CISM Review Questions

**Topic 1, INFORMATION SECURITY GOVERNANCE**

**QUESTION NO: 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 NO: 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 NO: 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 NO: 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 NO: 5**

Information security governance is PRIMARILY driven by:

**A.** technology constraints.

**B.** regulatory requirements.

**C.** litigation potential.

**D.** business strategy.

**QUESTION NO: 6**

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

**A.** Unrestricted data mining

**B.** Identity theft

**C.** Human rights protection D.

**D.** Identifiable personal data

**QUESTION NO: 7**

Investments in information security technologies should be based on:

**A.** vulnerability assessments.

**B.** value analysis.

**C.** business climate.

**D.** audit recommendations.

**QUESTION NO: 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 ease and value analysis.

**QUESTION NO: 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 NO: 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 NO: 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 NO: 12**

The MOST important component of a privacy policy is:

**A.** notifications.

**B.** warranties.

**C.** liabilities.

**D.** geographic coverage.

**QUESTION NO: 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 NO: 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 NO: 15**

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

**A.** strategy.

**B.** guidelines.

**C.** model.

**D.** architecture.

**QUESTION NO: 16**

8

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 NO: 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 NO: 18**

9

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 NO: 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 NO: 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 NO: 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 NO: 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 NO: 23**

Which of the following is MOST likely to be discretionary?

**A.** Policies

**B.** Procedures

**C.** Guidelines

**D.** Standards

**QUESTION NO: 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 NO: 25**

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

**A.** Standards

**B.** Procedures

**C.** Policies

**D.** Guidelines

**QUESTION NO: 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 NO: 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 NO: 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 NO: 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 NO: 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

**Topic 2 INFORMATION RISK MANAGEMENT**

**QUESTION NO: 140**

A risk mitigation report would include recommendations for

1. assessment
2. acceptance
3. evaluation.
4. quantification.

# QUESTION NO: 141

A risk management program should reduce risk to:

1. zero.
2. an acceptable level.
3. an acceptable percent of revenue.
4. an acceptable probability of occurrence.

# QUESTION NO: 142

The MOST important reason for conducting periodic risk assessments is because:

1. risk assessments are not always precise.
2. security risks are subject to frequent change.
3. reviewers can optimize and reduce the cost of controls.
4. it demonstrates to senior management that the security function can add value.

# QUESTION NO: 143

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

1. Overall risk is quantified
2. Inherent risk is eliminated
3. Residual risk is minimized
4. Control risk is tied to business units

# QUESTION NO: 144

Which of the following would generally have the GREATEST negative impact on an organization?

1. Theft of computer software
2. Interruption of utility services
3. Loss of customer confidence
4. Internal fraud resulting in monetary loss

# QUESTION NO: 145

A successful information security management program should use which of the following to determine the amount of resources devoted to mitigating exposures?

1. Risk analysis results
2. Audit report findings
3. Penetration test results
4. Amount of IT budget available

# QUESTION NO: 146

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

1. Static IP addressing
2. Internal address translation
3. Prospective employee background checks
4. Employee awareness certification program

# QUESTION NO: 147

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

1. original cost.
2. net cash flow.
3. net present value.
4. replacement cost.

# QUESTION NO: 148

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

1. of recovery.
2. to recreate.
3. if unavailable.
4. of emergency operations.

# QUESTION NO: 149

Acceptable risk is achieved when:

1. residual risk is minimized.
2. transferred risk is minimized.
3. control risk is minimized.
4. inherent risk is minimized.

# QUESTION NO: 150

The value of information assets is BEST determined by:

1. individual business managers.
2. business systems analysts.
3. information security management.
4. industry averages benchmarking.

# QUESTION NO: 151

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

1. Feasibility
2. Design
3. Development
4. Testing

# QUESTION NO: 152

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

1. policy development.
2. change management.
3. awareness training.
4. regular monitoring.

# QUESTION NO: 153

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

1. Gap analysis
2. Regression analysis
3. Risk analysis
4. Business impact analysis

# QUESTION NO: 154

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

1. Disaster declaration
2. Recovery of the backups
3. Restoration of the system
4. Return to business as usual processing

# QUESTION NO: 155

Which of the following results from the risk assessment process would BEST assist risk management decision making?

1. Control risk
2. Inherent risk
3. Risk exposure
4. Residual risk

# QUESTION NO: 156

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

1. Mitigating controls
2. Visibility of impact
3. Likelihood of occurrence
4. Incident frequency

# QUESTION NO: 157

Risk acceptance is a component of which of the following?

1. Assessment
2. Mitigation
3. Evaluation
4. Monitoring

# QUESTION NO: 158

Risk management programs are designed to reduce risk to:

1. a level that is too small to be measurable.
2. the point at which the benefit exceeds the expense.
3. a level that the organization is willing to accept.
4. a rate of return that equals the current cost of capital.

# QUESTION NO: 159

# How frequently should one re-assess their risks?

1. once a year for each business process and subprocess.
2. every three to six months for critical business processes.
3. by external parties to maintain objectivity.
4. annually or whenever there is a significant change.

# QUESTION NO: 160

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

1. quantify overall risk.
2. minimize residual risk.
3. eliminate inherent risk.
4. maximize the sum of all annualized loss expectancies (ALEs).

# QUESTION NO: 161

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

1. Theft of purchased software
2. Power outage lasting 24 hours
3. Permanent decline in customer confidence
4. Temporary loss of e-mail due to a virus attack

# QUESTION NO: 162

Which of the following will BEST prevent external security attacks?

1. Static IP addressing
2. Network address translation
3. Background checks for temporary employees
4. Securing and analyzing system access logs

# QUESTION NO: 163

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

1. original cost to acquire.
2. cost of the software stored.
3. annualized loss expectancy (ALE).
4. cost to obtain a replacement.

# QUESTION NO: 164

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

1. total cost of ownership.
2. priority of restoration.
3. annualized loss expectancy (ALE).
4. residual risk.

# QUESTION NO: 165

When residual risk is minimized:

1. acceptable risk is probable.
2. transferred risk is acceptable.
3. control risk is reduced.
4. risk is transferable.

# QUESTION NO: 166

Quantitative risk analysis is MOST appropriate when assessment data:

1. include customer perceptions.
2. contain percentage estimates.
3. do not contain specific details.
4. contain subjective information.

# QUESTION NO: 167

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

1. Evaluating a business impact analysis (BIA)
2. Developing a balanced business scorecard
3. Demonstrating the relationship between controls
4. Measuring current state vs. desired future state

# QUESTION NO: 168

Identification and prioritization of business risk enables project managers to:

1. Establish implementation milestones.
2. reduce the overall amount of slack time.
3. address areas with most significance.
4. accelerate completion of critical paths.

# QUESTION NO: 169

A risk analysis should:

1. include a benchmark of similar companies in its scope.
2. assume an equal degree of protection for all assets.
3. address the potential size and likelihood of loss.
4. give more weight to the likelihood vs. the size of the loss.

# QUESTION NO: 170

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

1. Disaster declaration
2. Before-image restoration
3. System restoration
4. After-image processing

**Topic 3, Information Security Program Development**

**QUESTION NO: 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 NO: 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 NO: 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.** D. Definition tables

**QUESTION NO: 278**

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

**A.** Centralized

**B.** Role-based

**C.** Decentralized

**D.** Discretionary

**QUESTION NO: 279**

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

**A.** Router

**B.** Firewall

**C.** Mail relay

**D.** Authentication server

**QUESTION NO: 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 NO: 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 NO: 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 NO: 283**

Which of the following is the BEST metric for evaluating the effectiveness of security awareness

twining? The number of:

**A.** password resets.

**B.** reported incidents.

**C.** incidents resolved.

**D.** access rule violations.

**QUESTION NO: 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 NO: 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 NO: 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 NO: 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 NO: 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 NO: 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 NO: 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

systems. Security baselines provide minimum recommended settings. Configuration management

**QUESTION NO: 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 NO: 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

**Answer: C**

**Explanation:**

**QUESTION NO: 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 NO: 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 NO: 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 NO: 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 NO: 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 NO: 298**

An intranet server should generally be placed on the:

**A.** internal network.

**B.** firewall server.

**C.** external router.

**D.** primary domain controller.

**QUESTION NO: 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 NO: 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 NO: 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 NO: 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 NO: 303**

Which of the following is the BEST method to provide a new user with their initial password for email 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 NO: 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 NO: 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

**Topic 4 INCIDENT MANAGEMENT AND RESPONSE**

**QUESTION NO: 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 NO: 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 NO: 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 NO: 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 NO: 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 NO: 550**

The FIRST priority when responding to a major security incident is:

**A.** documentation.

**B.** monitoring.

**C.** restoration.

**D.** containment.

**QUESTION NO: 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 NO: 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 NO: 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 NO: 554**

An incident response policy must contain:

**A.** updated call trees.

**B.** escalation criteria.

**C.** press release templates.

**D.** critical backup files inventory.

**QUESTION NO: 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 NO: 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 NO: 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 NO: 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 NO: 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 NO: 560**

Isaca CISM Exam

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

incoming mail is unnecessary overkill since only those e-mails containing attached picture files are

**QUESTION NO: 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 NO: 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 NO: 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

**Answer: B**

**QUESTION NO: 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 NO: 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 NO: 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 NO: 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 NO: 568**

Which of the following is the BEST way to verify that all critical production servers are utilizing upto-

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 NO: 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 NO: 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 NO: 571**

Which of the following is the MOST serious exposure of automatically updating virus signature

files on every desktop each Friday at 11:00 p.m. (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

**Answer: C**

**QUESTION NO: 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 NO: 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 NO: 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 NO: 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

CISM Review Answers and Explanations

**Topic 1, INFORMATION SECURITY GOVERNANCE**

**QUESTION NO: 1**

**Answer: B**

**Explanation:**

Prior to assessing technical vulnerabilities or levels of security awareness, an information security

manager needs to gain an understanding of the current business strategy and direction. A business impact analysis should be performed prior to developing a business continuity plan, but this would not be an appropriate first step in developing an information security strategy because it focuses on availability.

**QUESTION NO: 2**

**Answer: D**

**Explanation:**

Senior management seeks to understand the business justification for investing in security. This can best be accomplished by tying security to key business objectives. Senior management will not be as interested in technical risks or examples of successful attacks if they are not tied to the impact on business environment and objectives. Industry best practices are important to senior management but, again, senior management will give them the right level of importance when they

are presented in terms of key business objectives.

**QUESTION NO: 3**

**Answer: C**

**Explanation:**

Since the members of senior management are ultimately responsible for information security, they are the ultimate decision makers in terms of governance and direction. They are responsible forapproval of major policy statements and requests to fund the information security practice. Evaluation of vendors, assessment of risks and monitoring compliance with regulatory requirements are day-to-day responsibilities of the information security manager; in some organizations, business management is involved in these other activities, though their primary role

is direction and governance.

**QUESTION NO: 4**

**Answer: A**

**Explanation:**

The existence of a steering committee that approves all security projects would be an indication of the existence of a good governance program. Compliance with laws and regulations is part of the responsibility of the steering committee but it is not a full answer. Awareness training is important at all levels in any medium, and also an indicator of good governance. However, it must be guided and approved as a security project by the steering committee.

**QUESTION NO: 5**

**Answer: D**

**Explanation:**

Governance is directly tied to the strategy and direction of the business. Technology constraints, regulatory requirements and litigation potential are all important factors, but they are necessarily inline with the business strategy.

**QUESTION NO: 6**

**Answer: D**

**Explanation:**

Protection of identifiable personal data is the major focus of recent privacy regulations such as the

Health Insurance Portability and Accountability Act (HIPAA). Data mining is an accepted tool for

ad hoc reporting; it could pose a threat to privacy only if it violates regulator)' provisions. Identity

theft is a potential consequence of privacy violations but not the main focus of many regulations.

Human rights addresses privacy issues but is not the main focus of regulations.

**QUESTION NO: 7**

**Answer: B**

**Explanation:**

Investments in security technologies should be based on a value analysis and a sound business case. Demonstrated value takes precedence over the current business climate because it is ever changing. Basing decisions on audit recommendations would be reactive in nature and might not address the key business needs comprehensively. Vulnerability assessments are useful, but they do not determine whether the cost is justified.

**QUESTION NO: 8**

**Answer: B**

**Explanation:**

Retention of business records is generally driven by legal and regulatory requirements. Business strategy and direction would not normally apply nor would they override legal and regulatory requirements. Storage capacity and longevity are important but secondary issues. Business case and value analysis would be secondary to complying with legal and regulatory requirements.

**QUESTION NO: 9**

**Answer: B**

**Explanation:**

Centralization of information security management results in greater uniformity and better adherence to security policies. It is generally less expensive to administer due to the economics of scale. However, turnaround can be slower due to the lack of alignment with business units.

**QUESTION NO: 10**

**Answer: B**

**Explanation:**

Updated security policies are required to align management objectives with security procedures;

management objectives translate into policy, policy translates into procedures. Security

procedures will necessitate specialized teams such as the computer incident response and

management group as well as specialized tools such as the security mechanisms that comprise

the security architecture. Security awareness will promote the policies, procedures and

appropriate use of the security mechanisms.

**QUESTION NO: 11**

**Answer: B**

**Explanation:**

The chief operating officer (COO) is highly-placed within an organization and has the most

knowledge of business operations and objectives. The chief internal auditor and chief legal counsel are appropriate members of such a steering group. However, sponsoring the creation of the steering committee should be initiated by someone versed in the strategy and direction of the business. Since a security manager is looking to this group for direction, they are not in the best position to oversee formation of this group.

**QUESTION NO: 12**

**Answer: A**

**Explanation:**

Privacy policies must contain notifications and opt-out provisions: they are a high-level

management statement of direction. They do not necessarily address warranties, liabilities or geographic coverage, which are more specific.

**QUESTION NO: 13**

**Answer: C**

**Explanation:**

The cost of implementing security controls should not exceed the worth of the asset. Annualized loss expectancy represents the losses drat are expected to happen during a single calendar year. A security mechanism may cost more than this amount (or the cost of a single incident) and still be considered cost effective. Opportunity costs relate to revenue lost by forgoing the acquisition of an item or the making of a business decision.

**QUESTION NO: 14**

**Answer: C**

**Explanation:**

Conflicts of this type should be based on a risk analysis of the costs and benefits of allowing or disallowing an exception to the standard. It is highly improbable that a business objective could be changed to accommodate a security standard, while risk acceptance\* is a process that derives from the risk analysis.

**QUESTION NO: 15**

**Answer: D**

**Explanation:**

Minimum standards for securing the technical infrastructure should be defined in a security architecture document. This document defines how components are secured and the security services that should be in place. A strategy is a broad, high-level document. A guideline is advisory in nature, while a security model shows the relationships between components.

**QUESTION NO: 16**

**Answer: B**

**Explanation:**

A set of security objectives, processes, methods, tools and techniques together constitute a

security strategy. Although IT and business governance are intertwined, business controls may not be included in a security strategy. Budgets will generally not be included in an information security strategy. Additionally, until information security strategy is formulated and implemented, specific tools will not be identified and specific cost estimates will not be available. Firewall rule sets, network defaults and intrusion detection system (IDS) settings are technical details subject to

periodic change, and are not appropriate content for a strategy document.

**QUESTION NO: 17**

**Answer: A**

**Explanation:**

Information security exists to help the organization meet its objectives. The information security manager should identify information security needs based on organizational needs. Organizational or business risk should always take precedence. Involving each organizational unit in information security and establishing metrics to measure success will be viewed favorably by senior

management after the overall organizational risk is identified.

**QUESTION NO: 18**

**Answer: C**

**Explanation:**

Since management is ultimately responsible for information security, it should approve information security policy statements; the information security manager should not have final approval. Evaluation of third parties requesting access, assessment of disaster recovery plans and monitoring of compliance with physical security controls are acceptable practices and do not present any conflicts of interest.

**QUESTION NO: 19**

**Answer: D**

**Explanation:**

A steering committee should be in place to approve all security projects. The fact that the data center manager has final signoff for all security projects indicates that a steering committee is not being used and that information security is relegated to a subordinate place in the organization. This would indicate a failure of information security governance. It is not inappropriate for an oversight or steering committee to meet quarterly. Similarly, it may be desirable to have the chief information officer (CIO) approve the security policy due to the size of the organization and frequency of updates. Difficulty in filling vacancies is not uncommon due to the shortage of good, qualified information security professionals.

**QUESTION NO: 20**

**Answer: A**

**Explanation:**

Information security priorities may, at times, override technical specifications, which then must be rewritten to conform to minimum security standards. Regulatory and privacy requirements are government-mandated and, therefore, not subject to override. The needs of the business should always take precedence in deciding information security priorities.

**QUESTION NO: 21**

**Answer: B**

**Explanation:**

New information security managers should seek to build rapport and establish lines of

communication with senior management to enlist their support. Benchmarking peer organizations is beneficial to better understand industry best practices, but it is secondary to obtaining senior management support. Similarly, developing a security architecture and assembling an experienced staff are objectives that can be obtained later.

**QUESTION NO: 22**

**Answer: D**

**Explanation:**

Information security architecture should always be properly aligned with business goals and objectives. Alignment with IT plans or industry and security best practices is secondary by comparison.

**QUESTION NO: 23**

**Answer: C**

**Explanation:**

Policies define security goals and expectations for an organization. These are defined in more specific terms within standards and procedures. Standards establish what is to be done while procedures describe how it is to be done. Guidelines provide recommendations that business management must consider in developing practices within their areas of control; as such, they are discretionary.

**QUESTION NO: 24**

**Answer: A**

**Explanation:**

The most fundamental evaluation criterion for the appropriate selection of any security technology is its ability to reduce or eliminate business risks. Investments in security technologies should be based on their overall value in relation to their cost; the value can be demonstrated in terms of risk mitigation. This should take precedence over whether they use new or exotic technologies or how they are evaluated in trade publications.

**QUESTION NO: 25**

**Answer: C**

**Explanation:**

Policies are high-level statements of objectives. Because of their high-level nature and statement of broad operating principles, they are less subject to periodic change. Security standards and procedures as well as guidelines must be revised and updated based on the impact of technology changes.

**QUESTION NO: 26**

**Answer: D**

**Explanation:**

Long-term retention of business records may be severely impacted by changes in application systems and media. For example, data stored in nonstandard formats that can only be read and interpreted by previously decommissioned applications may be difficult, if not impossible, to recover. Business strategy and direction do not generally apply, nor do legal and regulatory requirements. Storage capacity and shelf life are important but secondary issues.

**QUESTION NO: 27**

**Answer: C**

**Explanation:**

Decentralization of information security management generally results in better alignment to business unit needs. It is generally more expensive to administer due to the lack of economies of scale. Uniformity in quality of service tends to vary from unit to unit.

**QUESTION NO: 28**

**Answer: B**

**Explanation:**

The chief operating officer (COO) is most knowledgeable of business operations and objectives. The chief privacy officer (CPO) and the chief legal counsel (CLC) may not have the knowledge of the day- to-day business operations to ensure proper guidance, although they have the same influence within the organization as the COO. Although the chief security officer (CSO) is knowledgeable of what is needed, the sponsor for this task should be someone with far-reaching influence across the organization.

**QUESTION NO: 29**

**Answer: D**

**Explanation:**

The development of trust in the integrity of information among stakeholders should be the primary goal of information security governance. Review of internal control mechanisms relates more to auditing, while the total elimination of risk factors is not practical or possible. Proactive involvement in business decision making implies that security needs dictate business needs when, in fact, just the opposite is true. Involvement in decision making is important only to ensure business data

integrity so that data can be trusted.

**QUESTION NO: 30**

**Answer: C**

**Explanation:**

Security architecture explains the use and relationships of security mechanisms. Security metrics measure improvement within the security practice but do not explain the use and relationships of security technologies. Process improvement models and network topology diagrams also do not describe the use and relationships of these technologies.

**Topic 2 INCIDENT Risk Management**

**QUESTION NO: 140**

# Answer: B Explanation:

Acceptance of a risk is an alternative to be considered in the risk mitigation process. Assessment. evaluation and risk quantification are components of the risk analysis process that are completed prior to determining risk mitigation solutions.

# QUESTION NO: 141

# Answer: B Explanation:

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

probability of the risk.

# QUESTION NO: 142

# Answer: B Explanation:

Risks are constantly changing. A previously conducted risk assessment may not include measured risks that have been introduced since the last assessment. Although an assessment can never be perfect and invariably contains some errors, this is not the most important reason for periodic reassessment. The fact that controls can be made more efficient to reduce costs is not sufficient. Finally, risk assessments should not be performed merely to justify the existence of the security function.

# QUESTION NO: 143

# Answer: C Explanation:

A successful risk management practice minimizes the residual risk to the organization. Choice A is incorrect because the fact that overall risk has been quantified does not necessarily indicate the existence of a successful risk management practice. Choice B is incorrect since it is virtually impossible to eliminate inherent risk. Choice D is incorrect because, although the tying of control risks to business may improve accountability, this is not as desirable as minimizing residual risk.

# QUESTION NO: 144

# Answer: C Explanation:

Although the theft of software, interruption of utility services and internal frauds are all significant, the loss of customer confidence is the most damaging and could cause the business to fail.

# QUESTION NO: 145

# Answer: A Explanation:

Risk analysis results are the most useful and complete source of information for determining the amount of resources to devote to mitigating exposures. Audit report findings may not address all risks and do not address annual loss frequency. Penetration test results provide only a limited view of exposures, while the IT budget is not tied to the exposures faced by the organization.

# QUESTION NO: 146

# Answer: C Explanation:

Because past performance is a strong predictor of future performance, background checks of prospective employees best prevents attacks from originating within an organization. Static IP addressing does little to prevent an internal attack. Internal address translation using non-routable addresses is useful against external attacks but not against internal attacks. Employees who certify that they have read security policies are desirable, but this does not guarantee that the employees behave honestly.

# QUESTION NO: 147

# Answer: D Explanation:

The value of a physical asset should be based on its replacement cost since this is the amount that would be needed to replace the asset if it were to become damaged or destroyed. Original cost may be significantly different than the current cost of replacing the asset. Net cash flow and net present value do not accurately reflect the true value of the asset.

# QUESTION NO: 148

# Answer: C Explanation:

The value of an information system should be based on the cost incurred if the system were to become unavailable. The cost to design or recreate the system is not as relevant since a business impact analysis measures the impact that would occur if an information system were to become unavailable. Similarly, the cost of emergency operations is not as relevant.

# QUESTION NO: 149

# Answer: A Explanation:

Residual risk is the risk that remains after putting into place an effective risk management program; therefore, acceptable risk is achieved when this amount is minimized. Transferred risk is risk that has been assumed by a third party and may not necessarily be equal to the minimal form of residual risk. Control risk is the risk that controls may not prevent/detect an incident with a measure of control effectiveness. Inherent risk cannot be minimized.

# QUESTION NO: 150

# Answer: A

# Explanation:

Individual business managers are in the best position to determine the value of information assets since they are most knowledgeable of the assets' impact on the business. Business systems developers and information security managers are not as knowledgeable regarding the impact on the business. Peer companies' industry averages do not necessarily provide detailed enough information nor are they as relevant to the unique aspects of the business.

# QUESTION NO: 151

# Answer: A Explanation:

Risk should be addressed as early in the development of a new application system as possible. In some cases, identified risks could be mitigated through design changes. If needed changes are not identified until design has already commenced, such changes become more expensive. For this reason, beginning risk assessment during the design, development or testing phases is not the best solution.

# QUESTION NO: 152

# Answer: B Explanation:

Change is a process in which new risks can be introduced into business processes and systems. For this reason, risk management should be an integral component of the change management process. Policy development, awareness training and regular monitoring, although all worthwhile activities, are not as effective as change management.

# QUESTION NO: 153

# Answer: D Explanation:

Recovery time objectives (RTOs) are a primary deliverable of a business impact analysis. RTOs relate to the financial impact of a system not being available. A gap analysis is useful in addressing the differences between the current state and an ideal future state. Regression analysis is used to test changes to program modules. Risk analysis is a component of the business impact analysis.

# QUESTION NO: 154

# Answer: C Explanation:

The recovery time objective (RTO) is based on the amount of time required to restore a system; disaster declaration occurs at the beginning of this period. Recovery of the backups occurs shortly after the beginning of this period. Return to business as usual processing occurs significantly later

Than the RTO. RTO is an "objective," and full restoration may or may not coincide with the RTO. RTO can be the minimum acceptable operational level, far short of normal operations.

# QUESTION NO: 155

# Answer: D Explanation:

Residual risk provides management with sufficient information to decide to the level of risk that an organization is willing to accept. Control risk is the risk that a control may not succeed in preventing an undesirable event. Risk exposure is the likelihood of an undesirable event occurring. Inherent risk is an important factor to be considered during the risk assessment.

# QUESTION NO: 156

# Answer: B Explanation:

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

# QUESTION NO: 157

# Answer: B Explanation:

Risk acceptance is one of the alternatives to be considered in the risk mitigation process. Assessment and evaluation are components of the risk analysis process. Risk acceptance is not a component of monitoring.

# QUESTION NO: 158

# Answer: C Explanation:

Risk should be reduced to a level that an organization is willing to accept. Reducing risk to a level too small to measure is impractical and is often cost-prohibitive. To tie risk to a specific rate of return ignores the qualitative aspects of risk that must also be considered. Depending on the risk preference of an organization, it may or may not choose to pursue risk mitigation to the point at which the benefit equals or exceeds the expense. Therefore, choice C is a more precise answer.

# QUESTION NO: 159

# Answer: D Explanation:

Risks are constantly changing. Choice D offers the best alternative because it takes into consideration a reasonable time frame and allows flexibility to address significant change. Conducting a risk assessment once a year is insufficient if important changes take place. Conducting a risk assessment every three-to-six months for critical processes may not be necessary, or it may not address important changes in a timely manner. It is not necessary for assessments to be performed by external parties.

# QUESTION NO: 160

# Answer: B Explanation:

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

# QUESTION NO: 161

# Answer: C Explanation:

A permanent decline in customer confidence does not lend itself well to measurement by quantitative techniques. Qualitative techniques are more effective in evaluating things such as customer loyalty and goodwill. Theft of software, power outages and temporary loss of e-mail can be quantified into monetary amounts easier than can be assessed with quantitative techniques.

# QUESTION NO: 162

# Answer: B Explanation:

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

# QUESTION NO: 163

# Answer: D Explanation:

The value of the server should be based on its cost of replacement. The original cost may be significantly different from the current cost and, therefore, not as relevant. The value of the software is not at issue because it can be restored from backup media. The ALE for all risks related to the server does not represent the server's value.

# QUESTION NO: 164

# Answer: B Explanation:

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

# QUESTION NO: 165

# Answer: A Explanation:

Since residual risk is the risk that remains after putting into place an effective risk management program, it is probable that the organization will decide that it is an acceptable risk if sufficiently minimized. Transferred risk is risk that has been assumed by a third party, therefore its magnitude is not relevant. Accordingly, choices B and D are incorrect since transferred risk does not necessarily indicate whether risk is at an acceptable level. Minimizing residual risk will not reduce control risk.

# QUESTION NO: 166

# Answer: B Explanation:

Percentage estimates are characteristic of quantitative risk analysis. Customer perceptions, lack of specific details or subjective information lend themselves more to qualitative risk analysis.

# QUESTION NO: 167

# Answer: D Explanation:

A gap analysis is most useful in addressing the differences between the current state and an ideal future state. It is not as appropriate for evaluating a business impact analysis (BIA), developing a balanced business scorecard or demonstrating the relationship between variables.

# QUESTION NO: 168

# Answer: C Explanation:

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

# QUESTION NO: 169

# Answer: C Explanation:

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

# QUESTION NO: 170

**Answer: B**

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

The recovery point objective (RPO) is the point in the processing flow at which system recovery should occur. This is the predetermined state of the application processing and data used to restore the system and to continue the processing flow. Disaster declaration is independent of this

processing checkpoint. Restoration of the system can occur at a later date, as does the return to normal, after-image processing.

**TOPIC 3 Information Security Program Development**

**QUESTION NO: 275**

**Answer: C**

**Explanation:**

Senior management represented in the security steering committee is in the best position to advocate the establishment of and continued support for an information security program. The chief operating officer (COO) will be a member of that committee. An internal auditor is a good advocate but is secondary to the influence of senior management. IT management has a lesser degree of influence and would also be part of the steering committee.

**QUESTION NO: 276**

**Answer: A**

**Explanation:**

Encryption of data in a virtual private network (VPN) ensures that transmitted information is not readable, even if intercepted. Firewalls and routers protect access to data resources inside the network and do not protect traffic in the public network. Biometric and two-factor authentication, by themselves, would not prevent a message from being intercepted and read.

**QUESTION NO: 277**

**Answer: D**

**Explanation:**

The effectiveness of virus detection software depends on virus signatures which are stored in virus definition tables. Software upgrades are related to the periodic updating of the program code, which would not be as critical. Intrusion detection and packet filtering do not focus on virus detection.

**QUESTION NO: 278**

**Answer: B**

**Explanation:**

Role-based access control allows users to be grouped into job-related categories, which

significantly cases the required administrative overhead. Discretionary access control would require a greater degree of administrative overhead. Decentralized access control generally requires a greater number of staff to administer, while centralized access control is an incomplete answer.

**QUESTION NO: 279**

**Answer: C**

**Explanation:**

A mail relay should normally be placed within a demilitarized zone (DMZ) to shield the internal network. An authentication server, due to its sensitivity, should always be placed on the internal network, never on a DMZ that is subject to compromise. Both routers and firewalls may bridge a DMZ to another network, but do not technically reside within the DMZ, network segment.

**QUESTION NO: 280**

An intrusion detection system should be placed:

**A.** outside the firewall.

**B.** on the firewall server.

**C.** on a screened subnet.

**Answer: C**

**Explanation:**

An intrusion detection system (IDS) should be placed on a screened subnet, which is a

demilitarized zone (DMZ). Placing it on the Internet side of the firewall would leave it defenseless. The same would be tmc of placing it on the external router, if such a thing were feasible. Since firewalls should be installed on hardened servers with minimal services enabled, it would be inappropriate to store the IDS on the same physical device.

**QUESTION NO: 281**

**Answer: C**

**Explanation:**

Having two entry points, each guarded by a separate firewall, is desirable to permit traffic load balancing. As they both connect to the Internet and to the same demilitarized zone (DMZ), such an arrangement is not practical for separating test from production or preventing a denial-of-service attack.

**QUESTION NO: 282**

**Answer: C**

**Explanation:**

An extranet server should be placed on a screened subnet, which is a demilitarized zone (DMZ). Placing it on the Internet side of the firewall would leave it defenseless. The same would be true of placing it on the external router, although this would not be possible. Since firewalls should be installed on hardened servers with minimal services enabled, it would be inappropriate to store the extranet on the same physical device.

**QUESTION NO: 283**

**Answer: B**

**Explanation:**

Reported incidents will provide an indicator of the awareness level of staff. An increase in reported incidents could indicate that the staff is paying more attention to security. Password resets and access rule violations may or may not have anything to do with awareness levels. The number of incidents resolved may not correlate to staff awareness.

**QUESTION NO: 284**

**Answer: A**

**Explanation:**

Security monitoring must focus on business-critical information to remain effectively usable by and credible to business users. Control risk is the possibility that controls would not detect an incident or error condition, and therefore is not a correct answer because monitoring would not directly assist in managing this risk. Network intrusions are not the only focus of monitoring mechanisms; although they should record all security violations, this is not the primary objective.

**QUESTION NO: 285**

**Answer: C**

**Explanation:**

Using computer-based training (CBT) presentations with end-of-section reviews provides feedback on how well users understand what has been presented. Periodic compliance reviews are a good tool to identify problem areas but do not ensure that procedures are known or understood. Focus groups may or may not provide meaningful detail. Although a signed employee acknowledgement is good, it does not indicate whether the material has been read and/or understood.

**QUESTION NO: 286**

**Answer: C**

**Explanation:**

Service level agreements (SLAs) provide metrics to which outsourcing firms can be held

accountable. This is more important than a limitation on the outsourcing firm's liability, a right-to terminate clause or a hold- harmless agreement which involves liabilities to third parties.

**QUESTION NO: 287**

**Answer: C**

**Explanation:**

The ratio of false positives to false negatives will indicate whether an intrusion detection system (IDS) is properly tuned to minimize the number of false alarms while, at the same time, minimizing the number of omissions. The number of attacks detected, successful attacks or the ratio of successful to unsuccessful attacks would not indicate whether the IDS is properly configured.

**QUESTION NO: 288**

**Answer: B**

**Explanation:**

Change management controls the process of introducing changes to systems. This is often the point at which a weakness will be introduced. Patch management involves the correction of software weaknesses and would necessarily follow change management procedures. Security baselines provide minimum recommended settings and do not prevent introduction of control weaknesses. Virus detection is an effective tool but primarily focuses on malicious code from external sources, and only for those applications that are online.

**QUESTION NO: 289**

**Answer: C**

**Explanation:**

The critical path method is most effective for determining how long a project will take. A waterfall chart is used to understand the flow of one process into another. A Gantt chart facilitates the proper estimation and allocation of resources. The Rapid Application Development (RAD) method is used as an aid to facilitate and expedite systems development.

**QUESTION NO: 290**

**Answer: A**

**Explanation:**

Patch management corrects discovered weaknesses by applying a correction (a patch) to the original program code. Change management controls the process of introducing changes to systems. Security baselines provide minimum recommended settings. Configuration management controls the updates to the production environment.

**QUESTION NO: 291**

**Answer: A**

**Explanation:**

Decisions regarding security should always weigh the potential loss from a risk against the existing controls. Each situation is unique; therefore, it is not advisable to always decide in favor of enforcing a standard. Redesigning the proposed change might not always be the best option because it might not meet the business needs. Implementing additional controls might be an option, but this would be done after the residual risk is known.

**QUESTION NO: 292**

**Answer: C**

**Explanation:**

Senior management that is part of the security steering committee is in the best position to approve plans to implement an information security governance framework. An internal auditor is secondary' to the authority and influence of senior management. Information security management should not have the authority to approve the security governance framework. Infrastructure management will not be in the best position since it focuses more on the technologies than on the business.

**QUESTION NO: 293**

**Answer: C**

**Explanation:**

Role-based access controls help ensure that users only have access to files and systems appropriate for their job role. Violation logs are detective and do not prevent unauthorized access. Baseline security standards do not prevent unauthorized access. Exit routines are dependent upon appropriate role-based access.

**QUESTION NO: 294**

**Answer: D**

**Explanation:**

Digital signatures ensure that transmitted information can be attributed to the named sender; this provides nonrepudiation. Steganographic techniques are used to hide messages or data within other files. Biometric and two-factor authentication is not generally used to protect internet data transmissions.

**QUESTION NO: 295**

**Answer: A**

**Explanation:**

New viruses are being introduced almost daily. The effectiveness of virus detection software depends on frequent updates to its virus signatures, which are stored on antivirus signature files so updates may be carried out several times during the day. At a minimum, daily updating should occur. Patches may occur less frequently. Weekly updates may potentially allow new viruses to infect the system.

**QUESTION NO: 296**

**Explanation:**

A web server should normally be placed within a demilitarized zone (DMZ) to shield the internal network. Database and file/print servers may contain confidential or valuable data and should always be placed on the internal network, never on a DMZ that is subject to compromise. Switches may bridge a DMZ to another network but do not technically reside within the DMZ network segment.

**QUESTION NO: 297**

**Answer: D**

**Explanation:**

A firewall should be placed on a (security) domain boundary. Placing it on a web server or screened subnet, which is a demilitarized zone (DMZ), does not provide any protection. Since firewalls should be installed on hardened servers with minimal services enabled, it is inappropriate to have the firewall and the intrusion detection system (IDS) on the same physical device.

**QUESTION NO: 298**

**Answer: A**

**Explanation:**

An intranet server should be placed on the internal network. Placing it on an external router leaves it defenseless. Since firewalls should be installed on hardened servers with minimal services enabled, it is inappropriate to store the intranet server on the same physical device as the firewall. Similarly, primary- domain controllers do not normally share the physical device as the intranet server.

**QUESTION NO: 299**

**Answer: D**

**Explanation:**

Two-factor authentication through the use of strong passwords combined with security tokens provides the highest level of security. Data encryption, digital signatures and strong passwords do not provide the same level of protection.

**QUESTION NO: 300**

**Answer: A**

**Explanation:**

By centralizing security management, the organization can ensure that security standards are applied to all systems equally and in line with established policy. Sanctions for noncompliance would not be the best way to correct poor management practices caused by work overloads or insufficient knowledge of security practices. Enforcement of policies is not solely the responsibility of IT management. Periodic compliance reviews would not correct the problems, by themselves, although reports to management would trigger corrective action such as centralizing security management.

**QUESTION NO: 301**

**Answer: B**

**Explanation:**

Reported incidents will provide an indicator as to the awareness level of staff. An increase in reported incidents could indicate that staff is paying more attention to security. Intrusion incidents and access rule violations may or may not have anything to do with awareness levels. A decrease in changes to security policies may or may not correlate to security awareness training.

**QUESTION NO: 302**

**Answer: A**

**Explanation:**

Data classification is determined by the business risk, i.e., the potential impact on the business of the loss, corruption or disclosure of information. It must be applied to information in all forms, both electronic and physical (paper), and should be applied by the data owner, not the security manager. Choice B is an incomplete answer because it addresses only privacy issues, while choice A is a more complete response. Systems are not classified per se, but the data they process and store should definitely be classified.

**QUESTION NO: 303**

**Answer: B**

**Explanation:**

Documenting the password on paper is not the best method even if sent through interoffice mail if the password is complex and difficult to memorize, the user will likely keep the printed password and this creates a security concern. A dummy (temporary) password that will need to be changed upon first logon is the best method because it is reset immediately and replaced with the user's choice of password, which will make it easier for the user to remember. If it is given to the wrong person, the legitimate user will likely notify security if still unable to access the system, so the security risk is low. Setting an account with no initial password is a security concern even if it is just for a few days. Choice D provides the greatest security threat because user IDs are typically

known by both users and security staff, thus compromising access for up to 30 days.

**QUESTION NO: 304**

**Answer: C**

**Explanation:**

The information security program should ideally be sponsored by business managers, as represented by key business process owners. Infrastructure management is not sufficiently independent and lacks the necessary knowledge regarding specific business requirements. A corporate audit department is not in as good a position to fully understand how an information security program needs to meet the needs of the business. Audit independence and objectivity will be lost, impeding traditional audit functions. Information security implements and executes the program. Although it should promote it at all levels, it cannot sponsor the effort due to insufficient

operational knowledge and lack of proper authority.

**QUESTION NO: 305**

**Answer: C**

**Explanation:**

Service levels are key to holding third parties accountable for adequate delivery of services. This is more important than termination conditions, privacy restrictions or liability limitations.

**Topic 4 INCIDENT MANAGEMENT AND RESPONSE**

**QUESTION NO: 545**

**Answer: B**

**Explanation:**

Prior to creating a detailed business continuity plan, it is important to determine the incremental daily cost of losing different systems. This will allow recovery time objectives to be determined which, in turn, affects the location and cost of offsite recovery facilities, and the composition and mission of individual recovery teams. Determining the cost to rebuild information processing facilities would not be the first thing to determine.

**QUESTION NO: 546**

**Answer: A**

**Explanation:**

To preserve the integrity of the desktop computer as an item of evidence, it should be immediately disconnected from all sources of power. Any attempt to access the information on the computer by copying, uploading or accessing it remotely changes the operating system (OS) and temporary files on the computer and invalidates it as admissible evidence.

**QUESTION NO: 547**

**Answer: D**

**Explanation:**

Sharing a hot site facility is sometimes necessary in the case of a major disaster. Also, first come, first served usually determines priority of access based on general industry practice. A hot site is not indefinite; the recovery plan should address a long-term outage. In case of a disaster affecting a localized geographical area, the vendor's facility and capabilities could be insufficient for all of its clients, which will all be competing for the same resource. Preference will likely be given to the larger corporations, possibly delaying the recovery of a branch that will likely be smaller than other clients based locally.

**QUESTION NO: 548**

**Answer: C**

**Explanation:**

Isolating the affected network segment will mitigate the immediate threat while allowing unaffected portions of the business to continue processing. Shutting off all network access points would create a denial of service that could result in loss of revenue. Dumping event logs and enabling trace logging, while perhaps useful, would not mitigate the immediate threat posed by the network attack.

**QUESTION NO: 549**

**Answer: C**

**Explanation:**

Decoy files, often referred to as honeypots, are the best choice for diverting a hacker away from critical files and alerting security of the hacker's presence. Firewalls and bastion hosts attempt to keep the hacker out, while screened subnets or demilitarized zones (DM/.s) provide a middle ground between the trusted internal network and the external untrusted Internet.

**QUESTION NO: 550**

**Answer: D**

**Explanation:**

The first priority in responding to a security incident is to contain it to limit the impact.

Documentation, monitoring and restoration are all important, but they should follow containment.

**QUESTION NO: 551**

**Answer: A**

**Explanation:**

Unless backup media are available, all other preparations become meaningless. Recovery site location and security are important, but would not prevent recovery in a disaster situation. Having a secondary hot site is also important, but not as important as having backup media available. Similarly, alternate data communication lines should be tested regularly and successfully but, again, this is not as critical.

**QUESTION NO: 552**

**Answer: D**

**Explanation:**

Disaster recovery testing requires the allocation of sufficient resources to be successful. Without the support of management, these resources will not be available, and testing will suffer as a result. Testing on weekends can be advantageous but this is not the most important choice. As vendor-provided hot sites are in a state of constant change, it is not always possible to have network addresses defined in advance. Although it would be ideal to provide for identical equipment at the hot site, this is not always practical as multiple customers must be served and equipment specifications will therefore vary.

**QUESTION NO: 553**

**Answer: A**

**Explanation:**

For security and privacy reasons, all organizational data and software should be erased prior to departure. Evaluations can occur back at the office after everyone is rested, and the overall results can be discussed and compared objectively.

**QUESTION NO: 554**

**Answer: B**

**Explanation:**

Escalation criteria, indicating the circumstances under which specific actions are to be undertaken, should be contained within an incident response policy. Telephone trees, press release templates and lists of critical backup files are too detailed to be included in a policy document.

**QUESTION NO: 555**

**Answer: A**

**Explanation:**

Since information security objectives should always be linked to the objectives of the business, it is imperative that business processes be allowed to continue whenever possible. Only when there is no alternative should these processes be interrupted. Although it is important to allow the security team to assess the characteristics of an attack, this is subordinate to the needs of the business. Permitting an incident to continue may expose the organization to additional damage. Evaluating the incident management process for deficiencies is valuable but it, too. is subordinate to allowing

business processes to continue.

**QUESTION NO: 556**

**Answer: B**

**Explanation:**

Post-incident reviews are beneficial in determining ways to improve the response process through lessons learned from the attack. Evaluating the relevance of evidence, who launched the attack or what areas were affected are not the primary purposes for such a meeting because these should have been already established during the response to the incident.

**QUESTION NO: 557**

**Answer: B**

**Explanation:**

If data centers are operating at or near capacity, it may prove difficult to recover critical operations at an alternate data center. Although line capacity is important from a mirroring perspective, this is secondary to having the necessary capacity to restore critical systems. By comparison, differences in logical and physical security and synchronization of system software releases are much easier issues to overcome and are, therefore, of less concern.

**QUESTION NO: 558**

Which of the following is MOST important in determining whether a disaster recovery test is successful?

**Answer: C**

**Explanation:**

To ensure that a disaster recovery test is successful, it is most important to determine whether all critical business functions were successfully recovered and duplicated. Although ensuring that only materials taken from offsite storage are used in the test is important, this is not as critical in determining a test's success. While full recovery of the processing infrastructure is a key recovery milestone, it does not ensure the success of a test. Achieving the RTOs is another important milestone, but does not necessarily prove that the critical business functions can be conducted, due to interdependencies with other applications and key elements such as data, staff, manual processes, materials and accessories, etc.

**QUESTION NO: 559**

**Answer: C**

**Explanation:**

The complexity and business sensitivity of the processing infrastructure and operations largely determines the viability of such an option; the concern is whether the recovery site meets the operational and security needs of the organization. The cost to build a redundant facility is not relevant since only a fraction of the total processing capacity is considered critical at the time of the disaster and recurring contract costs would accrue over time. Invocation costs are not a factor because they will be the same regardless. The incremental daily cost of losing different systems and the recovery time objectives (RTOs) do not distinguish whether a commercial facility is chosen. Resulting criticality from the business impact analysis (BIA) will determine the scope and

timeline of the recovery efforts, regardless of the recovery location.

**QUESTION NO: 560**

**Answer: B**

**Explanation:**

Until signature files can be updated, incoming e-mail containing picture file attachments should be blocked. Quarantining picture files already stored on file servers is not effective since these files must be intercepted before they are opened. Quarantine of all mail servers or blocking all incoming mail is unnecessary overkill since only those e-mails containing attached picture files are in question.

**QUESTION NO: 561**

**Answer: C**

**Explanation:**

In the case of a probe, the situation should be monitored and the affected network segment isolated. Rebooting the router, powering down the demilitarized zone (DMZ) servers and enabling server trace routing are not warranted.

**QUESTION NO: 562**

Which of the following terms and conditions represent a significant deficiency if included in a commercial hot site contract?

**Answer: B**

**Explanation:**

Equipment provided "at time of disaster (ATOD), not on floor" means that the equipment is not available but will be acquired by the commercial hot site provider ON a best effort basis. This leaves the customer at the mercy of the marketplace. If equipment is not immediately available, the recovery will be delayed. Many commercial providers do require sharing facilities in cases where there are multiple simultaneous declarations, and that priority may be established on a first come, first-served basis. It is also common for the provider to substitute equivalent or better equipment, as they are frequently upgrading and changing equipment.

**QUESTION NO: 563**

**Answer: B**

**Explanation:**

An assessment should be conducted to determine whether any permanent damage occurred and the overall system status. It is not necessary at this point to rebuild any servers. An impact analysis of the outage or isolating the demilitarized zone (DMZ) or screen subnet will not provide any immediate benefit.

**QUESTION NO: 564**

**Answer: A**

**Explanation:**

In a major disaster, staff can be injured or can be prevented from traveling to the hot site, so technical skills and business knowledge can be lost. It is therefore critical to maintain an updated copy of the detailed recovery plan at an offsite location. Continuity of the business requires adequate network redundancy, hot site infrastructure that is certified as compatible and clear criteria for declaring a disaster. Ideally, the business continuity program addresses all of these satisfactorily. However, in a disaster situation, where all these elements are present, but without the detailed technical plan, business recovery will be seriously impaired.

**QUESTION NO: 565**

**Answer: B**

**Explanation:**

Recovery criteria, indicating the circumstances under which specific actions are undertaken, should be contained within a business continuity policy. Telephone trees, business impact assessments (BIAs) and listings of critical backup files are too detailed to include in a policy document.

**QUESTION NO: 566**

**Answer: D**

**Explanation:**

The most important function of an intrusion detection system (IDS) is to identify potential attacks on the network. Identifying how the attack was launched is secondary. It is not designed specifically to identify weaknesses in network security or to identify patterns of suspicious logon attempts.

**QUESTION NO: 567**

**Answer: A**

**Explanation:**

If all of the plans exist only in electronic form, this presents a serious weakness if the electronic version is dependent on restoration of the intranet or other systems that are no longer available. Versioning control and tracking changes in personnel and plan assets is actually easier with an automated system. Broken hyperlinks are a concern, but less serious than plan accessibility.

**QUESTION NO: 568**

**Answer: D**

**Explanation:**

The only accurate way to check the signature files is to look at a sample of servers. The fact that an update was pushed out to a server does not guarantee that il was properly loaded onto that server. Checking the vendor information to the management console would still not be indicative as to whether the file was properly loaded on the server. Personnel should never release a virus, no matter how benign.

**QUESTION NO: 569**

**Answer: B**

**Explanation:**

Information security should check the intrusion detection system (IDS) logs and continue to monitor the situation. It would be inappropriate to take any action beyond that. In fact, updating the IDS could create a temporary exposure until the new version can be properly tuned. Rebooting the router and enabling server trace routing would not be warranted.

**QUESTION NO: 570**

**Answer: D**

**Explanation:**

For the software to be effective, it must be easy to maintain and keep current. Market share and annualized cost, links to the intrusion detection system (IDS) and automatic notifications are all secondary in nature.

**QUESTION NO: 571**

**Answer: C**

**Explanation:**

Updating virus signature files on a weekly basis carries the risk that the systems will be vulnerable to viruses released during the week; far more frequent updating is essential. All other issues are secondary to this very serious exposure.

**QUESTION NO: 572**

**Answer: C**

**Explanation:**

Business process owners are in the best position to understand the true impact on the business that a system outage would create. The business continuity coordinator, industry averages and even information security will not be able to provide that level of detailed knowledge.

**QUESTION NO: 573**

**Answer: D**

**Explanation:**

Technical recovery plans, network redundancy and equipment needs are all associated with infrastructure disaster recovery. Only recovery time objectives (RTOs) directly relate to business continuity.

**QUESTION NO: 574**

**Answer: C**

**Explanation:**

In most businesses where an e-commerce site is in place, it would need to be restored in a matter of hours, if not minutes. Contractor payroll, change management and fixed assets would not require as rapid a recovery time.

**QUESTION NO: 575**

**Answer: B**

**Explanation:**

Quickly ranking the severity criteria of an incident is a key element of incident response. The other choices refer to documents that would not likely be included in a computer incident response team (CIRT) manual.

50 Question Review

CISM 50 Question Review

1. 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 |

2. Which of the following would BEST ensure the success of information security governance within an organization?

|  |
| --- |
| A. The steering committee approves all security projects. |
| B. The security policy manual is distributed to all managers. |
| C. Security procedures are accessible on the company intranet. |
| D. The corporate network utilizes multiple screened subnets. |

3. 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 |

4. Which of the following BEST indicates the probability that a successful attack will occur?

|  |
| --- |
| A. Value of the target and level of protection is high |
| B. Motivation and ability of the attacker is high |
| C. Value of the target is high and protection is low |
| D. Motivation of the attacker and value of the target is high |

5. The results of an organizational risk analysis should FIRST be shared with:

|  |
| --- |
| A. external auditors. |
| B. stockholders. |
| C. senior management. |
| D. peer organizations. |

6. The GREATEST reduction in overhead costs for security administration would be provided by:

|  |
| --- |
| A. mandatory access control. |
| B. role-based access control. |
| C. decentralized access control. |
| D. discretionary access control. |

7. Which of the following should be developed FIRST?

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

8. Which of the following will BEST protect against deletion of data files by a former employee?

|  |
| --- |
| A. Preemployment screening |
| B. Close monitoring of users |
| C. Periodic awareness training |
| D. Efficient termination procedures |

9. 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 |

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

|  |
| --- |
| A. Chief security officer |
| B. Chief operating officer |
| C. Chief internal auditor |
| D. Chief legal counsel |

11. Risk management programs are designed to reduce risk to:

|  |
| --- |
| A. a level this 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 |

12. Access to a sensitive intranet application by mobile users can BEST be accomplished through:

|  |
| --- |
| A. data encryption. |
| B. digital signatures. |
| C. strong passwords. |
| D. two-factor authentication. |

13. 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 |

14. The PRIMARY objective of security awareness is to:

|  |
| --- |
| A. ensure that security policies are read and understood. |
| B. encourage security-conscious employee behavior. |
| C. meet legal and regulatory requirements. |
| D. put employees on notice in case follow-up action for noncompliance is necessary. |

15. 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 the 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. Permit a 90-day window to see if a problem occurs. |

16. Which of the following is the BEST method for ensuring that security procedures and guidelines are read and understood?

|  |
| --- |
| A. Periodic focus group meetings |
| B. Periodic reminder memos to management |
| C. Computer-based training (CBT) presentations |
| D. Employees signing an acknowledgement of receipt |

17. Which of the following is the MOST effective in preventing attacks that exploit weaknesses in operating systems?

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

18. Which of the following is the MOST important to ensure a successful recovery?

|  |
| --- |
| A. Backup media is stored offsite. |
| B. Patches and firmware are up-to-date. |
| C. More than one hot site is available. |
| D. Data communication lines are regularly tested. |

19. Which of the following is MOST likely to be discretionary?

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

20. 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. review the configuration of the IDS. |
| D. benchmark the IDS against a peer site. |

21. Which of the following would be the MOST appropriate task for a chief information security officer 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. |

22. 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. |

23. Which of the following is the MOST important element in ensuring 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. Organizational management is supportive. |

24. 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 |

25. The MOST important reason for conducting the same risk assessment more than once is because:

|  |
| --- |
| A. mistakes are often made in the initial reviews. |
| B. security risks are subject to frequent change. |
| C. different reviewers analyze risk factors differently. |
| D. it shows management that the security staff is adding value. |

26. Accountability by business process owners can BEST be obtained through:

|  |
| --- |
| A. periodic reminder memorandums. |
| B. strict enforcement of policies. |
| C. policies signed by IT management. |
| D. education and awareness meetings. |

27. Which of the following is the BEST indicator that security awareness training has been effective?

|  |
| --- |
| A. Have employees sign to confirm they have read the security policy. |
| B. More incidents are being reported. |
| C. A majority of employees have received training. |
| D. Feedback forms from training are favorable. |

28. Which of the following should be mandatory for any disaster recovery test?

|  |
| --- |
| A. Only materials taken from offsite storage or those predeployed at the hot site are used. |
| B. Participants are not informed in advance when the test is to be held. |
| C. Hot site personnel are not informed in advance when the test is to be held. |
| D. Key systems are restored to identical operating system (OS) releases and hardware configurations. |

29. Which of the following would normally be covered in an insurance policy for computer equipment coverage? Equipment:

|  |
| --- |
| A. leased to the insured by another company. |
| B. leased to another company by the insured. |
| C. under the direct control of another company. |
| D. located at and belonging to a service provider. |

30. A business continuity policy document should contain which of the following?

|  |
| --- |
| A. Telephone trees |
| B. Declaration criteria |
| C. Press release templates |
| D. A listing of critical backup files |

31. 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 events. |

32. Which of the following should management use to determine the amount of resources to devote to mitigating exposures?

|  |
| --- |
| A. Risk analysis results |
| B. Audit report findings |
| C. Penetration test results |
| D. Fixed percentage of IT budget |

33. Which of the following will MOST likely reduce the likelihood 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. |

34. Which of the following is MOST important when deciding whether to build an alternate facility or subscribe to a hot site operated by a third party?

|  |
| --- |
| A. Cost to rebuild information processing facilities. |
| B. Incremental daily cost of losing different systems. |
| C. Location and cost of commercial recovery facilities. |
| D. Estimated annualized loss expectancy from key risks. |

35. The MOST appropriate reporting base for the information security management function would be to report to the:

|  |
| --- |
| A. head of IT. |
| B. infrastructure director. |
| C. network manager. |
| D. chief information officer. |

36. When residual risk is minimized:

|  |
| --- |
| A. acceptable risk is achieved. |
| B. transferred risk is minimized. |
| C. control risk is reduced to zero. |
| D. residual risk equals transferred risk. |

37. 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. More aligned to business unit needs |
| D. Less total cost of ownership |

38. 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 defense in-depth. |
| B. separate test and production. |
| C. permit traffic load balancing. |
| D. prevent a denial-of-service attack. |

39. 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. |

40. When a minor security flaw is found in a new system that is about to be moved into production, this should be reported to:

|  |
| --- |
| A. senior management in a quarterly report. |
| B. users who may be impacted by the flaw. |
| C. executive management in an immediate report. |
| D. customers who may be impacted by the flaw. |

41. Which of the following is MOST indicative of the failure of information security governance within an organization?

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

42. The decision on whether new risks should fall under periodic or event-driven reporting should be based on:

|  |
| --- |
| A. severity and duration. |
| B. visibility and duration. |
| C. likelihood and duration. |
| D. absolute monetary value. |

43. What 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. |

44. 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. Build senior management support |
| C. Assemble an experienced staff |
| D. Interview peer organizations |

45. Acceptable risk is achieved when:

|  |
| --- |
| A. residual risk is minimized. |
| B. transferred risk is minimized. |
| C. control risk equals acceptable risk. |
| D. residual risk equals transferred risk. |

46. A risk management program should MOST importantly seek to:

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

47. Which of the following are seldom changed in response to technological changes?

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

48. The BEST way to integrate risk management into life cycle processes is through:

|  |
| --- |
| A. policy development. |
| B. change management. |
| C. awareness training. |
| D. regular monitoring. |

49. 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 logs |
| C. Role-based access controls |
| D. Intrusion detection system |

50. A risk assessment should be conducted:

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

**ANSWERS**

1. C

2. A

3. C

4. C

5. C

6. B

7. C

8. D

9. D

10. B

11. C

12. D

13. B

14. B

15. C

16. C

17. A

18. A

19. C

20. A

21. D

22. B

23. D

24. B

25. B

26. D

27. B

28. A

29. A

30. B

31. C

32. A

33. B

34. C

35. D

36. A

37. C

38. C

39. C

40. A

41. D

42. B

43. D

44. B

45. A

46. B

47. C

48. B

49. C

50.D