ISACA CISM

Certified Information Security Manager

Practice Exam Questions

Table of Contents

About the CISM Certification

ISACA's Certified Information Security Manager (CISM) certification indicates expertise in information security governance, program development and management, incident management and risk management. A CISM certification proves your expertise in these work-related domains:

- Information Security Governance
- Information Security Risk Management
- Information Security Program
- Incident Management

CISM Exam Content Outline

CISM validates your expertise in the four work-related domains listed below that are applicable across industry verticals:

- Information Security Governance – 17%
- Information Security Risk Management – 20%
- Information Security Program – 33%
- Incident Management – 33%

The CISM job practice consists of task and knowledge statements, organized by domains. The CISM exam contains 150 questions and covers four information security management areas. The job practice areas and statements represent a job practice analysis of the work performed by information security managers as validated by prominent industry leaders, subject matter experts, and industry practitioners.

Below are the key domains, subtopics and tasks candidates will be tested:

1	Information Security Governance
A	Enterprise Governance
1A1	Organizational Culture
1A2	Legal, Regulatory, and Contractual Requirements
1A3	Organizational Structures, Roles, and Responsibilities
B	Information Security Strategy
1B1	Information Security Strategy Development
1B2	Information Governance Frameworks and Standards
1B3	Strategic Planning (e.g. budgets, resources, business case)
2	Information Security Risk Management
A	Information Security Risk Assessment
2A1	Emerging Risk and Threat Landscape
2A2	Vulnerability and Control Deficiency Analysis
2A3	Risk Assessment and Analysis
B	Information Security Risk Response
2B1	Risk Treatment / Risk Response Options
2B2	Risk and Control Ownership
2B3	Risk Monitoring and Reporting
3	Information Security Program

A	Information Security Program Development
3A1	Information Security Program Resources (e.g. people, tools, technologies)
3A2	Information Asset Identification and Classification
3A3	Industry Standards and Frameworks for Information Security
3A4	Information Security Policies, Procedures, and Guidelines
3A5	Information Security Program Metrics
B	Information Security Program Management
3B1	Information Security Control Design and Selection
3B2	Information Security Control Implementation and Integrations
3B3	Information Security Control Testing and Evaluation
3B4	Information Security Awareness and Training
3B5	Management of External Services (e.g. providers, suppliers, third parties, fourth parties)
3B6	Information Security Program Communications and Reporting
4	Incident Management
A	Incident Management Readiness
4A1	Incident Response Plan
4A2	Business Impact Analysis (BIA)
4A3	Business Continuity Plan (BCP)
4A4	Disaster Recovery Plan (DRP)
4A5	Incident Classification/Categorization
4A6	Incident Management Training, Testing, and Evaluation
B	Incident Management Operations
4B1	Incident Management Tools and Techniques
4B2	Incident Investigation and Evaluation
4B3	Incident Containment Methods
4B4	Incident Response Communications (e.g. reporting, notification, escalation)
4B5	Incident Eradication and Recovery
4B6	Post-incident Review Practices

Secondary Classifications

Supporting Tasks

- Identify internal and external influences to the organization that impact the information security strategy.
- Establish and/or maintain an information security strategy in alignment with organizational goals and objectives.
- Establish and/or maintain an information security governance framework.
- Integrate information security governance into corporate governance.
- Establish and maintain information security policies to guide the development of standards, procedures, and guidelines.
- Develop business cases to support investments in information security.
- Gain ongoing commitment from senior leadership and other stakeholders to support the successful implementation of the information security strategy.
- Define, communicate, and monitor information security responsibilities throughout the organization and lines of authority.
- Compile and present reports to key stakeholders on the activities, trends, and overall effectiveness of the information security program.
- Evaluate and report information security metrics to key stakeholders.

- Establish and/or maintain the information security program in alignment with the information security strategy.
- Align the information security program with the operational objectives of other business functions.
- Establish and maintain information security processes and resources to execute the information security program.
- Establish, communicate, and maintain organizational information security policies, standards, guidelines, procedures, and other documentation.
- Establish, promote, and maintain a program for information security awareness and training.
- Integrate information security requirements into organizational processes to maintain the organization’s security strategy.
- Integrate information security requirements into contracts and activities of external parties.
- Monitor external parties' adherence to established security requirements.
- Define and monitor management and operational metrics for the information security program.
- Establish and/or maintain a process for information asset identification and classification.
- Identify legal, regulatory, organizational, and other applicable compliance requirements.
- Participate in and/or oversee the risk identification, risk assessment, and risk treatment process.
- Participate in and/or oversee the vulnerability assessment and threat analysis process.
- Identify, recommend, or implement appropriate risk treatment and response options to manage risk to acceptable levels based on organizational risk appetite.
- Determine whether information security controls are appropriate and effectively manage risk to an acceptable level.
- Facilitate the integration of information risk management into business and IT processes.
- Monitor for internal and external factors that may require reassessment of risk.
- Report on information security risk, including noncompliance and changes in information risk, to key stakeholders to facilitate the risk management decision-making process.
- Establish and maintain an incident response plan, in alignment with the business continuity plan and disaster recovery plan.
- Establish and maintain an information security incident classification and categorization process.
- Develop and implement processes to ensure the timely identification of information security incidents.
- Establish and maintain processes to investigate and document information security incidents in accordance with legal and regulatory requirements.
- Establish and maintain incident handling process, including containment, notification, escalation, eradication, and recovery.
- Organize, train, equip, and assign responsibilities to incident response teams.
- Establish and maintain incident communication plans and processes for internal and external parties.
- Evaluate incident management plans through testing and review, including table-top exercises, checklist review, and simulation testing at planned intervals.
- Conduct post-incident reviews to facilitate continuous improvement, including root-cause analysis, lessons learned, corrective actions, and reassessment of risk.

About the Exam Questions

This document contains 631 sample CISM exam questions.

Questions are broken down into the following sections:

- Information Security Governance
- Information Risk Management
- Information Security Program Development
- Information Security Program Management
- Incident Management and Response

The last page of this guide contains an answer sheet you can print off and use for tracking your answers to each question.

The answers to each question along with explanations can be found in the accompanying Answer Guide.

Topic 1: Information Security Governance

QUESTION 1
Which of the following should be the FIRST step in developing an information security plan?

A. Perform a technical vulnerabilities assessment
B. Analyze the current business strategy
C. Perform a business impact analysis
D. Assess the current levels of security awareness

QUESTION 2
Senior management commitment and support for information security can BEST be obtained through presentations that:

A. Use illustrative examples of successful attacks
B. Explain the technical risks to the organization
C. Evaluate the organization against best security practices
D. Tie security risks to key business objectives

QUESTION 3
The MOST appropriate role for senior management in supporting information security is the:

A. Evaluation of vendors offering security products
B. Assessment of risks to the organization
C. Approval of policy statements and funding
D. Monitoring adherence to regulatory requirements

QUESTION 4
Which of the following would BEST ensure the success of information security governance within an organization?

A. Steering committees approve security projects
B. Security policy training provided to all managers
C. Security training available to all employees on the intranet
D. Steering committees enforce compliance with laws and regulations

QUESTION 5
Information security governance is PRIMARILY driven by:

A. Technology constraints
B. Regulatory requirements
C. Litigation potential
D. Business strategy

QUESTION 6
Which of the following represents the MAJOR focus of privacy regulations?

A. Unrestricted data mining
B. Identity theft
C. Human rights protection
D. Identifiable personal data

QUESTION 7
Investments in information security technologies should be based on:

A. Vulnerability assessments
B. Value analysis
C. Business climate
D. Audit recommendations

QUESTION 8
Retention of business records should PRIMARILY be based on:

A. Business strategy and direction
B. Regulatory and legal requirements
C. Storage capacity and longevity
D. Business case and value analysis

QUESTION 9
Which of the following is characteristic of centralized information security management?

A. More expensive to administer
B. Better adherence to policies
C. More aligned with business unit needs
D. Faster turnaround of requests

QUESTION 10
Successful implementation of information security governance will FIRST require:

A. Security awareness training
B. Updated security policies
C. A computer incident management team
D. A security architecture

QUESTION 11
Which of the following individuals would be in the BEST position to sponsor the creation of an information security steering group?

A. Information security manager
B. Chief operating officer (COO)
C. Internal auditor
D. Legal counsel

QUESTION 12
The MOST important component of a privacy policy is:

A. Notifications
B. Warranties
C. Liabilities
D. Geographic coverage

QUESTION 13
The cost of implementing a security control should not exceed the:

A. Annualized loss expectancy
B. Cost of an incident
C. Asset value
D. Implementation opportunity costs

QUESTION 14
When a security standard conflicts with a business objective, the situation should be resolved by:

A. Changing the security standard
B. Changing the business objective
C. Performing a risk analysis
D. Authorizing a risk acceptance

QUESTION 15
Minimum standards for securing the technical infrastructure should be defined in a security:

A. Strategy
B. Guidelines
C. Model
D. Architecture

QUESTION 16
Which of the following is MOST appropriate for inclusion in an information security strategy?

A. Business controls designated as key controls
B. Security processes, methods, tools and techniques
C. Firewall rule sets, network defaults and intrusion detection system (IDS) settings
D. Budget estimates to acquire specific security tools

QUESTION 17
Senior management commitment and support for information security will BEST be attained by an information security manager by emphasizing:

A. Organizational risk
B. Organization wide metrics
C. Security needs
D. The responsibilities of organizational units

QUESTION 18
Which of the following roles would represent a conflict of interest for an information security manager?

A. Evaluation of third parties requesting connectivity
B. Assessment of the adequacy of disaster recovery plans
C. Final approval of information security policies
D. Monitoring adherence to physical security controls

QUESTION 19
Which of the following situations must be corrected FIRST to ensure successful information security governance within an organization?

A. The information security department has difficulty filling vacancies
B. The chief information officer (CIO) approves security policy changes
C. The information security oversight committee only meets quarterly
D. The data center manager has final signoff on all security projects

QUESTION 20
Which of the following requirements would have the lowest level of priority in information security?

A. Technical
B. Regulatory
C. Privacy
D. Business

QUESTION 21
When an organization hires a new information security manager, which of the following goals should this individual pursue FIRST?

A. Develop a security architecture
B. Establish good communication with steering committee members
C. Assemble an experienced staff
D. Benchmark peer organizations

QUESTION 22
It is MOST important that information security architecture be aligned with which of the following?

A. Industry best practices
B. Information technology plans
C. Information security best practices
D. Business objectives and goals

QUESTION 23
Which of the following is MOST likely to be discretionary?

A. Policies
B. Procedures
C. Guidelines
D. Standards

QUESTION 24
Security technologies should be selected PRIMARILY on the basis of their:

A. Ability to mitigate business risks
B. Evaluations in trade publications
C. Use of new and emerging technologies
D. Benefits in comparison to their costs

QUESTION 25
Which of the following are seldom changed in response to technological changes?

A. Standards
B. Procedures
C. Policies
D. Guidelines

QUESTION 26
The MOST important factor in planning for the long-term retention of electronically stored business records is to take into account potential changes in:

A. Storage capacity and shelf life
B. Regulatory and legal requirements
C. Business strategy and direction
D. Application systems and media

QUESTION 27
Which of the following is characteristic of decentralized information security management across a geographically dispersed organization?

A. More uniformity in quality of service
B. Better adherence to policies
C. Better alignment to business unit needs
D. More savings in total operating costs

QUESTION 28
Which of the following is the MOST appropriate position to sponsor the design and implementation of a new security infrastructure in a large global enterprise?

A. Chief security officer (CSO)
B. Chief operating officer (COO)
C. Chief privacy officer (CPO)
D. Chief legal counsel (CLC)

QUESTION 29
Which of the following would be the MOST important goal of an information security governance program?

A. Review of internal control mechanisms
B. Effective involvement in business decision making
C. Total elimination of risk factors
D. Ensuring trust in data

QUESTION 30
Relationships among security technologies are BEST defined through which of the following?

A. Security metrics
B. Network topology
C. Security architecture
D. Process improvement models

QUESTION 31
A business unit intends to deploy a new technology in a manner that places it in violation of existing information security standards. What immediate action should an information security manager take?

A. Enforce the existing security standard
B. Change the standard to permit the deployment
C. Perform a risk analysis to quantify the risk
D. Perform research to propose use of a better technology

QUESTION 32
Acceptable levels of information security risk should be determined by:

A. Legal counsel
B. Security management
C. External auditors
D. The steering committee

QUESTION 33
The PRIMARY goal in developing an information security strategy is to:

A. Establish security metrics and performance monitoring
B. Educate business process owners regarding their duties
C. Ensure that legal and regulatory requirements are met
D. Support the business objectives of the organization

QUESTION 34
Senior management commitment and support for information security can BEST be enhanced through:

A. A formal security policy sponsored by the chief executive officer (CEO)
B. Regular security awareness training for employees
C. Periodic review of alignment with business management goals
D. Senior management signoff on the information security strategy

QUESTION 35
When identifying legal and regulatory issues affecting information security, which of the following would represent the BEST approach to developing information security policies?

A. Create separate policies to address each regulation
B. Develop policies that meet all mandated requirements
C. Incorporate policy statements provided by regulators
D. Develop a compliance risk assessment

QUESTION 36
Which of the following MOST commonly falls within the scope of an information security governance steering committee?

A. Interviewing candidates for information security specialist positions
B. Developing content for security awareness programs
C. Prioritizing information security initiatives
D. Approving access to critical financial systems

QUESTION 37
Which of the following is the MOST important factor when designing information security architecture?

A. Technical platform interfaces
B. Scalability of the network
C. Development methodologies
D. Stakeholder requirements

QUESTION 38
Which of the following characteristics is MOST important when looking at prospective candidates for the role of chief information security officer (CISO)?

A. Knowledge of information technology platforms, networks and development methodologies
B. Ability to understand and map organizational needs to security technologies
C. Knowledge of the regulatory environment and project management techniques
D. Ability to manage a diverse group of individuals and resources across an organization

QUESTION 39
Which of the following are likely to be updated MOST frequently?

A. Procedures for hardening database servers
B. Standards for password length and complexity
C. Policies addressing information security governance
D. Standards for document retention and destruction

QUESTION 40
Who should be responsible for enforcing access rights to application data?

A. Data owners
B. Business process owners
C. The security steering committee
D. Security administrators

QUESTION 41
The chief information security officer (CISO) should ideally have a direct reporting relationship to the:

A. Head of internal audit
B. Chief operations officer (COO)
C. Chief technology officer (CTO)
D. Legal counsel

QUESTION 42
Which of the following is the MOST essential task for a chief information security officer (CISO) to perform?

A. Update platform-level security settings
B. Conduct disaster recovery test exercises
C. Approve access to critical financial systems
D. Develop an information security strategy paper

QUESTION 43
Developing a successful business case for the acquisition of information security software products can BEST be assisted by:

A. Assessing the frequency of incidents
B. Quantifying the cost of control failures
C. Calculating return on investment (ROI) projections
D. Comparing spending against similar organizations

QUESTION 44
When an information security manager is developing a strategic plan for information security, the timeline for the plan should be:

A. Aligned with the IT strategic plan
B. Based on the current rate of technological change
C. Three-to-five years for both hardware and software
D. Aligned with the business strategy

QUESTION 45
Which of the following is the MOST important information to include in a strategic plan for information security?

A. Information security staffing requirements
B. Current state and desired future state
C. IT capital investment requirements
D. Information security mission statement

QUESTION 46
Information security projects should be prioritized on the basis of:

A. Time required for implementation
B. Impact on the organization
C. Total cost for implementation
D. Mix of resources required

QUESTION 47
Which of the following is the MOST important information to include in an information security standard?

A. Creation date
B. Author name
C. Initial draft approval date
D. Last review date

QUESTION 48
Which of the following would BEST prepare an information security manager for regulatory reviews?

A. Assign an information security administrator as regulatory liaison
B. Perform self-assessments using regulatory guidelines and reports
C. Assess previous regulatory reports with process owners' input
D. Ensure all regulatory inquiries are sanctioned by the legal department

QUESTION 49
An information security manager at a global organization that is subject to regulation by multiple governmental jurisdictions with differing requirements should:

A. Bring all locations into conformity with the aggregate requirements of all governmental jurisdictions
B. Establish baseline standards for all locations and add supplemental standards as required
C. Bring all locations into conformity with a generally accepted set of industry best practices
D. Establish a baseline standard incorporating those requirements that all jurisdictions have in common

QUESTION 50
Which of the following BEST describes an information security manager's role in a multidisciplinary team that will address a new regulatory requirement regarding operational risk?

A. Ensure that all IT risks are identified
B. Evaluate the impact of information security risks
C. Demonstrate that IT mitigating controls are in place
D. Suggest new IT controls to mitigate operational risk

QUESTION 51
From an information security manager perspective, what is the immediate benefit of clearly-defined roles and responsibilities?

A. Enhanced policy compliance
B. Improved procedure flows
C. Segregation of duties
D. Better accountability

QUESTION 52
An internal audit has identified major weaknesses over IT processing. Which of the following should an information security manager use to BEST convey a sense of urgency to management?

A. Security metrics reports
B. Risk assessment reports
C. Business impact analysis (BIA)
D. Return on security investment report

QUESTION 53
Reviewing which of the following would BEST ensure that security controls are effective?

A. Risk assessment policies
B. Return on security investment
C. Security metrics
D. User access rights

QUESTION 54
Which of the following is responsible for legal and regulatory liability?

A. Chief security officer (CSO)
B. Chief legal counsel (CLC)
C. Board and senior management
D. Information security steering group

QUESTION 55
While implementing information security governance an organization should FIRST:

A. Adopt security standards
B. Determine security baselines
C. Define the security strategy
D. Establish security policies

QUESTION 56
The MOST basic requirement for an information security governance program is to:

A. Be aligned with the corporate business strategy
B. Be based on a sound risk management approach
C. Provide adequate regulatory compliance
D. Provide best practices for security initiatives

QUESTION 57
Information security policy enforcement is the responsibility of the:

A. Security steering committee
B. Chief information officer (CIO)
C. Chief information security officer (CISO)
D. Chief compliance officer (CCO)

QUESTION 58
A good privacy statement should include:

A. Notification of liability on accuracy of information
B. Notification that information will be encrypted
C. What the company will do with information it collects
D. A description of the information classification process

QUESTION 59
Which of the following would be MOST effective in successfully implementing restrictive password policies?

A. Regular password audits
B. Single sign-on system
C. Security awareness program
D. Penalties for noncompliance

QUESTION 60
When designing an information security quarterly report to management, the MOST important element to be considered should be the:

A. Information security metrics
B. Knowledge required to analyze each issue
C. Linkage to business area objectives
D. Baseline against which metrics are evaluated

QUESTION 61
An information security manager at a global organization has to ensure that the local information security program will initially ensure compliance with the:

A. Corporate data privacy policy
B. Data privacy policy where data is collected
C. Data privacy policy of the headquarters' country
D. Data privacy directive applicable globally

QUESTION 62
A new regulation for safeguarding information processed by a specific type of transaction has come to the attention of an information security officer. The officer should FIRST:

A. Meet with stakeholders to decide how to comply
B. Analyze key risks in the compliance process
C. Assess whether existing controls meet the regulation
D. Update the existing security/privacy policy

QUESTION 63
The PRIMARY objective of a security steering group is to:

A. Ensure information security covers all business functions
B. Ensure information security aligns with business goals
C. Raise information security awareness across the organization
D. Implement all decisions on security management across the organization

QUESTION 64
Data owners must provide a safe and secure environment to ensure confidentiality, integrity and availability of the transaction. This is an example of an information security:

A. Baseline
B. Strategy
C. Procedure
D. Policy

QUESTION 65
At what stage of the application development process should the security department initially become involved?

A. When requested
B. At testing
C. At programming
D. At detail requirements

QUESTION 66
A security manager is preparing a report to obtain the commitment of executive management to a security program. Inclusion of which of the following would be of MOST value?

A. Examples of genuine incidents at similar organizations
B. Statement of generally accepted best practices
C. Associating realistic threats to corporate objectives
D. Analysis of current technological exposures

QUESTION 67
The PRIMARY concern of an information security manager documenting a formal data retention policy would be:

A. Generally accepted industry best practices
B. Business requirements
C. Legislative and regulatory requirements
D. Storage availability

QUESTION 68
When personal information is transmitted across networks, there MUST be adequate controls over:

A. Change management
B. Privacy protection
C. Consent to data transfer
D. Encryption devices

QUESTION 69
An organization's information security processes are currently defined as ad hoc. In seeking to improve their performance level, the next step for the organization should be to:

A. Ensure that security processes are consistent across the organization
B. Enforce baseline security levels across the organization
C. Ensure that security processes are fully documented
D. Implement monitoring of key performance indicators for security processes

QUESTION 70
Who in an organization has the responsibility for classifying information?

A. Data custodian
B. Database administrator
C. Information security officer
D. Data owner

QUESTION 71
What is the PRIMARY role of the information security manager in the process of information classification within an organization?

A. Defining and ratifying the classification structure of information assets
B. Deciding the classification levels applied to the organization's information assets
C. Securing information assets in accordance with their classification
D. Checking if information assets have been classified properly

QUESTION 72
Logging is an example of which type of defense against systems compromise?

A. Containment
B. Detection
C. Reaction
D. Recovery

QUESTION 73
Which of the following is MOST important in developing a security strategy?

A. Creating a positive business security environment
B. Understanding key business objectives
C. Having a reporting line to senior management
D. Allocating sufficient resources to information security

QUESTION 74
Who is ultimately responsible for the organization's information?

A. Data custodian
B. Chief information security officer (CISO)
C. Board of directors
D. Chief information officer (CIO)

QUESTION 75
Which of the following factors is a PRIMARY driver for information security governance that does not require any further justification?

A. Alignment with industry best practices
B. Business continuity investment
C. Business benefits
D. Regulatory compliance

QUESTION 76
A security manager meeting the requirements for the international flow of personal data will need to ensure:

A. A data processing agreement
B. A data protection registration
C. The agreement of the data subjects
D. Subject access procedures

QUESTION 77
An information security manager mapping a job description to types of data access is MOST likely to adhere to which of the following information security principles?

A. Ethics
B. Proportionality
C. Integration
D. Accountability

QUESTION 78
Which of the following is the MOST important prerequisite for establishing information security management within an organization?

A. Senior management commitment
B. Information security framework
C. Information security organizational structure
D. Information security policy

QUESTION 79
What will have the HIGHEST impact on standard information security governance models?

A. Number of employees
B. Distance between physical locations
C. Complexity of organizational structure
D. Organizational budget

QUESTION 80
In order to highlight to management the importance of integrating information security in the business processes, a newly hired information security officer should FIRST:

A. Prepare a security budget
B. Conduct a risk assessment
C. Develop an information security policy
D. Obtain benchmarking information

QUESTION 81
Temporarily deactivating some monitoring processes, even if supported by an acceptance of operational risk, may not be acceptable to the information security manager if:

A. It implies compliance risks
B. Short-term impact cannot be determined
C. It violates industry security practices
D. Changes in the roles matrix cannot be detected

QUESTION 82
An outcome of effective security governance is:

A. Business dependency assessment
B. Strategic alignment
C. Risk assessment
D. Planning

QUESTION 83
How would an information security manager balance the potentially conflicting requirements of an international organization's security standards and local regulation?

A. Give organization standards preference over local regulations
B. Follow local regulations only
C. Make the organization aware of those standards where local regulations causes conflicts
D. Negotiate a local version of the organization standards

QUESTION 84
Who should drive the risk analysis for an organization?

A. Senior management
B. Security manager
C. Quality manager
D. Legal department

QUESTION 85
The FIRST step in developing an information security management program is to:

A. Identify business risks that affect the organization
B. Clarify organizational purpose for creating the program
C. Assign responsibility for the program
D. Assess adequacy of controls to mitigate business risks

QUESTION 86
Which of the following is the MOST important to keep in mind when assessing the value of information?

A. The potential financial loss
B. The cost of recreating the information
C. The cost of insurance coverage
D. Regulatory requirement

QUESTION 87
What would a security manager PRIMARILY utilize when proposing the implementation of a security solution?

A. Risk assessment report
B. Technical evaluation report
C. Business case
D. Budgetary requirements

QUESTION 88
To justify its ongoing security budget, which of the following would be of MOST use to the information security department?

A. Security breach frequency
B. Annualized loss expectancy (ALE)
C. Cost-benefit analysis
D. Peer group comparison

QUESTION 89
Which of the following situations would MOST inhibit the effective implementation of security governance:

A. The complexity of technology
B. Budgetary constraints
C. Conflicting business priorities
D. High-level sponsorship

QUESTION 90
To achieve effective strategic alignment of security initiatives, it is important that:

A. Steering committee leadership be selected by rotation
B. Inputs be obtained and consensus achieved between the major organizational units
C. The business strategy be updated periodically
D. Procedures and standards be approved by all departmental heads

QUESTION 91
What would be the MOST significant security risk when using wireless local area network (WLAN) technology?

A. Man-in-the-middle attack
B. Spoofing of data packets
C. Rogue access point
D. Session hijacking

QUESTION 92
When developing incident response procedures involving servers hosting critical applications, which of the following should be the FIRST to be notified?

A. Business management
B. Operations manager
C. Information security manager
D. System users

QUESTION 93
In implementing information security governance, the information security manager is PRIMARILY responsible for:

A. Developing the security strategy
B. Reviewing the security strategy
C. Communicating the security strategy
D. Approving the security strategy

QUESTION 94
An information security strategy document that includes specific links to an organization's business activities is PRIMARILY an indicator of:

A. Performance measurement
B. Integration
C. Alignment
D. Value delivery

QUESTION 95
When an organization is setting up a relationship with a third-party IT service provider, which of the following is one of the MOST important topics to include in the contract from a security standpoint?

A. Compliance with international security standards
B. Use of a two-factor authentication system
C. Existence of an alternate hot site in case of business disruption
D. Compliance with the organization's information security requirements

QUESTION 96
To justify the need to invest in a forensic analysis tool, an information security manager should FIRST:

A. Review the functionalities and implementation requirements of the solution
B. Review comparison reports of tool implementation in peer companies
C. Provide examples of situations where such a tool would be useful
D. Substantiate the investment in meeting organizational needs

QUESTION 97
The MOST useful way to describe the objectives in the information security strategy is through:

A. Attributes and characteristics of the “desired state”
B. Overall control objectives of the security program
C. Mapping the IT systems to key business processes
D. Calculation of annual loss expectations

QUESTION 98
In order to highlight to management the importance of network security, the security manager should FIRST:

A. Develop a security architecture
B. Install a network intrusion detection system (NIDS) and prepare a list of attacks
C. Develop a network security policy
D. Conduct a risk assessment

QUESTION 99
When developing an information security program, what is the MOST useful source of information for determining available resources?

A. Proficiency test
B. Job descriptions
C. Organization chart
D. Skills inventory

QUESTION 100
The MOST important characteristic of good security policies is that they:

A. State expectations of IT management
B. State only one general security mandate
C. Are aligned with organizational goals
D. Govern the creation of procedures and guidelines

QUESTION 101
An information security manager must understand the relationship between information security and business operations in order to:

A. Support organizational objectives
B. Determine likely areas of noncompliance
C. Assess the possible impacts of compromise
D. Understand the threats to the business

QUESTION 102
The MOST effective approach to address issues that arise between IT management, business units and security management when implementing a new security strategy is for the information security manager to:

A. Escalate issues to an external third party for resolution
B. Ensure that senior management provides authority for security to address the issues
C. Insist that managers or units not in agreement with the security solution accept the risk
D. Refer the issues to senior management along with any security recommendations

QUESTION 103
Obtaining senior management support for establishing a warm site can BEST be accomplished by:

A. Establishing a periodic risk assessment
B. Promoting regulatory requirements
C. Developing a business case
D. Developing effective metrics

QUESTION 104
Which of the following would be the BEST option to improve accountability for a system administrator who has security functions?

A. Include security responsibilities in the job description
B. Require the administrator to obtain security certification
C. Train the system administrator on penetration testing and vulnerability assessment
D. Train the system administrator on risk assessment

QUESTION 105
Which of the following is the MOST important element of an information security strategy?

A. Defined objectives
B. Time frames for delivery
C. Adoption of a control framework
D. Complete policies

QUESTION 106
A multinational organization operating in fifteen countries is considering implementing an information security program. Which factor will MOST influence the design of the Information security program?

A. Representation by regional business leaders
B. Composition of the board
C. Cultures of the different countries
D. IT security skills

QUESTION 107
Which of the following is the BEST justification to convince management to invest in an information security program?

A. Cost reduction
B. Compliance with company policies
C. Protection of business assets
D. Increased business value

QUESTION 108
On a company's e-commerce web site, a good legal statement regarding data privacy should include:

A. A statement regarding what the company will do with the information it collects
B. A disclaimer regarding the accuracy of information on its web site
C. Technical information regarding how information is protected
D. A statement regarding where the information is being hosted

QUESTION 109
The MOST important factor in ensuring the success of an information security program is effective:

A. Communication of information security requirements to all users in the organization
B. Formulation of policies and procedures for information security
C. Alignment with organizational goals and objectives
D. Monitoring compliance with information security policies and procedures

QUESTION 110
Which of the following would be MOST helpful to achieve alignment between information security and organization objectives?

A. Key control monitoring
B. A robust security awareness program
C. A security program that enables business activities
D. An effective security architecture

QUESTION 111
Which of the following BEST contributes to the development of a security governance framework that supports the maturity model concept?

A. Continuous analysis, monitoring and feedback
B. Continuous monitoring of the return on security investment (ROSI)
C. Continuous risk reduction
D. Key risk indicator (KRI) setup to security management processes

QUESTION 112
The MOST complete business case for security solutions is one that:

A. Includes appropriate justification
B. Explains the current risk profile
C. Details regulatory requirements
D. Identifies incidents and losses

QUESTION 113
Which of the following is MOST important to understand when developing a meaningful information security strategy?

A. Regulatory environment
B. International security standards
C. Organizational risks
D. Organizational goals

QUESTION 114
Which of the following is an advantage of a centralized information security organizational structure?

A. It is easier to promote security awareness
B. It is easier to manage and control
C. It is more responsive to business unit needs
D. It provides a faster turnaround for security requests

QUESTION 115
Which of the following would help to change an organization's security culture?

A. Develop procedures to enforce the information security policy
B. Obtain strong management support
C. Implement strict technical security controls
D. Periodically audit compliance with the information security policy

QUESTION 116
The BEST way to justify the implementation of a single sign-on (SSO) product is to use:

A. Return on investment (ROI)
B. A vulnerability assessment
C. Annual loss expectancy (ALE)
D. A business case

QUESTION 117
The FIRST step in establishing a security governance program is to:

A. Conduct a risk assessment
B. Conduct a workshop for all end users
C. Prepare a security budget
D. Obtain high-level sponsorship

QUESTION 118
An IS manager has decided to implement a security system to monitor access to the Internet and prevent access to numerous sites. Immediately upon installation, employees flood the IT helpdesk with complaints of being unable to perform business functions on Internet sites. This is an example of:

A. Conflicting security controls with organizational needs
B. Strong protection of information resources
C. Implementing appropriate controls to reduce risk
D. Proving information security's protective abilities

QUESTION 119
An organization's information security strategy should be based on:

A. Managing risk relative to business objectives
B. Managing risk to a zero level and minimizing insurance premiums
C. Avoiding occurrence of risks so that insurance is not required
D. Transferring most risks to insurers and saving on control costs

QUESTION 120
Which of the following should be included in an annual information security budget that is submitted for management approval?

A. A cost-benefit analysis of budgeted resources
B. All of the resources that are recommended by the business
C. Total cost of ownership (TCO)
D. Baseline comparisons

QUESTION 121
Which of the following is a benefit of information security governance?

A. Reduction of the potential for civil or legal liability
B. Questioning trust in vendor relationships
C. Increasing the risk of decisions based on incomplete management information
D. Direct involvement of senior management in developing control processes

QUESTION 122
Investment in security technology and processes should be based on:

A. Clear alignment with the goals and objectives of the organization
B. Success cases that have been experienced in previous projects
C. Best business practices
D. Safeguards that are inherent in existing technology

QUESTION 123
The data access requirements for an application should be determined by the:

A. Legal department
B. Compliance officer
C. Information security manager
D. Business owner

QUESTION 124
From an information security perspective, information that no longer supports the main purpose of the business should be:

A. Analyzed under the retention policy
B. Protected under the information classification policy
C. Analyzed under the backup policy
D. Protected under the business impact analysis (BIA)

QUESTION 125
The organization has decided to outsource the majority of the IT department with a vendor that is hosting servers in a foreign country. Of the following, which is the MOST critical security consideration?

A. Laws and regulations of the country of origin may not be enforceable in the foreign country
B. A security breach notification might get delayed due to the time difference
C. Additional network intrusion detection sensors should be installed, resulting in an additional cost
D. The company could lose physical control over the server and be unable to monitor the physical security posture of the servers

QUESTION 126
Effective IT governance is BEST ensured by:

A. Utilizing a bottom-up approach
B. Management by the IT department
C. Referring the matter to the organization's legal department
D. Utilizing a top-down approach

QUESTION 127
The FIRST step to create an internal culture that focuses on information security is to:

A. Implement stronger controls
B. Conduct periodic awareness training
C. Actively monitor operations
D. Gain the endorsement of executive management

QUESTION 128
Which of the following is the BEST method or technique to ensure the effective implementation of an information security program?

A. Obtain the support of the board of directors
B. Improve the content of the information security awareness program
C. Improve the employees' knowledge of security policies
D. Implement logical access controls to the information systems

QUESTION 129
When an organization is implementing an information security governance program, its board of directors should be responsible for:

A. Drafting information security policies
B. Reviewing training and awareness programs
C. Setting the strategic direction of the program
D. Auditing for compliance

QUESTION 130
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 own the process regarding the results and the assigned 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 assessment with executive management for final input
D. A new risk assessment and BIA are needed to resolve the disagreement

QUESTION 131
Who is responsible 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

QUESTION 132
An organization's board of directors has learned of recent legislation requiring organizations within the industry to enact specific safeguards to protect confidential customer information. What actions should the board take next?

A. Direct information security on what they need to do
B. Research solutions to determine the proper solutions
C. Require management to report on compliance
D. Nothing; information security does not report to the board

QUESTION 133
Information security should be:

A. Focused on eliminating all risks
B. A balance between technical and business requirements
C. Driven by regulatory requirements
D. Defined by the board of directors

QUESTION 134
What is the MOST important factor in the successful implementation of an enterprise-wide information security program?

A. Realistic budget estimates
B. Security awareness
C. Support of senior management
D. Recalculation of the work factor

QUESTION 135
What is the MAIN risk when there is no user management representation on the Information Security Steering Committee?

A. Functional requirements are not adequately considered
B. User training programs may be inadequate
C. Budgets allocated to business units are not appropriate
D. Information security plans are not aligned with business requirements

QUESTION 136
The MAIN reason for having the Information Security Steering Committee review a new security controls implementation plan is to ensure that:

A. The plan aligns with the organization's business plan
B. Departmental budgets are allocated appropriately to pay for the plan
C. Regulatory oversight requirements are met
D. The impact of the plan on the business units is reduced

QUESTION 137
Which of the following should be determined while defining risk management strategies?

A. Risk assessment criteria
B. Organizational objectives and risk appetite
C. IT architecture complexity
D. Enterprise disaster recovery plans

QUESTION 138
When implementing effective security governance within the requirements of the company's security strategy, which of the following is the MOST important factor to consider?

A. Preserving the confidentiality of sensitive data
B. Establishing international security standards for data sharing
C. Adhering to corporate privacy standards
D. Establishing system manager responsibility for information security

QUESTION 139
Which of the following is the BEST reason to perform a business impact analysis (BIA)?

A. To help determine the current state of risk
B. To budget appropriately for needed controls
C. To satisfy regulatory requirements
D. To analyze the effect on the business

Topic 2: Information Risk Management

QUESTION 140
A risk mitigation report would include recommendations for:

A. Assessment
B. Acceptance
C. Evaluation
D. Quantification

QUESTION 141
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

QUESTION 142
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

QUESTION 143
Which of the following BEST indicates a successful risk management practice?

A. Overall risk is quantified
B. Inherent risk is eliminated
C. Residual risk is minimized
D. Control risk is tied to business units

QUESTION 144
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

QUESTION 145
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

QUESTION 146
Which of the following will BEST protect an organization from internal security attacks?

A. Static IP addressing
B. Internal address translation
C. Prospective employee background checks
D. Employee awareness certification program

QUESTION 147
For risk management purposes, the value of an asset should be based on:

A. Original cost
B. Net cash flow
C. Net present value
D. Replacement cost

QUESTION 148
In a business impact analysis, the value of an information system should be based on the overall cost:

A. Of recovery
B. To recreate
C. If unavailable
D. Of emergency operations

QUESTION 149
Acceptable risk is achieved when:

A. Residual risk is minimized
B. Transferred risk is minimized
C. Control risk is minimized
D. Inherent risk is minimized

QUESTION 150
The value of information assets is BEST determined by:

A. Individual business managers
B. Business systems analysts
C. Information security management
D. Industry averages benchmarking

QUESTION 151
During which phase of development is it MOST appropriate to begin assessing the risk of a new application system?

A. Feasibility
B. Design
C. Development
D. Testing

QUESTION 152
The MOST effective way to incorporate risk management practices into existing production systems is through:

A. Policy development
B. Change management
C. Awareness training
D. Regular monitoring

QUESTION 153
Which of the following would be MOST useful in developing a series of recovery time objectives (RTOs)?

A. Gap analysis
B. Regression analysis
C. Risk analysis
D. Business impact analysis

QUESTION 154
The recovery time objective (RTO) is reached at which of the following milestones?

A. Disaster declaration
B. Recovery of the backups
C. Restoration of the system
D. Return to business-as-usual processing

QUESTION 155
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

QUESTION 156
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

QUESTION 157
Risk acceptance is a component of which of the following?

A. Assessment
B. Mitigation
C. Evaluation
D. Monitoring

QUESTION 158
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

QUESTION 159
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

QUESTION 160
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)

QUESTION 161
Which of the following risks would BEST be assessed using qualitative risk assessment techniques?

A. Theft of purchased software
B. Power outage lasting 24 hours
C. Permanent decline in customer confidence
D. Temporary loss of e-mail due to a virus attack

QUESTION 162
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

QUESTION 163
In performing a risk assessment on the impact of losing a server, the value of the server should be calculated using the:

A. Original cost to acquire
B. Cost of the software stored
C. Annualized loss expectancy (ALE)
D. Cost to obtain a replacement

QUESTION 164
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

QUESTION 165
When residual risk is minimized:

A. Acceptable risk is probable
B. Transferred risk is acceptable
C. Control risk is reduced
D. Risk is transferable

QUESTION 166
Quantitative risk analysis is MOST appropriate when assessment data:

A. Include customer perceptions
B. Contain percentage estimates
C. Do not contain specific details
D. Contain subjective information

QUESTION 167
Which of the following is the MOST appropriate use of gap analysis?

A. Evaluating a business impact analysis (BIA)
B. Developing a balanced business scorecard
C. Demonstrating the relationship between controls
D. Measuring current state vs. desired future state

QUESTION 168
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

QUESTION 169
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

QUESTION 170
The recovery point objective (RPO) requires which of the following?

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

QUESTION 171
Based on the information provided, which of the following situations presents the GREATEST information security risk for an organization with multiple, but small, domestic processing locations?

A. Systems operation procedures are not enforced
B. Change management procedures are poor
C. Systems development is outsourced
D. Systems capacity management is not performed

QUESTION 172
Which of the following BEST describes the scope of risk analysis?

A. Key financial systems
B. Organizational activities
C. Key systems and infrastructure
D. Systems subject to regulatory compliance

QUESTION 173
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

QUESTION 174
Which of the following is the PRIMARY reason for implementing a risk management program?

A. Allows the organization to eliminate risk
B. Is a necessary part of management's due diligence
C. Satisfies audit and regulatory requirements
D. Assists in incrementing the return on investment (ROI)

QUESTION 175
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

QUESTION 176
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

QUESTION 177
Which of the following risks would BEST be assessed using quantitative risk assessment techniques?

A. Customer data stolen
B. An electrical power outage
C. A web site defaced by hackers
D. Loss of the software development team

QUESTION 178
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

QUESTION 179
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

QUESTION 180
Ongoing tracking of remediation efforts to mitigate identified risks can BEST be accomplished through the use of which of the following?

A. Tree diagrams
B. Venn diagrams
C. Heat charts
D. Bar charts

QUESTION 181
Who would be in the BEST position to determine the recovery point objective (RPO) for business applications?

A. Business continuity coordinator
B. Chief operations officer (COO)
C. Information security manager
D. Internal audit

QUESTION 182
Which two components PRIMARILY must be assessed in an effective risk analysis?

A. Visibility and duration
B. Likelihood and impact
C. Probability and frequency
D. Financial impact and duration

QUESTION 183
Information security managers should use risk assessment techniques to:

A. Justify selection of risk mitigation strategies
B. Maximize the return on investment (ROI)
C. Provide documentation for auditors and regulators
D. Quantify risks that would otherwise be subjective

QUESTION 184
In assessing risk, it is MOST essential to:

A. Provide equal coverage for all asset types
B. Use benchmarking data from similar organizations
C. Consider both monetary value and likelihood of loss
D. Focus primarily on threats and recent business losses

QUESTION 185
When the computer incident response team (CIRT) finds clear evidence that a hacker has penetrated the corporate network and modified customer information, an information security manager should FIRST notify:

A. The information security steering committee
B. Customers who may be impacted
C. Data owners who may be impacted
D. Regulatory agencies overseeing privacy

QUESTION 186
Data owners are PRIMARILY responsible for establishing risk mitigation methods to address which of the following areas?

A. Platform security
B. Entitlement changes
C. Intrusion detection
D. Antivirus controls

QUESTION 187
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

QUESTION 188
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

QUESTION 189
The service level agreement (SLA) for an outsourced IT function does not reflect an adequate level of protection. In this situation an information security manager should:

A. Ensure the provider is made liable for losses
B. Recommend not renewing the contract upon expiration
C. Recommend the immediate termination of the contract
D. Determine the current level of security

QUESTION 190
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

QUESTION 191
When performing a quantitative risk analysis, which of the following is MOST important to estimate the potential loss?

A. Evaluate productivity losses
B. Assess the impact of confidential data disclosure
C. Calculate the value of the information or asset
D. Measure the probability of occurrence of each threat

QUESTION 192
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

QUESTION 193
The valuation of IT assets should be performed by:

A. An IT security manager
B. An independent security consultant
C. The chief financial officer (CFO)
D. The information owner

QUESTION 194
The PRIMARY objective of a risk management program is to:

A. Minimize inherent risk
B. Eliminate business risk
C. Implement effective controls
D. Minimize residual risk

QUESTION 195
After completing a full IT risk assessment, who can BEST decide which mitigating controls should be implemented?

A. Senior management
B. Business manager
C. IT audit manager
D. Information security officer (ISO)

QUESTION 196
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

QUESTION 197
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

QUESTION 198
Which of the following is MOST essential for a risk management program to be effective?

A. Flexible security budget
B. Sound risk baseline
C. New risks detection
D. Accurate risk reporting

QUESTION 199
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

QUESTION 200
Phishing is BEST mitigated by which of the following?

A. Security monitoring software
B. Encryption
C. Two-factor authentication
D. User awareness

QUESTION 201
The security responsibility of data custodians in an organization will include:

A. Assuming overall protection of information assets
B. Determining data classification levels
C. Implementing security controls in products they install
D. Ensuring security measures are consistent with policy

QUESTION 202
A security risk assessment exercise should be repeated at regular intervals because:

A. Business threats are constantly changing
B. Omissions in earlier assessments can be addressed
C. Repetitive assessments allow various methodologies
D. They help raise awareness on security in the business

QUESTION 203
Which of the following steps in conducting a risk assessment should be performed FIRST?

A. Identity business assets
B. Identify business risks
C. Assess vulnerabilities
D. Evaluate key controls

QUESTION 204
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

QUESTION 205
Which of the following risks is represented in the risk appetite of an organization?

A. Control
B. Inherent
C. Residual
D. Audit

QUESTION 206
Which of the following would a security manager establish to determine the target for restoration of normal processing?

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

QUESTION 207
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

QUESTION 208
Risk assessment should be built into which of the following systems development phases to ensure that risks are addressed in a development project?

A. Programming
B. Specification
C. User testing
D. Feasibility

QUESTION 209
Which of the following would help management determine the resources needed to mitigate a risk to the organization?

A. Risk analysis process
B. Business impact analysis (BIA)
C. Risk management balanced scorecard
D. Risk-based audit program

QUESTION 210
A global financial institution has decided not to take any further action on a denial of service (DoS) risk found by the risk assessment team. The MOST likely reason they made this decision is that:

A. There are sufficient safeguards in place to prevent this risk from happening
B. The needed countermeasure is too complicated to deploy
C. The cost of countermeasure outweighs the value of the asset and potential loss
D. The likelihood of the risk occurring is unknown

QUESTION 211
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

QUESTION 212
Which of the following types of information would the information security manager expect to have the LOWEST level of security protection in a large, multinational enterprise?

A. Strategic business plan
B. Upcoming financial results
C. Customer personal information
D. Previous financial results

QUESTION 213
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

QUESTION 214
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

QUESTION 215
An online banking institution is concerned that the breach of customer personal information will have a significant financial impact due to the need to notify and compensate customers whose personal information may have been compromised. The institution determines that residual risk will always be too high and decides to:

A. Mitigate the impact by purchasing insurance
B. Implement a circuit-level firewall to protect the network
C. Increase the resiliency of security measures in place
D. Implement a real-time intrusion detection system

QUESTION 216
What mechanisms are used to identify deficiencies that would provide attackers with an opportunity to compromise a computer system?

A. Business impact analyses
B. Security gap analyses
C. System performance metrics
D. Incident response processes

QUESTION 217
A common concern with poorly written web applications is that they can allow an attacker to:

A. Gain control through a buffer overflow
B. Conduct a distributed denial of service (DoS) attack
C. Abuse a race condition
D. Inject structured query language (SQL) statements

QUESTION 218
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)

QUESTION 219
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

QUESTION 220
A mission-critical system has been identified as having an administrative system account with attributes that prevent locking and change of privileges and name. Which would be the BEST approach to prevent successful brute forcing of the account?

A. Prevent the system from being accessed remotely
B. Create a strong random password
C. Ask for a vendor patch
D. Track usage of the account by audit trails

QUESTION 221
Attackers who exploit cross-site scripting vulnerabilities take advantage of:

A. A lack of proper input validation controls
B. Weak authentication controls in the web application layer
C. Flawed cryptographic secure sockets layer (SSL) implementations and short key lengths
D. Implicit web application trust relationships

QUESTION 222
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

QUESTION 223
A company recently developed a breakthrough technology. Since this technology could give this company a significant competitive edge, which of the following would FIRST govern how this information is to be protected?

A. Access control policy
B. Data classification policy
C. Encryption standards
D. Acceptable use policy

QUESTION 224
What is the BEST technique to determine which security controls to implement with a limited budget?

A. Risk analysis
B. Annualized loss expectancy (ALE) calculations
C. Cost-benefit analysis
D. Impact analysis

QUESTION 225
A company's mail server allows anonymous file transfer protocol (FTP) access which could be exploited. What process should the information security manager deploy to determine the necessity for remedial action?

A. A penetration test
B. A security baseline review
C. A risk assessment
D. A business impact analysis (BIA)

QUESTION 226
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

QUESTION 227
Because of its importance to the business, an organization wants to quickly implement a technical solution which deviates from the company's policies. An information security manager should:

A. Conduct a risk assessment and allow or disallow based on the outcome
B. Recommend a risk assessment and implementation only if the residual risks are accepted
C. Recommend against implementation because it violates the company's policies
D. Recommend revision of current policy

QUESTION 228
After a risk assessment study, a bank with global operations decided to continue doing business in certain regions of the world where identity theft is rampant. The information security manager should encourage the business to:

A. Increase its customer awareness efforts in those regions
B. Implement monitoring techniques to detect and react to potential fraud
C. Outsource credit card processing to a third party
D. Make the customer liable for losses if they fail to follow the bank's advice

QUESTION 229
The criticality and sensitivity of information assets is determined on the basis of:

A. Threat assessment
B. Vulnerability assessment
C. Resource dependency assessment
D. Impact assessment

QUESTION 230
Which program element should be implemented FIRST in asset classification and control?

A. Risk assessment
B. Classification
C. Valuation
D. Risk mitigation

QUESTION 231
When performing a risk assessment, the MOST important consideration is that:

A. Management supports risk mitigation efforts
B. Annual loss expectations (ALEs) have been calculated for critical assets
C. Assets have been identified and appropriately valued
D. Attack motives, means and opportunities be understood

QUESTION 232
The MAIN reason why asset classification is important to a successful information security program is because classification determines:

A. The priority and extent of risk mitigation efforts
B. The amount of insurance needed in case of loss
C. The appropriate level of protection to the asset
D. How protection levels compare to peer organizations

QUESTION 233
The BEST strategy for risk management is to:

A. Achieve a balance between risk and organizational goals
B. Reduce risk to an acceptable level
C. Ensure that policy development properly considers organizational risks
D. Ensure that all unmitigated risks are accepted by management

QUESTION 234
Which of the following would be the MOST important factor to be considered in the loss of mobile equipment with unencrypted data?

A. Disclosure of personal information
B. Sufficient coverage of the insurance policy for accidental losses
C. Intrinsic value of the data stored on the equipment
D. Replacement cost of the equipment

QUESTION 235
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

QUESTION 236
Which of the following would be MOST relevant to include in a cost-benefit analysis of a two-factor authentication system?

A. Annual loss expectancy (ALE) of incidents
B. Frequency of incidents
C. Total cost of ownership (TCO)
D. Approved budget for the project

QUESTION 237
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

QUESTION 238
What does a network vulnerability assessment intend to identify?

A. Zero-day vulnerabilities
B. Malicious software and spyware
C. Security design flaws
D. Misconfiguration and missing updates

QUESTION 239
Who is responsible for ensuring that information is classified?

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

QUESTION 240
After a risk assessment, it is determined that the cost to mitigate the risk is much greater than the benefit to be derived. The information security manager should recommend to business management that the risk be:

A. Transferred
B. Treated
C. Accepted
D. Terminated

QUESTION 241
When a significant security breach occurs, what should be reported FIRST to senior management?

A. A summary of the security logs that illustrates the sequence of events
B. An explanation of the incident and corrective action taken
C. An analysis of the impact of similar attacks at other organizations
D. A business case for implementing stronger logical access controls

QUESTION 242
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

QUESTION 243
Which of the following would be the MOST relevant factor when defining the information classification policy?

A. Quantity of information
B. Available IT infrastructure
C. Benchmarking
D. Requirements of data owners

QUESTION 244
To determine the selection of controls required to meet business objectives, an information security manager should:

A. Prioritize the use of role-based access controls
B. Focus on key controls
C. Restrict controls to only critical applications
D. Focus on automated controls

QUESTION 245
The MOST appropriate owner of customer data stored in a central database, used only by an organization's sales department, would be the:

A. Sales department
B. Database administrator
C. Chief information officer (CIO)
D. Head of the sales department

QUESTION 246
In assessing the degree to which an organization may be affected by new privacy legislation, information security management should FIRST:

A. Develop an operational plan for achieving compliance with the legislation
B. Identify systems and processes that contain privacy components
C. Restrict the collection of personal information until compliant
D. Identify privacy legislation in other countries that may contain similar requirements

QUESTION 247
Risk assessment is MOST effective when performed:

A. At the beginning of security program development
B. On a continuous basis
C. While developing the business case for the security program
D. During the business change process

QUESTION 248
Which of the following is the MAIN reason for performing risk assessment on a continuous basis?

A. Justification of the security budget must be continually made
B. New vulnerabilities are discovered every day
C. The risk environment is constantly changing
D. Management needs to be continually informed about emerging risks

QUESTION 249
There is a time lag between the time when a security vulnerability is first published, and the time when a patch is delivered. Which of the following should be carried out FIRST to mitigate the risk during this time period?

A. Identify the vulnerable systems and apply compensating controls
B. Minimize the use of vulnerable systems
C. Communicate the vulnerability to system users
D. Update the signatures database of the intrusion detection system (IDS)

QUESTION 250
Which of the following security activities should be implemented in the change management process to identify key vulnerabilities introduced by changes?

A. Business impact analysis (BIA)
B. Penetration testing
C. Audit and review
D. Threat analysis

QUESTION 251
Which of the following techniques MOST clearly indicates whether specific risk-reduction controls should be implemented?

A. Countermeasure cost-benefit analysis
B. Penetration testing
C. Frequent risk assessment programs
D. Annual loss expectancy (ALE) calculation

QUESTION 252
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

QUESTION 253
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

QUESTION 254
The PRIMARY reason for assigning classes of sensitivity and criticality to information resources is to provide a basis for:

A. Determining the scope for inclusion in an information security program
B. Defining the level of access controls
C. Justifying costs for information resources
D. Determining the overall budget of an information security program

QUESTION 255
An organization is already certified to an international security standard. Which mechanism would BEST help to further align the organization with other data security regulatory requirements as per new business needs?

A. Key performance indicators (KPIs)
B. Business impact analysis (BIA)
C. Gap analysis
D. Technical vulnerability assessment

QUESTION 256
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

QUESTION 257
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

QUESTION 258
The MOST effective use of a risk register is to:

A. Identify risks and assign roles and responsibilities for mitigation
B. Identify threats and probabilities
C. Facilitate a thorough review of all IT-related risks on a periodic basis
D. Record the annualized financial amount of expected losses due to risks

QUESTION 259
After obtaining commitment from senior management, which of the following should be completed NEXT when establishing an information security program?

A. Define security metrics
B. Conduct a risk assessment
C. Perform a gap analysis
D. Procure security tools

QUESTION 260
Which of the following are the essential ingredients of a business impact analysis (BIA)?

A. Downtime tolerance, resources and criticality
B. Cost of business outages in a year as a factor of the security budget
C. Business continuity testing methodology being deployed
D. Structure of the crisis management team

QUESTION 261
A risk management approach to information protection is:

A. Managing risks to an acceptable level, commensurate with goals and objectives
B. Accepting the security posture provided by commercial security products
C. Implementing a training program to educate individuals on information protection and risks
D. Managing risk tools to ensure that they assess all information protection vulnerabilities

QUESTION 262
Which of the following is the MOST effective way to treat a risk such as a natural disaster that has a low probability and a high impact level?

A. Implement countermeasures
B. Eliminate the risk
C. Transfer the risk
D. Accept the risk

QUESTION 263
To ensure that payroll systems continue on in an event of a hurricane hitting a data center, what would be the FIRST crucial step an information security manager would take in ensuring business continuity planning?

A. Conducting a qualitative and quantitative risk analysis
B. Assigning value to the assets
C. Weighing the cost of implementing the plan vs. financial loss
D. Conducting a business impact analysis (BIA)

QUESTION 264
An information security organization should PRIMARILY:

A. Support the business objectives of the company by providing security-related support services
B. Be responsible for setting up and documenting the information security responsibilities of the information security team members
C. Ensure that the information security policies of the company are in line with global best practices and standards
D. Ensure that the information security expectations are conveyed to employees

QUESTION 265
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

QUESTION 266
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

QUESTION 267
After assessing and mitigating the risks of a web application, who should decide on the acceptance of residual application risks?

A. Information security officer
B. Chief information officer (CIO)
C. Business owner
D. Chief executive officer (CEO)

QUESTION 268
The purpose of a corrective control is to:

A. Reduce adverse events
B. Indicate compromise
C. Mitigate impact
D. Ensure compliance

QUESTION 269
Which of the following is the MOST important requirement for setting up an information security infrastructure for a new system?

A. Performing a business impact analysis (BIA)
B. Considering personal information devices as part of the security policy
C. Initiating IT security training and familiarization
D. Basing the information security infrastructure on risk assessment

QUESTION 270
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

QUESTION 271
An information security manager is advised by contacts in law enforcement that there is evidence that his / her company is being targeted by a skilled gang of hackers known to use a variety of techniques, including social engineering and network penetration. The FIRST step that the security manager should take is to:

A. Perform a comprehensive assessment of the organization's exposure to the hacker's techniques
B. Initiate awareness training to counter social engineering
C. Immediately advise senior management of the elevated risk
D. Increase monitoring activities to provide early detection of intrusion

QUESTION 272
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

QUESTION 273
Which of the following authentication methods prevents authentication replay?

A. Password hash implementation
B. Challenge/response mechanism
C. Wired Equivalent Privacy (WEP) encryption usage
D. HTTP Basic Authentication

QUESTION 274
An organization has a process in place that involves the use of a vendor. A risk assessment was completed during the development of the process. A year after the implementation a monetary decision has been made to use a different vendor. What, if anything, should occur?

A. Nothing, since a risk assessment was completed during development
B. A vulnerability assessment should be conducted
C. A new risk assessment should be performed
D. The new vendor's SAS 70 type II report should be reviewed

Topic 3: Information Security Program Development

QUESTION 275
Who can BEST advocate the development of and ensure the success of an information security program?

A. Internal auditor
B. Chief operating officer (COO)
C. Steering committee
D. IT management

QUESTION 276
Which of the following BEST ensures that information transmitted over the Internet will remain confidential?

A. Virtual private network (VPN)
B. Firewalls and routers
C. Biometric authentication
D. Two-factor authentication

QUESTION 277
The effectiveness of virus detection software is MOST dependent on which of the following?

A. Packet filtering
B. Intrusion detection
C. Software upgrades
D. Definition tables

QUESTION 278
Which of the following is the MOST effective type of access control?

A. Centralized
B. Role-based
C. Decentralized
D. Discretionary

QUESTION 279
Which of the following devices should be placed within a DMZ?

A. Router
B. Firewall
C. Mail relay
D. Authentication server

QUESTION 280
An intrusion detection system should be placed:

A. Outside the firewall
B. On the firewall server
C. On a screened subnet
D. On the external router

QUESTION 281
The BEST reason for an organization to have two discrete firewalls connected directly to the Internet and to the same DMZ would be to:

A. Provide in-depth defense
B. Separate test and production
C. Permit traffic load balancing
D. Prevent a denial-of-service attack

QUESTION 282
An extranet server should be placed:

A. Outside the firewall
B. On the firewall server
C. On a screened subnet
D. On the external router

QUESTION 283
Which of the following is the BEST metric for evaluating the effectiveness of security awareness training? The number of:

A. Password resets
B. Reported incidents
C. Incidents resolved
D. Access rule violations

QUESTION 284
Security monitoring mechanisms should PRIMARILY:

A. Focus on business-critical information
B. Assist owners to manage control risks
C. Focus on detecting network intrusions
D. Record all security violations

QUESTION 285
Which of the following is the BEST method for ensuring that security procedures and guidelines are known and understood?

A. Periodic focus group meetings
B. Periodic compliance reviews
C. Computer-based certification training (CBT)
D. Employee's signed acknowledgement

QUESTION 286
When contracting with an outsourcer to provide security administration, the MOST important contractual element is the:

A. Right-to-terminate clause
B. Limitations of liability
C. Service level agreement (SLA)
D. Financial penalties clause

QUESTION 287
Which of the following is the BEST metric for evaluating the effectiveness of an intrusion detection mechanism?

A. Number of attacks detected
B. Number of successful attacks
C. Ratio of false positives to false negatives
D. Ratio of successful to unsuccessful attacks

QUESTION 288
Which of the following is MOST effective in preventing weaknesses from being introduced into existing production systems?

A. Patch management
B. Change management
C. Security baselines
D. Virus detection

QUESTION 289
Which of the following tools is MOST appropriate for determining how long a security project will take to implement?

A. Gantt chart
B. Waterfall chart
C. Critical path
D. Rapid Application Development (RAD)

QUESTION 290
Which of the following is MOST effective in preventing security weaknesses in operating systems?

A. Patch management
B. Change management
C. Security baselines
D. Configuration management

QUESTION 291
When a proposed system change violates an existing security standard, the conflict would be BEST resolved by:

A. Calculating the residual risk
B. Enforcing the security standard
C. Redesigning the system change
D. Implementing mitigating controls

QUESTION 292
Who can BEST approve plans to implement an information security governance framework?

A. Internal auditor
B. Information security management
C. Steering committee
D. Infrastructure management

QUESTION 293
Which of the following is the MOST effective solution for preventing internal users from modifying sensitive and classified information?

A. Baseline security standards
B. System access violation logs
C. Role-based access controls
D. Exit routines

QUESTION 294
Which of the following is generally used to ensure that information transmitted over the Internet is authentic and actually transmitted by the named sender?

A. Biometric authentication
B. Embedded steganographic
C. Two-factor authentication
D. Embedded digital signature

QUESTION 295
Which of the following is the MOST appropriate frequency for updating antivirus signature files for antivirus software on production servers?

A. Daily
B. Weekly
C. Concurrently with O/S patch updates
D. During scheduled change control updates

QUESTION 296
Which of the following devices should be placed within a demilitarized zone (DMZ)?

A. Network switch
B. Web server
C. Database server
D. File/print server

QUESTION 297
On which of the following should a firewall be placed?

A. Web server
B. Intrusion detection system (IDS) server
C. Screened subnet
D. Domain boundary

QUESTION 298
An intranet server should generally be placed on the:

A. Internal network
B. Firewall server
C. External router
D. Primary domain controller

QUESTION 299
Access control to a sensitive intranet application by mobile users can BEST be implemented through:

A. Data encryption
B. Digital signatures
C. Strong passwords
D. Two-factor authentication

QUESTION 300
When application-level security controlled by business process owners is found to be poorly managed, which of the following could BEST improve current practices?

A. Centralizing security management
B. Implementing sanctions for noncompliance
C. Policy enforcement by IT management
D. Periodic compliance reviews

QUESTION 301
Security awareness training is MOST likely to lead to which of the following?

A. Decrease in intrusion incidents
B. Increase in reported incidents
C. Decrease in security policy changes
D. Increase in access rule violations

QUESTION 302
The information classification scheme should:

A. Consider possible impact of a security breach
B. Classify personal information in electronic form
C. Be performed by the information security manager
D. Classify systems according to the data processed

QUESTION 303
Which of the following is the BEST method to provide a new user with their initial password for e-mail system access?

A. Interoffice a system-generated complex password with 30 days expiration
B. Give a dummy password over the telephone set for immediate expiration
C. Require no password but force the user to set their own in 10 days
D. Set initial password equal to the user ID with expiration in 30 days

QUESTION 304
An information security program should be sponsored by:

A. Infrastructure management
B. The corporate audit department
C. Key business process owners
D. Information security management

QUESTION 305
Which of the following is the MOST important item to include when developing web hosting agreements with third-party providers?

A. Termination conditions
B. Liability limits
C. Service levels
D. Privacy restrictions

QUESTION 306
The BEST metric for evaluating the effectiveness of a firewall is the:

A. Number of attacks blocked
B. Number of packets dropped
C. Average throughput rate
D. Number of firewall rules

QUESTION 307
Which of the following ensures that newly identified security weaknesses in an operating system are mitigated in a timely fashion?

A. Patch management
B. Change management
C. Security baselines
D. Acquisition management

QUESTION 308
The MAIN advantage of implementing automated password synchronization is that it:

A. Reduces overall administrative workload
B. Increases security between multi-tier systems
C. Allows passwords to be changed less frequently
D. Reduces the need for two-factor authentication

QUESTION 309
Which of the following tools is MOST appropriate to assess whether information security governance objectives are being met?

A. SWOT analysis
B. Waterfall chart
C. Gap analysis
D. Balanced scorecard

QUESTION 310
Which of the following is MOST effective in preventing the introduction of a code modification that may reduce the security of a critical business application?

A. Patch management
B. Change management
C. Security metrics
D. Version control

QUESTION 311
An operating system (OS) noncritical patch to enhance system security cannot be applied because a critical application is not compatible with the change. Which of the following is the BEST solution?

A. Rewrite the application to conform to the upgraded operating system
B. Compensate for not installing the patch with mitigating controls
C. Alter the patch to allow the application to run in a privileged state
D. Run the application on a test platform; tune production to allow patch and application

QUESTION 312
Which of the following is MOST important to the success of an information security program?

A. Security awareness training
B. Achievable goals and objectives
C. Senior management sponsorship
D. Adequate start-up budget and staffing

QUESTION 313
Which of the following is MOST important for a successful information security program?

A. Adequate training on emerging security technologies
B. Open communication with key process owners
C. Adequate policies, standards and procedures
D. Executive management commitment

QUESTION 314
Which of the following is the MOST effective solution for preventing individuals external to the organization from modifying sensitive information on a corporate database?

A. Screened subnets
B. Information classification policies and procedures
C. Role-based access controls
D. Intrusion detection system (IDS)

QUESTION 315
Which of the following technologies is utilized to ensure that an individual connecting to a corporate internal network over the Internet is not an intruder masquerading as an authorized user?

A. Intrusion detection system (IDS)
B. IP address packet filtering
C. Two-factor authentication
D. Embedded digital signature

QUESTION 316
What is an appropriate frequency for updating operating system (OS) patches on production servers?

A. During scheduled rollouts of new applications
B. According to a fixed security patch management schedule
C. Concurrently with quarterly hardware maintenance
D. Whenever important security patches are released

QUESTION 317
Which of the following devices should be placed within a DMZ?

A. Proxy server
B. Application server
C. Departmental server
D. Data warehouse server

QUESTION 318
A border router should be placed on which of the following?

A. Web server
B. IDS server
C. Screened subnet
D. Domain boundary

QUESTION 319
An e-commerce order fulfillment web server should generally be placed on which of the following?

A. Internal network
B. Demilitarized zone (DMZ)
C. Database server
D. Domain controller

QUESTION 320
Secure customer use of an e-commerce application can BEST be accomplished through:

A. Data encryption
B. Digital signatures
C. Strong passwords
D. Two-factor authentication

QUESTION 321
What is the BEST defense against a Structured Query Language (SQL) injection attack?

A. Regularly updated signature files
B. A properly configured firewall
C. An intrusion detection system
D. Strict controls on input fields

QUESTION 322
Which of the following is the MOST important consideration when implementing an intrusion detection system (IDS)?

A. Tuning
B. Patching
C. Encryption
D. Packet filtering

QUESTION 323
Which of the following is the MOST important consideration when securing customer credit card data acquired by a point-of-sale (POS) cash register?

A. Authentication
B. Hardening
C. Encryption
D. Nonrepudiation

QUESTION 324
Which of the following practices is BEST to remove system access for contractors and other temporary users when it is no longer required?

A. Log all account usage and send it to their manager
B. Establish predetermined automatic expiration dates
C. Require managers to e-mail security when the user leaves
D. Ensure each individual has signed a security acknowledgement

QUESTION 325
Primary direction on the impact of compliance with new regulatory requirements that may lead to major application system changes should be obtained from the:

A. Corporate internal auditor
B. System developers/analysts
C. Key business process owners
D. Corporate legal counsel

QUESTION 326
Which of the following is the MOST important item to consider when evaluating products to monitor security across the enterprise?

A. Ease of installation
B. Product documentation
C. Available support
D. System overhead

QUESTION 327
Which of the following is the MOST important guideline when using software to scan for security exposures within a corporate network?

A. Never use open-source tools
B. Focus only on production servers
C. Follow a linear process for attacks
D. Do not interrupt production processes

QUESTION 328
Which of the following BEST ensures that modifications made to in-house developed business applications do not introduce new security exposures?

A. Stress testing
B. Patch management
C. Change management
D. Security baselines

QUESTION 329
The advantage of Virtual Private Network (VPN) tunneling for remote users is that it:

A. Helps ensure that communications are secure
B. Increases security between multi-tier systems
C. Allows passwords to be changed less frequently
D. Eliminates the need for secondary authentication

QUESTION 330
Which of the following is MOST effective for securing wireless networks as a point of entry into a corporate network?

A. Boundary router
B. Strong encryption
C. Internet-facing firewall
D. Intrusion detection system (IDS)

QUESTION 331
Which of the following is MOST effective in protecting against the attack technique known as phishing?

A. Firewall blocking rules
B. Up-to-date signature files
C. Security awareness training
D. Intrusion detection monitoring

QUESTION 332
When a newly installed system for synchronizing passwords across multiple systems and platforms abnormally terminates without warning, which of the following should automatically occur FIRST?

A. The firewall should block all inbound traffic during the outage
B. All systems should block new logins until the problem is corrected
C. Access control should fall back to no synchronized mode
D. System logs should record all user activity for later analysis

QUESTION 333
Which of the following is the MOST important risk associated with middleware in a client-server environment?

A. Server patching may be prevented
B. System backups may be incomplete
C. System integrity may be affected
D. End-user sessions may be hijacked

QUESTION 334
An outsource service provider must handle sensitive customer information. Which of the following is MOST important for an information security manager to know?

A. Security in storage and transmission of sensitive data
B. Provider's level of compliance with industry standards
C. Security technologies in place at the facility
D. Results of the latest independent security review

QUESTION 335
Which of the following security mechanisms is MOST effective in protecting classified data that have been encrypted to prevent disclosure and transmission outside the organization's network?

A. Configuration of firewalls
B. Strength of encryption algorithms
C. Authentication within application
D. Safeguards over keys

QUESTION 336
In the process of deploying a new e-mail system, an information security manager would like to ensure the confidentiality of messages while in transit. Which of the following is the MOST appropriate method to ensure data confidentiality in a new e-mail system implementation?

A. Encryption
B. Digital certificate
C. Digital signature
D. Hashing algorithm

QUESTION 337
The MOST important reason that statistical anomaly-based intrusion detection systems (stat IDSs) are less commonly used than signature-based IDSs, is that stat IDSs:

A. Create more overhead than signature-based IDSs
B. Cause false positives from minor changes to system variables
C. Generate false alarms from varying user or system actions
D. Cannot detect new types of attacks

QUESTION 338
An information security manager uses security metrics to measure the:

A. Performance of the information security program
B. Performance of the security baseline
C. Effectiveness of the security risk analysis
D. Effectiveness of the incident response team

QUESTION 339
The MOST important success factor to design an effective IT security awareness program is to:

A. Customize the content to the target audience
B. Ensure senior management is represented
C. Ensure that all the staff is trained
D. Avoid technical content but give concrete examples

QUESTION 340
Which of the following practices completely prevents a man-in-the-middle (MitM) attack between two hosts?

A. Use security tokens for authentication
B. Connect through an IPSec VPN
C. Use https with a server-side certificate
D. Enforce static media access control (MAC) addresses

QUESTION 341
Which of the following features is normally missing when using Secure Sockets Layer (SSL) in a web browser?

A. Certificate-based authentication of web client
B. Certificate-based authentication of web server
C. Data confidentiality between client and web server
D. Multiple encryption algorithms

QUESTION 342
The BEST protocol to ensure confidentiality of transmissions in a business-to-customer (B2C) financial web application is:

A. Secure Sockets Layer (SSL)
B. Secure Shell (SSH)
C. IP Security (IPSec)
D. Secure/Multipurpose Internet Mail Extensions (S/MIME)

QUESTION 343
A message that has been encrypted by the sender's private key and again by the receiver's public key achieves:

A. Authentication and authorization
B. Confidentiality and integrity
C. Confidentiality and nonrepudiation
D. Authentication and nonrepudiation

QUESTION 344
When a user employs a client-side digital certificate to authenticate to a web server through Secure Socket Layer (SSL), confidentiality is MOST vulnerable to which of the following?

A. IP spoofing
B. Man-in-the-middle attack
C. Repudiation
D. Trojan

QUESTION 345
Which of the following is the MOST relevant metric to include in an information security quarterly report to the executive committee?

A. Security compliant servers trend report
B. Percentage of security compliant servers
C. Number of security patches applied
D. Security patches applied trend report

QUESTION 346
It is important to develop an information security baseline because it helps to define:

A. Critical information resources needing protection
B. A security policy for the entire organization
C. The minimum acceptable security to be implemented
D. Required physical and logical access controls

QUESTION 347
Which of the following BEST provides message integrity, sender identity authentication and nonrepudiation?

A. Symmetric cryptography
B. Public key infrastructure (PKI)
C. Message hashing
D. Message authentication code

QUESTION 348
Which of the following controls is MOST effective in providing reasonable assurance of physical access compliance to an unmanned server room controlled with biometric devices?

A. Regular review of access control lists
B. Security guard escort of visitors
C. Visitor registry log at the door
D. A biometric coupled with a PIN

QUESTION 349
To BEST improve the alignment of the information security objectives in an organization, the chief information security officer (CISO) should:

A. Revise the information security program
B. Evaluate a balanced business scorecard
C. Conduct regular user awareness sessions
D. Perform penetration tests

QUESTION 350
What is the MOST important item to be included in an information security policy?

A. The definition of roles and responsibilities
B. The scope of the security program
C. The key objectives of the security program
D. Reference to procedures and standards of the security program

QUESTION 351
In an organization, information systems security is the responsibility of:

A. All personnel
B. Information systems personnel
C. Information systems security personnel
D. Functional personnel

QUESTION 352
An organization without any formal information security program that has decided to implement information security best practices should FIRST:

A. Invite an external consultant to create the security strategy
B. Allocate budget based on best practices
C. Benchmark similar organizations
D. Define high-level business security requirements

QUESTION 353
When considering the value of assets, which of the following would give the information security manager the MOST objective basis for measurement of value delivery in information security governance?

A. Number of controls
B. Cost of achieving control objectives
C. Effectiveness of controls
D. Test results of controls

QUESTION 354
Which of the following would be the BEST metric for the IT risk management process?

A. Number of risk management action plans
B. Percentage of critical assets with budgeted remedial
C. Percentage of unresolved risk exposures
D. Number of security incidents identified

QUESTION 355
Which of the following is a key area of the ISO 27001 framework?

A. Operational risk assessment
B. Financial crime metrics
C. Capacity management
D. Business continuity management

QUESTION 356
The MAIN goal of an information security strategic plan is to:

A. Develop a risk assessment plan
B. Develop a data protection plan
C. Protect information assets and resources
D. Establish security governance

QUESTION 357
Which of the following, using public key cryptography, ensures authentication, confidentiality and nonrepudiation of a message?

A. Encrypting first by receiver's private key and second by sender's public key
B. Encrypting first by sender's private key and second by receiver's public key
C. Encrypting first by sender's private key and second decrypting by sender's public key
D. Encrypting first by sender's public key and second by receiver's private key

QUESTION 358
The main mail server of a financial institution has been compromised at the superuser level; the only way to ensure the system is secure would be to:

A. Change the root password of the system
B. Implement multifactor authentication
C. Rebuild the system from the original installation medium
D. Disconnect the mail server from the network

QUESTION 359
The IT function has declared that, when putting a new application into production, it is not necessary to update the business impact analysis (BIA) because it does not produce modifications in the business processes. The information security manager should:

A. Verify the decision with the business units
B. Check the system's risk analysis
C. Recommend update after post implementation review
D. Request an audit review

QUESTION 360
A risk assessment study carried out by an organization noted that there is no segmentation of the local area network (LAN). Network segmentation would reduce the potential impact of which of the following?

A. Denial of service (DoS) attacks
B. Traffic sniffing
C. Virus infections
D. IP address spoofing

QUESTION 361
The PRIMARY objective of an Internet usage policy is to prevent:

A. Access to inappropriate sites
B. Downloading malicious code
C. Violation of copyright laws
D. Disruption of Internet access

QUESTION 362
An internal review of a web-based application system finds the ability to gain access to all employees' accounts by changing the employee's ID on the URL used for accessing the account. The vulnerability identified is:

A. Broken authentication
B. Unvalidated input
C. Cross-site scripting
D. Structured query language (SQL) injection

QUESTION 363
A test plan to validate the security controls of a new system should be developed during which phase of the project?

A. Testing
B. Initiation
C. Design
D. Development

QUESTION 364
The MOST effective way to ensure that outsourced service providers comply with the organization's information security policy would be:

A. Service level monitoring
B. Penetration testing
C. Periodically auditing
D. Security awareness training

QUESTION 365
In order to protect a network against unauthorized external connections to corporate systems, the information security manager should BEST implement:

A. A strong authentication
B. IP anti-spoofing filtering
C. Network encryption protocol
D. Access lists of trusted devices

QUESTION 366
The PRIMARY driver to obtain external resources to execute the information security program is that external resources can:

A. Contribute cost-effective expertise not available internally
B. Be made responsible for meeting the security program requirements
C. Replace the dependence on internal resources
D. Deliver more effectively on account of their knowledge

QUESTION 367
Priority should be given to which of the following to ensure effective implementation of information security governance?

A. Consultation
B. Negotiation
C. Facilitation
D. Planning

QUESTION 368
The MAIN reason for deploying a public key infrastructure (PKI) when implementing an information security program is to:

A. Ensure the confidentiality of sensitive material
B. Provide a high assurance of identity
C. Allow deployment of the active directory
D. Implement secure sockets layer (SSL) encryption

QUESTION 369
Which of the following controls would BEST prevent accidental system shutdown from the console or operations area?

A. Redundant power supplies
B. Protective switch covers
C. Shutdown alarms
D. Biometric readers

QUESTION 370
Which of the following is the MOST important reason why information security objectives should be defined?

A. Tool for measuring effectiveness
B. General understanding of goals
C. Consistency with applicable standards
D. Management sign-off and support initiatives

QUESTION 371
What is the BEST policy for securing data on mobile universal serial bus (USB) drives?

A. Authentication
B. Encryption
C. Prohibit employees from copying data to USB devices
D. Limit the use of USB devices

QUESTION 372
When speaking to an organization's human resources department about information security, an information security manager should focus on the need for:

A. An adequate budget for the security program
B. Recruitment of technical IT employees
C. Periodic risk assessments
D. Security awareness training for employees

QUESTION 373
Which of the following would BEST protect an organization's confidential data stored on a laptop computer from unauthorized access?

A. Strong authentication by password
B. Encrypted hard drives
C. Multifactor authentication procedures
D. Network-based data backup

QUESTION 374
What is the MOST important reason for conducting security awareness programs throughout an organization?

A. Reducing the human risk
B. Maintaining evidence of training records to ensure compliance
C. Informing business units about the security strategy
D. Training personnel in security incident response

QUESTION 375
At what stage of the applications development process would encryption key management initially be addressed?

A. Requirements development
B. Deployment
C. Systems testing
D. Code reviews

QUESTION 376
The MOST effective way to ensure network users are aware of their responsibilities to comply with an organization's security requirements is:

A. Messages displayed at every logon
B. Periodic security-related e-mail messages
C. An Intranet web site for information security
D. Circulating the information security policy

QUESTION 377
Which of the following would be the BEST defense against sniffing?

A. Password protect the files
B. Implement a dynamic IP address scheme
C. Encrypt the data being transmitted
D. Set static media access control (MAC) addresses

QUESTION 378
A digital signature using a public key infrastructure (PKI) will:

A. Not ensure the integrity of a message
B. Rely on the extent to which the certificate authority (CA) is trusted
C. Require two parties to the message exchange
D. Provide a high level of confidentiality

QUESTION 379
When configuring a biometric access control system that protects a high-security data center, the system's sensitivity level should be set:

A. To a higher false reject rate (FRR)
B. To a lower crossover error rate
C. To a higher false acceptance rate (FAR)
D. Exactly to the crossover error rate

QUESTION 380
Which of the following is the BEST method to securely transfer a message?

A. Password-protected removable media
B. Facsimile transmission in a secured room
C. Using public key infrastructure (PKI) encryption
D. Steganography

QUESTION 381
Which of the following would be the FIRST step in establishing an information security program?

A. Develop the security policy
B. Develop security operating procedures
C. Develop the security plan
D. Conduct a security controls study

QUESTION 382
An organization has adopted a practice of regular staff rotation to minimize the risk of fraud and encourage cross-training. Which type of authorization policy would BEST address this practice?

A. Multilevel
B. Role-based
C. Discretionary
D. Attribute-based

QUESTION 383
Which of the following is the MOST important reason for an information security review of contracts? To help ensure that:

A. The parties to the agreement can perform
B. Confidential data are not included in the agreement
C. Appropriate controls are included
D. The right to audit is a requirement

QUESTION 384
For virtual private network (VPN) access to the corporate network, the information security manager is requiring strong authentication. Which of the following is the strongest method to ensure that logging onto the network is secure?

A. Biometrics
B. Symmetric encryption keys
C. Secure Sockets Layer (SSL)-based authentication
D. Two-factor authentication

QUESTION 385
Which of the following guarantees that data in a file have not changed?

A. Inspecting the modified date of the file
B. Encrypting the file with symmetric encryption
C. Using stringent access control to prevent unauthorized access
D. Creating a hash of the file, then comparing the file hashes

QUESTION 386
Which of the following mechanisms is the MOST secure way to implement a secure wireless network?

A. Filter media access control (MAC) addresses
B. Use a Wi-Fi Protected Access (WPA2) protocol
C. Use a Wired Equivalent Privacy (WEP) key
D. Web-based authentication

QUESTION 387
Which of the following devices could potentially stop a Structured Query Language (SQL) injection attack?

A. An intrusion prevention system (IPS)
B. An intrusion detection system (IDS)
C. A host-based intrusion detection system (HIDS)
D. A host-based firewall

QUESTION 388
Nonrepudiation can BEST be ensured by using:

A. Strong passwords
B. A digital hash
C. Symmetric encryption
D. Digital signatures

Topic 4: Information Security Program Management

QUESTION 389
The BEST way to ensure that security settings on each platform are in compliance with information security policies and procedures is to:

A. Perform penetration testing
B. Establish security baselines
C. Implement vendor default settings
D. Link policies to an independent standard

QUESTION 390
A web-based business application is being migrated from test to production. Which of the following is the MOST important management signoff for this migration?

A. User
B. Network
C. Operations
D. Database

QUESTION 391
The BEST way to ensure that information security policies are followed is to:

A. Distribute printed copies to all employees
B. Perform periodic reviews for compliance
C. Include escalating penalties for noncompliance
D. Establish an anonymous hotline to report policy abuses

QUESTION 392
The MOST appropriate individual to determine the level of information security needed for a specific business application is the:

A. System developer
B. Information security manager
C. Steering committee
D. System data owner

QUESTION 393
Which of the following will MOST likely reduce the chances of an unauthorized individual gaining access to computing resources by pretending to be an authorized individual needing to have their password reset?

A. Performing reviews of password resets
B. Conducting security awareness programs
C. Increasing the frequency of password changes
D. Implementing automatic password syntax checking

QUESTION 394
Which of the following is the MOST likely to change an organization's culture to one that is more security conscious?

A. Adequate security policies and procedures
B. Periodic compliance reviews
C. Security steering committees
D. Security awareness campaigns

QUESTION 395
The BEST way to ensure that an external service provider complies with organizational security policies is to:

A. Explicitly include the service provider in the security policies
B. Receive acknowledgment in writing stating the provider has read all policies
C. Cross-reference to policies in the service level agreement
D. Perform periodic reviews of the service provider

QUESTION 396
When an emergency security patch is received via electronic mail, the patch should FIRST be:

A. Loaded onto an isolated test machine
B. Decompiled to check for malicious code
C. Validated to ensure its authenticity
D. Copied onto write-once media to prevent tampering

QUESTION 397
In a well-controlled environment, which of the following activities is MOST likely to lead to the introduction of weaknesses in security software?

A. Applying patches
B. Changing access rules
C. Upgrading hardware
D. Backing up files

QUESTION 398
Which of the following is the BEST indicator that security awareness training has been effective?

A. Employees sign to acknowledge the security policy
B. More incidents are being reported
C. A majority of employees have completed training
D. No incidents have been reported in three months

QUESTION 399
Which of the following metrics would be the MOST useful in measuring how well information security is monitoring violation logs?

A. Penetration attempts investigated
B. Violation log reports produced
C. Violation log entries
D. Frequency of corrective actions taken

QUESTION 400
Which of the following change management activities would be a clear indicator that normal operational procedures require examination? A high percentage of:

A. Similar change requests
B. Change request postponements
C. Canceled change requests
D. Emergency change requests

QUESTION 401
Which of the following is the MOST important management signoff for migrating an order processing system from a test environment to a production environment?

A. User
B. Security
C. Operations
D. Database

QUESTION 402
Prior to having a third party perform an attack and penetration test against an organization, the MOST important action is to ensure that:

A. The third party provides a demonstration on a test system
B. Goals and objectives are clearly defined
C. The technical staff has been briefed on what to expect
D. Special backups of production servers are taken

QUESTION 403
When a departmental system continues to be out of compliance with an information security policy's password strength requirements, the BEST action to undertake is to:

A. Submit the issue to the steering committee
B. Conduct an impact analysis to quantify the risks
C. Isolate the system from the rest of the network
D. Request a risk acceptance from senior management

QUESTION 404
Which of the following is MOST important to the successful promotion of good security management practices?

A. Security metrics
B. Security baselines
C. Management support
D. Periodic training

QUESTION 405
Which of the following environments represents the GREATEST risk to organizational security?

A. Locally managed file server
B. Enterprise data warehouse
C. Load-balanced, web server cluster
D. Centrally managed data switch

QUESTION 406
Nonrepudiation can BEST be assured by using:

A. Delivery path tracing
B. Reverse lookup translation
C. Out-of-hand channels
D. Digital signatures

QUESTION 407
Of the following, the BEST method for ensuring that temporary employees do not receive excessive access rights is:

A. Mandatory access controls
B. Discretionary access controls
C. Lattice-based access controls
D. Role-based access controls

QUESTION 408
Which of the following areas is MOST susceptible to the introduction of security weaknesses?

A. Database management
B. Tape backup management
C. Configuration management
D. Incident response management

QUESTION 409
Security policies should be aligned MOST closely with:

A. Industry best practices
B. Organizational needs
C. Generally accepted standards
D. Local laws and regulations

QUESTION 410
The BEST way to determine if an anomaly-based intrusion detection system (IDS) is properly installed is to:

A. Simulate an attack and review IDS performance
B. Use a honeypot to check for unusual activity
C. Audit the configuration of the IDS
D. Benchmark the IDS against a peer site

QUESTION 411
The BEST time to perform a penetration test is after:

A. An attempted penetration has occurred
B. An audit has reported weaknesses in security controls
C. Various infrastructure changes are made
D. A high turnover in systems staff

QUESTION 412
Successful social engineering attacks can BEST be prevented through:

A. Pre-employment screening
B. Close monitoring of users' access patterns
C. Periodic awareness training
D. Efficient termination procedures

QUESTION 413
What is the BEST way to ensure that an intruder who successfully penetrates a network will be detected 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

QUESTION 414
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 (OS) security patches have not been applied
D. Database security defaults to ERP settings

QUESTION 415
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

QUESTION 416
Which of the following will BEST ensure that management takes ownership of the decision-making process for information security?

A. Security policies and procedures
B. Annual self-assessment by management
C. Security steering committees
D. Security awareness campaigns

QUESTION 417
Which of the following is the MOST appropriate individual to implement and maintain the level of information security needed for a specific business application?

A. System analyst
B. Quality control manager
C. Process owner
D. Information security manager

QUESTION 418
What is the BEST way to ensure that contract programmers comply with organizational security policies?

A. Explicitly refer to contractors in the security standards
B. Have the contractors acknowledge in writing the security policies
C. Create penalties for noncompliance in the contracting agreement
D. Perform periodic security reviews of the contractors

QUESTION 419
Which of the following activities is MOST likely to increase the difficulty of totally eradicating malicious code that is not immediately detected?

A. Applying patches
B. Changing access rules
C. Upgrading hardware
D. Backing up files

QUESTION 420
Security awareness training should be provided to new employees:

A. On an as-needed basis
B. During system user training
C. Before they have access to data
D. Along with department staff

QUESTION 421
What is the BEST method to verify that all security patches applied to servers were properly documented?

A. Trace change control requests to operating system (OS) patch logs
B. Trace OS patch logs to OS vendor's update documentation
C. Trace OS patch logs to change control requests
D. Review change control documentation for key servers

QUESTION 422
A security awareness program should:

A. Present top management's perspective
B. Address details on specific exploits
C. Address specific groups and roles
D. Promote security department procedures

QUESTION 423
The PRIMARY objective of security awareness is to:

A. Ensure that security policies are understood
B. Influence employee behavior
C. Ensure legal and regulatory compliance
D. Notify of actions for noncompliance

QUESTION 424
Which of the following will BEST protect against malicious activity by a former employee?

A. Pre-employment screening
B. Close monitoring of users
C. Periodic awareness training
D. Effective termination procedures

QUESTION 425
Which of the following represents a PRIMARY area of interest when conducting a penetration test?

A. Data mining
B. Network mapping
C. Intrusion Detection System (IDS)
D. Customer data

QUESTION 426
The return on investment of information security can BEST be evaluated through which of the following?

A. Support of business objectives
B. Security metrics
C. Security deliverables
D. Process improvement models

QUESTION 427
To help ensure that contract personnel do not obtain unauthorized access to sensitive information, an information security manager should PRIMARILY:

A. Set their accounts to expire in six months or less
B. Avoid granting system administration roles
C. Ensure they successfully pass background checks
D. Ensure their access is approved by the data owner

QUESTION 428
Information security policies should:

A. Address corporate network vulnerabilities
B. Address the process for communicating a violation
C. Be straightforward and easy to understand
D. Be customized to specific groups and roles

QUESTION 429
Which of the following is the BEST way to ensure that a corporate network is adequately secured against external attack?

A. Utilize an intrusion detection system
B. Establish minimum security baselines
C. Implement vendor recommended settings
D. Perform periodic penetration testing

QUESTION 430
Which of the following presents the GREATEST exposure to internal attack on a network?

A. User passwords are not automatically expired
B. All network traffic goes through a single switch
C. User passwords are encoded but not encrypted
D. All users reside on a single internal subnet

QUESTION 431
Which of the following provides the linkage to ensure that procedures are correctly aligned with information security policy requirements?

A. Standards
B. Guidelines
C. Security metrics
D. IT governance

QUESTION 432
Which of the following are the MOST important individuals to include as members of an information security steering committee?

A. Direct reports to the chief information officer
B. IT management and key business process owners
C. Cross-section of end users and IT professionals
D. Internal audit and corporate legal departments

QUESTION 433
Security audit reviews should PRIMARILY:

A. Ensure that controls operate as required
B. Ensure that controls are cost-effective
C. Focus on preventive controls
D. Ensure controls are technologically current

QUESTION 434
Which of the following is the MOST appropriate method to protect a password that opens a confidential file?

A. Delivery path tracing
B. Reverse lookup translation
C. Out-of-band channels
D. Digital signatures

QUESTION 435
What is the MOST effective access control method to prevent users from sharing files with unauthorized users?

A. Mandatory
B. Discretionary
C. Walled garden
D. Role-based

QUESTION 436
Which of the following is an inherent weakness of signature-based intrusion detection systems?

A. A higher number of false positives
B. New attack methods will be missed
C. Long duration probing will be missed
D. Attack profiles can be easily spoofed

QUESTION 437
Data owners are normally responsible for which of the following?

A. Applying emergency changes to application data
B. Administering security over database records
C. Migrating application code changes to production
D. Determining the level of application security required

QUESTION 438
Which of the following is the MOST appropriate individual to ensure that new exposures have not been introduced into an existing application during the change management process?

A. System analyst
B. System user
C. Operations manager
D. Data security officer

QUESTION 439
What is the BEST way to ensure users comply with organizational security requirements for password complexity?

A. Include password construction requirements in the security standards
B. Require each user to acknowledge the password requirements
C. Implement strict penalties for user noncompliance
D. Enable system-enforced password configuration

QUESTION 440
Which of the following is the MOST appropriate method for deploying operating system (OS) patches to production application servers?

A. Batch patches into frequent server updates
B. Initially load the patches on a test machine
C. Set up servers to automatically download patches
D. Automatically push all patches to the servers

QUESTION 441
Which of the following would present the GREATEST risk to information security?

A. Virus signature files updates are applied to all servers every day
B. Security access logs are reviewed within five business days
C. Critical patches are applied within 24 hours of their release
D. Security incidents are investigated within five business days

QUESTION 442
The PRIMARY reason for using metrics to evaluate information security is to:

A. Identify security weaknesses
B. Justify budgetary expenditures
C. Enable steady improvement
D. Raise awareness on security issues

QUESTION 443
What is the BEST method to confirm that all firewall rules and router configuration settings are adequate?

A. Periodic review of network configuration
B. Review intrusion detection system (IDS) logs for evidence of attacks
C. Periodically perform penetration tests
D. Daily review of server logs for evidence of hacker activity

QUESTION 444
Which of the following is MOST important for measuring the effectiveness of a security awareness program?

A. Reduced number of security violation reports
B. A quantitative evaluation to ensure user comprehension
C. Increased interest in focus groups on security issues
D. Increased number of security violation reports

QUESTION 445
Which of the following is the MOST important action to take when engaging third-party consultants to conduct an attack and penetration test?

A. Request a list of the software to be used
B. Provide clear directions to IT staff
C. Monitor intrusion detection system (IDS) and firewall logs closely
D. Establish clear rules of engagement

QUESTION 446
Which of the following will BEST prevent an employee from using a USB drive to copy files from desktop computers?

A. Restrict the available drive allocation on all PCs
B. Disable universal serial bus (USB) ports on all desktop devices
C. Conduct frequent awareness training with noncompliance penalties
D. Establish strict access controls to sensitive information

QUESTION 447
Which of the following is the MOST important area of focus when examining potential security compromise of a new wireless network?

A. Signal strength
B. Number of administrators
C. Bandwidth
D. Encryption strength

QUESTION 448
Good information security standards should:

A. Define precise and unambiguous allowable limits
B. Describe the process for communicating violations
C. Address high-level objectives of the organization
D. Be updated frequently as new software is released

QUESTION 449
Good information security procedures should:

A. Define the allowable limits of behavior
B. Underline the importance of security governance
C. Describe security baselines for each platform
D. Be updated frequently as new software is released

QUESTION 450
What is the MAIN drawback of e-mailing password-protected zip files across the Internet? They:

A. All use weak encryption.
B. Are decrypted by the firewall.
C. May be quarantined by mail filters.
D. May be corrupted by the receiving mail server.

QUESTION 451
A major trading partner with access to the internal network is unwilling or unable to remediate serious information security exposures within its environment. Which of the following is the BEST recommendation?

A. Sign a legal agreement assigning them all liability for any breach
B. Remove all trading partner access until the situation improves
C. Set up firewall rules restricting network traffic from that location
D. Send periodic reminders advising them of their noncompliance

QUESTION 452
Documented standards/procedures for the use of cryptography across the enterprise should PRIMARILY:

A. Define the circumstances where cryptography should be used
B. Define cryptographic algorithms and key lengths
C. Describe handling procedures of cryptographic keys
D. Establish the use of cryptographic solutions

QUESTION 453
Which of the following is the MOST immediate consequence of failing to tune a newly installed intrusion detection system (IDS) with the threshold set to a low value?

A. The number of false positives increases
B. The number of false negatives increases
C. Active probing is missed
D. Attack profiles are ignored

QUESTION 454
What is the MOST appropriate change management procedure for the handling of emergency program changes?

A. Formal documentation does not need to be completed before the change
B. Business management approval must be obtained prior to the change
C. Documentation is completed with approval soon after the change
D. All changes must follow the same process

QUESTION 455
Who is ultimately responsible for ensuring that information is categorized and that protective measures are taken?

A. Information security officer
B. Security steering committee
C. Data owner
D. Data custodian

QUESTION 456
The PRIMARY focus of the change control process is to ensure that changes are:

A. Authorized
B. Applied
C. Documented
D. Tested

QUESTION 457
An information security manager has been asked to develop a change control process. What is the FIRST thing the information security manager should do?

A. Research best practices
B. Meet with stakeholders
C. Establish change control procedures
D. Identify critical systems

QUESTION 458
A critical device is delivered with a single user and password that is required to be shared for multiple users to access the device. An information security manager has been tasked with ensuring all access to the device is authorized. Which of the following would be the MOST efficient means to accomplish this?

A. Enable access through a separate device that requires adequate authentication
B. Implement manual procedures that require password change after each use
C. Request the vendor to add multiple user IDs
D. Analyze the logs to detect unauthorized access

QUESTION 459
Which of the following documents would be the BEST reference to determine whether access control mechanisms are appropriate for a critical application?

A. User security procedures
B. Business process flow
C. IT security policy
D. Regulatory requirements

QUESTION 460
Which of the following is the MOST important process that an information security manager needs to negotiate with an outsource service provider?

A. The right to conduct independent security reviews
B. A legally binding data protection agreement
C. Encryption between the organization and the provider
D. A joint risk assessment of the system

QUESTION 461
Which resource is the MOST effective in preventing physical access tailgating / piggybacking?

A. Card key door locks
B. Photo identification
C. Awareness training
D. Biometric scanners

QUESTION 462
In business-critical applications, where shared access to elevated privileges by a small group is necessary, the BEST approach to implement adequate segregation of duties is to:

A. Ensure access to individual functions can be granted to individual users only
B. Implement role-based access control in the application
C. Enforce manual procedures ensuring separation of conflicting duties
D. Create service accounts that can only be used by authorized team members

QUESTION 463
In business-critical applications, user access should be approved by the:

A. Information security manager
B. Data owner
C. Data custodian
D. Business management

QUESTION 464
In organizations where availability is a primary concern, the MOST critical success factor of the patch management procedure would be the:

A. Testing time window prior to deployment
B. Technical skills of the team responsible
C. Certification of validity for deployment
D. Automated deployment to all the servers

QUESTION 465
To ensure that all information security procedures are functional and accurate, they should be designed with the involvement of:

A. End users
B. Legal counsel
C. Operational units
D. Audit management

QUESTION 466
An information security manager reviewed the access control lists and observed that privileged access was granted to an entire department. Which of the following should the information security manager do FIRST?

A. Review the procedures for granting access
B. Establish procedures for granting emergency access
C. Meet with data owners to understand business needs
D. Redefine and implement proper access rights

QUESTION 467
When security policies are strictly enforced, the initial impact is that:

A. They may have to be modified more frequently
B. They will be less subject to challenge
C. The total cost of security is increased
D. The need for compliance reviews is decreased

QUESTION 468
A business partner of a factory has remote read-only access to material inventory to forecast future acquisition orders. An information security manager should PRIMARILY ensure that there is:

A. An effective control over connectivity and continuity
B. A service level agreement (SLA) including code escrow
C. A business impact analysis (BIA)
D. A third-party certification

QUESTION 469
Which of the following should be in place before a black box penetration test begins?

A. IT management approval
B. Proper communication and awareness training
C. A clearly stated definition of scope
D. An incident response plan

QUESTION 470
What is the MOST important element to include when developing user security awareness material?

A. Information regarding social engineering
B. Detailed security policies
C. Senior management endorsement
D. Easy-to-read and compelling information

QUESTION 471
What is the MOST important success factor in launching a corporate information security awareness program?

A. Adequate budgetary support
B. Centralized program management
C. Top-down approach
D. Experience of the awareness trainers

QUESTION 472
Which of the following events generally has the highest information security impact?

A. Opening a new office
B. Merging with another organization
C. Relocating the data center
D. Rewiring the network

QUESTION 473
The configuration management plan should PRIMARILY be based upon input from:

A. Business process owners
B. The information security manager
C. The security steering committee
D. IT senior management

QUESTION 474
Which of the following is the MOST effective, positive method to promote security awareness?

A. Competitions and rewards for compliance
B. Lock-out after three incorrect password attempts
C. Strict enforcement of password formats
D. Disciplinary action for noncompliance

QUESTION 475
An information security program should focus on:

A. Best practices also in place at peer companies
B. Solutions codified in international standards
C. Key controls identified in risk assessments
D. Continued process improvement

QUESTION 476
Who should determine the appropriate classification of accounting ledger data located on a database server and maintained by a database administrator in the IT department?

A. Database administrator (DBA)
B. Finance department management
C. Information security manager
D. IT department management

QUESTION 477
Which of the following would be the MOST significant security risk in a pharmaceutical institution?

A. Compromised customer information
B. Unavailability of online transactions
C. Theft of security tokens
D. Theft of a Research and Development laptop

QUESTION 478
Which of the following is the BEST tool to maintain the currency and coverage of an information security program within an organization?

A. The program's governance oversight mechanisms
B. Information security periodicals and manuals
C. The program's security architecture and design
D. Training and certification of the information security team

QUESTION 479
Which of the following would BEST assist an information security manager in measuring the existing level of development of security processes against their desired state?

A. Security audit reports
B. Balanced scorecard
C. Capability maturity model (CMM)
D. Systems and business security architecture

QUESTION 480
Who is responsible for raising awareness of the need for adequate funding for risk action plans?

A. Chief information officer (CIO)
B. Chief financial officer (CFO)
C. Information security manager
D. Business unit management

QUESTION 481
Managing the life cycle of a digital certificate is a role of a(n):

A. System administrator
B. Security administrator
C. System developer
D. Independent trusted source

QUESTION 482
Which of the following would be MOST critical to the successful implementation of a biometric authentication system?

A. Budget allocation
B. Technical skills of staff
C. User acceptance
D. Password requirements

QUESTION 483
Change management procedures to ensure that disaster recovery / business continuity plans are kept up-to-date can be BEST achieved through which of the following?

A. Reconciliation of the annual systems inventory to the disaster recovery / business continuity plans
B. Periodic audits of the disaster recovery / business continuity plans
C. Comprehensive walk-through testing
D. Inclusion as a required step in the system life cycle process

QUESTION 484
When a new key business application goes into production, the PRIMARY reason to update relevant business impact analysis (BIA) and business continuity / disaster recovery plans is because:

A. This is a requirement of the security policy
B. Software licenses may expire in the future without warning
C. The asset inventory must be maintained
D. Service level agreements may not otherwise be met

QUESTION 485
To reduce the possibility of service interruptions, an entity enters into contracts with multiple Internet service providers (ISPs). Which of the following would be the MOST important item to include?

A. Service level agreements (SLAs)
B. Right to audit clause
C. Intrusion detection system (IDS) services
D. Spam filtering services

QUESTION 486
To mitigate a situation where one of the programmers of an application requires access to production data, the information security manager could BEST recommend to:

A. Create a separate account for the programmer as a power user
B. Log all of the programmers' activity for review by supervisor
C. Have the programmer sign a letter accepting full responsibility
D. Perform regular audits of the application

QUESTION 487
Before engaging outsourced providers, an information security manager should ensure that the organization's data classification requirements:

A. Are compatible with the provider's own classification
B. Are communicated to the provider
C. Exceed those of the outsourcer
D. Are stated in the contract

QUESTION 488
What is the GREATEST risk when there is an excessive number of firewall rules?

A. One rule may override another rule in the chain and create a loophole
B. Performance degradation of the whole network
C. The firewall may not support the increasing number of rules due to limitations
D. The firewall may show abnormal behavior and may crash or automatically shut down

QUESTION 489
Which of the following would be the MOST appropriate physical security solution for the main entrance to a data center?

A. Mantrap
B. Biometric lock
C. Closed-circuit television (CCTV)
D. Security guard

QUESTION 490
What is the GREATEST advantage of documented guidelines and operating procedures from a security perspective?

A. Provide detailed instructions on how to carry out different types of tasks
B. Ensure consistency of activities to provide a more stable environment
C. Ensure compliance to security standards and regulatory requirements
D. Ensure reusability to meet compliance to quality requirements

QUESTION 491
What is the BEST way to ensure data protection upon termination of employment?

A. Retrieve identification badge and card keys
B. Retrieve all personal computer equipment
C. Erase all of the employee's folders
D. Ensure all logical access is removed

QUESTION 492
The MOST important reason for formally documenting security procedures is to ensure:

A. Processes are repeatable and sustainable
B. Alignment with business objectives
C. Auditability by regulatory agencies
D. Objective criteria for the application of metrics

QUESTION 493
Which of the following is the BEST approach for an organization desiring to protect its intellectual property?

A. Conduct awareness sessions on intellectual property policy
B. Require all employees to sign a nondisclosure agreement
C. Promptly remove all access when an employee leaves the organization
D. Restrict access to a need-to-know basis

QUESTION 494
The "separation of duties" principle is violated if which of the following individuals has update rights to the database access control list (ACL)?

A. Data owner
B. Data custodian
C. Systems programmer
D. Security administrator

QUESTION 495
An account with full administrative privileges over a production file is found to be accessible by a member of the software development team. This account was setup to allow the developer to download non-sensitive production data for software testing purposes. The information security manager should recommend which of the following?

A. Restrict account access to read only
B. Log all usage of this account
C. Suspend the account and activate only when needed
D. Require that a change request be submitted for each download

QUESTION 496
Which would be the BEST recommendation to protect against phishing attacks?

A. Install an antispam system
B. Publish security guidance for customers
C. Provide security awareness to the organization's staff
D. Install an application-level firewall

QUESTION 497
Which of the following is the BEST indicator that an effective security control is built into an organization?

A. The monthly service level statistics indicate a minimal impact from security issues
B. The cost of implementing a security control is less than the value of the assets
C. The percentage of systems that is compliant with security standards
D. The audit reports do not reflect any significant findings on security

QUESTION 498
What is the BEST way to alleviate security team understaffing while retaining the capability in-house?

A. Hire a contractor that would not be included in the permanent headcount
B. Outsource with a security services provider while retaining the control internally
C. Establish a virtual security team from competent employees across the company
D. Provide cross training to minimize the existing resources gap

QUESTION 499
An information security manager wishing to establish security baselines would:

A. Include appropriate measurements in the system development life cycle
B. Implement the security baselines to establish information security best practices
C. Implement the security baselines to fulfill laws and applicable regulations in different jurisdictions
D. Leverage information security as a competitive advantage

QUESTION 500
Requiring all employees and contractors to meet personnel security/suitability requirements commensurate with their position sensitivity level and subject to personnel screening is an example of a security:

A. Policy
B. Strategy
C. Guideline
D. Baseline

QUESTION 501
An organization's information security manager has been asked to hire a consultant to help assess the maturity level of the organization's information security management. The MOST important element of the request for proposal (RFP) is the:

A. References from other organizations
B. Past experience of the engagement team
C. Sample deliverable
D. Methodology used in the assessment

QUESTION 502
Several business units reported problems with their systems after multiple security patches were deployed. The FIRST step in handling this problem would be to:

A. Assess the problems and institute rollback procedures, if needed
B. Disconnect the systems from the network until the problems are corrected
C. Immediately uninstall the patches from these systems
D. Immediately contact the vendor regarding the problems that occurred

QUESTION 503
When defining a service level agreement (SLA) regarding the level of data confidentiality that is handled by a third-party service provider, the BEST indicator of compliance would be the:

A. Access control matrix
B. Encryption strength
C. Authentication mechanism
D. Data repository

QUESTION 504
The PRIMARY reason for involving information security at each stage in the systems development life cycle (SDLC) is to identify the security implications and potential solutions required for:

A. Identifying vulnerabilities in the system
B. Sustaining the organization's security posture
C. The existing systems that will be affected
D. Complying with segregation of duties

QUESTION 505
The implementation of continuous monitoring controls is the BEST option where:

A. Incidents may have a high impact and frequency
B. Legislation requires strong information security controls
C. Incidents may have a high impact but low frequency
D. Electronic commerce is a primary business driver

QUESTION 506
A third party was engaged to develop a business application. Which of the following would an information security manager BEST test for the existence of back doors?

A. System monitoring for traffic on network ports
B. Security code reviews for the entire application
C. Reverse engineering the application binaries
D. Running the application from a high-privileged account on a test system

QUESTION 507
An information security manager reviewing firewall rules will be MOST concerned if the firewall allows:

A. Source routing
B. Broadcast propagation
C. Unregistered ports
D. Non-standard protocols

QUESTION 508
What is the MOST cost-effective means of improving security awareness of staff personnel?

A. Employee monetary incentives
B. User education and training
C. A zero-tolerance security policy
D. Reporting of security infractions

QUESTION 509
Which of the following is the MOST effective at preventing an unauthorized individual from following an authorized person through a secured entrance (tailgating or piggybacking)?

A. Card-key door locks
B. Photo identification
C. Biometric scanners
D. Awareness training

QUESTION 510
Data owners will determine what access and authorizations users will have by:

A. Delegating authority to data custodian
B. Cloning existing user accounts
C. Determining hierarchical preferences
D. Mapping to business needs

QUESTION 511
Which of the following is the MOST likely outcome of a well-designed information security awareness course?

A. Increased reporting of security incidents to the incident response function
B. Decreased reporting of security incidents to the incident response function
C. Decrease in the number of password resets
D. Increase in the number of identified system vulnerabilities

QUESTION 512
Which item would be the BEST to include in the information security awareness training program for new general staff employees?

A. Review of various security models
B. Discussion of how to construct strong passwords
C. Review of roles that have privileged access
D. Discussion of vulnerability assessment results

QUESTION 513
A critical component of a continuous improvement program for information security is:

A. Measuring processes and providing feedback
B. Developing a service level agreement (SLA) for security
C. Tying corporate security standards to a recognized international standard
D. Ensuring regulatory compliance

QUESTION 514
The management staff of an organization that does not have a dedicated security function decides to use its IT manager to perform a security review. The MAIN job requirement in this arrangement is that the IT manager:

A. Report risks in other departments
B. Obtain support from other departments
C. Report significant security risks
D. Have knowledge of security standards

QUESTION 515
An organization has implemented an enterprise resource planning (ERP) system used by 500 employees from various departments. Which of the following access control approaches is MOST appropriate?

A. Rule-based
B. Mandatory
C. Discretionary
D. Role-based

QUESTION 516
An organization plans to contract with an outside service provider to host its corporate web site. The MOST important concern for the information security manager is to ensure that:

A. An audit of the service provider uncovers no significant weakness
B. The contract includes a nondisclosure agreement (NDA) to protect the organization's intellectual property
C. The contract should mandate that the service provider will comply with security policies
D. The third-party service provider conducts regular penetration testing

QUESTION 517
Which of the following is the MAIN objective in contracting with an external company to perform penetration testing?

A. To mitigate technical risks
B. To have an independent certification of network security
C. To receive an independent view of security exposures
D. To identify a complete list of vulnerabilities

QUESTION 518
A new port needs to be opened in a perimeter firewall. Which of the following should be the FIRST step before initiating any changes?

A. Prepare an impact assessment report
B. Conduct a penetration test
C. Obtain approval from senior management
D. Back up the firewall configuration and policy files

QUESTION 519
An organization plans to outsource its customer relationship management (CRM) to a third-party service provider. Which of the following should the organization do FIRST?

A. Request that the third-party provider perform background checks on their employees
B. Perform an internal risk assessment to determine needed controls
C. Audit the third-party provider to evaluate their security controls
D. Perform a security assessment to detect security vulnerabilities

QUESTION 520
Which of the following would raise security awareness among an organization's employees?

A. Distributing industry statistics about security incidents
B. Monitoring the magnitude of incidents
C. Encouraging employees to behave in a more conscious manner
D. Continually reinforcing the security policy

QUESTION 521
Which of the following is the MOST appropriate method of ensuring password strength in a large organization?

A. Attempt to reset several passwords to weaker values
B. Install code to capture passwords for periodic audit
C. Sample a subset of users and request their passwords for review
D. Review general security settings on each platform

QUESTION 522
What is the MOST cost-effective method of identifying new vendor vulnerabilities?

A. External vulnerability reporting sources
B. Periodic vulnerability assessments performed by consultants
C. Intrusion prevention software
D. Honey pots located in the DMZ

QUESTION 523
Which of the following is the BEST approach for improving information security management processes?

A. Conduct periodic security audits
B. Perform periodic penetration testing
C. Define and monitor security metrics
D. Survey business units for feedback

QUESTION 524
An effective way of protecting applications against Structured Query Language (SQL) injection vulnerability is to:

A. Validate and sanitize client-side inputs
B. Harden the database listener component
C. Normalize the database schema to the third normal form
D. Ensure that the security patches are updated on operating systems

QUESTION 525
The root cause of a successful cross site request forgery (XSRF) attack against an application is that the vulnerable application:

A. Uses multiple redirects for completing a data commit transaction
B. Has implemented cookies as the sole authentication mechanism
C. Has been installed with a non-legitimate license key
D. Is hosted on a server along with other applications

QUESTION 526
Of the following, retention of business records should be PRIMARILY based on:

A. Periodic vulnerability assessment
B. Regulatory and legal requirements
C. Device storage capacity and longevity
D. Past litigation

QUESTION 527
An organization is entering into an agreement with a new business partner to conduct customer mailings. What is the MOST important action that the information security manager needs to perform?

A. A due diligence security review of the business partner's security controls
B. Ensuring that the business partner has an effective business continuity program
C. Ensuring that the third party is contractually obligated to all relevant security requirements
D. Talking to other clients of the business partner to check references for performance

QUESTION 528
An organization that outsourced its payroll processing performed an independent assessment of the security controls of the third party, per policy requirements. Which of the following is the MOST useful requirement to include in the contract?

A. Right to audit
B. Non-disclosure agreement
C. Proper firewall implementation
D. Dedicated security manager for monitoring compliance

QUESTION 529
Which of the following is the MOST critical activity to ensure the ongoing security of outsourced IT services?

A. Provide security awareness training to the third-party provider's employees
B. Conduct regular security reviews of the third-party provider
C. Include security requirements in the service contract
D. Request that the third-party provider comply with the organization's information security policy

QUESTION 530
An organization's operations staff places payment files in a shared network folder and then the disbursement staff picks up the files for payment processing. This manual intervention will be automated some months later, thus cost-efficient controls are sought to protect against file alterations. Which of the following would be the BEST solution?

A. Design a training program for the staff involved to heighten information security awareness
B. Set role-based access permissions on the shared folder
C. The end user develops a PC macro program to compare sender and recipient file contents
D. Shared folder operators sign an agreement to pledge not to commit fraudulent activities

QUESTION 531
Which of the following BEST ensures that security risks will be re-evaluated when modifications in application developments are made?

A. A problem management process
B. Background screening
C. A change control process
D. Business impact analysis (BIA)

QUESTION 532
Which is the BEST way to measure and prioritize aggregate risk deriving from a chain of linked system vulnerabilities?

A. Vulnerability scans
B. Penetration tests
C. Code reviews
D. Security audits

QUESTION 533
In which of the following system development life cycle (SDLC) phases are access control and encryption algorithms chosen?

A. Procedural design
B. Architectural design
C. System design specifications
D. Software development

QUESTION 534
Which of the following is generally considered a fundamental component of an information security program?

A. Role-based access control systems
B. Automated access provisioning
C. Security awareness training
D. Intrusion prevention systems (IPSs)

QUESTION 535
How would an organization know if its new information security program is accomplishing its goals?

A. Key metrics indicate a reduction in incident impacts
B. Senior management has approved the program and is supportive of it
C. Employees are receptive to changes that were implemented
D. There is an immediate reduction in reported incidents

QUESTION 536
A benefit of using a full disclosure (white box) approach as compared to a blind (black box) approach to penetration testing is that:

A. It simulates the real-life situation of an external security attack
B. Human intervention is not required for this type of test
C. Less time is spent on reconnaissance and information gathering
D. Critical infrastructure information is not revealed to the tester

QUESTION 537
Which of the following is the BEST method to reduce the number of incidents of employees forwarding spam and chain e-mail messages?

A. Acceptable use policy
B. Setting low mailbox limits
C. User awareness training
D. Taking disciplinary action

QUESTION 538
Which of the following is the BEST approach to mitigate online brute-force attacks on user accounts?

A. Passwords stored in encrypted form
B. User awareness
C. Strong passwords that are changed periodically
D. Implementation of lock-out policies

QUESTION 539
Which of the following measures is the MOST effective deterrent against disgruntled staff abusing their privileges?

A. Layered defense strategy
B. System audit log monitoring
C. Signed acceptable use policy
D. High-availability systems

QUESTION 540
The advantage of sending messages using steganographic techniques, as opposed to utilizing encryption, is that:

A. The existence of messages is unknown
B. Required key sizes are smaller
C. Traffic cannot be sniffed
D. Reliability of the data is higher in transit

QUESTION 541
As an organization grows, exceptions to information security policies that were not originally specified may become necessary at a later date. In order to ensure effective management of business risks, exceptions to such policies should be:

A. Considered at the discretion of the information owner
B. Approved by the next higher person in the organizational structure
C. Formally managed within the information security framework
D. Reviewed and approved by the security manager

QUESTION 542
There is reason to believe that a recently modified web application has allowed unauthorized access. Which is the BEST way to identify an application backdoor?

A. Black box pen test
B. Security audit
C. Source code review
D. Vulnerability scan

QUESTION 543
Simple Network Management Protocol v2 (SNMP v2) is used frequently to monitor networks. Which of the following vulnerabilities does it always introduce?

A. Remote buffer overflow
B. Cross site scripting
C. Clear text authentication
D. Man-in-the-middle attack

QUESTION 544

Which of the following is the FIRST phase in which security should be addressed in the development cycle of a project?

A. Design
B. Implementation
C. Application security testing
D. Feasibility

Topic 5: Incident Management and Response

QUESTION 545
Which of the following should be determined FIRST when establishing a business continuity program?

A. Cost to rebuild information processing facilities
B. Incremental daily cost of the unavailability of systems
C. Location and cost of offsite recovery facilities
D. Composition and mission of individual recovery teams

QUESTION 546
A desktop computer that was involved in a computer security incident should be secured as evidence by:

A. Disconnecting the computer from all power sources
B. Disabling all local user accounts except for one administrator
C. Encrypting local files and uploading exact copies to a secure server
D. Copying all files using the operating system (OS) to write-once media

QUESTION 547
A company has a network of branch offices with local file/print and mail servers; each branch individually contracts a hot site. Which of the following would be the GREATEST weakness in recovery capability?

A. Exclusive use of the hot site is limited to six weeks
B. The hot site may have to be shared with other customers
C. The time of declaration determines site access priority
D. The provider services all major companies in the area

QUESTION 548
Which of the following actions should be taken when an online trading company discovers a network attack in progress?

A. Shut off all network access points
B. Dump all event logs to removable media
C. Isolate the affected network segment
D. Enable trace logging on all event

QUESTION 549
The BEST method for detecting and monitoring a hacker's activities without exposing information assets to unnecessary risk is to utilize:

A. Firewalls
B. Bastion hosts
C. Decoy files
D. Screened subnets

QUESTION 550
The FIRST priority when responding to a major security incident is:

A. Documentation
B. Monitoring
C. Restoration
D. Containment

QUESTION 551
Which of the following is the MOST important to ensure a successful recovery?

A. Backup media is stored offsite
B. Recovery location is secure and accessible
C. More than one hot site is available
D. Network alternate links are regularly tested

QUESTION 552
Which of the following is the MOST important element to ensure the success of a disaster recovery test at a vendor-provided hot site?

A. Tests are scheduled on weekends
B. Network IP addresses are predefined
C. Equipment at the hot site is identical
D. Business management actively participates

QUESTION 553
At the conclusion of a disaster recovery test, which of the following should ALWAYS be performed prior to leaving the vendor's hot site facility?

A. Erase data and software from devices
B. Conduct a meeting to evaluate the test
C. Complete an assessment of the hot site provider
D. Evaluate the results from all test scripts

QUESTION 554
An incident response policy must contain:

A. Updated call trees
B. Escalation criteria
C. Press release templates
D. Critical backup files inventory

QUESTION 555
The BEST approach in managing a security incident involving a successful penetration should be to:

A. Allow business processes to continue during the response
B. Allow the security team to assess the attack profile
C. Permit the incident to continue to trace the source
D. Examine the incident response process for deficiencies

QUESTION 556
A post-incident review should be conducted by an incident management team to determine:

A. Relevant electronic evidence
B. Lessons learned
C. Hacker's identity
D. Areas affected

QUESTION 557
An organization with multiple data centers has designated one of its own facilities as the recovery site. The MOST important concern is the:

A. Communication line capacity between data centers
B. Current processing capacity loads at data centers
C. Differences in logical security at each center
D. Synchronization of system software release versions

QUESTION 558
Which of the following is MOST important in determining whether a disaster recovery test is successful?

A. Only business data files from offsite storage are used
B. IT staff fully recovers the processing infrastructure
C. Critical business processes are duplicated
D. All systems are restored within recovery time objectives (RTOs)

QUESTION 559
Which of the following is MOST important when deciding whether to build an alternate facility or subscribe to a third-party hot site?

A. Cost to build a redundant processing facility and invocation
B. Daily cost of losing critical systems and recovery time objectives (RTOs)
C. Infrastructure complexity and system sensitivity
D. Criticality results from the business impact analysis (BIA)

QUESTION 560
A new e-mail virus that uses an attachment disguised as a picture file is spreading rapidly over the Internet. Which of the following should be performed FIRST in response to this threat?

A. Quarantine all picture files stored on file servers
B. Block all e-mails containing picture file attachments
C. Quarantine all mail servers connected to the Internet
D. Block incoming Internet mail, but permit outgoing mail

QUESTION 561
When a large organization discovers that it is the subject of a network probe, which of the following actions should be taken?

A. Reboot the router connecting the DMZ to the firewall
B. Power down all servers located on the DMZ segment
C. Monitor the probe and isolate the affected segment
D. Enable server trace logging on the affected segment

QUESTION 562
Which of the following terms and conditions represent a significant deficiency if included in a commercial hot site contract?

A. A hot site facility will be shared in multiple disaster declarations
B. All equipment is provided "at time of disaster, not on floor"
C. The facility is subject to a "first-come, first-served" policy
D. Equipment may be substituted with equivalent model

QUESTION 563
Which of the following should be performed FIRST in the aftermath of a denial-of-service attack?

A. Restore servers from backup media stored offsite
B. Conduct an assessment to determine system status
C. Perform an impact analysis of the outage
D. Isolate the screened subnet

QUESTION 564
Which of the following is the MOST important element to ensure the successful recovery of a business during a disaster?

A. Detailed technical recovery plans are maintained offsite
B. Network redundancy is maintained through separate providers
C. Hot site equipment needs are recertified on a regular basis
D. Appropriate declaration criteria have been established

QUESTION 565
The business continuity policy should contain which of the following?

A. Emergency call trees
B. Recovery criteria
C. Business impact assessment (BIA)
D. Critical backups inventory

QUESTION 566
The PRIMARY purpose of installing an intrusion detection system (IDS) is to identify:

A. Weaknesses in network security
B. Patterns of suspicious access
C. How an attack was launched on the network
D. Potential attacks on the internal network

QUESTION 567
When an organization is using an automated tool to manage and house its business continuity plans, which of the following is the PRIMARY concern?

A. Ensuring accessibility should a disaster occur
B. Versioning control as plans are modified
C. Broken hyperlinks to resources stored elsewhere
D. Tracking changes in personnel and plan assets

QUESTION 568
Which of the following is the BEST way to verify that all critical production servers are utilizing up-to-date virus signature files?

A. Verify the date that signature files were last pushed out
B. Use a recently identified benign virus to test if it is quarantined
C. Research the most recent signature file and compare to the console
D. Check a sample of servers that the signature files are current

QUESTION 569
Which of the following actions should be taken when an information security manager discovers that a hacker is foot printing the network perimeter?

A. Reboot the border router connected to the firewall
B. Check IDS logs and monitor for any active attacks
C. Update IDS software to the latest available version
D. Enable server trace logging on the DMZ segment

QUESTION 570
Which of the following are the MOST important criteria when selecting virus protection software?

A. Product market share and annualized cost
B. Ability to interface with intrusion detection system (IDS) software and firewalls
C. Alert notifications and impact assessments for new viruses
D. Ease of maintenance and frequency of updates

QUESTION 571
Which of the following is the MOST serious exposure of automatically updating virus signature files on every desktop each Friday at 11:00 pm (23.00 hrs)?

A. Most new viruses' signatures are identified over weekends
B. Technical personnel are not available to support the operation
C. Systems are vulnerable to new viruses during the intervening week
D. The update's success or failure is not known until Monday

QUESTION 572
When performing a business impact analysis (BIA), which of the following should calculate the recovery time and cost estimates?

A. Business continuity coordinator
B. Information security manager
C. Business process owners
D. Industry averages benchmarks

QUESTION 573
Which of the following is MOST closely associated with a business continuity program?

A. Confirming that detailed technical recovery plans exist
B. Periodically testing network redundancy
C. Updating the hot site equipment configuration every quarter
D. Developing recovery time objectives (RTOs) for critical functions

QUESTION 574
Which of the following application systems should have the shortest recovery time objective (RTO)?

A. Contractor payroll
B. Change management
C. E-commerce web site
D. Fixed asset system

QUESTION 575
A computer incident response team (CIRT) manual should PRIMARILY contain which of the following documents?

A. Risk assessment results
B. Severity criteria
C. Emergency call tree directory
D. Table of critical backup files

QUESTION 576
The PRIMARY purpose of performing an internal attack and penetration test as part of an incident response program is to identify:

A. Weaknesses in network and server security
B. Ways to improve the incident response process
C. Potential attack vectors on the network perimeter
D. The optimum response to internal hacker attacks

QUESTION 577
Which of the following would represent a violation of the chain of custody when a backup tape has been identified as evidence in a fraud investigation? The tape was:

A. Removed into the custody of law enforcement investigators
B. Kept in the tape library pending further analysis
C. Sealed in a signed envelope and locked in a safe under dual control
D. Handed over to authorized independent investigators

QUESTION 578
When properly tested, which of the following would MOST effectively support an information security manager in handling a security breach?

A. Business continuity plan
B. Disaster recovery plan
C. Incident response plan
D. Vulnerability management plan

QUESTION 579
Isolation and containment measures for a compromised computer have been taken and information security management is now investigating. What is the MOST appropriate next step?

A. Run a forensics tool on the machine to gather evidence
B. Reboot the machine to break remote connections
C. Make a copy of the whole system's memory
D. Document current connections and open Transmission Control Protocol/User Datagram Protocol (TCP / UDP) ports

QUESTION 580
Why is "slack space" of value to an information security manager as part of an incident investigation?

A. Hidden data may be stored there
B. The slack space contains login information
C. Slack space is encrypted
D. It provides flexible space for the investigation

QUESTION 581
What is the PRIMARY objective of a post-event review in incident response?

A. Adjust budget provisioning
B. Preserve forensic data
C. Improve the response process
D. Ensure the incident is fully documented

QUESTION 582
Detailed business continuity plans should be based PRIMARILY on:

A. Consideration of different alternatives
B. The solution that is least expensive
C. Strategies that cover all applications
D. Strategies validated by senior management

QUESTION 583
A web server in a financial institution that has been compromised using a super-user account has been isolated, and proper forensic processes have been followed. The next step should be to:

A. Rebuild the server from the last verified backup
B. Place the web server in quarantine
C. Shut down the server in an organized manner
D. Rebuild the server with original media and relevant patches

QUESTION 584
Evidence from a compromised server has to be acquired for a forensic investigation. What would be the BEST source?

A. A bit-level copy of all hard drive data
B. The last verified backup stored offsite
C. Data from volatile memory
D. Backup servers

QUESTION 585
In the course of responding to an information security incident, the BEST way to treat evidence for possible legal action is defined by:

A. International standards
B. Local regulations
C. Generally accepted best practices
D. Organizational security policies

QUESTION 586
Emergency actions are taken at the early stage of a disaster with the purpose of preventing injuries or loss of life and:

A. Determining the extent of property damage
B. Preserving environmental conditions
C. Ensuring orderly plan activation
D. Reducing the extent of operational damage

QUESTION 587
What is the FIRST action an information security manager should take when a company laptop is reported stolen?

A. Evaluate the impact of the information loss
B. Update the corporate laptop inventory
C. Ensure compliance with reporting procedures
D. Disable the user account immediately

QUESTION 588
Which of the following actions should take place immediately after a security breach is reported to an information security manager?

A. Confirm the incident
B. Determine impact
C. Notify affected stakeholders
D. Isolate the incident

QUESTION 589
When designing the technical solution for a disaster recovery site, the PRIMARY factor that should be taken into consideration is the:

A. Services delivery objective
B. Recovery time objective (RTO)
C. Recovery window
D. Maximum tolerable outage (MTO)

QUESTION 590
In designing a backup strategy that will be consistent with a disaster recovery strategy, the PRIMARY factor to be taken into account will be the:

A. Volume of sensitive data
B. Recovery point objective (RPO)
C. Recovery time objective (RTO)
D. Interruption window

QUESTION 591
An intrusion detection system (IDS) should:

A. Run continuously
B. Ignore anomalies
C. Require a stable, rarely changed environment
D. Be located on the network

QUESTION 592
The PRIORITY action to be taken when a server is infected with a virus is to:

A. Isolate the infected server(s) from the network
B. Identify all potential damage caused by the infection
C. Ensure that the virus database files are current
D. Establish security weaknesses in the firewall

QUESTION 593
Which of the following provides the BEST confirmation that the business continuity/disaster recovery plan objectives have been achieved?

A. The recovery time objective (RTO) was not exceeded during testing
B. Objective testing of the business continuity/disaster recovery plan has been carried out consistently
C. The recovery point objective (RPO) was proved inadequate by disaster recovery plan testing
D. Information assets have been valued and assigned to owners per the business continuity plan, disaster recovery plan

QUESTION 594
Which of the following situations would be the MOST concern to a security manager?

A. Audit logs are not enabled on a production server
B. The logon ID for a terminated systems analyst still exists on the system
C. The help desk has received numerous results of users receiving phishing e-mails
D. A Trojan was found to be installed on a system administrator's laptop

QUESTION 595
A customer credit card database has been breached by hackers. The FIRST step in dealing with this attack should be to:

A. Confirm the incident
B. Notify senior management
C. Start containment
D. Notify law enforcement

QUESTION 596
A root kit was used to capture detailed accounts receivable information. To ensure admissibility of evidence from a legal standpoint, once the incident was identified and the server isolated, the next step should be to:

A. Document how the attack occurred
B. Notify law enforcement
C. Take an image copy of the media
D. Close the accounts receivable system

QUESTION 597
When collecting evidence for forensic analysis, it is important to:

A. Ensure the assignment of qualified personnel
B. Request the IT department do an image copy
C. Disconnect from the network and isolate the affected devices
D. Ensure law enforcement personnel are present before the forensic analysis commences

QUESTION 598
What is the BEST method for mitigating against network denial of service (DoS) attacks?

A. Ensure all servers are up-to-date on OS patches
B. Employ packet filtering to drop suspect packets
C. Implement network address translation to make internal addresses non-routable
D. Implement load balancing for Internet facing devices

QUESTION 599
To justify the establishment of an incident management team, an information security manager would find which of the following to be the MOST effective?

A. Assessment of business impact of past incidents
B. Need of an independent review of incident causes
C. Need for constant improvement on the security level
D. Possible business benefits from incident impact reduction

QUESTION 600
A database was compromised by guessing the password for a shared administrative account and confidential customer information was stolen. The information security manager was able to detect this breach by analyzing which of the following?

A. Invalid logon attempts
B. Write access violations
C. Concurrent logons
D. Firewall logs

QUESTION 601
Which of the following is an example of a corrective control?

A. Diverting incoming traffic upon responding to the denial of service (DoS) attack
B. Filtering network traffic before entering an internal network from outside
C. Examining inbound network traffic for viruses
D. Logging inbound network traffic

QUESTION 602
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 (DNS)
C. Time server
D. Proxy server

QUESTION 603
An organization has been experiencing a number of network-based security attacks that all appear to originate internally. The BEST course of action is to:

A. Require the use of strong passwords
B. Assign static IP addresses
C. Implement centralized logging software
D. Install an intrusion detection system (IDS)

QUESTION 604
A serious vulnerability is reported in the firewall software used by an organization. Which of the following should be the immediate action of the information security manager?

A. Ensure that all OS patches are up-to-date
B. Block inbound traffic until a suitable solution is found
C. Obtain guidance from the firewall manufacturer
D. Commission a penetration test

QUESTION 605
An organization keeps backup tapes of its servers at a warm site. To ensure that the tapes are properly maintained and usable during a system crash, the MOST appropriate measure the organization should perform is to:

A. Use the test equipment in the warm site facility to read the tapes
B. Retrieve the tapes from the warm site and test them
C. Have duplicate equipment available at the warm site
D. Inspect the facility and inventory the tapes on a quarterly basis

QUESTION 606
Which of the following processes is critical for deciding prioritization of actions in a business continuity plan?

A. Business impact analysis (BIA)
B. Risk assessment
C. Vulnerability assessment
D. Business process mapping

QUESTION 607
In addition to backup data, which of the following is the MOST important to store offsite in the event of a disaster?

A. Copies of critical contracts and service level agreements (SLAs)
B. Copies of the business continuity plan
C. Key software escrow agreements for the purchased systems
D. List of emergency numbers of service providers

QUESTION 608
An organization has learned of a security breach at another company that utilizes similar technology. The FIRST thing the information security manager should do is:

A. Assess the likelihood of incidents from the reported cause
B. Discontinue the use of the vulnerable technology
C. Report to senior management that the organization is not affected
D. Remind staff that no similar security breaches have taken place

QUESTION 609
Which of the following is the MOST important consideration for an organization interacting with the media during a disaster?

A. Communicating specially drafted messages by an authorized person
B. Refusing to comment until recovery
C. Referring the media to the authorities
D. Reporting the losses and recovery strategy to the media

QUESTION 610
During the security review of organizational servers it was found that a file server containing confidential human resources (HR) data was accessible to all user IDs. As a FIRST step, the security manager should:

A. Copy sample files as evidence
B. Remove access privileges to the folder containing the data
C. Report this situation to the data owner
D. Train the HR team on properly controlling file permissions

QUESTION 611
If an organization considers taking legal action on a security incident, the information security manager should focus PRIMARILY on:

A. Obtaining evidence as soon as possible
B. Preserving the integrity of the evidence
C. Disconnecting all IT equipment involved
D. Reconstructing the sequence of events

QUESTION 612
Which of the following has the highest priority when defining an emergency response plan?

A. Critical data
B. Critical infrastructure
C. Safety of personnel
D. Vital records

QUESTION 613
The PRIMARY purpose of involving third-party teams for carrying out post event reviews of information security incidents is to:

A. Enable independent and objective review of the root cause of the incidents
B. Obtain support for enhancing the expertise of the third-party teams
C. Identify lessons learned for further improving the information security management process
D. Obtain better buy-in for the information security program

QUESTION 614
The MOST important objective of a post incident review is to:

A. Capture lessons learned to improve the process
B. Develop a process for continuous improvement
C. Develop a business case for the security program budget
D. Identify new incident management tools

QUESTION 615
Which of the following is the BEST mechanism to determine the effectiveness of the incident response process?

A. Incident response metrics
B. Periodic auditing of the incident response process
C. Action recording and review
D. Post incident review

QUESTION 616
The FIRST step in an incident response plan is to:

A. Notify the appropriate individuals
B. Contain the effects of the incident to limit damage
C. Develop response strategies for systematic attacks
D. Validate the incident

QUESTION 617
An organization has verified that its customer information was recently exposed. Which of the following is the FIRST step a security manager should take in this situation?

A. Inform senior management
B. Determine the extent of the compromise
C. Report the incident to the authorities
D. Communicate with the affected customers

QUESTION 618
A possible breach of an organization's IT system is reported by the project manager. What is the FIRST thing the incident response manager should do?

A. Run a port scan on the system
B. Disable the logon ID
C. Investigate the system logs
D. Validate the incident

QUESTION 619
The PRIMARY consideration when defining recovery time objectives (RTOs) for information assets is:

A. Regulatory requirements
B. Business requirements
C. Financial value
D. IT resource availability

QUESTION 620
What task should be performed once a security incident has been verified?

A. Identify the incident
B. Contain the incident
C. Determine the root cause of the incident
D. Perform a vulnerability assessment

QUESTION 621
An information security manager believes that a network file server was compromised by a hacker. Which of the following should be the FIRST action taken?

A. Ensure that critical data on the server are backed up
B. Shut down the compromised server
C. Initiate the incident response process
D. Shut down the network

QUESTION 622
An unauthorized user gained access to a merchant's database server and customer credit card information. Which of the following would be the FIRST step to preserve and protect unauthorized intrusion activities?

A. Shut down and power off the server
B. Duplicate the hard disk of the server immediately
C. Isolate the server from the network
D. Copy the database log file to a protected server

QUESTION 623
Which of the following would be a MAJOR consideration for an organization defining its business continuity plan (BCP) or disaster recovery program (DRP)?

A. Setting up a backup site
B. Maintaining redundant systems
C. Aligning with recovery time objectives (RTOs)
D. Data backup frequency

QUESTION 624
Which of the following would be MOST appropriate for collecting and preserving evidence?

A. Encrypted hard drives
B. Generic audit software
C. Proven forensic processes
D. Log correlation software

QUESTION 625
Of the following, which is the MOST important aspect of forensic investigations?

A. The independence of the investigator
B. Timely intervention
C. Identifying the perpetrator
D. Chain of custody

QUESTION 626
In the course of examining a computer system for forensic evidence, data on the suspect media was inadvertently altered. Which of the following should have been the FIRST course of action in the investigative process?

A. Perform a backup of the suspect media to new media
B. Perform a bit-by-bit image of the original media source onto new media
C. Make a copy of all files that are relevant to the investigation
D. Run an error-checking program on all logical drives to ensure that there are no disk errors

QUESTION 627
Which of the following recovery strategies has the GREATEST chance of failure?

A. Hot site
B. Redundant site
C. Reciprocal arrangement
D. Cold site

QUESTION 628
Recovery point objectives (RPOs) can be used to determine which of the following?

A. Maximum tolerable period of data loss
B. Maximum tolerable downtime
C. Baseline for operational resiliency
D. Time to restore backups

QUESTION 629
Which of the following disaster recovery testing techniques is the MOST cost-effective way to determine the effectiveness of the plan?

A. Preparedness tests
B. Paper tests
C. Full operational tests
D. Actual service disruption

QUESTION 630
When electronically stored information is requested during a fraud investigation, which of the following should be the FIRST priority?

A. Assigning responsibility for acquiring the data
B. Locating the data and preserving the integrity of the data
C. Creating a forensically sound image
D. Issuing a litigation hold to all affected parties

QUESTION 631
When creating a forensic image of a hard drive, which of the following should be the FIRST step?

A. Identify a recognized forensics software tool to create the image
B. Establish a chain of custody log
C. Connect the hard drive to a write blocker
D. Generate a cryptographic hash of the hard drive contents

Answer Sheet

Record your answers to each question on the sheets below. The correct answers to each question along with explanations can be found in the accompanying Answer Guide.

Question	Answer	Question	Answer	Question	Answer	Question	Answer	Question	Answer	Question	Answer
1		2		3		4		5		6	
7		8		9		10		11		12	
13		14		15		16		17		18	
19		20		21		22		23		24	
25		26		27		28		29		30	
31		32		33		34		35		36	
37		38		39		40		41		42	
43		44		45		46		47		48	
49		50		51		52		53		54	
55		56		57		58		59		60	
61		62		63		64		65		66	
67		68		69		70		71		72	
73		74		75		76		77		78	
79		80		81		82		83		84	
85		86		87		88		89		90	
91		92		93		94		95		96	
97		98		99		100		101		102	
103		104		105		106		107		108	
109		110		111		112		113		114	
115		116		117		118		119		120	
121		122		123		124		125		126	
127		128		129		130		131		132	
133		134		135		136		137		138	
139		140		141		142		143		144	
145		146		147		148		149		150	
151		152		153		154		155		156	

Question	Answer	Question	Answer	Question	Answer	Question	Answer	Question	Answer	Question	Answer
157		158		159		160		161		162	
163		164		165		166		167		168	
169		170		171		172		173		174	
175		176		177		178		179		180	
181		182		183		184		185		186	
187		188		189		190		191		192	
193		194		195		196		197		198	
199		200		201		202		203		204	
205		206		207		208		209		210	
211		212		213		214		215		216	
217		218		219		220		221		222	
223		224		225		226		227		228	
229		230		231		232		233		234	
235		236		237		238		239		240	
241		242		243		244		245		246	
247		248		249		250		251		252	
253		254		255		256		257		258	
259		260		261		262		263		264	
265		266		267		268		269		270	
271		272		273		274		275		276	
277		278		279		280		281		282	
283		284		285		286		287		288	
289		290		291		292		293		294	
295		296		297		298		299		300	
301		302		303		304		305		306	
307		308		309		310		311		312	
313		314		315		316		317		318	
319		320		321		322		323		324	
325		326		327		328		329		330	
331		332		333		334		335		336	

Question	Answer	Question	Answer	Question	Answer	Question	Answer	Question	Answer	Question	Answer
337		338		339		340		341		342	
343		344		345		346		347		348	
349		350		351		352		353		354	
355		356		357		358		359		360	
361		362		363		364		365		366	
367		368		369		370		371		372	
373		374		375		376		377		378	
379		380		381		382		383		384	
385		386		387		388		389		390	
391		392		393		394		395		396	
397		398		399		400		401		402	
403		404		405		406		407		408	
409		410		411		412		413		414	
415		416		417		418		419		420	
421		422		423		424		425		426	
427		428		429		430		431		432	
433		434		435		436		437		438	
439		440		441		442		443		444	
445		446		447		448		449		450	
451		452		453		454		455		456	
457		458		459		460		461		462	
463		464		465		466		467		468	
469		470		471		472		473		474	
475		476		477		478		479		480	
481		482		483		484		485		486	
487		488		489		490		491		492	
493		494		495		496		497		498	
499		500		501		502		503		504	
505		506		507		508		509		510	
511		512		513		514		515		516	

Question	Answer	Question	Answer	Question	Answer	Question	Answer	Question	Answer	Question	Answer
517		518		519		520		521		522	
523		524		525		526		527		528	
529		530		531		532		533		534	
535		536		537		538		539		540	
541		542		543		544		545		546	
547		548		549		550		551		552	
553		554		555		556		557		558	
559		560		561		562		563		564	
565		566		567		568		569		570	
571		572		573		574		575		576	
577		578		579		580		581		582	
583		584		585		586		587		588	
589		590		591		592		593		594	
595		596		597		598		599		600	
601		602		603		604		605		606	
607		608		609		610		611		612	
613		614		615		616		617		618	
619		620		621		622		623		624	
625		626		627		628		629		630	
631											