BRAINWARE UNIVERSITY

Term End Examination 2021 - 22
Programme – Master of Science in Advanced Networking & Cyber Security
Course Name – Cyber Risk Management
Course Code - MNCS204
(Semester II)

Time allotted : 1 Hrs.15 Min. **Full Marks : 60**

[The figure in the margin indicates full marks.]

Group-A

(Multiple Choice Type Question) 1 x 60=60

Choose the correct alternative from the following :

(1) The primary responsibility of the information security steering committee is:

a) Direction setting and performance monitoring
b) Information security policy development
c) Information security control implementation
d) Provision of information security training for employees

(2) Which of the following would be included in an information security strategic plan?

a) Specifications for planned hardware purchases
b) Analysis of future business objectives
c) Target dates for information security projects
d) Annual budgetary targets for the security department

(3) The most important responsibility of an information security manager in an organization is:

a) Recommending and monitoring security policies
b) Promoting security awareness within the organization
c) Establishing procedures for security policies
d) Administering physical and logical access controls

(4) On which of the following would an information security strategy place the most emphasis?

a) Business goals and objectives
b) Technology plans and deliverables
c) Industry best practices
d) Security metrics

(5) Which of the following best describes an information security department's strategic planning process?

a) The department will have either short-range or long-range plans depending on the organization's broader plans and objectives.

b) The department's strategic plan must be time and project oriented, but not so detailed as to address and help determine priorities to meet business needs.

c) Long-range planning for the department should recognize organizational goals, technological advances, and regulatory requirements.

d) Short-range planning for the department does not need to be integrated into the long-range plans of the organization because technological advances will drive the department plans much quicker than organizational plans.

(6) To ensure that an organization's password policy is effective, it must provide two key elements: difficult to guess; and

a) Be encrypted at all times

b) Contain a number of characters

c) Must be changed periodically

d) Controlled by security administration

(7) "Least privilege" is defined as:

a) The level of authorization granted to a user that is under investigation

b) Access to, knowledge of, or possession of information based on need to perform assigned job duties

c) Only most restrictive privileges granted based on need for job performance

d) Level of trust that is granted to system users

(8) An organization's log-on screen must contain three statements: the system is for authorized users, activities will be monitored, and

a) Wrongful activities will be turned over to HR.

b) By completing the log-on process you agree to the monitoring.

c) Password must not be shared.

d) Violators will be prosecuted.

(9) The purpose of change control is to:

a) Track changes to system hardware, software, firmware, and documentation.

b) Maintain visibility of changes to the system.

c) Ensure that changes to the system are approved.

d) To track and approve changes to system hardware, software, firmware, and documentation.

(10) The principle of separation of duties is useful in:

a) Reducing the opportunity for fraud

b) Identifying critical positions

c) Developing job descriptions

d) Conducting background investigations

(11) What are the three objectives of information security?

a) Prevent, detect, respond

b) Integrity, authenticity, and completeness

c) Confidentiality, integrity, and availability

d) Identification, authentication, non-repudiation

(12) Need-to-know is defined as

a) Access to, knowledge of, or possession of information based on need to perform security duties

b) Possession of information based on need to perform assigned duties

c) Access to, knowledge of, or possession of information based on need to perform assigned job duties

d) Knowledge of information or activities based on need to perform job functions

(13) A financial estimate designed to help consumers and enterprise managers assess direct and indirect costs related to the purchase of any capital investment, such as (but not limited to) computer software or hardware is termed:

a) Return on investment
b) Return on security investment
c) Total value of asset compensation
d) Total cost of ownership

(14) This recent piece of legislation requires annual affirmation of management's responsibility for internal controls over financial reporting. Management must attest to effectiveness based on an evaluation and the auditor must attest and report on management's evaluation.

a) Foreign Corrupt Practices Act
b) Sarbanes–Oxley
c) Model Business Corporation Act
d) Gramm–Leach–Bliley Act

(15) An annual report of the state of information security should be presented to the information security steering committee. This reporting requirement has been established in the current legislation and information security international standards. This report should not be confused with a standard feature audit performed by the audit staff nor is it part of some third-party certification process. Who is responsible for presenting this annual report?

a) CISO
b) CTO
c) CEO
d) CFO

(16) This individual is responsible for the organization's planning, budgeting, and performance, including its information security components. Decisions made in this area should be based on an effective risk management program.

a) Information owner
b) Information security administrator
c) General auditor
d) Chief information security officer

(17) Any information security program must get its direction from executive management. The requirements of today's laws and regulations have identified either the organization's board of directors or what other body as responsible for instituting an effective program?

a) Information security steering committee
b) Business operations approval team
c) Crisis management team
d) Cyber incident response board

(18) Unlike the policy development process, the use of a team to develop procedures will actually slow the process down. Many security professionals reach this stage of the information security program and believe that the bulk of their work is complete and now it will be up to whom to write the procedures?

a) Technical writer
b) Help desk administrator
c) Subject matter expert
d) Socially awkward male

(19) There are three types of policies and you will use each type at different times in your information security program and throughout the organization to support the business process or mission. The policy that is used to establish the organization's overall vision and direction is termed:

a) Global (Tier 1)
b) Topic-specific (Tier 2)
c) Application-specific (Tier 3)
d) System-specific (Tier 4)

(20) A director shall discharge his or her duties: in good faith; with the care an ordinarily prudent person in a like position would exercise under similar circumstances; and in a manner he or she reasonably believes is in the best interest of the enterprise. This responsibility is termed:

a) Duty of loyalty
b) Duty of fairness
c) Fiduciary duty
d) Duty of care

(21) The group who is charged with the responsibility to "assess the adequacy of and compliance with management, operating, and financial controls, as well as the administrative and operational effectiveness of organizational units" is who?

a) Information security
b) Auditing staff
c) Corporate council
d) Government and regulatory affairs

(22) This organization got its start in 1967, when a small group of individuals with similar jobs—auditing controls in the computer systems that were becoming increasingly critical to the operations of their organizations—sat down to discuss the need for a centralized source of information and guidance in the field. This organization is called:

a) Data Processing Management Association (DPMA)
b) Information Systems Security Association (ISSA)
c) Information Systems Audit and Control Association (ISACA)
d) American Society for Industrial Security (ASIS)

(23) The Cyber Security Industrial Alliance published their National Agenda for Information Security in 2006 in December, 2005. In this document the Alliance noted that "Information assurance in the private sector is critical to creating a more secure infrastructure." The report recommended that the federal government "encourage" CEOs to review cyber security measures at board meetings. This effort will help senior executives understand what?

a) Their personal liability for noncompliance
b) Their responsibilities when accessing material inside information
c) The security-related implications of Sarbanes–Oxley, GLBA, and HIPAA
d) The impact of ROSI on profit margins

(24) Which of the following is a key drawback in the use of quantitative risk analysis? It:

a) Applies numeric measurements to qualitative elements
b) Attempts to assign numeric values to exposures of assets
c) Is based on a criticality analysis of information assets
d) Produces the results in numeric (percentage, probability) form

(25) Acceptable risk is usually:

a) Subjectively determined
b) Objectively determined
c) Less than residual risk
d) Based on loss expectancy

(26) The cost of mitigating a risk should not exceed the:

a) Annual loss expectancy
b) Value of the physical asset
c) Expected benefit to be derived
d) Cost to the perpetrator to exploit the weakness

(27) Which of the following is the best source for developing Recovery Time Objectives (RTO)?

a) Industry averages
b) Tape restore statistics
c) Business impact analysis
d) Previous recovery test results

(28) In providing risk reporting to management, the most appropriate vehicle for the initial reporting of a major security incident would be to include it in a:

a) Quarterly report
b) Special report
c) Monthly report
d) Weekly report

(29) To determine if a threat poses a risk, the risk management team must determine the impact and

a) Vulnerability
b) Probability
c) Identification
d) Reason

(30) To accept the potential risk and continue operating or to implement controls to lower the risk to an acceptable level is termed:

a) Risk assumption b) Risk avoidance
c) Risk sharing d) Risk management

(31) Two forms of risk assessment are:

a) Analytical and assessment b) Technical and procedural
c) Qualitative and quantitative d) Subjective and objective

(32) The process used to demonstrate that the costs of implementing controls can be justified by the reduction of a risk level is:

a) Probability and impact b) Vulnerability assessment
c) Compliance checking d) Cost benefit

(33) The process for determining the acceptable level of impact on organization applications, systems, and business processes is called:

a) Risk analysis b) Risk assessment
c) Business impact analysis d) Project impact analysis

(34) Three basic threat categories include human, natural, and what additional category?

a) Possible b) Probable
c) Engineering d) Environmental

(35) The potential for a particular event to successfully exercise a particular vulnerability is called:

a) Threat b) Risk
c) Impact d) Probability

(36) Another term for project impact analysis is:

a) Risk assessment b) Cost benefit
c) Security management d) Risk analysis

(37) Risk management encompasses three processes: risk assessment, risk mitigation, and what other element?

a) System development life cycle b) Risk analysis
c) Evaluation and assessment d) Threat analysis

(38) Effective risk management must be totally integrated into what process?

a) IPL b) SDLC
c) Security perimeter d) Disposal

(39) Senior management depends on an effective risk analysis process to make informed business decisions. This management responsibility is called:

a) Due diligence b) Due proxy
c) Due date d) DEW line

(40) What is the first process in the risk management methodology?

a) Records retention b) Likelihood
c) Fault tolerance d) Risk analysis

(41) The results of the likelihood that a given threat-source were to be used is termed:

a) Vulnerability b) Risk
c) Control d) Probability

(42) There are three basic forms of threat-sources. These are human threats, environmental threats, and what other kind of threat?

a) Tangible b) Intangible
c) Terror d) Natural

(43) A flaw or weakness in system security procedures, design, implementation, or internal controls that could be exercised and result in a security breach or violation of the system’s security policy is called:

a) Vulnerability
b) Typical
c) Virus
d) Logic bomb

(44) Two major types of risk analysis are:

a) Threat and controls
b) Errors and omissions
c) Quantitative and qualitative
d) Vulnerability and management

(45) A systematic methodology used by senior management to reduce mission risk is termed:

a) Risk transfer
b) Risk limitation
c) Accepting the risk
d) Risk mitigation

(46) To convey a risk by using other options to compensate for loss, such as purchasing insurance, is referred to as:

a) Risk transfer
b) Risk assumption
c) Risk planning
d) Risk limitation

(47) To check a risk by implementing controls that minimize the adverse impact of the threat’s exercising a vulnerability (such as use of supporting, preventive, detective controls) is referred to as:

a) Risk transfer
b) Risk assumption
c) Risk planning
d) Risk limitation

(48) The types of controls focused on stopping a security breach from occurring in the first place are termed:

a) Containment
b) Preventive
c) Detection
d) Recovery

(49) An audit log is an example of what type of control?

a) Containment
b) Preventive
c) Detection
d) Recovery

(50) To allocate resources and implement cost-effective controls, organizations, after identifying all possible controls and evaluating their feasibility and effectiveness, should perform what form of additional analysis?

a) Vulnerability analysis
b) Cost-benefit analysis
c) Qualitative
d) Quantitative

(51) Which of the following is not a responsibility of the data or systems owner?

a) To identify, describe, and designate the sensitivity of their applications systems
b) To ensure that appropriate security control requirements are included in specifications
c) To assess security requirements by evaluating application assets, threats, and vulnerabilities
d) To develop industry best practices

(52) Which of the following attacks would compromise the integrity of system information?

a) Denial-of-service
b) Smurf
c) SQL Injection
d) Fraggle

(53) Which of the following is not an example of the platform component of information technology infrastructure?

a) Switch security b) Operating system security

c) Application security d) Anti-virus

(54) Which of the following is an example of the network component of information technology infrastructure?

a) Switch security b) Operating system security

c) Application security d) Anti-virus

(55) When implementing a security control, an information security manager needs to be especially aware of:

a) Change control management b) What the organization's competition is doing

c) A promotion to production procedure d) The impact on the end-user community

(56) Which of the following is an advantage of an open system?

a) End-user support. b) The source code can be verified.

c) Difficulty in management. d) All users are always permitted to access the system.

(57) What would be a disadvantage of deploying a proxy-based firewall?

a) Proxy-based firewalls may not support custom applications. b) Proxy-based firewalls inspect to only the network layer of the OSI model.

c) Proxy-based firewalls cannot block unwanted traffic. d) Proxy-based firewalls do not provide network address translation.

(58) Which of the following is true of a stateful inspection firewall?

a) Stateful inspection firewalls protect through all layers of the OSI model. b) Stateful inspection firewalls support more custom applications than other firewalls.

c) Stateful inspection firewalls are faster then other firewalls. d) Stateful inspection firewalls do not provide network address translation.

(59) Which of the following would be an advantage to deploying public key (asymmetric) as opposed to private key (symmetric) encryption technologies?

a) Public key is more scalable. b) Public key encryption is faster.

c) Public key requires less infrastructure. d) Private key is easier on the end-user community.

(60) What term is best defined as a model used to determine the security and functionality of a proposed project?

a) Prototype b) Checkpoint

c) Journaling d) Service level agreement