION 1649
Which of the following BEST supports the incident management process for attacks on an organization's supply chain?

A. Performing integration testing with vendor systems
B. Establishing communication paths with vendors
C. Requiring security awareness training for vendor staff
D. Including service level agreements (SLAs) in vendor contracts

Answer: D

QUESTION 1650
Which of the following is a potential indicator of inappropriate Internet use by staff?

A. Increased reports of slow system performance
B. Increased number of weaknesses from vulnerability scans
C. Increased help desk calls for password resets
D. Reduced number of pings on firewalls

Answer: A

QUESTION 1651
Which of the following is a PRIMARY function of an incident response team?

A. To provide a business impact analysis (BIA)
B. To provide a risk assessment for zero-day vulnerabilities
C. To provide effective incident mitigation
D. To provide a single point of contact for critical incidents

Answer: C

QUESTION 1652
In a call center, the BEST reason to conduct a social-engineering exercise is to:

A. gain funding for information security initiatives.
B. improve password policy.
C. minimize the likelihood of successful attacks.
D. identify candidates for additional security training

Answer: C

QUESTION 1653

Which of the following will BEST enhance the privacy of data in transit for an online transaction system?

A. Masking sensitive data
B. Requiring two-factor authentication
C. Using a secure communications protocol
D. Requiring a digital signature

Answer: C

QUESTION 1654
A CEO requires that information security risk management is practiced at the organizational level through a central risk register. Which of the following is the MOST important reason to report a summary of this risk register to the board?

A. To ensure alignment with industry standards and trends
B. To facilitate alignment between risk management and organizational objectives
C. To comply with the organization's regulatory and legal requirements
D. To ensure adequate funding is available for risk management and mitigation

Answer: B

QUESTION 1655
An organization has decided to conduct a postmortem analysis after experiencing a loss from an information security attack. The PRIMARY purpose of this analysis should be to:

A. update information security policies.
B. evaluate the impact.
C. document lessons learned.
D. prepare for criminal prosecution.

Answer: C

QUESTION 1656
Which of the following would be MOST useful when illustrating to senior management the status of a recently implemented information security governance framework?

A. A maturity model
B. A threat assessment
C. A risk assessment
D. Periodic testing results

Answer: D

QUESTION 1657
Which of the following metrics BEST demonstrates the effectiveness of an organization's security awareness strategy?

A. Trends in mean time to resolution of security incidents
B. Number of security incidents reported to the help desk
C. Pass rate of knowledge assessments completed after end user security training
D. Percentage of end user computers and devices infected with malware

Answer: B

QUESTION 1658
Which of the following should be the PRIMARY consideration when developing an incident response plan?

A. Management support
B. Previously reported incidents
C. The definition of an incident
D. Compliance with regulations

Answer: C

QUESTION 1659
Which of the following reports would provide the BEST overview of the progress of an information security program to senior management?

A. Inventory of information technology security controls
B. Heat map of the current risk landscape
C. Results of the last penetration test
D. Key performance indicators (KPIs) related to security initiatives

Answer: B

QUESTION 1660
The information security team has determined an additional security solution is needed to enhance the organization's security posture.
What should the information security manager do NEXT to move forward with this initiative?

A. Proceed with vendor selection.
B. Evaluate available products.
C. Initiate vendor due-diligence.
D. Create a business case.

Answer: D

QUESTION 1661
Management has expressed concern that they are not kept fully informed of key information security risks associated with the organization.
Which of the following should be done FIRST to address this concern?

A. Determine the desired metrics and develop a reporting schedule.
B. Provide a report on information security industry trends and benchmarks.
C. Prepare a presentation on information security initiatives for management
D. Develop an ongoing risk and security awareness training program for management.

Answer: A

QUESTION 1662
Which of the following is the BEST method to ensure compliance with password standards?

A. Using password-cracking software
B. Implementing password-synchronization software
C. A user-awareness program
D. Automated enforcement of password syntax rules

Answer: D

QUESTION 1663

Which of the following information security metrics would be MOST meaningful to executive management in assessing the effectiveness of the information security strategy?

A. Monthly cost of maintaining information security controls
B. Monthly cost of interruptions in core processes due to security incidents
C. Percentage of systems that are patched within the required time period
D. Number of information security policy violations reported quarterly

Answer: B

QUESTION 1664
A regulatory compliance issue has been identified in a critical business application, but remediating the issue would significantly impact
business operations. What information would BEST enable senior management to make an informed decision?

A. Industry benchmarks and best practices
B. Costs associated with compensating controls
C. Risk assessment results and recommendations
D. Impact analysis and treatment option

Answer: C

QUESTION 1665
Which of the following is the MOST important factor to be considered when reviewing an information security strategy?

A. Frequency of security incidents
B. Benchmarking to industry peers
C. Evolving business goals
D. Unmitigated risk

Answer: C

QUESTION 1666
For event logs to be acceptable for incident investigation, which of the following is MOST important to implement on all systems to establish a proper trail of evidence?

A. Source confidentiality
B. Event data integrity
C. Time synchronization
D. Access to the logs

Answer: D

QUESTION 1667
The PRIMARY purpose of establishing an information security governance framework should be to:

A. establish the business case for strategic integration of information security in organizational efforts.
B. align corporate governance, activities, and investments to information security goals.
C. align information security strategy and investments to support organizational activities.
D. document and communicate how the information security program functions within the organization.

Answer: C

QUESTION 1668
\Which of the following is MOST important to emphasize when presenting cyber attack information to gain Senior management support for control enhancements?

A. Recent cyber attacks in the same industry sector
B. Control gaps within defense-in-depth architecture
C. Impacts to the business
D. Threats against internal systems

Answer: C

QUESTION 1669
Which of the following is MOST important to determine before developing information security program metrics?

A. Who will use the metrics
B. How performance will be reported
C. Who will own the metrics
D. How the data will be collected

Answer: A

QUESTION 1670
Fingerprint biometrics are BEST used for:

A. identification,
B. authorization,
C. access control.
D. authentication.

Answer: C

QUESTION 1671
In which cloud model does the cloud service buyer assume the MOST security responsibility?

A. Platform as a Service (PaaS)
B. Infrastructure as a Service (laaS)
C. Software as a Service (SaaS)
D. Disaster Recovery as a Service (DRaasS)

Answer: A

QUESTION 1672
Which of the following is the BEST indicator of an organization's information security status?

A. Controls audit
B. Penetration test
C. Threat analysis
D. Intrusion detection log analysis

Answer: A

QUESTION 1673
Which of the following is the GREATEST concern with employees investigating and responding to security breaches

they report'?

A. Segregation of duty violations
B. Loss of business productivity
C. Evidence contamination
D. Loss of confidential information

Answer: C

QUESTION 1674
Which of the following is the MOST effective way to address an organization's security concerns during contract negotiations with a third party?

A. Ensure security is involved in the procurement process.
B. Communicate security policy with the third-party vender.
C. Conduct an information security audit on the third-party vendor.
D. Review the third-party contract with the organization's legal department.

Answer: A

QUESTION 1675
An organization has contracted with a third-party e-commerce provider. VVhich of the following is MOST important for the information security managerto examine during the subsequent compliance review period?

A. Changes to the provider's controls and infrastructure
B. Right-to-audit provisions in the contract
C. Adherence to the service level agreement
D. Financial provisions and maintenance expenses

Answer: A

QUESTION 1676
The likelihood of a successful intrusion is a function of

A. value and desirability to the intruder.
B. threat and vulnerability levels.
C. configuration and maintenance of log monitoring system.
D. opportunity and asset value.

Answer: B

QUESTION 1677
What is the FIRST line of defense against criminal insider activities?

A. Signing security agreements by critical personnel
B. Monitoring employee activities
C. Validating the integrity of personnel
D. stringent and enforced access controls

Answer: D

QUESTION 1678
A business manager has decided not to implement a control based on the risk assessment of a mission-critical business application because of its impact on performance. What is the information security manager's BEST course of

action'?

A. Instruct the business managerto implement the mitigation control.
B. Update the organization's risk profile.
C. Escalate the issue to senior management for a final decision.
D. Recommend possible compensating controls.

Answer: D

QUESTION 1679
A newly appointed information security manager has been asked to update all security-related policies and procedures that have been Static for five years or more. What is the BEST next step?

A. To update in accordance with the best business practices
B. To assess corporate culture
C. To perform a risk assessment of the current IT environment
D. To gain an understanding of the current business direction

Answer: C

QUESTION 1680
Which of the following is the GREATEST benefit of conducting an organization-wide security awareness program?

A. More security incidents are detected.
B. The security strategy is promoted.
C. Fewer security incidents are reported.
D. Security behavior is improved.

Answer: A

QUESTION 1681
An organization wants to integrate information security into its human resource management processes. Which of the following should be the FIRST step?

A. Benchmark the processes with best practice to identify gaps.
B. Assess the business objectives of the processes.
C. Identify information security risk associated with the processes.
D. Evaluate the cost of information security integration.

Answer: B

QUESTION 1682
An organization that uses external cloud services extensively is concerned with risk monitoring and timely response. The BEST way to address this concern is to ensure:

A. a right-to-audit clause is included in contracts.
B. the availability of continuous technical support.
C. internal security standards are in place.
D. appropriate service level agreements (SLAs) are in place.

Answer: D

QUESTION 1683
Which of the following should an information security manager perform FIRST when an organization's residual risk has

increased?

A. Communicate the information to senior management.
B. Transfer the risk to third parties.
C. Implement security measures to reduce the risk.
D. Assess the business impact.

Answer: D

QUESTION 1684
Determining the risk for a particular threat/vulnerability pair before controls are applied can be expressed as:

A. the magnitude of the impact, should a threat exploit a vulnerability.
B. a function of the likelihood and impact, should a threat exploit a vulnerability.
C. a function of the cost and effectiveness of controls over a vulnerability.
D. the likelihood of a given threat attempting to exploit a vulnerability,

Answer: B

QUESTION 1685
Which of the following is MOST important to the effectiveness of an information security steering committee?

A. The committee has strong regulatory knowledge.
B. The committee has cross-organizational representation.
C. The committee has strong representation from IT.
D. The committee is driven by industry best practices.

Answer: B

QUESTION 1686
An organization engages 4 third-party vendor to monitor and support a financial application under scrutiny by regulators. Maintaining strict data integrity and confidentiality for this application is critical to the business. Which of the following controls would MOST effectively manage risk to the organization?

A. Implementing periodic access reviews of vendor employees
B. Disabling vendor access and only re-enabling when access is needed
C. Activating access and data logging
D. Implementing segregation of duties between systems and data

Answer: C

QUESTION 1687
Which of the following is the MOST important consideration during a forensics investigation?

A. Chain of custody
B. Disclosure requirements
C. Management directives
D. Evidence hardening

Answer: A

QUESTION 1688
The information security manager of a multinational organization has been asked to consolidate the information security policies of its regional locations. Which of the following would be of GREATEST concern?

A. Disparate reporting lines
B. Varying threat environments
C. Conflicting legal requirements
D. Differences in work culture

Answer: C

QUESTION 1689
Which of the following is the PRIMARY advantage of using an incident severity rating system'?

A. It enables risk information to be updated.
B. It provides senior management with visibility to the criticality.
C. It allows the detection of an incident as it is occurring.
D. It enables efficient incident response.

Answer: D

QUESTION 1690
Which of the following will BEST facilitate informed decision making when presenting an information security risk assessment report to senior management?

A. Utilizing color coding to indicate risk impacts to the business
B. Prioritizing residual risks
C. Benchmarking risk assessment results
D. Presenting risk assessment results regularly

Answer: A

QUESTION 1691
When outsourcing application development to a third party, which of the following is the BEST way to ensure the organization's security requirements are met?

A. Perform independent security testing of the developed applications
B. Include a right to audit the system development lifecycle in the contract.
C. Require the third-party provider to document its security methodology.
D. Provide training in secure application coding to the third-party staff.

Answer: A

QUESTION 1692
Which of the following is MOST important to include when developing a business case for information security resources?

A. Gap analysis
B. Senior management input
C. Risk assessment
D. Cost-benefit analysis

Answer: D

QUESTION 1693
Embedding security responsibilities into jab descriptions is important PRIMARILY because it

A. supports access management.
B. strengthens employee accountability.
C. aligns security to the human resources function.
D. simplifies development of the security awareness program.

Answer: B

QUESTION 1694
Which of the following is the FIRST step in developing a business continuity plan (BCPY}?

A. Determine the business recovery strategy.
B. Identify the applications with the shortest recovery time objectives (RTOs).
C. Determine available resources.
D. Identify critical business processes.

Answer: D

QUESTION 1695
What is the BEST way to reduce the impact of a successful ransomware attack?

A. Purchase or renew cyber insurance policies.
B. Mionitor the network and provide alerts on intrusions.
C. Perform frequent backups and store them offline.
D. Include provisions to pay ransoms in the information security budget.

Answer: D

QUESTION 1696
Which of the following should be the PRIMARY outcome of an information security program?

A. Strategic alignment
B. Cost reduction
C. Threat reduction
D. Risk elimination

Answer: A

QUESTION 1697
Recovery time objectives (RTOs) are BEST determined by

A. executive management.
B. business continuity officers.
C. database administrators.
D. business managers.

Answer: D

QUESTION 1698
Which of the following is the MOST important consideration when selecting members for an information security steering committee?

A. Business expertise
B. Cross-functional composition
C. Tenure in the organization

D. Information security expertise

Answer: B

QUESTION 1699
Which of the following is the MOST effective mechanism for communicating risk status and trends to senior management?

A. Threat assessment
B. Key risk indicators (KRIs)
C. Business impact analysis (BIA)
D. Risk assessment

Answer: B

QUESTION 1700
Which of the following is the MOST significant contributor to the effectiveness of an incident response plan?

A. Defined key performance indicators (KPIs)
B. Sufficient financial resources
C. Incident response team experience
D. Regular tabletop exercises

Answer: D

QUESTION 1701
Which of the following activities MUST be performed by an information security manager for change requests?

A. Scan IT systems for operating system vulnerabilities.
B. Perform penetration testing on affected system.
C. Assess impact on information security risk.
D. Review change in business requirements for information security.

Answer: D

QUESTION 1702
An information security manager should begin a business continuity planning (BCP) process by:

A. defining the recovery point objectives (RPOs).
B. Identifying alternative processing sites.
C. performing a business impact analysis (BIA).
D. defining the business objectives

Answer: C

QUESTION 1703
Which of the following processes BEST supports the evaluation of incident response effectiveness?

A. Root cause analysis
B. Incident logging
C. Postincident review
D. Chain of custody

Answer: A