CISM Review

CISM Study Review

Governance is accountable for:

Risk Appetite

Goals:

- Providing strategic vision and direction
- Maintaining Compliance with Laws and Regulations
- Reaching security and business objectives
- Ensure that risks are managed appropriately and proactively
- Verify that the enterprise's resources are used responsibly

Management is Responsible

To Determine the "how"

Assesses, implements, and monitors

Risk Tolerance and Thresholds

Security Strategy should:

- Indicate necessary resources
- Constraints
- A roadmap
- Includes people, processes, technologies and other resources
- A security architecture: defining business drivers, resource relationships and process flows
- Achieving the desired state is a long-term goal of a series of projects or program
    - Gap analysis examines difference between current state and desired state
        - CMM

Security Program helps us accomplish the strategy

- Must determine goals first
- Basis for Security Program is Risk Management
- Elements of a security Program include
    - Policies—brought statements from Senior management, not likely to change often
    - Standards: Define policy—may change as technology or practices change
    - Processes &Procedures
        - Step-by-step guides
        - Must be formally documented and repeatable and sustainable
    - Guidelines
        - Suggestions--Not mandatory
    - Controls
    - Managerial(Administrative)

        - Mandatory Vacations
        - Separation of Duties
        - Principle of least privilege
            - Limit administrative access
        - Need to Know
    - Operational (and Physical)
    - Technical(Logical)
        - Firewalls provide isolation between security zones (Trusted, untrusted, semi-trusted)
            - Semi-trusted is DMZ (should include Web, Mail, DNS, honeypots, and IDS)—screened subnet
        - NAT/PAT
            - Provides protection by obscuring internal systems and allowing them to use a single external address
        - Single sign on allows a user to have a single username/password to access many resources
            - Kerberos is symmetric system that is ticket based to allow access.
    - Training, Awareness and education
        - Reduce Human Risk
        - Indications of effectiveness
            - Increase in security events reported
        - Indications that employees understand
            - Quantitative assessments of employee knowledge
    - Compliance enforcement
    - Technologies
    - Personnel security
    - Organizational structure
    - Skills
    - Outsourced security providers
    - Other organizational support and assurance providers
    - Facilities
    - Environmental security
    - 3rd party management
        - Driven by contract and SLA
        - Right to audit
    - Configuration/Change management—promote security and stability
        - Nothing happens on the fly---follow the process
            - Exceptions should be documented and provide instructions for escalation

- Alignment with business objectives
    - Ensures we use resources In areas that will impact the business the most
    - Helps deliver value
    - Governance is accountable for approval of the alignment

- Addressing Risk
    - Identification: First step—just identifies and categorizes risk—begins the risk register
    - Assessment/Analysis: Assigns value: Qualitative is subjective, Quantitative is Objective
        - Analysis helps us to determine the mitigation strategy (which controls we put in place)
        - Purpose is to provide justification for controls
    - Mitigation/Response: Implement a control based on cost/benefit analysis
        - Don't implement anything without metrics
        - Establish KPIs and KRI to help evaluation process
        - Most important is for a control to meet its objectives
        - Limit Administrative Access to EVERYTHING
        - Reduce: Lessen probability and/or impact
        - Transfer
            - SLAs,
            - Cloud
            - Insurance
        - Accept when cost of countermeasure exceeds value of asset or potential for loss
        - Residual risk must be brought into alignment with Acceptable risk
        -
    - Monitoring and Controlling
        - Variance analysis
            - Are controls meeting their objectives
            - Tools: KPI, KRI, Balanced Scorecard
                - a Balanced Scorecard:
                    - measuring tool for goal attainment
                    - assess whether information security governance objectives are being met
                    - can track the effectiveness of how an organization executes it information security strategy and determine areas of improvement
                -
            - Risk Register
            - Input from business units
- Security Posture: the approach your business takes to **security**, from planning to implementation. It is comprised of technical and non-technical policies, procedures and controls, which protect you from both internal and external threats.
-

Incidence response goal is to minimize impact on the business

- Investigate first---violation analysis
- Unless instructed to do so, don't act…notify CIRT
- Best way to ensure controls will work is to test them—pen tests and vulnerability assessments
    - Most important is that objectives are defined
    - Second should be signed approval from senior management

- Segment and affected system or network
    - Do NOT turn off systems, reboot, or conduct investigations
    - Forensics requires collection of evidence from most to least volatile
        - Maintain chain of custody
- Cryptography:
    - Symmetric
        - Out of band key exchange
        - Not Scalable
        - No non-repudiation
        - FAST
    - Asymmetric
        - Allows key exchange without sending sensitive information (only public key is shared
            - Confidentiality—Receiver's public
            - Integrity—hashing
            - Authenticity—Sender's private key
            - Non-repudiation—hash is encrypted with sender's private key (digital signature)
        - Digital Certificates are commonly used for purpose of authentication
    - Intrusion Detection System
        - HIDS—only examine a single host
        - NIDS examine a network segment.
            - Placed in DMZ and Internal network
        - Can look for
            - signatures (can't detect zero day attacks)
            - behaviors (can have false positives)
- Business Continuity—safety net under risk management
    - Long term health of business no matter what
    - Includes a DRP focused on IT and immediacy of the disaster
    - All decisions stem from BIA (must be signed off from management)
        - Assesses Criticality of processes/systems and prioritizes them)
    - Protect human life first
    - Must start with policy
    - RTO—maximum amount of time a service can be inaccessible before the loss is unacceptable to senior management
    - RPO—tolerance for data loss
    - Cold site---facility with nothing but power/plumbing
    - Warm site—nothing proprietary, but would have basic business needs (furniture, phones, etc
    - Hot site---ready to go as soon as most current data is restored
    - Testing is essential—should mimic a disaster as much as possible.
        - Only use resources at offsite facility or those located outside the building
        - 5 types of tests
            - Checklist

- Tabletop (structured Walkthrough)
- Simulation
- Parallel
- Full interruption

Testing Day:

Get a good night's sleep before---don't stay up all night cramming

Get up in plenty of time to get to testing center…If late for any reason, call!

Be mindful of the clock—200 questions in four hours

Chose the beast answer. Trust your instincts

Limit the number of questions you change

Many questions are "MOST" or "BEST" which means multiple answers are true…which one solves the problem best, most efficiently or is most closely aligned with isaca

USE THE 600 QUESTIONS

Search for "most" "least" "best" "except"

Think alignment with business goals, risk management, cost/benefit analysis, measure objectives

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