1) (A) A test has not been made to ensure that local resources could maintain security and service standards

when recovering from a disaster or incident.

2) (D) Run an automated tool to verify the security patches on production servers.

3) (D) Establish regular IT risk management meetings to identify and assess risk, and create a mitigation plan as

input to the organization's risk management.

4) (D) Confidential documents leaving the internal network

5) (A) Approve and document the change the next business day

6) (D) Development of a risk assessment

7) (A) Implement a log management process.

8) (B) Implement accountability rules within the organization.

9) (C) Discovery

10) (A) Server configuration has been hardened appropriately.

11) (C) Project management

12) (A) data owners.

13) (C) Confirm the content of the agreement with both departments.

14) (B) Recovery time objectives (RTOs) were met.

15) (B) Computer-assisted audit techniques (CAATs)

16) (A) Publish a report based on the available information, highlighting the potential security weaknesses and the

requirement for follow-up audit testing.

17) (A) Implement a properly documented process for application role change requests

18) (C) The vendor of custom-written software goes out of business.

19) (C) attack problems that require consideration of a large number of input variables.

20) (C) Shoulder surfing

21) (A) lower confidence coefficient, resulting in a smaller sample size.

22) (A) Power line conditioners

23) (B) agrees to be subject to external security reviews.

24) (D) User education

25) (B) verify the software is in use through testing.

26) (B) execution of the disaster recovery plan could be impacted.

27) (C) Project steering committee

28) (B) Phishing

29) (B) Both entities are vulnerable to the same incident.

30) (B) backed by sufficient and appropriate audit evidence.

31) (D) minimize the impact of an adverse event.

32) (A) nonpersonalized access cards are given to the cleaning staff, who use a sign-in sheet but show no proof of

identity.

33) (B) Faulty migration of historical data from the old system to the new system

34) (C) Purpose, objective and scope of the audit

35) (C) Determine the highest-risk systems and plan accordingly.

36) (A) Elliptical curve cryptography (ECC)

37) (B) Return on investment (ROI) analysis

38) (A) System owners

39) (B) business case be updated and possible corrective actions be identified.

40) (A) the existence of a data retention policy

41) (A) effectiveness of the QA function because it should interact between project management and user

management.

42) (B) A vulnerability

43) (B) To ensure that investments are made according to business requirements

44) (B) During the test, some of the backup systems were defective or not working, causing the test of these

systems to fail.

45) (A) Piggybacking

46) (B) All files and folders on hard disks are separately deleted, and the hard disks are formatted before leaving

the organization.

47) (A) Requirements should be tested in terms of importance and frequency of use.

48) (A) Program output testing

49) (C) Intrusion detection system (IDS)

50) (A) Business processes owners

51) (D) Unauthorized network activities

52) (A) Applicable statutory requirements

53) (C) a deployment plan based on sequenced phases.

54) (A) implementing security awareness training.

55) (B) The replacement effort consists of several independent projects without integrating the resource allocation

in a portfolio management approach.

56) (C) document the finding and explain the risk of using shared IDs.

57) (B) Implementing measures to prevent session hijacking attacks

58) (A) discuss the scope of the audit.

59) (B) is installed on an operating system with default settings.

60) (C) Review policy to see if a formal exception process is required.

61) (D) session key with the receiver's public key.

62) (B) IT management

63) (C) develop the audit plan on the basis of a detailed risk assessment.

64) (A) Ensure that the IT security risk assessment has a clearly defined scope

65) (A) use this information to launch attacks.

66) (D) request all standards that have been adopted by the organization

67) (D) Perform an end-to-end walk-through of the process

68) (B) Mitigation

69) (C) Performance measures were not included in the SLA.

70) (D) tracing.

71) (C) Program evaluation review technique (PERT)

72) (A) User management

73) (B) the client's change management process is adequate.

74) (C) Focus on auditing high-risk areas.

75) (D) Data owner