Test du CISM

Attention, les questions, comme l'examen, ne sont disponibles qu'en anglais.

1. 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.

2. Which of the following should be developed FIRST?

A. Standards

B. Procedures

C. Policies

D. Guidelines

3. 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

4. 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.

5. 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.

6. 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.

7. 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

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

A. Standards

B. Procedures

C. Policies

D. Guidelines

9. 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

10. 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.

11. 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.

12. 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.

13. 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

14. 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.

15. 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.

16. 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.

17. 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.

18. 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.

19. 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.

20. 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.

21. 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

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

A. external auditors.

B. stockholders.

C. senior management.

D. peer organizations.

23. 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.

24. 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.

25. 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.

26. 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

27. 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

28. 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

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

A. Network switch

B. Web server

C. Database server

D. File/print server

30. 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.

31. An information security program should be sponsored by:

A. infrastructure management.

B. the corporate legal department.

C. key business process owners.

D. quality assurance management.

32. 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.

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 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.

35. Which of the following metrics would be the MOST useful in measuring how well information security is monitoring violation logs? The number of:

A. penetration attempts investigated.

B. violation log reports reviewed.

C. violation log entries reviewed.

D. hours charged to the review process.

36. When a departmental system continues to remain out of compliance with the information security policy's password strength requirements, the BEST action to undertake is to:

A. submit the issue to an external arbitration group.

B. conduct an impact analysis to quantify the risks.

C. isolate the system from the rest of the network.

D. grant a special waiver that is subject to annual renewal.

37. Nonrepudiation can BEST be assured by using:

A. delivery path tracing.

B. reverse lookup translation.

C. out-of-band channels.

D. digital signatures.

38. 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.

39. The BEST time to perform a penetration test is after a(n):

A. attempted penetration has occurred.

B. audit has discovered a lack of security controls.

C. number of systems infrastructure changes are made.

D. turnover in systems administrative staff.

40. Sign-on mechanisms should be configured so that they:

A. display no identifying details until after sign-on is completed successfully.

B. store authentication details as clear text in automated routines, such as in scripts.

C. validate sign-on information as it is entered.

D. enable additional sign-on attempts.

41. 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.

42. 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

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. 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.

45. 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.

46. 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.

47. 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.

48. 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.

49. 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

50. 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.

Réponses :

1-A ; 2-C ; 3-B ; 4-A ; 5-D ; 6-D ; 7-B ; 8-C ;9-C ;10-C

11-D ; 12-B ; 13-A ; 14-A ; 15-B ; 16-D ; 17-D ; 18-B ; 19-A ; 20-A

21-C ; 22-C ; 23-B ; 24-C ; 25-D ; 26-C ; 27-D ; 28-C ; 29-B ; 30-D

31-C ; 32-B ; 33-B ; 34-B ; 35-A ; 36-B ; 37-D ;38-A ; 39-C

40-A ; 41-B ; 42-D ;43-D ;44-C ;45-A ; 46-D ;47-C ; 48-C ;49-B ; 50-A

Le test est-il concluant ? N'oubliez pas que l'obtention du CISM est subordonnée à la réalisation d'un score supérieur ou égal à 75%. Entraînez-vous et bon courage !