CISSE ADVANCED LEVEL

ELECTIVE II

INFORMATION SYSTEMS SECURITY

TUESDAY: 19 August 2025. Afternoon Paper. **Time Allowed: 2 hours.**

This paper consists of fifty (50) Multiple Choice Questions. Answer ALL questions by indicating the letter (A, B, C or D) that represents the correct answer. Each question is allocated two (2) marks.

1. A healthcare worker mistakenly forwards patient medical records to an unauthorised third-party email account. Which one of the following types of threats does this scenario represent?
   A. Loss of data availability
   B. Accidental insider threat
   C. Infection by malicious software
   D. Breach of data confidentiality (2 marks)

2. A hacker was able to insert harmful SQL code into a company's web application because it failed to check user input. Which one of the following types of vulnerability does this scenario illustrate?
   A. Buffer overflow
   B. Injection flaw
   C. Weak authentication
   D. Phishing (2 marks)

3. A company runs the risk of social engineering attacks when it fails to educate employees on recognising phishing emails. This security gap violates the organisational requirement of _____.
   A. security awareness training
   B. employee productivity metrics
   C. data encryption standards
   D. incident response protocol (2 marks)

4. Brute-force attacks cannot be detected by an organisation if it does not keep track of the quantity of unsuccessful login attempts across all of its systems. This oversight is a failure to track which key IS security metric?
   A. System uptime
   B. Antivirus update frequency
   C. Account lockout metrics
   D. Number of active users (2 marks)

5. An audit failure occurred due to the organisation's inability to implement security controls aligned with best practices for ensuring confidentiality, integrity and availability (CIA). Which one of the following frameworks was **NOT** adhered to?
A. PRINCE2
B. ISO/IEC 27001
C. Agile Manifesto
D. PMP (2 marks)

6. A financial services company was fined for failing to disclose a customer financial records data breach within the required time frame. This is a violation of which of the following regulations?
A. Payment Card Industry Data Security Standard (PCI DSS)
B. General Data Protection Regulation (GDPR)
C. Health Insurance Portability and Accountability Act (HIPAA)
D. Gramm-Leach-Bliley Act (GLBA) (2 marks)

7. An enterprise is implementing a Data Loss Prevention (DLP) strategy to proactively detect and mitigate the exposure of sensitive information across its systems. Considering both accuracy and scalability, which one of the following techniques offers the **MOST** comprehensive approach for identifying sensitive data in diverse and dynamic environments?
A. Utilising random sampling of data repositories
B. Employing rule-based signature detection techniques
C. Implementing fingerprinting with deep content inspection
D. Initiating basic connectivity tests through network pings (2 marks)

8. A breach occurred at a nearby institution of higher learning when staff members violated the institution's information security policy by exchanging passwords over private messaging applications. Which one of the following governance principles was **NOT** enforced?
A. Policy enforcement and compliance
B. Accountability and responsibility
C. Least privilege access
D. Confidentiality classification (2 marks)

9. A telecommunications corporation's data center detected unusual network traffic outside regular business hours, leading to unauthorised access attempts targeting subscriber records. Which one of the following intrusion detection systems (IDS) functionalities led to alerting the security team?
A. Signature-based detection
B. Anomaly-based detection
C. Packet filtering
D. Encryption enforcement (2 marks)

10. Which one of the following techniques is used to test the integrity of transaction processing systems?
A. Penetration testing
B. Parallel simulation
C. Patch management
D. Configuration review (2 marks)

11. After a ransomware attack encrypted farmers' records at a Tea Factory, the IT department is tasked with recovery. To resume operations with minimal data loss, which one of the following strategies is **MOST** effective?
    A. Reinstalling the operating system and starting from scratch
    B. Paying the ransom to the attackers
    C. Relying on endpoint antivirus quarantine
    D. Restoring from a recent verified offline backup (2 marks)

12. A multinational financial firm observes a significant increase in outbound email traffic from its customer service department, particularly during non-working hours. The emails often include large attachments containing structured data. Which Data Loss Prevention (DLP) control would **BEST** help detect and prevent potential data exfiltration in this scenario?
    A. Configure Email DLP policies to inspect and block sensitive data patterns in outbound attachments
    B. Implement a DLP policy that blocks all outbound emails with attachments during non-business hours
    C. Use Endpoint DLP to monitor clipboard, USB and file transfer activity on employee devices
    D. Deploy a firewall rule to block all outbound traffic from the customer service department during non-working hours (2 marks)

13. Which one of the following core data protection principles is violated when a business provides third-party vendors access to users' personal data without obtaining prior user consent?
    A. Use data only for specified purposes
    B. Be lawful, fair and transparent
    C. Ensure all data remains accurate
    D. Collect only data needed for processing (2 marks)

14. Which one of the following controls is an example of a preventive control in business continuity plan (BCP)?
    A. Restoring systems from backup
    B. Using a generator for power backup
    C. Installing antivirus software
    D. Running a recovery test (2 marks)

15. A newly formed organisation intends to contract with a third-party provider to handle some IT activities as it grows. What management control should be enforced to ensure data integrity and accountability?
    A. Implement secure encryption for all outgoing and incoming data
    B. Establish clear service-level agreements with reporting clauses
    C. Conduct regular internal audits with defined compliance metrics
    D. Enforce access controls with regular privilege reviews (2 marks)

16. An organisation is implementing remote access for staff members as part of its workforce expansion. Which one of the following operational controls should be implemented to ensure secure access?
    A. Use data loss prevention software across the network
    B. Mandate cybersecurity awareness training for all employees
    C. Provide VPN access with multi-factor authentication
    D. Implement firewalls with intrusion prevention systems (2 marks)

17. ABC Ltd. experienced a ransomware attack that encrypted client records, prompting the IT staff to create a disaster recovery plan. How does identifying critical IS assets support this effort?
A. It prioritises restoring key systems to resume operations fast
B. It supports HR by aligning recruitment with essential IT roles
C. It enhances report visuals but doesn't aid recovery efforts
D. It limits reliance on vendors but doesn't address system recovery (2 marks)

18. XYZ dry Cleaners wants to automate system scans and patch updates to minimise malware threats across its network. Which one of the following technical controls would **BEST** meet this need?
A. Increase physical security staffing at the server room facility
B. Deploy automated endpoint protection and system update solutions
C. Enforce a standardised clean desk procedure across departments
D. Organise regular cybersecurity training sessions for employees (2 marks)

19. SkyMed Solutions Ltd plans to enforce strong password practices to mitigate the risk of unauthorised access to sensitive employee and customer information. Which one of the following policies would **MOST** effectively support this objective?
A. Enforce screen locking automatically after user inactivity
B. Restrict usage of USB storage on office computers
C. Enforce password changes every 90 days with rules
D. Require mandatory use of multi-factor authentication (2 marks)

20. The Beba Fashion design company plans to expand into new business areas and wants to ensure its security practices consistently align with its evolving business objectives. Which strategic approach should the organisation adopt?
A. Implement network segmentation
B. Use firewall rulesets
C. A risk management framework
D. Perform vulnerability scans (2 marks)

21. Following a recent audit, SDS Inc. was advised to enhance its incident response readiness. The security role primarily responsible for developing and coordinating the company's incident response plan is referred to as the _____.
A. chief information security officer
B. incident response coordinator
C. incident responder
D. security analyst (2 marks)

22. Which one of the following tools would be **MOST** appropriate for conducting a vulnerability assessment on a cloud-based application?
A. Visual Studio Code
B. Postman
C. Nessus
D. Wireshark (2 marks)

23. Kijivu Night Guards Ltd is updating its information systems security policy to include incident response procedures. Which one of the following elements should be included in the updated policy?
A. A monthly financial audit schedule
B. A detailed software inventory for all endpoint devices
C. A list of all company employees and their contact information
D. Clearly defined roles and responsibilities for incident response (2 marks)

24. A local auto dealer wants to test web application security prior to launching its digital banking platform. Which penetration testing tool would be appropriate for identifying common web application vulnerabilities like SQL injection and XSS?
A. Burp Suite
B. Wireshark
C. TCPdump
D. Nmap (2 marks)

25. The Criminal Investigative Department (CID) must present the results of a forensic investigation in a format that is legally admissible. The professional responsible for compiling and presenting these findings in accordance with legal standards is _____.
A. systems analyst
B. digital evidence examiner
C. forensic accountant
D. network system administrator (2 marks)

26. An online payment platform is integrating third-party APIs into its transaction platform and wants to ensure security risks are minimised during architectural planning. Which one of the following methodologies is used to identify trust boundaries and threat surfaces during architectural risk analysis?
A. Agile
B. Blue Teaming
C. Red Teaming
D. STRIDE (2 marks)

27. A digital payment platform must ensure that transaction data is not altered by unauthorised parties during transmission. Which core security principle is being addressed in this scenario?
A. Confidentiality
B. Non-repudiation
C. Integrity
D. Availability (2 marks)

28. The Bring Your Own Device (BYOD) policy is being implemented by a global shipping organisation in an effort to increase employee flexibility. In order to promote accountability and secure usage behaviors that align with the organisation's security goals, which organisational element is essential?
A. Acceptable Use Policy (AUP)
B. Mobile Device Management (MDM)
C. Endpoint Detection and Response (EDR)
D. Role-Based Access Control (RBAC) (2 marks)

29. A Security Information and Event Management (SIEM) system is put into place by a technology company. The primary objective of integrating such a tool into the incident management process is to_____.

A. automatically block all types of security threats in real-time
B. centralise the detection analysis and response to incidents
C. eliminate the need for a dedicated incident response team
D. improve routine system maintenance and software updates (2 marks)

30. A manufacturing company conducts a Business Impact Analysis (BIA) to classify its processes based on their criticality. The primary purpose of assigning impact levels to business functions during the BIA is to _____.

A. identify redundant employees in each department
B. determine the business functions that are responsible for non-compliance
C. evaluate employee performance and align it with business goals
D. prioritise recovery actions and allocate resources during disruption (2 marks)

31. A bank's Security Operations Center (SOC) team has detected unauthorised access attempts and now seeks to assess internal response mechanisms through adversary simulation. Which penetration testing framework **BEST** supports realistic attack emulation and red teaming in such scenarios?

A. OWASP Testing Guide
B. PTES
C. MITRE ATT&CK Framework
D. NIST SP 800-115 (2 marks)

32. A data center determines the Recovery Time Objective (RTO) and Recovery Point Objective (RPO) for essential systems. Which one of the following statements **BEST** explains the significance of RTO and RPO in a Business Continuity Plan (BCP)?

A. They define security protocols used to prevent unauthorised data access
B. They establish how frequently backup data should be tested and verified
C. They identify acceptable limits for downtime and data loss in a disaster
D. They ensure that systems comply with all data storage regulations (2 marks)

33. A startup company is expanding rapidly and hires new staff every month. To align new hiring's with the organisation's information security objectives, which one of the following cultural norms should be emphasised during onboarding?

A. Prioritise rapid project delivery over enforcing security protocols
B. Foster accountability, confidentiality and routine incident reporting
C. Encourage team-based trust through shared credentials and open platforms
D. Promote independent decision-making and broad access to internal systems (2 marks)

34. A system auditor is conducting parallel testing as part of disaster recovery plan evaluation. The main objective of this test is to_____.

A. verify operations at the recovery site while the main system is still running
B. measure staff readiness when responding to simulated emergency drills
C. confirm that data backups are working and can be restored if needed
D. simulate a full-scale outage at the main data center environment (2 marks)

35. Your immediate supervisor has asked you to look through system logs for signs of brute-force login attempts. Which auditing technique from the list below **BEST** achieves this objective?
A. Track administrative privilege escalations
B. Audit successful remote desktop connections
C. Record file permission changes
D. Monitor and log failed login attempts over time (2 marks)

36. Your company has detected a zero-day vulnerability affecting the email server. Which immediate action should be prioritised to mitigate the risk of exploitation?
A. Reboot the server to stop possible active threats
B. Isolate the server and apply temporary mitigation
C. Notify users and advise against using the server
D. Wait for the vendor patch and apply it when available (2 marks)

37. A network analyst identified an outdated firewall with a known vulnerability being actively exploited. What risk management step would you advise him to take to ensure system integrity?
A. Accept the risk and monitor the firewall for future updates
B. Conduct a routine risk assessment and report findings in the next review meeting
C. Document the incident and defer action until the quarterly maintenance cycle
D. Immediately patch or replace the vulnerable firewall and implement compensating controls (2 marks)

38. An online store has adopted a new incident management plan. To ensure its successful implementation, what specific cultural values and practices should the organisation foster among its employees?
A. Strict hierarchical decision-making and limiting information to management only
B. Encouraging transparency, accountability and a culture of continuous learning
C. Relying solely on the IT department to manage and respond to incidents
D. Emphasing punishment for mistakes to deter future incidents (2 marks)

39. A security engineer has detected multiple failed login attempts targeting a privileged account from a foreign IP address. Which one of the following should be the immediate steps in the incident response process?
A. Notify senior management and legal counsel about the attack
B. Wait for additional login attempts to confirm the pattern then report
C. Isolate the affected account and block the suspicious IP address
D. Conduct a full forensic investigation before taking any action (2 marks)

40. Miss Wendy, a new employee in the finance division, has permissions to edit Human Resource (HR) records and access financial applications. The area of Information Systems (IS) security concerned with addressing such an issue is called _____.
A. access control
B. cryptography
C. network security
D. data backup (2 marks)

41. A dissatisfied former employee removes critical research data from the company's servers shortly before their account is terminated. This incident is an example of _____.
A. social engineering attack
B. insider threat
C. denial of service attack
D. physical security breach (2 marks)

42. There is a significant danger of unauthorised access when sensitive client data is stored without encryption. This practice is a breach of data protection principle known as _____.
A. data minimisation
B. accuracy and integrity
C. storage limitation
D. integrity and confidentiality (2 marks)

43. ABC Bank put in place an intrusion detection system that does more than just report suspicious activity, it actively blocks it in real time. Which of the following **BEST** describes the system in use?
A. Network-Based Intrusion Detection System (NIDS)
B. Host-Based Intrusion Detection System (HIDS)
C. Intrusion Prevention System (IPS)
D. Security Information and Event Management (SIEM) (2 marks)

44. A pharmaceutical company experienced a data breach caused by malware that used lateral movement to infect multiple devices across the internal network. Which one of the following measures would **BEST** minimise the impact of such an attack?
A. Deploying network segmentation and internal firewalls
B. Implementing strong password policies for all users
C. Regularly updating the company website with security certificates
D. Using a VPN for remote access (2 marks)

45. After applying a patch, a configuration file becomes corrupted, causing a vital application to crash at a Meteorological Agency lab. To ensure the fastest possible restoration of service, which recovery strategy should be used?
A. Rewriting the application from scratch
B. Disabling further patch installations permanently
C. Continuing operation with corrupted configurations
D. Rolling back the patch using snapshot-based restore (2 marks)

46. Jitume Enterprises has deployed new servers and wants to reduce configuration errors in future deployments. Which operational control should the organisation implement to achieve this goal?
A. Implement a standardised configuration management process for all future deployments
B. Set up a physical access control system to secure the server rooms from intruders
C. Develop an employee training program focused on general security awareness topics
D. Introduce stronger password policies for users accessing the new deployed servers (2 marks)

47. Insider threats and data leaks are concerns for a government service delivery unit. Which one of the following administrative controls would help reduce this risk?
A. Encrypt all files stored on external hard drives
B. Establish a role-based access control (RBAC) policy
C. Install motion detectors in the server room
D. Set BIOS passwords on all company laptops (2 marks)

48. A five-star hotel has observed inconsistent security standard implementation across departments. To address this, what type of centralised governance structure should the hotel establish to ensure uniformity and accountability in its security program?
A. Incident response plan
B. Role-based access control
C. Centralised IT security team
D. Decentralised firewall configuration (2 marks)

49. Assuming an organisation does a vulnerability assessment, the team in charge of interpreting the data and proposing concrete remediation measures to executive leadership is known as the _____.
A. risk management team
B. incident response team
C. vulnerability assessment team
D. executive steering committee (2 marks)

50. Sensitive citizen data is being processed through a government portal. The technique used to protect the confidentiality of application logic and hinder reverse engineering of the code is known as _____.
A. encryption
B. code obfuscation
C. access control
D. two-factor authentication (2 marks)

.....

CISSE ADVANCED LEVEL

ELECTIVE II

INFORMATION SYSTEMS SECURITY

WEDNESDAY: 23 April 2025. Afternoon Paper. **Time Allowed: 2 hours.**

This paper consists of fifty (50) Multiple Choice Questions. Answer ALL questions by indicating the letter (A, B, C or D) that represents the correct answer. Each question is allocated two (2) marks.

1. Which one of the following statements explains the relationship between threats, vulnerabilities and risks?
   A. Risks arise when vulnerabilities are exploited by threats
   B. Threats eliminate risks by exposing vulnerabilities
   C. Vulnerabilities mitigate risks caused by threats
   D. Threats and vulnerabilities are independent of risks (2 marks)

   ANSWER: A

2. The purpose of a threat model in cybersecurity is to _____.
   A. identify vulnerabilities in a system
   B. create a backup plan for natural disasters
   C. categorise and prioritise potential threats
   D. eliminate all risks from a system (2 marks)

   ANSWER: C

3. The primary purpose of risk assessment is to _____.
   A. remove all threats from a system
   B. prioritise risks and allocate resources for mitigation
   C. ensure all vulnerabilities are eliminated
   D. identify potential legal issues (2 marks)

   ANSWER: B

4. Which one of the following statements **BEST** exemplifies how management controls can support the effectiveness of other security controls?
   A. Implementing a strong firewall to block unauthorised network traffic
   B. Conducting regular security awareness training for employees
   C. Encrypting sensitive data both at rest and in transit
   D. Implementing a system for intrusion detection and prevention (2 marks)

   ANSWER: B

5. Which one of the following statements **BEST** describes the relationship between information systems (IS) security standards and regulations?
   A. Standards are legally binding, while regulations are voluntary guidelines
   B. Regulations are legally binding, while standards are voluntary guidelines
   C. Standards and regulations are both legally binding.
   D. Standards and regulations have no legal implications (2 marks)

   ANSWER: B

6. The first step in asset classification is _____.
   A. assigning access permissions
   B. determining asset ownership
   C. identifying all organisational assets
   D. applying encryption to data (2 marks)

   ANSWER: C

7. Which one of the following terminologies refers to the classification level for highly sensitive information that, if disclosed, could cause severe harm to an organisation?
   A. Public
   B. Internal
   C. Confidential
   D. Restricted (2 marks)

   ANSWER: D

8. Which one of the following statements refers to a key component of information security governance?
   A. Monitoring information technology (IT) support tickets
   B. Developing a security policy framework
   C. Installing antivirus software
   D. Reducing the number of network device (2 marks)

   ANSWER: B

9. The persons who are responsible for establishing information security governance in an organisation are _____.
   A. information technology (IT) support staff
   B. security analysts
   C. executive leadership and the board of directors
   D. end users (2 marks)

   ANSWER: C

10. Which one of the following statements explains the relationship between information security governance and information technology (IT) governance?
   A. They are unrelated processes
   B. Information security governance is a subset of IT governance
   C. IT governance is a subset of information security governance
   D. Both are entirely independent functions (2 marks)

   ANSWER: B

11. Which one of the following statements is key principle of information security governance?
   A. Focuses only on technical solutions
   B. Integration of security into business processes
   C. Minimise security spending
   D. Ignores regulatory compliance (2 marks)

   ANSWER: B

12. Which one of the following frameworks is the leading and widely recognised for information security governance?
   A. COBIT
   B. ITIL
   C. ISO/IEC 27001
   D. PMI-PMP (2 marks)

   ANSWER: A

13. The term "risk appetite" in the context of security governance refers to the _____.
    A. desire of an organisation to avoid all risks
    B. level of risk an organisation is willing to accept
    C. total number of vulnerabilities in a system
    D. amount of money spent on security solutions (2 marks)

    ANSWER: B

14. Which one of the following statements is **NOT** a key element of security governance?
    A. Strategic alignment
    B. Risk management
    C. Resource optimisation
    D. Threat exploitation (2 marks)

    ANSWER: D

15. Which one of the following statements is a critical success factor for effective information security governance?
    A. Sole focus on technical controls
    B. Strong leadership support and engagement
    C. Avoiding investment in employee training
    D. Ignoring user access policies (2 marks)

    ANSWER: B

16. The common step in the recovery process after a system failure involves _____.
    A. conducting a post-incident review
    B. ignoring backup data
    C. disabling all system alerts
    D. avoiding root cause analysis (2 marks)

    ANSWER: A

17. In reference to disaster recovery, the term, RTO (Recovery Time Objective) refers to the _____.
    A. maximum amount of data loss acceptable
    B. target duration to restore normal operations after a failure
    C. total cost of implementing recovery measures
    D. maximum allowable downtime for maintenance (2 marks)

    ANSWER: B

18. Which one of the following statements is an example of a failure recovery strategy?
    A. Regular system updates
    B. Increasing network bandwidth
    C. Optimising server speed
    D. Backing up critical data (2 marks)

    ANSWER: D

19. Which one of the following terms is an example of a local law or regulation related to data protection in Kenya?
    A. Data Protection Act 2019
    B. General Data Protection Regulation (GDPR)
    C. California Consumer Privacy Act (CCPA)
    D. Federal Information Security Management Act (FISMA) (2 marks)

    ANSWER: A

20. The type of backup that involves copying only data that has changed since the last backup is known as _____.
    A. incremental backup
    B. full backup
    C. differential backup
    D. continuous backup (2 marks)

    ANSWER: A

21. Which one of the following **BEST** demonstrates a strong alignment between information security (IS) security and organisational strategy?
    A. Implementing the latest firewalls and intrusion detection systems
    B. Mandating the use of strong passwords for all employees
    C. Conducting regular security audits and vulnerability assessments
    D. Developing an IS security strategy that directly supports the organisation's business objectives and risk tolerance (2 marks)

    ANSWER: D

22. In disaster recovery planning, the term "cold site" refers to a _____.
    A. fully operational duplicate system
    B. site with basic infrastructure but no active systems
    C. cloud-based backup storage solution
    D. temporary location for IT support (2 marks)

    ANSWER: B

23. Which one of the following statements is **NOT** a best practice for failure recovery?
    A. Keeping detailed documentation of recovery processes
    B. Regularly testing recovery plans
    C. Training employees on disaster recovery protocols
    D. Relying solely on a single backup system (2 marks)

    ANSWER: D

24. Which one of the following statements is an advantage of cloud-based disaster recovery solutions?
    A. Scalability and remote accessibility
    B. High initial hardware costs
    C. Increased on-premises infrastructure
    D. Limited storage capacity (2 marks)

    ANSWER: A

25. A common type of data protection solution is _____.
    A. Endpoint Security
    B. Virtual Private Network (VPN)
    C. Load Balancer
    D. Firewall (2 marks)

    ANSWER: A

26. In Data Loss Prevention (DLP) the term ‘data in motion’ refers to _____.
    A. Data stored in the cloud
    B. Data being actively transmitted across networks
    C. Data saved on physical drives
    D. Archived data (2 marks)

    ANSWER: B

27. Which one of the following statements is **NOT** a feature of a Data Loss Prevention (DLP) solution?
    A. Data encryption
    B. Data classification
    C. Content filtering
    D. Intrusion detection (2 marks)

    ANSWER: D

28. The key principle of data privacy is data _____.
    A. redundancy
    B. minimisation
    C. centralisation
    D. proliferation (2 marks)

ANSWER: B

29. Which one of the following statements is a primary goal of "Recovery from Failure" in the context of network and computer security?
    A. Preventing unauthorised access to systems and data
    B. Detecting and responding to malicious network activity
    C. Ensuring the availability of critical systems and data after a disruption
    D. Implementing strong passwords and access controls (2 marks)

ANSWER: C

30. Which one of the following explanations is an example of a technical security control?
    A. Encryption
    B. Employee training
    C. Security policies
    D. Physical locks (2 marks)

ANSWER: A

31. Which one of the following statements is **NOT** an example of a preventive control?
    A. Firewalls
    B. Data encryption
    C. Incident response plans
    D. Multi-factor authentication (2 marks)

ANSWER: C

32. Which one of the following statements explains how operational controls differ from technological controls in the context of information systems (IS) security?
    A. Operational controls focus on hardware and software solutions while technological controls focus on human behaviour
    B. Operational controls focus on human behavior and procedures while technological controls focus on hardware and software solutions
    C. Operational controls are only relevant for small businesses while technological controls are necessary for all organisations
    D. Operational controls are more expensive to implement than technological controls (2 marks)

ANSWER: B

33. In information security, the term "compensating control" refers to a _____.
    A. primary control mechanism
    B. backup control used when primary controls are not feasible
    C. control that increases the speed of incident response
    D. control focused on detecting intrusions (2 marks)

ANSWER: B

34. The primary purpose of an organisational security policy is to _____.
    A. monitor employee productivity
    B. ensure compliance with legal and regulatory requirements
    C. outline rules and guidelines for protecting organisational assets
    D. enforce penalties for security breaches (2 marks)

ANSWER: C

35. Which one of the following statements explains the meaning of the abbreviation, BYOD (Bring Your Own Device) policy?
A. Guidelines for employees using personal devices for work
B. Policies for purchasing company-owned devices
C. Rules for connecting company devices to personal networks
D. Regulations for disposing of outdated devices (2 marks)

ANSWER: A

36. Which one of the following tools is primarily used for network scanning and vulnerability assessment during penetration testing?
A. Metasploit
B. Wireshark
C. Nmap
D. Burp Suite (2 marks)

ANSWER: C

37. The **MAIN** purpose of the Metasploit framework is to _____.
A. analyse network traffic
B. automate and execute exploits against vulnerable systems
C. collect and organise penetration testing reports
D. scan systems for open ports (2 marks)

ANSWER: B

38. Which one of the following tools is **BEST** known for capturing and analysing network packets in penetration testing?
A. Burp Suite
B. Nessus
C. Wireshark
D. John the Ripper (2 marks)

ANSWER: C

39. Effective evaluation of organisational information security (IS) security could contribute to overall business success by _____.
A. increasing IT spending to enhance security measures
B. identifying and mitigating risks that could disrupt business operations
C. ensuring that all employees are aware of the latest security threats
D. implementing the most technologically advanced security solutions (2 marks)

ANSWER: B

40. Which one of the following statements explains the function of the Kali Linux operating system in penetration testing?
A. It is used for web application testing only
B. It is a security-focused Linux distribution with pre-installed penetration testing tools
C. It is used exclusively for wireless network analysis
D. It is a framework for creating malware (2 marks)

ANSWER: B

41. The primary objective of embedding an information security culture within an organisation is to _____.
A. ensure regulatory compliance
B. increase employee awareness about data breaches
C. foster a proactive approach to managing information security risks
D. reduce operational costs (2 marks)

ANSWER: C

42. Which one of the following statements explains why top management support is crucial for embedding an information security culture?
A. They can allocate funds for security software
B. They can enforce strict security measures across the organisation
C. Their commitment sets an example and drives organisation-wide participation
D. They are the only ones who need to understand security policies (2 marks)

ANSWER: C

43. Which one of the following statements explains how organisations can measure the effectiveness of their information security culture?
A. Conducting random security audits and reviewing incident reports
B. Relying on employee complaints about security issues
C. Asking only top management to evaluate the culture
D. Ignoring employee feedback and focusing on technology updates (2 marks)

ANSWER: A

44. Which one of the following statements is key challenge when embedding an information security culture in an organisation?
A. Ensuring top-down communication about security policies
B. Securing budget for cybersecurity tools
C. Increasing the size of the IT security team
D. Overcoming resistance to change and security policies among employees (2 marks)

ANSWER: D

45. Organisations can handle resistance to security changes among employees by _____.
A. implementing strict penalties for non-compliance
B. offering clear communication, training and support for adopting changes
C. eliminating security changes altogether
D. only focusing on security compliance and ignoring employee input (2 marks)

ANSWER: B

46. Which one of the following statements explains the difference between a Business Continuity Plan (BCP) and a Disaster Recovery Plan (DRP)?
A. A DRP focuses only on IT systems, while BCP covers broader business operations
B. A BCP only involves staff communication, while DRP covers hardware recovery
C. A DRP is less important than a BCP
D. A DRP covers staff evacuation plans, while BCP handles communication with customers (2 marks)

ANSWER: A

47. Which one of the following statements is a key consideration when identifying critical information security (IS) assets for data protection?
A. Hardware specifications
B. Business impact:
C. User accessibility
D. Software version (2 marks)

ANSWER: B

48. The information system (IS) audit tool that can be used to perform a penetration test on a web application to identify security flaws is known as _____.
A. Kali Linux
B. QuickBooks Audit
C. Splunk
D. Microsoft Excel (2 marks)

ANSWER: A

49. Which one of the following information system (IS) audit tools can be used for encryption and decryption testing during an audit?
A. Nessus
B. OpenSSL
C. NetFlow
D. Nmap (2 marks)

ANSWER: B

50. The role of forensic audit tools in an information system (IS) audit is to _____.
A. monitor employee behavior and performance
B. recover and analyse data related to security incidents or breaches
C. evaluate the speed and efficiency of IT systems
D. manage IT budgets and costs (2 marks)

ANSWER: B

.....

CISSE ADVANCED LEVEL

ELECTIVE II

INFORMATION SYSTEMS SECURITY

TUESDAY: 20 August 2024. Afternoon Paper. **Time Allowed: 2 hours.**

This paper consists of fifty (50) Multiple Choice Questions. Answer ALL questions by indicating the letter (A, B, C or D) that represents the correct answer. Each question is allocated two (2) marks.

1. Information that could seriously harm a firm if it were released without permission is categorised as _____.
   A. internal
   B. public
   C. secret
   D. confidential (2 marks)

2. What is the primary purpose of information security metrics?
   A. To increase the complexity of security systems
   B. To measure the effectiveness of security policies and controls
   C. To track information security incidents
   D. To reduce the budget allocated for information security (2 marks)

3. The average length required to recover from a security breach is referred to as _____.
   A. mean time to recovery
   B. vulnerability scan results
   C. incident response time
   D. security awareness training participation (2 marks)

4. In the context of information security metrics, what does “Number of detected incidents” indicate?
   A. The effectiveness of security awareness training
   B. The number of unauthorised access attempts
   C. The total number of security incidents detected over a specific period
   D. The time taken to respond to security incidents (2 marks)

5. What type of vulnerability is caused by improper input validation in software?
   A. Physical vulnerability
   B. Human vulnerability
   C. Network vulnerability
   D. Application vulnerability (2 marks)

6. What is the primary purpose of a Distributed Denial of Service (DDoS) attack?
   A. To gain unauthorised access to sensitive data
   B. To encrypt data and demand a ransom
   C. To disrupt the availability of services
   D. To install spyware on a victim’s computer (2 marks)

7. What does a high “false positive rate” in security monitoring indicate?
   A. Many security incidents are detected accurately
   B. Legitimate actions are incorrectly flagged as security incidents
   C. Few security incidents are detected
   D. All security incidents are ignored (2 marks)

8. Information security governance guarantees that an organisation's information security strategy and objectives are consistent with its business goals and regulatory obligations. Which one of the following is an essential part of information security governance?
   A. Policy development and enforcement
   B. Network topology design
   C. Marketing strategy
   D. Software development lifecycle (2 marks)

9. Information security (IS) entails putting safeguards in place to protect information's confidentiality, integrity and availability from unauthorised access, disclosure, disruption, alteration or destruction. What is the primary objective of risk management in IS security?
   A. Reducing employee headcount
   B. Mitigating risks to information assets
   C. Enhancing public relations
   D. Maximising profits (2 marks)

10. Which one of the following is a key component of information security governance?
   A. Implementing firewall rules
   B. Conducting regular vulnerability scans
   C. Establishing a security policy framework
   D. Monitoring network traffic (2 marks)

11. Who is typically responsible for overseeing information security governance within an organisation?
   A. Network administrator
   B. Chief Information Security Officer (CISO)
   C. Database administrator
   D. Marketing manager (2 marks)

12. Which one of the following is a standard that provides a framework for establishing, implementing, maintaining and continually improving an information security management system (ISMS)?
   A. PCI DSS
   B. GDPR
   C. HIPAA
   D. ISO/IEC 27001 (2 marks)

13. Which type of Intrusion Detection System (IDS) monitors events in real time, identifying suspicious activity and sounding an alarm?
   A. Anomaly-based IDS
   B. Signature-based IDS
   C. Host-based IDS
   D. Network-based IDS (2 marks)

14. Why is it important to regularly review and update information security policies?
   A. To reduce the need for employee training
   B. Align with current business practices
   C. To increase the complexity of the policies
   D. To submit to the regulator (2 marks)

15. What is Disaster Recovery Planning (DRP) primarily intended to achieve?
   A. Identifying unauthorised access
   B. Monitoring network traffic
   C. Ensuring business functions continue during a disaster
   D. Recovering systems and data after significant disruptions (2 marks)

16. Which framework emphasises a risk-based approach to managing information security?
   A. COBIT
   B. NIST Cybersecurity Framework
   C. Six Sigma
   D. PRINCE2 (2 marks)

17. Which one of the following **BEST** defines the process of determining an organisation's important assets?
    A. Implementing a new payroll system
    B. Developing a customer feedback survey
    C. Conducting a marketing campaign to promote new products
    D. Categorising data based on its importance to the organisation (2 marks)

18. What does the NIST Cybersecurity Framework provide?
    A. A methodology for software testing
    B. Guidelines for improving critical infrastructure in cybersecurity
    C. A process for managing project timelines
    D. Techniques for optimising supply chain operations (2 marks)

19. What is a critical component of an organisation's data privacy strategy?
    A. Reducing the number of employees in the IT department
    B. Increasing the number of physical security guards
    C. Installing the latest video conferencing software
    D. Implementing security measures to protect against unauthorised access (2 marks)

20. In the context of information security, what is the main purpose of risk assessment?
    A. To create a firewall
    B. To install antivirus software
    C. Evaluate risks to information assets
    D. To back up data (2 marks)

21. What is the advantage of using a Host-based Intrusion Prevention System (HIPS)?
    A. It can protect against threats that do not generate network traffic
    B. It eliminates the need for network firewalls
    C. It is easier to deploy on large networks
    D. It provides centralised monitoring of all network traffic (2 marks)

22. Which control type focuses on the administrative oversight of security policies and procedures?
    A. Technological controls
    B. Operational controls
    C. Management controls
    D. Physical controls (2 marks)

23. Which technique simulates cyberattacks to identify vulnerabilities?
    A. Security audits
    B. Compliance reviews
    C. Risk assessments
    D. Penetration testing (2 marks)

24. Which one of the following is a common challenge associated with implementing Data Loss Prevention (DLP) solutions?
    A. Increasing data transfer speeds
    B. Ensuring compliance with international data privacy regulations
    C. Managing false positives and negatives
    D. Simplifying network architecture (2 marks)

25. What is a **KEY** benefit of having a well-defined security policy?
    A. Reduces the need for employee training
    B. Ensures consistent security practices across the organisation
    C. Increases the complexity of security systems
    D. Lowers the cost of security technologies (2 marks)

26. Information Security (IS) policies are essential frameworks that define how an organisation manages and protects its information assets. Why is it important to establish a feedback mechanism?
    A. To eliminate the need for regular policy updates
    B. To ensure for continuous improvement
    C. To reduce the number of security controls in place
    D. To ensure employees do not participate in security training (2 marks)

27. In the context of penetration testing, what is the main function of metasploit?
    A. Password cracking
    B. Network scanning
    C. Wireless network testing
    D. Exploitation framework (2 marks)

28. Which one of the following tools can be used to capture packets and audit wireless networks?
    A. Hashcat
    B. Burp suite
    C. Aircrack-ng
    D. Nessus (2 marks)

29. Which step involves attempting to get administrator privileges by increasing the amount of access?
    A. Privilege escalation
    B. Maintaining access
    C. Gaining access
    D. Scanning (2 marks)

30. Which section of the penetration test report summarises the test, including its scope and major findings?
    A. Technical details
    B. Executive summary
    C. Risk assessment
    D. Appendix (2 marks)

31. Which one of the following is an example of a technical control in information security?
    A. Security awareness training
    B. Firewall installation
    C. Company security policies
    D. Physical locks on server rooms (2 marks)

32. Which one of the following describes a compensating control?
    A. A control that is designed to catch an issue after it occurs
    B. A control that substitutes for the failure of another control
    C. A control that focuses on environmental factors
    D. A control that prevents access to physical location (2 marks)

33. What technique is commonly used in threat modeling to identify potential threats?
    A. SWOT analysis
    B. STRIDE
    C. PEST analysis
    D. Gantt charts (2 marks)

34. Information Security (IS) culture in an organisation entails the collective mindset, attitudes, behaviours and practices regarding the protection of sensitive information and IT assets within that organisation. Why is it important to embed a strong IS security culture?
    A. Conducting quarterly financial audits
    B. Leadership commitment and promotion of security importance
    C. Hosting annual social events
    D. Increasing marketing budget (2 marks)

35. Integrating security into an organisation’s decision-making and business processes ensures?
    A. Security is disregarded in operational planning
    B. Security is managed solely by external consultants
    C. Security is only the IT department's responsibility
    D. Security is considered in all business activities (2 marks)

36. Which type of policy outlines how to handle and protect sensitive information?
    A. Data classification policy
    B. Hardware maintenance policy
    C. Employee dress code policy
    D. Customer service policy (2 marks)

37. Which one of the following statements **BEST** illustrates the purpose of Business Impact Analysis (BIA)?
A. To calculate insurance premiums
B. To identify the causes of disruptions
C. To assess the impact of natural disasters
D. To evaluate potential impacts of disruptions on critical business functions (2 marks)

38. Business continuity planning (BCP) involves creating a strategy to ensure that essential functions can continue during and after a disaster or emergency. What is the first step in business continuity planning?
A. Developing continuity strategies
B. Risk assessment
C. Training employees
D. Testing the plan (2 marks)

39. In the context of IS auditing, what is the primary purpose of using network sniffers?
A. Monitoring system performance
B. Generating audit reports
C. Identifying security vulnerabilities
D. Analysing network traffic patterns (2 marks)

40. Which tool is commonly used for network reconnaissance and scanning during penetration testing?
A. Wireshark
B. Nikto
C. Nessus
D. Nmap (2 marks)

41. What is the primary goal of business continuity management (BCM)?
A. To maximise profits and minimise expenditure
B. To ensure legal and regulatory compliance
C. To minimise the impact of disruptions on business operations
D. To increase employee satisfaction and comfort (2 marks)

42. Which one of the following tools is widely used to assess a system's resilience against distributed denial of service (DDoS) attacks?
A. Network analyser
B. Load balancer
C. Protocol analyser
D. DDoS mitigation software (2 marks)

43. Which one of the following is a benefit of adopting redundancy for recovery from failure?
A. It eliminates the need for backups
B. It reduces the cost of hardware
C. It increases fault tolerance
D. It decreases system performance (2 marks)

44. What is the purpose of reviewing logs and documentation during an information security audit?
A. To increase network bandwidth as appropriate
B. To ensure compliance with regulatory requirements
C. To manage customer complaints effectively
D. To improve employee morale and performance (2 marks)

45. Which one of the following is required for the successful implementation of Data Loss Prevention (DLP)?
A. Complete reliance on automated tools
B. Involvement of only IT department
C. Understanding of regulatory requirements and organisational policies
D. Use of open-source DLP software exclusively (2 marks)

46. What type of metric is used to measure qualitative security?
A. Number of security incidents per month
B. Severity level of vulnerabilities
C. Financial losses due to security breaches
D. Average time taken to resolve security incidents (2 marks)

47. Which one of the following is a common area of focus during an information security audit?
    A. Employee break room cleanliness
    B. Server hardware specifications
    C. Access controls and user permissions
    D. Product pricing strategies (2 marks)

48. Which framework is usually used to implement IS security governance into practice?
    A. Control Objectives for Information and Related Technologies (COBIT)
    B. International Organisation for Standardisation (ISO) 27001
    C. National Institute of Standards and Technology (NIST) SP 800-53
    D. Institute of Electrical and Electronics Engineers (IEEE) (2 marks)

49. Which phase of an information security audit does **NOT** involve making any presentations?
    A. Planning
    B. Fieldwork
    C. Reporting
    D. Follow-up (2 marks)

50. In the context of business impact analysis, which one of the following statements **BEST** describes the term Recovery Time Objective (RTO)?
    A. The maximum tolerable downtime for a business function
    B. The duration for which a business function can be disrupted without severe consequences
    C. The time required to recover data after a disaster
    D. The time required to restore a business function to normalcy after a disruption (2 marks)

……

CISSE ADVANCED LEVEL

ELECTIVE II

INFORMATION SYSTEMS SECURITY

TUESDAY: 23 April 2024. Afternoon Paper. **Time Allowed: 2 hours.**

Answer ALL questions by indicating the letter (A, B, C or D) that represents the correct answer. This paper is made up of fifty (50) Multiple Choice Questions. Each question is allocated two (2) marks.

1. In the context of information security, which one of the following terms involves operations such as inserting, updating and deleting records or data from the database?
   A. Data cleaning
   B. Data protection
   C. Data modelling
   D. Data modification (2 marks)

2. Which component of an organisation's information security strategy ensures data availability, preventing data loss and facilitating the quick restoration of systems in the event of security incidents, disasters or other unforeseen events?
   A. Access control
   B. Backup and recovery
   C. Database hardening
   D. Audit and monitoring (2 marks)

3. What is a structured approach to assessing and managing risks within a particular context, such as a business, project or financial portfolio known as?
   A. Risk model
   B. Vulnerability management
   C. Threat assessment
   D. Penetration testing (2 marks)

4. What is the primary objective of implementing IS security within an organisation?
   A. Maximising profits
   B. Minimising costs
   C. Protecting information assets
   D. Enhancing user experience (2 marks)

5. Which metric assesses the number of security incidents reported or detected within a specific time frame?
   A. Vulnerability severity index
   B. Security incident rate
   C. Compliance audit score
   D. Risk exposure ratio (2 marks)

6. Which one of the following statements **BEST** describes the term vulnerability?
   A. The impact of a security incident
   B. Malicious software designed to compromise security
   C. The likelihood of a security incident occurring
   D. A weakness in a system that can be exploited (2 marks)

7. Which one of the following CIA Triad's components deals with safeguarding data from unauthorised access?
   A. Integrity
   B. Availability
   C. Confidentiality
   D. Honesty (2 marks)

8. What is the primary goal of intrusion prevention systems (IPS)?
   A. Monitoring network traffic
   B. Detecting security vulnerabilities
   C. Blocking and mitigating malicious activities
   D. Encrypting data transmissions (2 marks)

9. In order to reduce security concerns, which of the following is a proactive measure?
   A. Regular security awareness training
   B. Patching and updating software
   C. Data encryption after a breach
   D. Incident response planning (2 marks)

10. Which one of the following is a fundamental component of information security governance?
   A. Access control
   B. Policy and compliance
   C. Incident response
   D. Firewalls (2 marks)

11. In the context of information security governance, what is the significance of periodic security audits?
   A. They focus only on network security
   B. They slow down the system performance
   C. They are only a legal requirement
   D. They identify and rectify security vulnerabilities (2 marks)

12. What is a potential limitation of an IPS?
   A. It may generate false positives
   B. It requires manual intervention for each security incident
   C. It is primarily effective against internal threats
   D. It can replace the need for firewall protection (2 marks)

13. Which objective of Information System (IS) security involves implementing measures to detect and respond to security incidents and breaches?
   A. Prevention
   B. Detection
   C. Recovery
   D. Mitigation (2 marks)

14. Which one of the following is a type of malicious code or software that is intentionally inserted into an information system or network to execute a harmful action when certain conditions are met?
   A. Back door
   B. Logic bomb
   C. Bot
   D. Feature (2 marks)

15. What does the metric "false positive rate" indicate in Information System (IS) security assessments?
   A. Percentage of valid security incidents
   B. Percentage of security controls that fail
   C. Percentage of detected threats that are false alarms
   D. Percentage of security vulnerabilities detected (2 marks)

16. Which one of the following **BEST** describes the important and valuable data that an organisation has and that is essential to its success and operation as a whole?
   A. Threats
   B. Information assets
   C. Weaponisation
   D. Mitigation (2 marks)

17. In the context of information security, the process of identifying, managing and resolving security incidents to minimise their impact on an organisation's assets, systems and data is known as:
A. Contingency plan
B. Business continuity
C. Risk management
D. Incident management (2 marks)

18. Which one of the following data protection principles highlights that information **MUST** be true, current and pertinent for the purpose of which it is processed?
A. Data minimisation
B. Accuracy
C. Purpose limitation
D. Storage limitation (2 marks)

19. Which type of information security control is designed to prevent unauthorised access to systems and data?
A. Detective control
B. Preventive control
C. Corrective control
D. Deterrent control (2 marks)

20. Which one of the following **BEST** describes the purpose of a Data Protection Impact Assessment (DPIA)?
A. To assess the impact of a data breach
B. To analyse the speed of data transmission
C. To identify and mitigate risks to individuals' privacy
D. To determine the cost of data storage (2 marks)

21. Which control is implemented to deter potential attackers and unauthorised individuals from attempting to exploit vulnerabilities?
A. Corrective control
B. Preventive control
C. Detective control
D. Deterrent control (2 marks)

22. A structured set of guidelines, best practices, standard and processes designed to help organisations manage and protect their information assets is known as:
A. Information security governance
B. Information security framework
C. Information security checklist
D. Information security management (2 marks)

23. Which of the following information security checklist requirements ensures suppliers adhere to security standards and contractual obligations?
A. Risk assessment
B. Access control
C. Endpoint security
D. Vendor security (2 marks)

24. Controls are classified according to the categories; preventive, detective and corrective. Which one of the following is a preventive control?
A. Contingency planning
B. Quality information
C. Reconciliations
D. Access control software (2 marks)

25. In the context of information security, what is the main objective of a security incident log?
A. Recording details of security incidents
B. Identifying security vulnerabilities
C. Real-time monitoring of network traffic
D. Implementing access controls (2 marks)

26. Which one of the following **BEST** describes the primary focus of organisational strategy?
    A. Minimising employee turnover
    B. Achieving long-term goals and objectives
    C. Maximising quarterly profits
    D. Enhancing customer service (2 marks)

27. Which technical security control is designed to restrict access to a network by analysing and controlling incoming and outgoing network traffic?
    A. Firewall
    B. Antivirus software
    C. Intrusion detection system (IDS)
    D. Encryption (2 marks)

28. Which one of the following refers to the process of analysing and categorising individuals, entities or systems based on their security-related characteristics and behaviours?
    A. Security policy
    B. Security profiling
    C. Demilitarised zone
    D. Security control (2 marks)

29. What does network segmentation primarily aim to achieve from a technical security perspective?
    A. Enhancing network performance
    B. Reducing the attack surface and limiting the spread of security incidents
    C. Securing physical access points
    D. Monitoring network traffic (2 marks)

30. Which one of the following is **NOT** considered a primary information security management objective?
    A. Confidentiality
    B. Integrity
    C. Availability
    D. Authorisation (2 marks)

31. What is the primary objective of a password policy?
    A. To define the organisational password structure
    B. To specify the types of authentication methods used
    C. To establish guidelines for creating and managing passwords
    D. To outline the procedures for resetting passwords (2 marks)

32. What is the primary responsibility of a Chief Information Security Officer (CISO)?
    A. Managing network infrastructure
    B. Developing software applications
    C. Overseeing the organisation's information security program
    D. Providing end-user support (2 marks)

33. Which one of the following refers to unauthorised and intentional attempt to compromise the security of an information system or network by injecting or executing malware?
    A. Application bypass attack
    B. Malicious code attack
    C. Dictionary attack
    D. Password guessing attack (2 marks)

34. Which one of the following components is typically included in an information security policy?
    A. Organisational chart
    B. List of approved software applications
    C. Statement of management commitment to information security
    D. Inventory of hardware assets (2 marks)

35. What purpose does a communication plan serve in the handling of incidents?
    A. To keep all incident information confidential
    B. To avoid any communication during an incident
    C. To share incident details with the public immediately
    D. To facilitate effective communication during and after an incident (2 marks)

36. Which one of the following **BEST** describes the role of employees in fostering an information security culture?
    A. Implementing security technologies
    B. Reporting security incidents
    C. Enforcing security policies
    D. Managing security budgets (2 marks)

37. Which one of the following refers to the strategic decision by an organisation to accept and manage certain risks internally rather than transferring them to an external party or mitigating them through additional security measures?
    A. Risk avoidance
    B. Risk reduction
    C. Risk sharing
    D. Risk retention (2 marks)

38. Which penetration testing tool is commonly used to discover and map network devices and services?
    A. Metasploit
    B. Wireshark
    C. Nmap
    D. Burp Suite (2 marks)

39. Which one of the following is **NOT** a component of a disaster recovery plan?
    A. Backup and recovery procedures
    B. Risk assessment
    C. Employee training
    D. Marketing strategy (2 marks)

40. What is the primary function of a vulnerability scanner tool in penetration testing?
    A. To simulate attacks and exploit vulnerabilities
    B. To detect and assess security vulnerabilities in systems and applications
    C. To encrypt data transmissions between network devices
    D. To analyse network traffic for anomalies and potential threats (2 marks)

41. Which type of testing uses a disaster simulation tool to assess the success of a disaster recovery plan?
    A. Full-scale exercise
    B. Tabletop exercise
    C. Parallel testing
    D. Walkthrough testing (2 marks)

42. How can organisations promote a strong information security culture among employees?
    A. By implementing punitive measures for security policy violations
    B. By integrating security awareness into daily operations and communications
    C. By restricting access to information and resources
    D. By prioritising security over business objectives (2 marks)

43. What is the main objective of information systems auditing utilising automated audit tools?
    A. Increase manual effort
    B. Decrease audit accuracy
    C. Slow down the audit process
    D. Enhance audit efficiency and effectiveness (2 marks)

44. Which one of the following is a fundamental element of a business continuity plan?
    A. Business impact analysis (BIA)
    B. Marketing strategy
    C. Financial forecasting
    D. Product development (2 marks)

45. Which phase of the system development lifecycle (SDLC) is primarily focused on identifying security requirements and defining security controls?
    A. Design phase
    B. Implementation phase
    C. Testing phase
    D. Planning phase (2 marks)

46. It is essential that security findings be communicated with the audience in mind. What does this signify?
    A. Share only positive findings with executives
    B. Adapt the level of detail and language to match the audience's understanding
    C. Use technical jargon to impress technical staff
    D. Exclude recommendations to avoid confusion (2 marks)

47. Why is it important to classify and prioritise incidents during the incident management process?
    A. To assign blame and responsibility
    B. To determine the financial impact of the incident
    C. To allocate resources effectively and address the most critical incidents first
    D. To identify the root cause of the incident (2 marks)

48. How will awareness and training programs contribute to the development of an information security culture?
    A. They educate employees and promote a security-conscious mindset
    B. They are primarily for management level only
    C. They only benefit IT professionals
    D. They are unnecessary and should be skipped (2 marks)

49. Which one of the following is a strategic decision made by an organisation to acknowledge and tolerate a certain level of risk without implementing additional measures to mitigate it?
    A. Risk reduction
    B. Risk avoidance
    C. Risk transfer
    D. Risk acceptance (2 marks)

50. What does the principle of fail-safe defaults aim to achieve in building secure systems?
    A. To ensure that systems continue to operate even when certain components fail
    B. To establish secure configurations and settings as the default option
    C. To minimise system complexity
    D. To reduce system maintenance costs (2 marks)

.....

CISSE ADVANCED LEVEL

ELECTIVE II

INFORMATION SYSTEMS SECURITY

TUESDAY: 5 December 2023. Afternoon Paper. **Time Allowed: 2 hours.**

Answer ALL questions by indicating the letter (A, B, C or D) that represents the correct answer. This paper is made up of fifty (50) Multiple Choice Questions. Each question is allocated two (2) marks.

1. Which of the following database security principles and strategies set up alerts to notify administrators of unusual or potentially malicious activities?
   A. Access Control
   B. Backup and Recovery
   C. Database Hardening
   D. Audit and Monitoring (2 marks)

2. Which of the following is a collection of rules, processes and technology designed to ensure that data is handled securely and per applicable laws and regulations?
   A. Data transformation
   B. Data Protection
   C. Data Privacy
   D. Data modification (2 marks)

3. Mr. Telow Orwa, a security manager, wants to identify when operating system files change on a regular basis. Which of the following tools is required for this task?
   A. Event logging
   B. File system integrity monitoring tool
   C. Intrusion detection tool
   D. Log analysis tool (2 marks)

4. Which of the following is an important phase that entails a systematic examination and evaluation of a security incident or breach within an organisation?
   A. Preparation
   B. Detection and analysis
   C. Post-incident analysis
   D. Containment, Eradication and Recovery (2 marks)

5. Which of the following is the **BEST** way to perform assessment on a critical business application in order to evaluate what additional controls may be required to protect the program and its databases?
   A. Perform a quantitative risk assessment, then perform a qualitative risk assessment
   B. Perform a qualitative risk assessment first, then perform a quantitative risk assessment
   C. Perform a quantitative risk assessment only
   D. Perform a qualitative risk assessment only (2 marks)

6. Which of the following sets the direction for an organisation's security efforts, ensuring that security aligns with business objectives, is effectively managed, and consistently applied throughout the organisation?
   A. Security Framework
   B. Security Governance
   C. Third-Party Risk Management
   D. Security Incident Reporting and Documentation (2 marks)

7. Which of the following is a priority asset that needs to be addressed in cyber security management?
   A. Electronic data
   B. Company hardware
   C. System users
   D. System licenses (2 marks)

8. Which of the following **BEST** describes an intrusion detection system?
   A. It is a control system
   B. It is a monitoring system
   C. It detects and presents intrusions
   D. It needs the latest threat data (2 marks)

9. Which of the following is **NOT** a type of recovery procedure that recovers the entire system after failure?
   A. Instance recovery
   B. Crash recovery
   C. Media recovery
   D. System recovery (2 marks)

10. Which of the following can help in addressing brute force attacks in an organisation but requires technical intervention to setup?
   A. User education
   B. Adding password complexity
   C. Setting login attempts limits
   D. Two factor authentication

11. Port scanning helps identify and access open ports and services. Which of the following tools may be used by novice users for this task?
   A. Ping
   B. TCP connect
   C. CMD
   D. Stealth scanning (2 marks)

12. Vulnerability Assessment (VA) and Penetration Testing (PT) are useful security management processes.

   What follows a VAPT exercise?
   A. Finding vulnerabilities on the target
   B. Knowledge of the system configurations
   C. Prioritising fixing of the identified flaws
   D. Responding to the audit queries (2 marks)

13. Which one of the following steps is the **MOST** overlooked yet it is the foundation in securing your servers?
   A. Making sure you have a secure password for your root and administrator users
   B. Removing default users from servers
   C. Removing remote access from the default root/administrator accounts
   D. Configuring your firewall rules for remote access (2 marks)

14. Often questions about personal information are optional as they may be used to facilitate suspicious transactions. Which of the following would cause you to be **MOST** suspicious?
   A. Month of birth
   B. Maiden name
   C. Year of birth
   D. Favorite meal (2 marks)

15. Which of the following traditionally motivates a penetration testing exercise?
   A. An audit requirement
   B. A regulatory requirement
   C. To address known gaps
   D. To enhance system security (2 marks)

16. Which of the following details would **MOST** concern the board as a cyber security measure?
    A. Preparedness level
    B. Number of incidents
    C. Unidentified devices on your internal network
    D. Intrusion attempts (2 marks)

17. Which of the following is the systematic process of identifying, categorising, valuing and managing the many assets inside an organisation that are crucial to its information security posture?
    A. Vulnerability management
    B. Configuration management
    C. Asset management
    D. Asset servicing (2 marks)

18. Which of the following is a malicious attempt to disrupt the normal operation of a network, service or website by flooding it with traffic or requests and leaving it inaccessible to legitimate users?
    A. Denial of service
    B. Traffic analysis
    C. Masquerading
    D. Packet analysis (2 marks)

19. The process of finding, collecting, archiving and analysing electronically stored information (ESI) for the purposes of legal investigations, litigation or regulatory compliance is known as:
    A. System discovery
    B. Electronic discovery
    C. Search and seizure
    D. Subpoena (2 marks)

20. Which of the following is a recovery process that entails detecting unusual network activity, uncovering malware or discovering unauthorised access?
    A. Containment
    B. Investigation and analysis
    C. Remediation
    D. Incident identification (2 marks)

21. A firm has created its first-ever computer security incident response procedure. What type of test should be performed first?
    A. Document review
    B. Parallel test
    C. Simulation
    D. Walkthrough (2 marks)

22. Which of the following terms relate to the total number of potential entry points, vulnerabilities and paths that attackers can take to infiltrate a system, network or application?
    A. Attack points
    B. Attack vectors
    C. Attack surfaces
    D. Attack arenas (2 marks)

23. Bulls Ltd, a steel firm, has had many virus infections on its desktop PCs. Which of the following remedies would **NOT** be effective in reducing viral infections?
    A. Install an anti-virus gateway web proxy server
    B. Install anti-virus on its web servers
    C. Install anti-virus on the central management console
    D. Install anti-virus on its e-mail servers (2 marks)

24. An organisation's business records differ in sensitivity and handling needs. There is no policy in place that specifies how any of these records should be safeguarded. What does this organisation lack?
    A. Storage and handling procedures
    B. Separation of duties
    C. Information security policy
    D. Data classification policy (2 marks)

25. Miss Selwom Lellet, an executive in one of the country's major consulting firms received notice of a lawsuit connected to activity in one of the operations departments. How should the company respond?
A. Cease all purging activities until further notice
B. Alter retention schedules and begin purging the oldest information
C. Purge all information older than timelines specified in its retention schedule
D. Hire an outside organisation to perform all purging activities (2 marks)

26. The risk assessment method where an organisation obtains insurance to cover potential losses is known as:
A. Risk reduction
B. Risk avoidance
C. Risk transfer
D. Risk acceptance (2 marks)

27. A county government recently had its financial applications audited. According to the audit report, there were various segregation-of-duties concerns connected to ICT support for the application. What exactly does this mean?
A. ICT needs to begin the practice of job rotation
B. Individuals in ICT have too many roles or privileges
C. The duties of personnel are not formally defined
D. ICT personnel should not have access to financial data (2 marks)

28. Which of the following is **BEST** suited to streamline and enhance an organisation's ability to detect, respond to and mitigate security incidents, threats and vulnerabilities?
A. Security information and event management (SIEM)
B. Security orchestration, automation and response (SOAR)
C. Common Vulnerability Scoring System (CVSS)
D. Fuzzer (2 marks)

29. In the case of a disruptive incident, which of the following is a comprehensive strategy and set of policies and procedures that a company establishes to enable the continuation of important business operations and the recovery of data and IT systems?
A. Failover
B. High availability
C. Fault tolerance
D. Disaster recovery (2 marks)

30. A Network Security administrator is configuring resource permissions in an application. The security manager learned that he may create objects with access permissions and then assign certain users to those things. The access control paradigm that is most similar to this is?
A. Capability list
B. Mandatory access control (MAC)
C. Role based access control (RBAC)
D. Discretionary access control (DAC) (2 marks)

31. An intruder attempts to break into a program in order to discover and exploit vulnerabilities or weaknesses in the application's security mechanisms in order to obtain unauthorised access or control over the system on which it runs. What is the most likely approach for the intruder?
A. Application bypass attack
B. Malicious code attack
C. Dictionary attack
D. Password guessing attack (2 marks)

32. Which of the following describes the organisation's responsibilities and diligence in preserving its information assets and systems?
A. Integrity
B. Due care
C. Due diligence
D. Due process (2 marks)

33. Which of the following represents the numerous channels or entry points through which bad actors can exploit vulnerabilities or weaknesses in a target system's defenses?
A. Scope
B. User interaction
C. Attack complexity
D. Attack vector (2 marks)

34. A company employs hundreds of office workers who utilise computers to complete their tasks. What is the **MOST** effective strategy for informing staff about security issues?
A. Include security policy in the employee handbook
B. Perform security awareness training at the time of hire
C. Perform security awareness training at the time of hire and annually thereafter
D. Require employees to sign the corporate security policy (2 marks)

35. Which of the following stops possible risks or dangers from occurring in the first place, rather than attempting to reduce or manage them after they have occurred?
A. Risk avoidance
B. Risk Reduction
C. Risk sharing
D. Risk retention (2 marks)

36. A solid, management-driven model of security-related activities such as policy, risk management, standards and processes exists within an organisation. This model can **BEST** be described as:
A. Risk management
B. Security governance
C. Security oversight
D. Security control (2 marks)

37. Which of the following terms applies to the practice of safeguarding individual computer devices inside a network or enterprise environment?
A. Incident response
B. Application security
C. Patch management
D. Endpoint security (2 marks)

38. Following the completion of a risk assessment procedure, a company was able to reduce the risk by implementing detective and preventative controls. However, these safeguards did not eliminate all risk. What choices does the company have for dealing with the remaining risk?
A. None; the organisation must accept the risk
B. The organisation must either accept or transfer the risk
C. Accept, avoid, reduce or transfer the risk
D. Does not apply - remaining risk cannot be treated further (2 marks)

39. Which of the following has the sole objective of minimising damage, reducing recovery time and maintaining business continuity?
A. Security incident plan
B. Operational plan
C. Service plan
D. Business continuity plan (2 marks)

40. An employee in a company requests more information than is necessary. Which principle should be used to deny this request?
A. Separation of duties
B. Need to know
C. Least privilege
D. Job rotation (2 marks)

41. Multiple degrees of security are applied in an information system, covering both resources and users. A user cannot access resources below his level in this system and he cannot develop resources above his level. Which of the following access control models corresponds to this?
A. Access matrix
B. Clark-Wilson
C. Bell-LaPadula
D. Biba (2 marks)

42. Which of the following is a network segment within a company's network infrastructure that is intended to offer an additional layer of security between the internal network and external networks such as the internet?
A. Security policy
B. Security profiling
C. Demilitarised zone
D. Security control (2 marks)

43. Any user that accesses a sensitive information system is required to enter a valid user identification and a strong password. The procedure of validating and accepting this information is known as:
A. Authentication
B. Two-factor authentication
C. Single sign-on
D. Strong authentication (2 marks)

44. Which of the following hackers are used by organisations as part of their cyber security management process?
A. Junior hackers
B. Black hats
C. Grey hats
D. White hats (2 marks)

45. Which of the following is **NOT** a step that should be taken when conducting a security audit?
A. Selecting security audit criteria
B. Assessing staff training
C. Identifying threats
D. Reviewing logs and responses to events (2 marks)

46. Security systems that contain redundant hardware, software and power supply components that create an environment to provide continuous uninterrupted service are referred to as:
A. Fault-tolerant computer systems
B. High-availability computing systems
C. Mirroring systems
D. Business planning systems (2 marks)

47. The audit technique where the auditor verifies accounting transactions with documentary evidence is referred to as:
A. Confirmation
B. Vouching
C. Reconciliation
D. Physical examination (2 marks)

48. Computer Aided Audit Tools (CAATs) can be used to perform the following audit procedures, **EXCEPT**:
A. Tests of details of transactions and balances
B. Tests of general controls
C. Performing analytical review procedures
D. Firewall testing (2 marks)

49. The type of security control which does **NOT** involve source removal but reduces exposure to a receptor is referred to as?
A. Operational control
B. Management control
C. Technological control
D. Receptor control (2 marks)

50. Which of the following is **NOT** a type of audit report?

A. Unqualified audit report
B. Qualified audit report
C. Adverse audit report
D. Non-disclaimer audit report (2 marks)

.....

CISSE ADVANCED LEVEL

ELECTIVE II

INFORMATION SYSTEMS SECURITY

TUESDAY: 22 August 2023. Afternoon Paper. **Time Allowed: 2 hours.**

Answer ALL questions by indicating the letter (A, B, C or D) that represents the correct answer. This paper is made up of fifty (50) Multiple Choice Questions. Each question is allocated two (2) marks.

1. Which one of the following entails protecting an individual's rights through organisations adhering to regulations and business practices?
   A. Data transformation
   B. Data privacy
   C. Data modification
   D. Data integrity

2. Which of the following refers to a set of technologies that protects the usability and integrity of organsation's infrastructure by preventing the entry or proliferation within a network of a wide variety of potential threats?
   A. Database Security
   B. Physical Security
   C. Information Security
   D. Network Security

3. Which of the following enables an organisation to identify and communicate information about the threats that may impact a particular system or network?
   A. Risk model
   B. Threat Intelligence
   C. Threat modeling
   D. Threat Assessment

4. Which of the following is a common model that forms the basis for the development of security systems by finding vulnerabilities and methods for creating solutions in an organisation?
   A. CIA triad
   B. Parkerian hexad
   C. Bell-LaPadula
   D. Clarke Wilson Security Model

5. Which of the following will alert a computer user so that he/she can react quickly to stop further damage once an intrusion is detected?
   A. IPS immediately shuts down the process.
   B. NIDS immediately shuts down the process.
   C. NIDS immediately stops the thread
   D. IPS immediately stops the thread

6. Risk management is the process of identifying, assessing and controlling threats to an organisation's capital and earnings. Failing to detect a material error would represent which type of risk?
   A. Overall Audit Risk
   B. Control Risk
   C. Inherent Risk
   D. Detection Risk

7. With reference to incident response process, which phase detects the occurrence of an issue and decides whether or not it is actually an incident so that it can be responded to it appropriately?
   A. Preparation
   B. Post-incident analysis
   C. Detection and analysis
   D. Containment, Eradication and Recovery

8. Which of the following is a multifaceted strategic plan where layered security would be one aspect of defense when deployed in an organisation?
   A. Security in depth
   B. Layered defense
   C. Zero trust
   D. Defense in breadth

9. Which of the following is a written document in an organisation that outlines how to protect the organisation from threats and handle situations when they do occur?
   A. Security standard
   B. Security policy
   C. Security mechanism
   D. Security implementation

10. Which one of the following is **NOT** a component of security management?
   A. Confidentiality
   B. Digital signature
   C. Authenticity
   D. Non-repudiation

11. Which one of the following when deployed gravitates towards the facility being protected by an organisation?
   A. Network operations
   B. Security Audits
   C. Reconnaissance operations
   D. Security operations

12. A comprehensive system testing process ultimately boosts the product quality and in the long run is able to meet the organisational objective. The following features are associated with which type of testing?
   (i) It tests both functional as well as non-functional requirements of the application.
   (ii) Knowledge/access to the coding/design/internal architecture of the software is not required.
   (iii) Testers can work independently from developers thus ensuring unbiased and end-user centric testing.
   A. White box testing
   B. Gray box testing
   C. Black box testing
   D. Blue box testing

13. Which of the following is the testing process used to identify and assign severity levels to as many security defects as possible in a given timeframe?
   A. Vulnerability Assessment
   B. Vulnerability Management
   C. Patch Management
   D. Risk Management

14. An audit aims to establish whether information systems (IS) are safeguarding corporate assets, maintaining the integrity of stored and communicated data, supporting corporate objectives effectively and operating efficiently. Risk-control-Matrix is developed in which step of IS audit?
   A. Analysis
   B. Planning
   C. Fieldwork
   D. Reporting

15. Which of the following refers to a collection of procedures and technology designed to address external and internal threats to business security by helping organisation move towards digital transformation strategy?
    A. Devsecops
    B. Cybersecurity
    C. Cloud Computing
    D. Cloud Security

16. Which of the following refers to a body of information, defined and managed as a single unit so it can be understood, shared, protected and exploited efficiently?
    A. Threats
    B. Weaponisation
    C. Information assets
    D. Mitigation

17. Which of the following relates to organisation's readiness to maintain critical functions after an emergency or disruption?
    A. Business continuity
    B. Risk Management
    C. Contingency plan
    D. Incident Management

18. A disaster is an unexpected problem resulting in a slowdown, interruption, or network outage in an IT system within an organisation? Which one of the following is **NOT** a disaster recovery plan method?
    A. Backup
    B. Password Manager
    C. Cold site
    D. Virtualisation

19. The phase of penetration testing that entails scanning and asset analysis where the tester uses network scanning tool such as NMAP to identify which assets are available and to gather some basic information about them such as operating system, open ports and running services is known as?
    A. Pre-engagement phase
    B. Vulnerability analysis phase
    C. Reconnaissance phase
    D. Discovery phase

20. A compliance test is an audit that determines whether an organisation is following its own policies and procedures in a particular area. Which of the following is **NOT** a compliance test related to information systems?
    A. Determining whether passwords are changed periodically
    B. Determining whether systems logs are reviewed
    C. Reconciling account balances
    D. Determining whether program changes are authorised

21. Which of the following refers to processes and practices of technologies designed to protect networks, computers, programs and data from unwanted or deliberate intrusions?
    A. Information systems security control
    B. Information systems security policy
    C. Information systems security threat
    D. Information systems security feature

22. Which one of the following refers to a framework of policies, practices and strategies that align organisational resources toward protecting information through cybersecurity measures?
    A. Information security framework
    B. Information security governance
    C. Information security checklist
    D. Information security management

23. Which one of the following is **NOT** a type of control in information security?
    A. Technical
    B. Administrative
    C. Physical
    D. Conceptual

24. The document declaring the preliminary commitment of one party to do business with another by outlining the main terms of a prospective deal in business transactions is referred to as?
    A. Audit exit report
    B. Audit comprehensive report
    C. Audit letter of intent
    D. Audit charter

25. Which of the following information system threats can perform Distributed Denial-of-Service (DDoS) attacks through a network of computers infected by malware that are under the control of a single attacking party?
    A. Botnet
    B. Trojan horse
    C. Ransomware
    D. Rootkits

26. Which of the following refers to a structured process used to identify security requirements, pinpoint security threats and potential vulnerabilities, quantify threat and vulnerability criticality and prioritise remediation methods?
    A. Architecture review
    B. Threat modeling
    C. Design authority
    D. Threat hunting

27. A Firewall is the barrier that sits between a private internal network and the public Internet within an organisation. Which of the following statements **BEST** illustrates the purpose of firewall usage in an organisation?
    A. To protect hardware against hazard
    B. To increase speed of internet connection
    C. To protect the computer from viruses and malware
    D. To filter traffic that is moving in and out of the organisation

28. Which of the following is the security characterisation of an entity, a service or a component in terms of security objectives as well as security properties?
    A. Security policy
    B. Demilitarised zone
    C. Security profiling
    D. Security control

29. Information security tools plays a big role in ensuring organisations protect information. Which of the following statements illustrates the main difference between implementation of IDS and IPS devices?
    A. An IDS would allow malicious traffic to pass before it is addressed whereas an IPS stops it immediately
    B. An IDS can negatively impact packet flow whereas an IPS cannot
    C. An IDS needs to be deployed together with a firewall device whereas an IPS can replace a firewall
    D. An IDS uses signature based technology to detect malicious packets whereas an IPS uses profile based technology

30. Which of the following is a risk assessment tool that is designed to convey the common attributes and severity of vulnerabilities in computer hardware and software systems?
    A. Security information and event management (SIEM)
    B. Common Vulnerability Scoring System (CVSS)
    C. Security Orchestration, Automation, and Response (SOAR)
    D. Fuzzer

31. Which of the following enables organisation's system software to respond to a failure in hardware or software by making it continue operating despite failures or malfunctions?
    A. Failover
    B. High availability
    C. Disaster recovery
    D. Fault tolerance

32. Which of the following refers to a means of restricting access to system resources based on the sensitivity of the information contained in the system resource and the formal authorisation of users to access information of such sensitivity?
    A. Capability list
    B. Role based access control (RBAC)
    C. Mandatory access control (MAC)
    D. Discretionary access control (DAC)

33. Which of the following is centered around strategies to limit the impact of a threat against data in custody?
    A. Mitigation
    B. Probability
    C. Assessment
    D. Risk

34. Security controls focused on_____ are designed to prevent data from being modified or misused by an unauthorised party.
    A. Due care
    B. Integrity
    C. Due diligence
    D. Due process

35. Which of the following exploitation metrics expresses the number of components, software, hardware or networks that are beyond the attacker's control and that must be present for a vulnerability to be successfully exploited?
    A. Scope
    B. User interaction
    C. Attack vector
    D. Attack complexity

36. Which of the following is **NOT** part of risk management process?
    A. Identify assets, vulnerabilities and threats
    B. Implementation of risk response
    C. Irregular risk monitoring and response evaluation
    D. Determination of risk response plan action

37. System vulnerability affirms weakness in an information system or implementation that could be exploited or triggered by a threat source. Which of the following risk response takes measures to reduce vulnerability?
    A. Risk reduction
    B. Risk avoidance
    C. Risk sharing
    D. Risk retention

38. Which of the following vulnerability management life cycle determines a baseline risk profile to eliminate risks based on asset criticality, vulnerability, threats and asset classification?
    A. Discover
    B. Assess
    C. Report
    D. Remediate

39. Which of the following refers to the process of applying vendor-issued updates to close security vulnerabilities and optimise the performance of software and devices?
A. Incident response
B. Application security
C. Endpoint security
D. Patch management

40. Which device management activity addresses the inventory and control of hardware and software configurations?
A. Asset management
B. Vulnerability management
C. Configuration management
D. Mobile device management

41. Which of the following entails analysis of patterns in communications for the purpose of gaining intelligence about a system or its users?
A. Traffic analysis
B. Masquerading
C. Denial of service
D. Packet analysis

42. Which device management activity involves the implementation of systems that track the location and configuration of networked devices and software across an organisation?
A. Investment management
B. Asset management
C. Hedge fund
D. Private equity

43. Which of the following defines an organisation's plans for responding to incidents?
A. Recovery testing
B. Recovery run
C. Failure recovery
D. Recovery strategy

44. Data integrity ensures overall accuracy, completeness, and consistency of data. Which of the following attacks threatens integrity?
A. Denial of service
B. Packet analysis
C. Masquerading
D. Traffic analysis

45. Which of the following includes malware, viruses, email attachments, web pages, pop-ups, instant messages, text messages, and social engineering.
A. Attack points
B. Attack surfaces
C. Attack vectors
D. Attack arenas

46. Which of the following category of National Institute of Standards and Technology (NIST) aligns itself to the following activities?
(i) Identity Management and Access Control
(ii) Information Protection Processes and Procedures
(iii) Maintenance
A. Identify
B. Protect
C. Detect
D. Respond

47. During which stage would you develop and implement the appropriate activities to identify the occurrence of an information security event?
A. Protect
B. Recover
C. Identify
D. Detect

48. When establishing a server profile for an organisation, which element describes the type of service that an application is allowed to run on the server?
    A. Service account
    B. Software environment
    C. User account
    D. Listening port

49. Which of the following is a free and open source Linux distribution for intrusion detection, security monitoring and log management for events happening in an organisation?
    A. Suricata
    B. Splunk
    C. Security Onion
    D. Zeek

50. Which of the following statement **BEST** describes threat-vulnerability (T-V) pairing?
    A. Comparison between known malware and system risks
    B. Identification of threats and vulnerabilities and matching of threats with vulnerabilities
    C. Detection of malware against a central vulnerability research center
    D. Advisory notice from a vulnerability research center

……..

CISSE ADVANCED LEVEL

ELECTIVE II

INFORMATION SYSTEMS SECURITY

TUESDAY: 25 April 2023. Afternoon Paper. **Time Allowed: 2 hours.**

Answer ALL questions by indicating the letter (A, B, C or D) that represents the correct answer. This paper is made up of fifty (50) Multiple Choice Questions. Each question is allocated two (2) marks.

1. Which of the following is the most cost-effective data loss prevention step?
   A. Staff awareness training
   B. Use of DLP software
   C. System auditing
   D. Operational excellence

2. Which of the following protects sensitive information from unauthorised activities, including inspection, modification, recording, and any disruption or destruction?
   A. Network Security
   B. Database Security
   C. Physical Security
   D. Information Security

3. Bidii Ltd implemented IT governance, what is the next phase in the life cycle of governance that they should do?
   A. Measuring objectives
   B. Initiating improvements
   C. Updating the program
   D. Investment justification

4. Which of the following is **NOT** an access control security service?
   A. Availability
   B. Authorisation
   C. Authentication
   D. Accounting

5. Which one of the following helps a cyber security management staff to feel better equipped to serve the organisation?
   A. Technology graduates
   B. Software Tools
   C. System Certifications
   D. Inter departmental Support

6. An intrusion detection system (IDS) is a device or software application that monitors a network for malicious activity or policy violations. Which of the following is **NOT** a feature of IDS?
   A. It runs continually without human supervision.
   B. It is programmed to interpret certain series of packets.
   C. It is fault tolerant in the sense that it survives a system crash.
   D. It looks for attack signatures in network traffic.

7. There are a few steps that one has to implement in order to keep their personal computer at home computer secure. Which one of the following is **NOT** recommended for a personal home computer?
   A. Implement a 2-way or multi-factor authentication
   B. Use uncommon alphanumeric passwords and secure them
   C. Update your computer regularly
   D. Install a good antivirus to protect your computer from malware

8. Development and implementation of appropriate activities to maintain plans for resilience and to restore any capabilities or services that were impaired due to information security event is done at which of the following stages?
   A. Respond
   B. Protect
   C. Detect
   D. Recover

9. Which phase of National Institute of Standards and Technology (NIST) determines specifically what happened, why it happened, and what we can do to keep it from happening again in the context of incident response?
   A. Preparation phase
   B. Detection and analysis
   C. Post-incident analysis
   D. Containment, eradication and recovery.

10. Which of the following provides security at the application level?
   A. Defense in breadth
   B. Defense in depth
   C. Layered defense
   D. Layered security

11. A network intrusion protection system (NIPS) protects computer networks from unauthorised access and malicious activity. Assuming NIPS has identified a threat, which type of security data will be generated and sent to a logging device?
   A. Transaction
   B. Alert
   C. Session
   D. Statistical

12. Which of the following information security metrics are important for senior executives in the organisations?
   A. Percentage of IT budget spent on security as compared to peer institutions
   B. Reduction in sensitive data exposures due to stolen or vulnerable desktops/laptops
   C. Percentage increase over time of departments with mission continuity plans
   D. Significant reduction in sensitive data stored on desktops/laptops

13. Penetration testing entails using tools, techniques, and processes as attackers to find and demonstrate the business impacts of weaknesses in a system. Which of the following statements **BEST** illustrates social engineering?
   A. Using force to gain access to the information you need
   B. Hacking either telecommunication or wireless networks to gain access to the information you need
   C. Using force to gain all the information available.
   D. Using manipulation to deceive people that you are someone you are not to gain access to the information you need

14. Which of the following is the main security risk of penetration testing?
   A. It can conceal aggression that is unrelated to the test.
   B. It can affect user connectivity and resource access
   C. It can disrupt the normal business environment.
   D. It can weaken the network's security level

15. Which of the following is the process of identifying, evaluating, treating, and reporting security vulnerabilities in systems and the software that runs on them?
   A. Vulnerability management
   B. Security vulnerability
   C. Patch management
   D. Risk management

16. Vulnerability assessment is a systematic review of security weaknesses in an information system. Which of the following is a type of vulnerability assessment software that can check for weak passwords on the network?
    A. Wireshark
    B. Password cracker
    C. Performance Monitor
    D. Antivirus software

17. Mr. John an IT Practitioner was contracted to perform forensic analysis on information systems of a multinational company. Which of the following should he do first?
    A. Scan for virus
    B. Analyse the files
    C. Modify operating system
    D. Backup the system

18. Which of the following is the first step in a VPN security management process?
    A. Data is decrypted for visibility
    B. The encryption standard is defined
    C. Data is routed to the VPN server
    D. Data is encrypted by the server

19. Which of following statements is **TRUE**?
    A. A threat is a weakness or gap in a system
    B. A vulnerability causes potential harm to an organisation
    C. A risk happens when a threat exploits a vulnerability
    D. A risk occurs when a vulnerability exploits a threat

20. Which of the following can help an organisation's employee prevent identity theft?
    A. Avoid online sharing of confidential information.
    B. Use strong passwords, and change them at regular intervals.
    C. Do not provide your bank information on untrustworthy websites.
    D. Protect your system with advanced firewall and spyware tools.

21. Disaster recovery (DR) is an organisation's ability to respond to and recover from an event that negatively affects business operations. Which of the following is a disaster recovery strategy?
    A. Priority
    B. Risk avoidance
    C. Risk response planning
    D. Risk monitoring

22. In an infrastructure network which of the following will **NOT** be considered a domain risk?
    A. Demilitarised zone
    B. Disaster Recovery Plan
    C. Private network
    D. Mobile Users

23. A business continuity plan (BCP) is a system of prevention and recovery from potential threats to a company. Which of the following originates from most operational requirements?
    A. Analysis of recovery strategy
    B. The system architecture
    C. Disaster recovery planning
    D. Analysis of business impacts

24. A business impact analysis (BIA) should identify the operational and financial impacts resulting from the disruption of business functions and processes. Which one of the following is **NOT** an impact to consider?
    A. Lost sales and income
    B. Regulatory fines
    C. Strategic Plan
    D. Customer dissatisfaction or defection

25. Phishing attacks may end up getting sensitive information through its interactions, which of the following is **NOT** a type of phishing attack?
    A. Memory phishing
    B. Email phishing
    C. Spear Phishing
    D. Whaling

26. Computing resources include hardware and software that can be accessed from information system. What should an information technologist take into consideration in order to restore a server, its files and data after a major system failure?
    A. Implement recovery procedures
    B. Restore from storage media backup
    C. Perform a parallel test
    D. Perform a check list test

27. IT governance (ITG) ensures effective and efficient use of IT in enabling an organisation to achieve its goals. Which of the following is **NOT** considered a component of ITG?
    A. Control planning
    B. Security assessment
    C. Managing incident response
    D. Control development

28. IT compliance ensures organisations operate within a specific set of privacy and security requirements, guidelines, and best practices. Which of the following components is **NOT** part of IT compliance?
    A. IT Audit
    B. Security assessment
    C. IT Compliance assessment
    D. Control development

29. An organisation sends magazines to different people, they sent requests for different information sets at different times, which of the following would raise your eyebrows that the requests are not genuine?
    A. Email address
    B. Birth date
    C. Phone number
    D. Password

30. Which of the following outlines the overall authority, scope and responsibilities of the information security audit function?
    A. Audit exit report
    B. Audit comprehensive report
    C. Audit charter
    D. Audit letter of intent

31. IT audit determines whether IT controls protect corporate assets, ensure data integrity and are aligned with the business's overall goals. Which of the following stages can one obtain audit response verification?
    A. Follow-up
    B. Report
    C. Assessment
    D. Planning

32. Which of the following statements **BEST** describes threat profile?
    A. What is the likelihood of threat happening
    B. What threats or risks will affect the asset
    C. What is the likelihood of threats mitigated
    D. What would be the impact of the asset

33. In the campus computer lab, someone logged in to her Gmail account and when she left she ensured that the account was not left open. Later on, though someone reassessed her account from that browser and send malicious emails to several of her colleagues. Which is the most likely scenario that may have caused this?
    A. She may have used a simple password to access her email
    B. She may have shared her password with several people
    C. Someone may have visited the browser’s history to access her account
    D. She may have forgotten to logout of her account

34. A pen tester's tool that intercepts and changes traffic flowing between the pen tester's browser and the web server of the organisation with the goal to find and exploit HTML application vulnerabilities, which enable the tester to launch attacks like XSS and cross site request forgery (CSRF) is referred to as?
A. Web proxy
B. Network Sniffers
C. Port Scanner
D. Vulnerability scanner

35. Which of the following can be used to identify the vulnerabilities left by developers, thereby protecting the possibility of data leakage and adding another layer of security?
A. Vulnerability scan
B. Code review
C. Manual testing
D. Automated testing

36. The following are benefits of carrying out a Privacy Impact Assessment **EXCEPT?**
A. Identification of privacy risks and impacts
B. Assessment of the impacts and the likelihood of new information system privacy risks
C. Gaining valuable information that contribute to the design of privacy protection
D. Make sure that there is an internal breach reporting procedure in place

37. Mr. David a Network security manager has been tasked to set up resource permissions in an application. He established objects with access permissions and assigned them to individual users. Which of the following access control model was used?
A. Access matrix
B. Mandatory access control (MAC)
C. Role based access control (RBAC)
D. Discretionary access control (DAC)

38. Which of the following relates to the likelihood of a threat source taking advantage of a vulnerability?
A. Risk
B. Mitigation
C. Probability
D. Assessment

39. Which of the following involves auditing a company's IT infrastructure and processes with a focus on security assessment?
A. IT Due care
B. IT Due diligence
C. Due process
D. Compliance

40. Information security program consists of activities, projects, and initiatives supporting an organisation's information technology framework. Which of the following is **NOT** included in information security program?
A. Security Policy
B. Assignment of roles and responsibilities
C. Information assist classification
D. Site-wide outages

41. Which of the following statements **BEST** describes system security policy?
A. Password strength rules that are used to determine whether a new password is valid.
B. Defining a custom set of account properties and key privileges
C. A brief, high-level statement defining what is and is not permitted during the operation of the system.
D. Prevent employees in an organisation to use their personally owned devices for work-related activities

42. Open-source intelligence (OSINT) can be used in penetration testing. Which of the following statements best describes the purpose of OSINT?
A. Company documentation labeled "Confidential" on an internal company storage share requiring authentication
B. Any information or data obtained via publicly available sources that is used to aid or drive decision-making processes
C. Press release drafts found on an undocumented web page inside a company's intranet
D. Information gained by source code analysis of free and open-source software (FOSS)

43. Under General Data Protection Regulation (GDPR) legislation that updated and unified data privacy, what is the period of time an organisation should notify a supervising authority in case of a data breach?
    A. Within 48 hours
    B. Within 12 hours
    C. Within 24 hours
    D. Within 72 hours

44. As information system security manager, you have decided to enlighten a group of interns in your organisation on logical access control. Which of the following will **NOT** be a good idea when it comes to password security?
    A. Using a password manager to securely store your login information.
    B. Changing your passwords on a regular basis, such as every three-to-six months.
    C. Writing your passwords down on a sticky note that you keep near your computer.
    D. Creating unique, long, complex passwords for each and every online account you have.

45. Data integrity ensures overall accuracy, completeness, and consistency of data. Which of the following attacks threatens integrity?
    A. Masquerading
    B. Traffic analysis
    C. Denial of service
    D. Packet analysis

46. Which of the following is concerned with individual user rights?
    A. General access
    B. Functional authorisation
    C. Functional authentication
    D. Auto verification

47. A procedure that allows for restart of a failed system in a way that either eliminates or minimises the amount of incorrect system results is known as?
    A. Recovery testing
    B. Recovery strategy
    C. Recovery run
    D. Failure recovery

48. In information system a security flaw, glitch, or weakness can be found in software code and exploited by an attacker. Which term refers to cyclic practice for identifying, classifying and solving the vulnerabilities in a system?
    A. Vulnerability measurement
    B. Vulnerability management
    C. Bug bounty
    D. Bug protection

49. Which of the following is a set of policies concerning various information security management developed for managing risk management principles and countermeasures for ensuring security through rules and regulations?
    A. Information Security Management System
    B. Information Server Management System
    C. Information Security Management Software
    D. Internet Server Management System

50. A written report is the primary deliverable from a penetration testing engagement. Which of the following entails executive summary, methodology, and findings of a pen test report?
    A. Report audience
    B. Report content
    C. Secure distribution
    D. Note-taking

……..

CISSE ADVANCED LEVEL

ELECTIVE II

INFORMATION SYSTEMS SECURITY

TUESDAY: 6 December 2022. Afternoon Paper. **Time Allowed: 2 hours.**

Answer ALL questions by indicating the letter (A, B, C or D) that represents the correct answer. The paper is made up of fifty (50) multiple choice questions. Each question is allocated two (2) marks.

1. The type of approach based information technology audit where the auditor is provided with detailed information regarding the organisation that is to be audited is referred to as?
   A. Black box audit
   B. White box audit
   C. Grey box audit
   D. Blue box audit

2. IT security audit is important for the following reasons **EXCEPT**?
   A. To keep the organisation updated with security measures
   B. To identify physical security vulnerabilities.
   C. To identify security opportunities before the hackers
   D. To help in formulating new security policies for the organisation

3. Which of the following is the second phase in the penetration testing process of the Information System audit?
   A. Gaining system access
   B. Scanning
   C. Planning and Reconnaissance
   D. Persistent Access

4. The type of auditing technique where the auditor verifies accounting transactions with documentary evidence is referred to as?
   A. Vouching
   B. Confirmation
   C. Reconciliation
   D. Testing

5. The motivation of internal threat that involves stealing information for another organisation is referred to as?
   A. Fraud
   B. Sabotage
   C. Espionage
   D. Revenge

6. The physical control that requires employees to tap their ID pass on a reader that will unlock the gate and allow them to pass through is referred to as?
   A. Turnstiles
   B. Electronic Doors
   C. Mantraps
   D. Security Guards

7. Which of the following is **NOT** a penetration testing method?
   A. External testing
   B. Triple blind testing
   C. Internal testing
   D. Blind testing

8. A cyber security attack that involves the creation of a false stream or modification of the data stream is referred to as?
   A. Active attack
   B. Passive attack
   C. Cryptographic attack
   D. Encryption

9. A cyber security methodology that combines best practices and technology to prevent the exposure of sensitive information outside of an organisation is referred to as?
   A. Email security
   B. Sandboxing
   C. Intrusion prevention system
   D. Data loss prevention

10. Robust network security will protect against all of the following **EXCEPT?**
   A. Worms
   B. Viruses
   C. Intrusion
   D. Spyware

11. A social engineering attack technique where the attacker uses a false promise to lure users into a trap that steals their personal information is referred to as?
   A. Baiting
   B. Scareware
   C. Pretexting
   D. Phishing

12. During network security penetration testing, the results of the penetration test are compiled into a report detailing all of the following **EXCEPT?**

   A. None sensitive data that was accessed
   B. Specific vulnerabilities that were exploited
   C. Sensitive data that was accessed
   D. The amount of time the pen tester was able to remain in the system undetected

13. The type of audit report which shows that the company is not compliant with any of the GAAP's guidelines for financial reporting and thus portrays gross misstatements on their assets and liabilities is referred to as?
   A. Disclaimer report
   B. Adverse audit report
   C. Qualified report
   D. Clean report

14. In the structure of the auditor's report, the auditor's opinion section will include the following details **EXCEPT?**
   A. Auditing timespan
   B. Financial records
   C. A statement on the company's compliance with GAAP guidelines
   D. Auditing cost

15. Which of the following is the step that involves prioritizing the incident and providing initial support to incident management?
   A. Incident detection
   B. Incident starter
   C. Prioritisation and support
   D. Investigation and diagnosis

16. The area of IT service management where the IT team returns a service to normalcy after disruption as fast as possible is referred to as?
    A. IT incident plan
    B. IT incident management
    C. IT incident control
    D. IT incident monitor

17. The information systems security goal which ensures the accuracy and reliability of the information stored on the computer systems is referred to as?
    A. Integrity
    B. Confidentiality
    C. Availability
    D. Conformity

18. With reference to the organizational information assets and classification, when the loss of confidentiality, integrity or availability is be expected to have a limited adverse effect on organizational operations, the impact is considered to be?
    A. Low
    B. Moderate
    C. High
    D. Average

19. The process of organising data into categories that ensure easy retrieval, sorting and storage of data is referred to as?
    A. Data cleansing
    B. Data classification
    C. Data modification
    D. Data preprocessing

20. In order to keep customer dissatisfaction at bay and reduce recovery timescales, every business needs to incorporate the following **EXCEPT?**
    A. Plan an effective response
    B. Ensure effective communication
    C. Identify potential risks and vulnerabilities
    D. Build a data processing structure

21. Which of the following is **NOT** one of the four P's of business continuity planning?
    A. Providers
    B. Plans
    C. People
    D. Premises

22. Which of the following is the second step in the development of an effective business continuity plan?
    A. Identification of threats
    B. Adoption of controls for prevention and mitigation
    C. Conducting a business impact analysis
    D. Identification of risks

23. Which type of backup subscription service will allow a business to recover quickest?
    A. A cold site
    B. A warm site
    C. A hot site
    D. A mobile or rolling backup service

24. An activity that can help to examine the impact of different disasters on an organisation's safety, finances, marketing, business reputation, legal compliance and quality assurance is referred to as?
    A. Business impact analysis
    B. Risk analysis
    C. Business process
    D. Disaster recovery

25. Which of the following **CANNOT** be classified as a component of disaster recovery plan?
    A. Policy statement
    B. Key personnel and disaster recovery team
    C. Directions on how to reach the recovery site
    D. A list of hardware and systems that staff will use in the recovery

26. A location that can be used by an organisation to recover and restore its data, technology infrastructure and operations when the primary data centre is unavailable is referred to as?
    A. Disaster recovery point
    B. Disaster recovery home
    C. Disaster recovery site
    D. Disaster recovery lab

27. Which of the following is **NOT** a reason why an organisation should implement a security policy?
    A. To set clear expectations
    B. To guide in the implementation of user controls
    C. To help in meeting the regulatory requirements
    D. To improve organisational efficiency and help in meeting business objectives

28. Which of the following can be classified as an issue specific security policy?
    A. Bring-your-own-device (BYOD) policy
    B. Multimedia policy
    C. Software policy
    D. Technical policy

29. Which of the following can be classified as controls that include software or hardware mechanisms to protect data?
    A. Administrative controls
    B. Logical controls
    C. Physical controls
    D. Environmental controls

30. Which of the following **CANNOT** be classified as a control function?
    A. Detective controls
    B. Preventive controls
    C. Corrective controls
    D. Administrative controls

31. A security function that involves the application of a method of measurement to one or more entities of a system which incorporates an assessable security property to obtain a measured value is referred to as
    A. Security measure
    B. Security metric
    C. Security value
    D. Security plan

32. Which of the following describes an intentional and malicious effort by an individual to breach the systems of another individual or organisation over the internet?
    A. Cyberattack
    B. Cybersecurity
    C. Cyber vulnerability
    D. Cyberwarfare

33. Which of the following is a type of cybercrime attack initiated by cybercriminals to masquerade as a senior player at an organisation and directly target senior or other important individuals of a given organisation?
    A. Whaling
    B. Smishing
    C. Spear phishing
    D. Vishing

34. Which one of the following access controls entails users assigning access rights based on rules user specify?
A. Mandatory access control (MAC)
B. Attribute Based Access Control (ABAC)
C. Role based Access Control (RBAC)
D. Discretionary access control (DAC)

35. Which one of the following does not fall in the category of digital crime?
A. Fraud and identity theft
B. Information warfare
C. Phishing scams
D. Cyber reconnaissance

36. What is the term that relates to a weakness exhibited in a system or a network?
A. Threat
B. Attack
C. Vulnerability
D. Exploit

37. What is the name of a hacking approach used by Cybercriminals to design fake websites purposely meant to manipulate traffic?
A. Pharming
B. Spamming
C. Clone phishing
D. Cross site scripting

38. What is the mechanism of transforming messages to make them secure and immune to attacks?
A. Stenography
B. Obfuscation
C. Cryptography
D. Cryptonalysis

39. Which of the following tricks a web user into clicking on something different from what the user perceives they are clicking on.
A. Likejacking
B. Clickjacking
C. Cursorjacking
D. Filejacking

40. Which of the following is **NOT** a type of intrusion detection system?
A. Network intrusion detection system
B. DM-based intrusion detection system
C. Host-based intrusion detection system
D. Perimeter intrusion detection system

41. Which of the following is **NOT** a detection method of intrusion prevention systems?
A. Signature-based
B. Statistical anomaly-based
C. Stateful protocol analysis
D. Stateless protocol analysis

42. Information systems security laws and regulations will govern the following **EXCEPT?**
A. Acquisition of information
B. Transmission of information
C. Conversion of information
D. Storage of information

43. Which of the following is **NOT** a guideline for data confidentiality?
    A. Encrypt sensitive files
    B. Manage data access
    C. Logically secure devices and paper documents
    D. Securely dispose of data, devices, and paper records

44. The following are key parts of security governance **EXCEPT**?
    A. Organisational structure
    B. Organisational culture
    C. Roles and responsibilities
    D. Strategic planning

45. An information security governance framework helps in the preparation for risks or events before they occur by forcing users to continually reevaluate critical IT and business functions through all of the following **EXCEPT?**
    A. Threat and vulnerability analysis
    B. Data governance and threat protection
    C. Aligning corporate strategy and IT strategy
    D. Integrated risk management functions

46. Which of the following **BEST** defines the controls over the information technology (IT) environment, computer operations, program development and program changes.
    A. IT general controls
    B. IT application controls
    C. IT environmental controls
    D. IT input controls

47. With reference to information system security, which of the following best describes the consequences that a business will face if there is a successful attack?
    A. Mitigation
    B. Impact
    C. Vulnerability
    D. Risk

48. Which of the following is the fourth stage of the security risk assessment methodology?
    A. Application characterisation
    B. Threat analysis
    C. Risk likelihood determination
    D. Architectural vulnerability assessment

49. Which of the following is **NOT** a management control?
    A. Cybernetic controls
    B. Stochastic controls
    C. Reward and compensation controls
    D. Planning controls

50. Which of the following is **NOT** a type of Secure Sockets Layer (SSL) certificate?
    A. Single domain
    B. Wildcard
    C. Multi-domain
    D. Domain validation

……..

CISSE ADVANCED LEVEL

ELECTIVE II

INFORMATION SYSTEMS SECURITY

TUESDAY: 2 August 2022. Afternoon paper. **Time Allowed: 2 hours.**

The paper is made up of fifty (50) multiple choice questions. Answer ALL questions by indicating the letter (A, B, C or D) that represents the correct answer. Each question is allocated two (2) marks.

1. What do you consider as a primary target for protection by cyber security efforts
   A. Hardware
   B. Software
   C. Personal Information
   D. Financial data (2 marks)

2. Which of the following element of cyber security is the most critical to an organization
   A. Network security
   B. Application security
   C. End-user education
   D. Business continuity planning (2 marks)

3. Which of the following is an integrated method of network security management
   A. Encryption
   B. Hashing
   C. Firewall
   D. Proxy server (2 marks)

4. Vulnerability Assessment (VA) and Penetration Testing (PT) are a useful security management process. What follows a VAPT exercise?
   A. Finding vulnerabilities on the target
   B. Knowledge of the system configurations
   C. Prioritizing fixing of the identified flaws
   D. Responding to the audit queries (2 marks)

5. Firewalls are necessary for securing your network, to ensure that these are successful some additional steps may be required , which of these is a key aid.
   A. Security policies
   B. System logs
   C. Server configurations
   D. User name and passwords (2 marks)

6. Which of the following steps is the most overlooked yet foundation in securing your servers?
   A. Make sure you have a secure password for your root and administrator users
   B. Remove default users from servers
   C. Remove remote access from the default root/administrator accounts
   D. configure your firewall rules for remote access (2 marks)

7. Data Leakage is an intentional or unintentional transmission of data from within the organization to an external unauthorised destination. Which of the following is the most common in organisations?
   A. Accidental Breach
   B. Intentional Breach
   C. System Hack
   D. System Engineering (2 marks)

8. Following are some common cyber attacks that could adversely affect your system.
   A. Malware
   B. Phishing
   C. Password Attacks
   D. Man in the Middle (2 marks)

9. Brute Force helps attackers find out the right credentials by repetitively trying all the permutations and combinations of possible credentials. Which of the following ways is the most effective in preventing this in a timely manner?
   A. Increasing the minimum length for password.
   B. Increasing the password complexity
   C. Limiting the login attempts
   D. Using two factor authentication (2 marks)

10. Port Scanning is the technique used to identify open ports and service available on a host. Which of the following techniques is not applicable for this?
   A. Ping Scan
   B. TCP Connect
   C. Stealth Scanning
   D. Telnet (2 marks)

11. An OSI model is a reference model for how applications communicate over a network. Which of the following statements is true?
   A. The data link layer is responsible for packet forwarding
   B. The network later is responsible for end-to-end communication over the network
   C. The physical layer is responsible for transmission of digital data
   D. The transport layer provides an interface between application and the network (2 marks)

12. Which of the following should the information security professional be most concerned about?
   A. Threats
   B. Vulnerabilities
   C. Risks
   D. Third parties (2 marks)

13. Considering the widespread use of VPNs, which of the following is considered a critical step in the data protection process?
   A. Data sent by client to the VPN point
   B. Data encrypted at the VPN point
   C. Data decrypted at the VPN point
   D. Decrypted data is sent to the client (2 marks)

14. Which is common identity theft vulnerability in a typical call center?
   A. Sharing information online
   B. Sharing passwords
   C. Using computers unattended
   D. Sharing computers (2 marks)

15. Which of the following is not true of white hat hackers
   A. They are hired by companies
   B. They fix vulnerabilities
   C. They exploit security staff
   D. They are skilled individuals (2 marks)

16. Which of the practices below is the most common way of handling man in the middle attacks?
   A. Use VPN
   B. Force HTTPs
   C. Public key pair based authentication
   D. Use of encryption (2 marks)

17. DDOS attacks cause servers to refuse to provide services to genuine clients. Which of the following is a predominant such attack?
    A. Crash attacks
    B. Flooding attacks
    C. Worm attacks
    D. Trojan horse (2 marks)

18. Which of the following is considered an application layer protocol?
    A. TCP
    B. NFS
    C. UDP
    D. ICMP (2 marks)

19. Botnets includes multiple devices in the security breach, which of the following is not a motivation for a botnet.
    A. Steal data
    B. Send spams
    C. DDOs attack
    D. Delay messaging (2 marks)

20. Which of the following components makes the difference in a salted hash value protection mechanism?
    A. The user password
    B. Hash value of the password
    C. Random salt value
    D. The combined value stored in the database (2 marks)

21. Which of the following requires data protection at rest
    A. Database Users
    B. Emails being sent
    C. Network communication
    D. Application logins (2 marks)

22. Which of the following is the primary method used by self-learning security systems
    A. Data mining
    B. Pattern recognition
    C. Natural language processing
    D. High powered computers (2 marks)

23. Which of the following best describes the role of a VLAN
    A. Saves data from prying eyes while in transit
    B. Means to logically segregate networks
    C. Used to connect two points in a secured and encrypted tunnel
    D. Used to extend the capability of network service (2 marks)

24. In a phishing attack the trustworthy person seeks to steal sensitive information through email or instant message. Which of the following user actions expose them to multiple attacks of this nature?
    A. Entering sensitive information in the webpages that you don't trust
    B. Logging off websites
    C. Using complex passwords on emails
    D. Installation of antivirus software with Internet Security (2 marks)

25. SQL injections are used to take over database servers. What do you consider as a primary method to prevent these attacks?
    A. Use prepared statements
    B. User access management
    C. Use Stored Procedures
    D. Validate user input (2 marks)

26. What is the most typical risk of clicking links for e-cards that may be sent to you from a friend inviting you for a birthday
    A. The attachment may contain viruses
    B. Clicking the link may infect the computer
    C. Email address may be faked
    D. The website of origin may not be legitimate (2 marks)

27. Often questions about personal information are optional as they may be used to facilitate suspicious transactions. Which of the following would cause you to be most suspicious
    A. Month of birth
    B. Maiden name
    C. Year of birth
    D. Favorite meal (2 marks)

28. What actions would secure your email account that you access from a public computer?
    A. Use strong passwords
    B. logout of your emails before you leave
    C. clear the cache before you exit
    D. don't use public computers (2 marks)

29. If you experience a situation when your computer screen starts to move around on its own and click on things on the desktop, what would be an immediate action to take.
    A. Call your co-workers over so they can see
    B. Disconnect your computer from the network
    C. Tell your supervisor
    D. Turn your computer off (2 marks)

30. Which of the following passwords pulled from a database meets UCSC's password requirements?
    A. @#$)*&^%
    B. akHGksmLN
    C. UcSc4Evr!
    D. Password1 (2 marks)

31. What would your professional advice be for someone who receives an email from their bank telling them that there is a problem with their bank account and they should follow a link to fix it?
    A. Follow the link and solve the problem
    B. Ignore the email all together
    C. Delete the email
    D. Report the email as spam (2 marks)

32. Which of the following is the most typical cause of hacked passwords?
    A. Out of date software patches
    B. No antivirus software or out of date software
    C. Using easy to guess passwords
    D. Sharing and/or writing passwords down. (2 marks)

33. Which of the following benefits of cyber security management is generally overlooked?
    A. Protection of the business against ransomware, malware, social engineering, and phishing.
    B. Good protection for both data as well as networks
    C. Increase in recovery time after a breach
    D. Prevention of unauthorized users (2 marks)

34. What is the primary function of a firewall?
    A. Protect systems from malware
    B. Prevent remote access to the system
    C. Filter access to content
    D. Manage user access to application (2 marks)

35. Secure Sockets Layer secures information on transit. Which of the following would be critical for a school to protect.
    A. Information in online transactions
    B. Payment made through digital channels
    C. List of students who have registered for courses
    D. Number of applications that are available (2 marks)

36. Which of the following channels is the greatest contributor to data leakage in contemporary organizations?

A. Email
B. optical media
C. laptops
D. USB keys (2 marks)

37. Networking sniffing analyses data packets sent over the network. In which ways does a hacker best utilize this technology?
A. Getting sensitive data such as password
B. Getting list of internal IPs
C. Eavesdrop on chat messages
D. Monitor data package over a network (2 marks)

38. Which of the servers below should the system administrators be most concerned about in their network setup.
A. DNS Server
B. Proxy Server
C. Active Directory Server
D. Database Server (2 marks)

39. Which of the following best describes the process of salting to enhance user access management?
A. Salting uses special characters
B. Salting adds special characters to the password
C. Salting safeguards passwords
D. Salting prevents attackers who know passwords across the system (2 marks)

40. Which of the following represents a limitation of the SSL that it does not address?
A. It verifies the senders identity
B. It provides security for data on the server
C. It protects the server against data breach
D. It handles server side encryption (2 marks)

41. Which of the following cloud services would have the greatest impact when the vulnerabilities are exploited by a threat factor
A. Software as a service
B. Platforms as a service
C. Infrastructure as a service
D. Database as a service (2 marks)

42. Getting insurance is a possible option for handling residual risk, which risk handling mechanism does it represent?
A. Reduce it
B. Avoid it
C. Transfer it
D. Accept it (2 marks)

43. Which of the following cyber attacks can be used by hackers to damage your network
A. Phishing
B. DDoS
C. Man in the middle
D. User ignorance (2 marks)

44. Which of the following certifications may not be relevant for a corporate information security officer?
A. CISA
B. MOUS
C. CISM
D. CISSP (2 marks)

45. A common approach to managing information security is through corporate agreements, which of these is a primary tool that facilitates this?
A. End user license agreements
B. None disclosure agreements
C. Service level agreements
D. Software development agreements (2 marks)

46. Information security management has multiple tenets. Which of these is concerned with system change management?
    A. Availability
    B. Integrity
    C. Confidentiality
    D. Non-repudiation (2 marks)

47. Which of the following steps preceeds the information classification steps
    A. Assignment of security protection
    B. Inventory listing
    C. Asset ownership determination
    D. Classification based on value (2 marks)

48. Which of the following is not considered a management security control:
    A. Conducting security training awareness
    B. Review of the employee lifestyle
    C. Crafting system security policy
    D. Patching of computer servers (2 marks)

49. Which of the following factors may most be overlooked but would cause a delay on the system recovery time?
    A. Weather conditions
    B. Staff availability
    C. Incident declaration and decision
    D. Unavailable system backups (2 marks)

50. Which of the following is the most common source of information that can be used to initiate a cyber-attack when they access a public WIFI.
    A. Emails,
    B. Browsing history
    C. Passwords
    D. Credit card data (2 marks)

……..