1 An IS auditor observes that one of the servers on the perimeter network is running a vulnerable operating system. What is the MOST likely implication due to the existence of a system vulnerability?

A. The server is susceptible to an attack.
B. An attack will occur.
C. A control must be designed as a countermeasure.
D. The likelihood of threats will increase.

2 An information security policy stating that "the display of passwords must be masked or suppressed" addresses which of the following attack methods?

A. Piggybacking
B. Dumpster diving
C. Shoulder surfing
D. Impersonation

3 The determination of an enterprise's IT risk appetite is BEST determined by:

A. the chief legal officer.
B. security management.
C. the audit committee.
D. the steering committee.

4 An IS auditor has been asked to participate in project initiation meetings for a critical project. The IS auditor's MAIN concern should be that the:

A. complexity and risks associated with the project have been analyzed.
B. resources needed throughout the project have been determined.
C. project deliverables have been identified.
D. a contract for external parties involved in the project has been completed.

5 During a logical access controls review, an IS auditor observes that user accounts are shared. The GREATEST risk resulting from this situation is that:

A. an unauthorized user may use the ID to gain access.
B. user access management is time consuming.
C. passwords are easily guessed.
D. user accountability may not be established.

6 Which of the following responsibilities would MOST likely compromise the independence of an IS auditor when reviewing the risk management process?

A. Participating in the design of the risk management framework
B. Advising on different implementation techniques
C. Facilitating risk awareness training
D. Performing due diligence of the risk management processes

7 Which of the following would BEST mitigate the threat to an enterprise's data security from insider attacks?

A. Formalizing a corporate information security policy
B. Providing security training to employees
C. Providing competitive compensation for key positions
D. Performing adequate screening for potential employees

8 The decisions and actions of an IS auditor are MOST likely to affect which of the following risks?

A. Inherent
B. Control
C. Detection
D. Business

9 A financial services enterprise has a small IT department, and individuals perform more than one role. Which of the following practices represents the GREATEST risk?

A. The developers promote code into the production environment.
B. The business analyst writes the requirements and performs functional testing.
C. The IT manager also performs systems administration.
D. The database administrator (DBA) also performs data backups

10 An organization has terminated a database administrator (DBA). The organization immediately removes all of the DBA's access to all company systems. The DBA threatens that the database will be deleted in two months unless he/she is paid a large sum of money. Which of the following would the former DBA MOST likely use to delete the database?

A. Virus infection
B. Worm infection
C. Denial-of-service (DoS) attack
D. Logic bomb attack

11 An IS auditor has been assigned to review an organization's information security policy. Which of the following issues represents the HIGHEST potential risk?

A. The policy has not been updated in more than one year.
B. The policy includes no revision history.
C. The policy is approved by the security administrator.
D. The company does not have an information security policy committee.

12 An IS auditor is evaluating management's risk assessment of information systems. The IS auditor should FIRST review:

A. the controls already in place.
B. the effectiveness of the controls in place.
C. the mechanism for monitoring the risks related to the assets.
D. the threats/vulnerabilities affecting the assets.

13 The GREATEST risk when end users have access to a database at its system level, instead of through the application, is that the users can:

A. make unauthorized changes to the database directly, without an audit trail.
B. make use of a system query language (SQL) to access information
C. remotely access the database.
D. update data without authentication.

14 Assessing IT risks is BEST achieved by:

A. evaluating threats associated with existing IT assets and IT projects.
B. using the firm's past actual loss experience to determine current exposure.
C. reviewing published loss statistics from comparable organizations.
D. reviewing IT control weaknesses identified in audit reports.

15 Which of the following does a lack of adequate security controls represent?

A. Threat
B. Asset
C. Impact
D. Vulnerability

16 During an audit, an IS auditor notices that the IT department of a medium-sized organization has no separate risk management function, and the organization's operational risk documentation only contains a few broadly described IT risks. What is the MOST appropriate recommendation in this situation?

A. Create an IT risk management department and establish an IT risk framework with the aid of external risk management experts.
B. Use common industry standard aids to divide the existing risk documentation into several individual risks which will be easier to handle.
C. No recommendation is necessary since the current approach is appropriate for a medium-sized organization.
D. Establish regular IT risk management meetings to identify and assess risks, and create a mitigation plan as input to the organization's risk management.

17 When evaluating the collective effect of preventive, detective or corrective controls within a process, an IS auditor should be aware of which of the following?

A. The point at which controls are exercised as data flow through the system
B. Only preventive and detective controls are relevant
C. Corrective controls can only be regarded as compensating
D. Classification allows an IS auditor to determine which controls are missing

18 Before implementing controls, management should PRIMARILY ensure that the controls:

A. satisfy a requirement in addressing a risk issue.
B. do not reduce productivity.
C. are based on a cost-benefit analysis.
D. are detective or corrective

19 The MOST effective control for addressing the risk of piggybacking is:

A. a single entry point with a receptionist.
B. the use of smart cards.
C. a biometric door lock.
D. a deadman door.

20 Sharing risk is a key factor in which of the following methods of managing risk?

A. Transferring risk
B. Tolerating risk
C. Terminating risk
D. Treating risk

21 Which of the following is the primary objective for implementing ERM?

A. Implement right level of controls.
B. Better availability of information.
C. Tighter security at lower cost.
D. Implement IT best practices.

22 The MOST important benefit of implementing IT risk management process is that it helps in:

A. optimizing internal control framework.
B. ensuring residual risk is at acceptable level.
C. prioritizing business functions for audit planning.
D. complying with regulatory requirements.

23 Which of the following is a major risk factor?

A. Existence of inflationary trends.
B. Vendor launches new software.
C. Board of directors elects new chairman.
D. Change in government post elections.

24 The level to which an enterprise can accept financial loss from a new initiative is:

A. Risk tolerance
B. Risk management
C. Risk appetite
D. Risk acceptance

25 Designing and implementing a control to reduce the likelihood and/or impact of risk materializing is a:

A. Risk acceptance
B. Risk transfer
C. Risk treatment
D. Risk transfer

26 Which of the following is a valid risk statement?

A. Network service provider is unable to meet bandwidth.
B. Hacker attempts to launch attack on web site.
C. Application server crash due to power failure.
D. Delay in servicing customers due to network congestion.

27 Which of the following is primary reason for periodic review of risk? The changes in:

A. risk factors
B. risk appetite
C. budget
D. risk strategy

28 Which of the following is a strategic IT risk?

A. IS audit may not identify critical non-compliance.
B. Non-availability of networks impacting services to customers.
C. New application may not achieve expected benefits.
D. Defer replacement of obsolete hardware.

29 Which of the following is the most essential action after evaluation of inherent risks?

A. Evaluate implemented controls.
B. Update risk register.
C. Prepare heat map.
D. Prioritized evaluated risk.

30 Which of the following scenarios has the highest impact?

A. Absence of business continuity plan.
B. Absence of Security operations center.
C. Absence of monitoring of SLA.
D. Absence of risk management process.

31 Which of the following is the best strategy to address the risk of non-compliance?

A. Maintain inventory compliance requirements.
B. Embedding risk of non-compliance in operations.
C. Appointing chief compliance officer.
D. Implement IT governance framework.

32 Implementing IT risk management process is essential for implementing IT governance because IT risk management primarily helps enterprise in:

A. Protecting and securing IT resources.
B. Arriving at likelihood and impact of risk.
C. Optimizing cost of control based on risk.
D. Monitoring performance of resources.

33 IS auditor observed that logical access controls implemented are weak. The IS auditor should next:

A. analyze the risk associated and report the finding.
B. advise auditee management on ways to strengthen the controls.
C. check for existence of compensating controls.
D. report the weakness as non-compliance

34 Which of the following observation by IS auditor will be reported in audit report as a security risk?

A. retired employee meeting data center manager in data center
B. data center manager meeting resigned employee in meeting room
C. resigned employee meeting HR personnel in reception area
D. retired employee have submitted access card to security guard

35 In order to ensure appropriate continuity plan it is necessary that risk manager must:

A. prioritize IT assets based on criticality of assets
B. express impact of risk based on loss to business
C. focus on physical risks affecting human life
D. ensure residual risks are more than risk appetite

36 The role of IT risk management in implementing IT governance can best be described as:

A. Determine levels of risk appetite and risk tolerance
B. Help management to take risk informed decisions
C. Accept risks based on cost-benefits of controls
D. Review overall risk profile of organization regularly

37 While prioritizing audit cycle, internal audit department focuses on key business areas for audit mainly based on:

A. business strategy.
B. requests from auditee.
C. fixed periodic interval.
D. results of risk assessment

38 A risk practitioner reviews previous IS audit findings PRIMARILY to understand:

A. vulnerabilities in system.
B. threats to IT infrastructure.
C. additional controls required.
D. changes in IT risk profile.

39 What is the MOST effective method to evaluate the potential impact of legal, regulatory and contractual requirements on business objectives?

A. A compliance-oriented gap analysis
B. Interviews with business process stakeholders
C. A mapping of compliance requirements to policies and procedures
D. A compliance-oriented business impact analysis (BIA)

40 Shortly after performing the annual review and revision of corporate policies, a risk practitioner becomes aware that a new law may affect security requirements for the human resources system. The risk practitioner should:

A. analyze in detail how the law may affect the enterprise.
B. ensure necessary adjustments are implemented during the next review cycle.
C. initiate an ad hoc revision of the corporate policy.
D. notify the system custodian to implement changes.

41 The PRIMARY concern of a risk practitioner documenting a formal data retention policy is:

A. storage availability.
B. applicable organizational standards.
C. generally accepted industry best practices.
D. business requirements.

42. Overall business risk for a particular threat can be expressed as the:

A. magnitude of the impact should a threat source successfully exploit the vulnerability.
B. likelihood of a given threat source exploiting a given vulnerability.
C. product of the probability and magnitude of the impact if a threat exploits a vulnerability.
D. collective judgment of the risk assessment team.

43 Which of the following is the GREATEST risk of a policy that inadequately defines data and system ownership?

A. Audit recommendations may not be implemented.
B. Users may have unauthorized access to originate, modify or delete data.
C. User management coordination does not exist.
D. Specific user accountability cannot be established.

44 Who should be accountable for the risk to an IT system that supports a critical business process?

A. IT management
B. Senior management
C. The risk management department
D. System users

45 Which of the following provides the BEST view of risk management?

A. An interdisciplinary team
B. A third-party risk assessment service provider
C. The enterprise's IT department
D. The enterprise's internal compliance department

46 Who is MOST likely responsible for data classification?

A. The data user
B. The data owner
C. The data custodian
D. The system administrator

47 An enterprise has learned of a security breach at another entity that utilizes similar technology. The MOST important action a risk practitioner should take is to:

A. assess the likelihood of the incident occurring at the risk practitioner's enterprise.
B. discontinue the use of the vulnerable technology.
C. report to senior management that the enterprise is not affected.
D. remind staff that no similar security breaches have taken place.

48 The MAIN objective of IT risk management is to:

A. prevent loss of IT assets.
B. provide timely management reports.
C. ensure regulatory compliance.
D. enable risk-aware business decisions

49 Which of the following is the BEST risk identification technique for an enterprise that allows employees to identify risk anonymously?

A. The Delphi technique
B. Isolated pilot groups
C. A strengths, weaknesses, opportunities and threats (SWOT) analysis
D. A root cause analysis

50 Which of the following is the PRIMARY reason that a risk practitioner determines the security boundary prior to conducting a risk assessment?

A. To determine which laws and regulations apply
B. To determine the scope of the risk assessment
C. To determine the business owner(s) of the system
D. To decide between conducting a quantitative or qualitative analysis