Okay, here is a 100-question multiple-choice practice exam designed to help you prepare for the Certified in Cybersecurity (CC) exam. This exam mirrors the domain weights and question format you can expect.

Certified in Cybersecurity (CC) Practice Exam

Instructions: This is a practice exam. Choose the best answer for each question.

Domain 1: Security Principles (26 Questions)

1. Which of the following best describes the principle of **confidentiality**?

    a. Ensuring that data is accurate and trustworthy.
    b. Ensuring that data is accessible when needed.
    c. Ensuring that information is not disclosed to unauthorized individuals, entities, or processes.
    d. Ensuring that actions can be traced back to a specific individual.

2. The "CIA Triad" is a foundational concept in cybersecurity. What do the letters C, I, and A stand for?

    a. Control, Integrity, Authentication
    b. Confidentiality, Integrity, Availability
    c. Certification, Identification, Authorization
    d. Compliance, Information, Access

3. Which security principle aims to ensure that data has not been altered in an unauthorized manner?

    a. Confidentiality
    b. Availability
    c. Non-repudiation
    d. Integrity

4. The concept of "least privilege" means:

    a. Users should have the maximum privileges necessary to perform their job functions.
    b. All users should have the same level of access to systems.
    c. Users should only be given the minimum access rights and permissions needed to perform their job responsibilities.
    d. Privileges should be reviewed and audited annually.

5. What is the primary purpose of a security awareness program?

    a. To implement new security technologies.
    b. To punish employees who violate security policies.
    c. To educate employees about security risks and their responsibilities in protecting company assets.
    d. To solely focus on technical staff for security training.

6. Which of the following is an example of a **threat** in cybersecurity?

    a. An unpatched software vulnerability.
    b. A malicious actor attempting to exploit a weakness.
    c. The potential financial loss from a data breach.
    d. A security control like a firewall.

7. A weakness in a system or its design that can be exploited by a threat is known as a:

    a. Risk
    b. Vulnerability
    c. Impact
    d. Countermeasure

8. What is **risk assessment**?

    a. The process of implementing security controls.
    b. The process of identifying, analyzing, and evaluating risks.
    c. The process of responding to a security incident.
    d. The process of developing security policies.

9. Which of the following describes **risk acceptance**?

    a. Implementing controls to reduce the likelihood or impact of a risk.
    b. Shifting the impact of a risk to a third party, such as by purchasing insurance.
    c. Deciding not to take action to address a risk, often because the cost of mitigation outweighs the potential impact.
    d. Eliminating the source of the risk.

10. What is the term for a security event that has been confirmed to be a breach or an attack?

a. An alert
b. An incident
c. A vulnerability
d. A threat

11. Which of the following is a key component of **due care**?

a. Establishing formal policies and procedures.
b. The ongoing maintenance and operational activities that ensure security controls remain effective.
c. Ignoring identified risks.
d. Documenting every single employee action.

12. Establishing written security policies, standards, and procedures is an example of exercising:

a. Due process
b. Due diligence
c. Risk avoidance
d. Threat modeling

13. What does the principle of **defense in depth** involve?

a. Relying on a single, strong security control.
b. Implementing multiple layers of security controls, so if one layer fails, another may still protect the assets.
c. Focusing security efforts only on the network perimeter.
d. Prioritizing physical security over logical security.

14. Which of the following best defines **non-repudiation**?

a. Ensuring data is available when needed.
b. Preventing unauthorized disclosure of information.
c. Providing proof of the integrity and origin of data, and ensuring that an action cannot be denied by the actor who performed it.
d. Ensuring data is accurate and complete.

15. What is the primary goal of data classification?

a. To make all data publicly accessible.
b. To determine the appropriate level of security controls needed to protect data based on its sensitivity and value.
c. To encrypt all organizational data by default.
d. To reduce the amount of data an organization stores.

16. A company's acceptable use policy (AUP) typically outlines:

a. The procedures for incident response.
b. The rules and guidelines for how employees are permitted to use company IT resources.
c. The steps for recovering from a disaster.
d. The technical specifications of the company's network infrastructure.

17. What is the term for the likelihood of a threat exploiting a vulnerability, combined with the potential impact?

a. Control
b. Asset
c. Risk
d. Policy

18. Which of the following is a type of **physical security control**?

a. Firewall
b. Encryption
c. Security guard
d. Antivirus software

19. Which of the following is a type of **technical (or logical) security control**?

a. Fences
b. Security policies
c. Access control lists (ACLs)
d. Background checks

20. From a security perspective, what is the primary concern with "shadow IT"?

a. It increases IT department workload.
b. It involves the use of IT systems, devices, software, applications, and services without explicit IT department approval, potentially bypassing security controls.
c. It often leads to higher software licensing costs.

d. It primarily affects employee productivity.

21. What is the purpose of a privacy policy?

a. To outline how an organization collects, uses, discloses, and manages customer or client data.
b. To define employee responsibilities for using company equipment.
c. To describe the organization's network topology.
d. To list the company's approved software vendors.

22. Which of the following is an example of a **deterrent control**?

a. An intrusion detection system (IDS) alarm.
b. A "Beware of Dog" sign or visible security cameras.
c. Data backups.
d. Encryption of data at rest.

23. The process of verifying the identity of a user, system, or service is known as:

a. Authorization
b. Accounting
c. Authentication
d. Auditing

24. Which security principle is primarily concerned with making sure that information and systems are usable for their intended purpose when required?

a. Confidentiality
b. Integrity
c. Availability
d. Non-repudiation

25. What is the primary purpose of security governance?

a. To select specific security software.
b. To ensure that security strategies are aligned with business objectives and that security efforts are effectively managed.
c. To conduct daily security scans.
d. To respond to individual security alerts.

26. Which of the following best describes a **security policy**?

a. A detailed step-by-step guide for performing a specific security task.
b. A high-level statement from management that defines an organization's security goals and objectives.
c. A technical configuration setting for a firewall.
d. A list of approved software for company use.

Domain 2: Business Continuity (BC), Disaster Recovery (DR) & Incident Response Concepts (10 Questions)

27. What is the primary goal of a Business Continuity Plan (BCP)?

a. To restore IT infrastructure after a disaster.
b. To ensure that critical business functions can continue during and after a disruption.
c. To investigate security incidents.
d. To prosecute individuals who attack company systems.

28. Which plan specifically focuses on the recovery of IT systems and infrastructure after a major disruption?

a. Business Continuity Plan (BCP)
b. Incident Response Plan (IRP)
c. Disaster Recovery Plan (DRP)
d. Risk Management Plan

29. What is a Business Impact Analysis (BIA) primarily used for?

a. To identify and analyze the potential effects of a disruptive event on critical business functions.
b. To select specific backup software.
c. To define user access roles.
d. To test network security controls.

30. The **Recovery Time Objective (RTO)** refers to:

a. The maximum amount of data that an organization can afford to lose.
b. The target time set for the restoration of IT and business functions after a disaster occurs.
c. The frequency with which backups should be performed.
d. The point in time to which data must be restored.

31. The **Recovery Point Objective (RPO)** defines:

    a. The target time to get a system back online.
    b. The location of the alternate recovery site.
    c. The maximum acceptable amount of data loss an organization can tolerate, measured in time.
    d. The individuals responsible for declaring a disaster.

32. Which of the following is a common type of alternate processing site that is fully equipped and configured, ready to operate within hours?

    a. Cold site
    b. Warm site
    c. Hot site
    d. Mobile site

33. The first phase in a typical Incident Response Plan (IRP) is:

    a. Containment
    b. Eradication
    c. Preparation
    d. Recovery

34. During which phase of incident response would an organization attempt to remove the cause of the incident (e.g., malware)?

    a. Preparation
    b. Identification
    c. Containment
    d. Eradication

35. What is the primary purpose of the "lessons learned" phase in incident response?

    a. To assign blame for the incident.
    b. To improve security measures and the incident response process itself based on the experience.
    c. To calculate the financial impact of the incident.
    d. To immediately restore all affected systems.

36. Which of the following is crucial for an effective Business Continuity Plan (BCP) and Disaster Recovery Plan (DRP)?

    a. Keeping the plans secret from all employees.
    b. Never updating the plans once they are created.
    c. Regular testing, training, and updating of the plans.
    d. Focusing solely on natural disasters.

Domain 3: Access Controls Concepts (22 Questions)

37. Which of the following is NOT a primary type of access control?

    a. Preventive
    b. Detective
    c. Corrective
    d. Predictive

38. What is the primary purpose of **authentication** in access control?

    a. To determine what resources a user can access.
    b. To verify the claimed identity of a user, system, or service.
    c. To keep a record of user actions.
    d. To assign security labels to data.

39. Which authentication factor is based on "something you know"?

    a. Fingerprint scan
    b. Smart card
    c. Password
    d. Security token (hardware)

40. A fingerprint scan is an example of which type of authentication factor?

    a. Something you know
    b. Something you have
    c. Something you are (biometrics)
    d. Somewhere you are (location)

41. Multi-Factor Authentication (MFA) requires:

a. At least two different passwords.
b. Two or more different types of authentication factors (e.g., something you know and something you have).
c. A very long and complex password.
d. Authentication from multiple devices.

42. What does **authorization** determine in the context of access control?

a. Whether a user's password is correct.
b. The identity of the user.
c. What actions an authenticated user is allowed to perform on a particular resource.
d. When a user last logged in.

43. Which access control model grants access based on a user's job function or role within an organization?

a. Discretionary Access Control (DAC)
b. Mandatory Access Control (MAC)
c. Role-Based Access Control (RBAC)
d. Rule-Based Access Control

44. In a Discretionary Access Control (DAC) model, who typically has the authority to grant or deny access to resources?

a. A central security administrator only.
b. The operating system.
c. The owner of the resource.
d. The security system based on pre-defined rules.

45. Which access control model uses security labels assigned to objects (files) and subjects (users) to determine access?

a. Role-Based Access Control (RBAC)
b. Discretionary Access Control (DAC)
c. Mandatory Access Control (MAC)
d. Attribute-Based Access Control (ABAC)

46. What is the principle of "separation of duties"?

a. All critical tasks should be performed by a single, highly trusted individual.
b. No single individual should have control over all aspects of a critical task or process, to prevent fraud or error.
c. Employees should be physically separated based on their department.
d. Users should only have access to their own data.

47. Which of the following is an example of a logical access control?

a. A locked door
b. A security guard
c. A password policy
d. A fence

48. User provisioning refers to:

a. The process of training users on security awareness.
b. The process of creating, managing, and deactivating user accounts and their access rights.
c. The process of monitoring user activity.
d. The process of assigning passwords to users.

49. What is the term for reviewing user access rights and privileges to ensure they are still appropriate and necessary?

a. User provisioning
b. Access recertification or entitlement review
c. Password cracking
d. Identity federation

50. Which of the following best describes "implicit deny"?

a. All access is allowed by default unless explicitly denied.
b. If a specific access permission is not explicitly granted, it should be denied.
c. Users can grant access to resources they own.
d. Access decisions are based on user roles.

51. What type of access control uses characteristics (attributes) of the user, resource, and environment to make access decisions?

a. Mandatory Access Control (MAC)
b. Discretionary Access Control (DAC)
c. Role-Based Access Control (RBAC)

d. Attribute-Based Access Control (ABAC)

52. Single Sign-On (SSO) allows a user to:

a. Use the same password for all personal and work accounts.
b. Authenticate once and gain access to multiple related but independent software systems.
c. Bypass all authentication requirements.
d. Share their login credentials with team members.

53. What is the primary risk associated with weak password policies?

a. Increased network bandwidth consumption.
b. Higher likelihood of unauthorized access through guessed or cracked passwords.
c. Slower system performance.
d. More frequent software updates.

54. Which of these is "something you have" for authentication?

a. A PIN
b. A retina scan
c. A smart card or hardware token
d. A passphrase

55. The process of keeping track of a user's activity while accessing network resources is called:

a. Authentication
b. Authorization
c. Accounting (or Auditing)
d. Administration

56. What is a common issue with default account credentials?

a. They are usually very complex and hard to remember.
b. They are often publicly known and provide an easy entry point for attackers if not changed.
c. They automatically expire after a short period.
d. They provide the least privileged access by default.

57. Which type of access control is typically enforced by the operating system and relies on security labels?

a. Discretionary Access Control (DAC)
b. Role-Based Access Control (RBAC)
c. Mandatory Access Control (MAC)
d. Rule-Based Access Control

58. When a user leaves a company, what is the most important access control step to take regarding their accounts?

a. Change their password.
b. Monitor their account for suspicious activity.
c. Disable or delete their accounts promptly.
d. Reduce their access privileges.

Domain 4: Network Security (24 Questions)

59. What is the primary function of a firewall?

a. To detect and remove malware from computers.
b. To filter network traffic based on a defined set of security rules, acting as a barrier between a trusted internal network and an untrusted external network.
c. To encrypt data transmitted over the network.
d. To authenticate users accessing the network.

60. Which type of firewall inspects the full content of network packets, including application layer data?

a. Packet filtering firewall
b. Stateful inspection firewall
c. Next-Generation Firewall (NGFW) or Application Layer Firewall
d. Circuit-level gateway

61. An Intrusion Detection System (IDS) primarily:

a. Prevents intrusions from occurring.
b. Monitors network or system activities for malicious activities or policy violations and produces reports or alerts.
c. Encrypts all network traffic.
d. Manages user access to network resources.

62. What is the main difference between an Intrusion Detection System (IDS) and an Intrusion Prevention System (IPS)?

a. An IDS only logs malicious activity, while an IPS encrypts it.
b. An IDS is host-based, while an IPS is network-based.
c. An IDS detects and alerts, while an IPS can also take action to block or stop the detected malicious activity.
d. An IDS uses signature-based detection, while an IPS uses anomaly-based detection.

63. What is a DMZ (Demilitarized Zone) in network security?

a. A highly secured internal network segment.
b. A part of the network that is completely isolated from the internet.
c. A perimeter network segment that is isolated from the internal secure network and provides a buffer zone for servers that need to be accessible from the internet (e.g., web servers, email servers).
d. A network that uses military-grade encryption.

64. Which network protocol is commonly used to securely manage and configure network devices remotely?

a. Telnet
b. HTTP
c. SSH (Secure Shell)
d. FTP

65. What is the purpose of Network Address Translation (NAT)?

a. To encrypt IP addresses.
b. To assign public IP addresses to every device on a private network.
c. To translate private IP addresses used within an internal network to a public IP address (or addresses) for routing on the internet, often hiding the internal network structure.
d. To filter malicious IP addresses.

66. A Virtual Private Network (VPN) is primarily used to:

a. Increase internet connection speed.
b. Create a secure, encrypted connection over a less secure network, such as the internet.
c. Block advertisements on websites.
d. Distribute malware.

67. Which of the following is a common wireless security protocol that provides strong encryption for Wi-Fi networks?

a. WEP (Wired Equivalent Privacy)
b. WPA (Wi-Fi Protected Access)
c. WPA2 (Wi-Fi Protected Access 2) or WPA3
d. SSID (Service Set Identifier)

68. What is a MAC address?

a. A logical address used for routing packets on the internet.
b. A physical hardware address uniquely identifying a network interface card (NIC).
c. A type of encryption algorithm.
d. A security protocol for email.

69. Port scanning is a technique used to:

a. Identify open ports and services running on a network host.
b. Encrypt network traffic.
c. Block unwanted network connections.
d. Increase network performance.

70. What is the purpose of a proxy server?

a. To directly connect internal clients to the internet without filtering.
b. To act as an intermediary for requests from clients seeking resources from other servers, often used for filtering, logging, and caching.
c. To assign IP addresses to clients.
d. To encrypt all network traffic by default.

71. Which OSI model layer is responsible for routing packets between networks?

a. Layer 1 (Physical Layer)
b. Layer 2 (Data Link Layer)
c. Layer 3 (Network Layer)
d. Layer 4 (Transport Layer)

72. TCP (Transmission Control Protocol) is a:

a. Connectionless protocol that is fast but unreliable.
b. Connection-oriented protocol that provides reliable, ordered, and error-checked delivery of a stream of octets.
c. Protocol used for assigning IP addresses.
d. Protocol used for resolving domain names to IP addresses.

73. DNS (Domain Name System) is used to:

a. Encrypt web traffic.
b. Translate human-readable domain names (e.g., www.google.com (https://www.google.com)) into machine-readable IP addresses.
c. Filter network traffic.
d. Manage user authentication.

74. What type of network attack involves overwhelming a target system with a flood of traffic from multiple compromised computer systems (a botnet)?

a. Phishing
b. Man-in-the-Middle (MitM)
c. Distributed Denial of Service (DDoS)
d. SQL Injection

75. "Honeypots" are systems designed to:

a. Securely store sensitive company data.
b. Attract and trap attackers, diverting them from legitimate targets and allowing their activities to be studied.
c. Encrypt wireless network traffic.
d. Authenticate users to the network.

76. What is the primary function of an ARP (Address Resolution Protocol)?

a. To route packets between different networks.
b. To resolve IP addresses to MAC addresses on a local network.
c. To encrypt data packets.
d. To assign IP addresses dynamically.

77. Which of the following is a security concern associated with open Wi-Fi networks?

a. They are always faster than secured networks.
b. Data transmitted over them is typically not encrypted by default, making it susceptible to eavesdropping.
c. They require complex passwords to access.
d. They are immune to denial-of-service attacks.

78. The practice of segmenting a network into smaller, isolated sub-networks is known as:

a. Network bonding
b. Network bridging
c. Network segmentation or subnetting
d. Network address translation

79. What is the primary purpose of DHCP (Dynamic Host Configuration Protocol)?

a. To resolve domain names to IP addresses.
b. To automatically assign IP addresses and other network configuration parameters to devices on a network.
c. To encrypt network communications.
d. To filter network traffic based on port numbers.

80. Which layer of the OSI model is responsible for the physical transmission of data bits?

a. Layer 1 (Physical Layer)
b. Layer 2 (Data Link Layer)
c. Layer 7 (Application Layer)
d. Layer 4 (Transport Layer)

81. A common technique attackers use to make their traffic appear to originate from a different IP address is called:

a. IP routing
b. IP spoofing
c. IP fragmentation
d. IP multicasting

82. Which of the following best describes endpoint security?

a. Securing only the network perimeter.
b. Securing end-user devices such as laptops, desktops, and mobile devices.
c. Securing data centers.

d. Securing cloud services.

Domain 5: Security Operations (18 Questions)

83. What is the primary purpose of security logging and monitoring?

a. To slow down network traffic for easier analysis.
b. To record events occurring in an organization's IT systems and networks, and to detect and respond to security incidents.
c. To provide users with access to sensitive data.
d. To automatically fix all security vulnerabilities.

84. A Security Information and Event Management (SIEM) system is primarily used to:

a. Manage user passwords.
b. Conduct penetration testing.
c. Collect, correlate, and analyze log data from various sources to detect and respond to security threats.
d. Deploy software updates.

85. What is vulnerability scanning?

a. A manual process of exploiting known vulnerabilities.
b. An automated process of proactively identifying security weaknesses in systems and networks.
c. The process of responding to a security incident.
d. The process of creating data backups.

86. Penetration testing is best described as:

a. A passive scan for known vulnerabilities.
b. A simulated cyberattack against your computer system to check for exploitable vulnerabilities, often involving manual exploitation attempts.
c. The daily monitoring of security logs.
d. The installation of antivirus software.

87. What is the purpose of a patch management program?

a. To develop new software features.
b. To identify, acquire, test, and install software updates (patches) to fix vulnerabilities and improve functionality.
c. To manage physical security patches on equipment.
d. To monitor network traffic for malicious patches.

88. Which of the following is a key step in a typical change management process?

a. Implementing changes without documentation.
b. Avoiding any testing of changes before deployment.
c. Reviewing and approving proposed changes, testing them, and having a rollback plan.
d. Making changes directly in the production environment during business hours.

89. Digital forensics is the process of:

a. Predicting future cyberattacks.
b. Collecting, preserving, analyzing, and presenting digital evidence in a legally admissible manner.
c. Developing security software.
d. Erasing all data from compromised systems.

90. What is the "chain of custody" in digital forensics?

a. The process of encrypting evidence.
b. A chronological documentation trail showing the seizure, custody, control, transfer, analysis, and disposition of physical or electronic evidence.
c. The network path taken by malicious traffic.
d. A list of all users who accessed a system.

91. Which of the following is a common indicator of compromise (IOC)?

a. A planned system maintenance window.
b. Unusual outbound network traffic or logins from unexpected geographic locations.
c. Successful user logins during normal business hours.
d. Regularly scheduled data backups.

92. What is the primary goal of configuration management in security operations?

a. To allow users to configure their own security settings without oversight.
b. To establish and maintain a consistent and secure configuration for all systems and software.
c. To disable all security configurations for better performance.
d. To frequently change system configurations randomly to confuse attackers.

93. Data loss prevention (DLP) tools are used to:

    a. Recover lost data from backups.
    b. Identify, monitor, and protect sensitive data from being exfiltrated or used in an unauthorized manner.
    c. Encrypt all data on the network.
    d. Increase data storage capacity.

94. In the context of security operations, what is an "event"?

    a. Any confirmed security breach.
    b. Any observable occurrence in a system or network.
    c. Only malicious activities.
    d. A planned company gathering.

95. What is the primary purpose of security audits?

    a. To punish employees for policy violations.
    b. To independently assess the effectiveness of an organization's security controls, policies, and procedures against a defined standard.
    c. To develop new security policies.
    d. To conduct real-time incident response.

96. Which of the following is crucial for secure software development?

    a. Writing code as quickly as possible, without security reviews.
    b. Incorporating security considerations and testing throughout the entire software development lifecycle (SDLC).
    c. Relying solely on developers to find and fix their own security flaws.
    d. Avoiding the use of any third-party libraries.

97. User awareness training is a critical component of security operations because:

    a. It fulfills a compliance checkbox with minimal effort.
    b. Users are often the first line of defense and can be targets for social engineering attacks.
    c. It replaces the need for technical security controls.
    d. It is only necessary for IT staff.

98. What is the primary objective of a "red team" exercise?

    a. To defend the organization's network against simulated attacks.
    b. To test the organization's detection and response capabilities by mimicking real-world attackers' tactics, techniques, and procedures (TTPs).
    c. To implement new security controls.
    d. To conduct routine vulnerability scanning.

99. What is the role of a "blue team" in cybersecurity exercises?

    a. To simulate attacks on the organization.
    b. To defend against real or simulated attacks, test incident response plans, and identify areas for security improvement.
    c. To develop new attack tools.
    d. To manage the organization's budget for security.

100. Why is it important to have an asset inventory in security operations?

    a. It is primarily for financial accounting purposes.
    b. To know what assets (hardware, software, data) the organization has, where they are located, and their value or criticality, in order to effectively protect them.
    c. To track employee attendance.
    d. To list all potential vendors.

End of Practice Exam

Answer Key: *(I will provide the answer key after you've had a chance to go through the questions, or you can request it when you're ready! This will give you a better practice experience.)*

Note on the real exam: Remember, the actual CC exam will be 2 hours long, with 100 multiple-choice items. A passing grade is 700 out of 1000 points. Starting October 1, 2025, the exam will be a variable-length Computer Adaptive Test (CAT) with 100-125 items.

This practice exam is intended to cover the domains and give you a feel for the type of questions. Good luck with your studies for the Certified in Cybersecurity certification! Let me know when you'd like the answer key.

Answer Key: Certified in Cybersecurity (CC) Practice Exam

Domain 1: Security Principles

```
c) Ensuring that information is not disclosed to unauthorized individuals, entities, or processes.
b) Confidentiality, Integrity, Availability
d) Integrity
c) Users should only be given the minimum access rights and permissions needed to perform their job responsibilities.
c) To educate employees about security risks and their responsibilities in protecting company assets.
b) A malicious actor attempting to exploit a weakness.
b) Vulnerability
b) The process of identifying, analyzing, and evaluating risks.
c) Deciding not to take action to address a risk, often because the cost of mitigation outweighs the potential impact.
b) An incident
b) The ongoing maintenance and operational activities that ensure security controls remain effective.
b) Due diligence
b) Implementing multiple layers of security controls, so if one layer fails, another may still protect the assets.
c) Providing proof of the integrity and origin of data, and ensuring that an action cannot be denied by the actor who performed it.
b) To determine the appropriate level of security controls needed to protect data based on its sensitivity and value.
b) The rules and guidelines for how employees are permitted to use company IT resources.
c) Risk
c) Security guard
c) Access control lists (ACLs)
b) It involves the use of IT systems, devices, software, applications, and services without explicit IT department approval, potentia
a) To outline how an organization collects, uses, discloses, and manages customer or client data.
b) A "Beware of Dog" sign or visible security cameras.
c) Authentication
c) Availability
b) To ensure that security strategies are aligned with business objectives and that security efforts are effectively managed.
b) A high-level statement from management that defines an organization's security goals and objectives.
```

Domain 2: Business Continuity (BC), Disaster Recovery (DR) & Incident Response Concepts 27. b) To ensure that critical business functions can continue during and after a disruption. 28. c) Disaster Recovery Plan (DRP) 29. a) To identify and analyze the potential effects of a disruptive event on critical business functions. 30. b) The target time set for the restoration of IT and business functions after a disaster occurs. 31. c) The maximum acceptable amount of data loss an organization can tolerate, measured in time. 32. c) Hot site 33. c) Preparation 34. d) Eradication 35. b) To improve security measures and the incident response process itself based on the experience. 36. c) Regular testing, training, and updating of the plans.

Domain 3: Access Controls Concepts 37. d) Predictive (While predictive analysis is used in security, it's not traditionally listed as a primary type of access control alongside preventive, detective, corrective, and deterrent/compensating). 38. b) To verify the claimed identity of a user, system, or service. 39. c) Password 40. c) Something you are (biometrics) 41. b) Two or more different types of authentication factors (e.g., something you know and something you have). 42. c) What actions an authenticated user is allowed to perform on a particular resource. 43. c) Role-Based Access Control (RBAC) 44. c) The owner of the resource. 45. c) Mandatory Access Control (MAC) 46. b) No single individual should have control over all aspects of a critical task or process, to prevent fraud or error. 47. c) A password policy 48. b) The process of creating, managing, and deactivating user accounts and their access rights. 49. b) Access recertification or entitlement review 50. b) If a specific access permission is not explicitly granted, it should be denied. 51. d) Attribute-Based Access Control (ABAC) 52. b) Authenticate once and gain access to multiple related but independent software systems. 53. b) Higher likelihood of unauthorized access through guessed or cracked passwords. 54. c) A smart card or hardware token 55. c) Accounting (or Auditing) 56. b) They are often publicly known and provide an easy entry point for attackers if not changed. 57. c) Mandatory Access Control (MAC) 58. c) Disable or delete their accounts promptly.

Domain 4: Network Security 59. b) To filter network traffic based on a defined set of security rules, acting as a barrier between a trusted internal network and an untrusted external network. 60. c) Next-Generation Firewall (NGFW) or Application Layer Firewall 61. b) Monitors network or system activities for malicious activities or policy violations and produces reports or alerts. 62. c) An IDS detects and alerts, while an IPS can also take action to block or stop the detected malicious activity. 63. c) A perimeter network segment that is isolated from the internal secure network and provides a buffer zone for servers that need to be accessible from the internet (e.g., web servers, email servers). 64. c) SSH (Secure Shell) 65. c) To translate private IP addresses used within an internal network to a public IP address (or addresses) for routing on the internet, often hiding the internal network structure. 66. b) To create a secure, encrypted connection over a less secure network, such as the internet. 67. c) WPA2 (Wi-Fi Protected Access 2) or WPA3 68. b) A physical hardware address uniquely identifying a network interface card (NIC). 69. a) Identify open ports and services running on a network host. 70. b) To act as an intermediary for requests from clients seeking resources from other servers, often used for filtering, logging, and caching. 71. c) Layer 3 (Network Layer) 72. b) Connection-oriented protocol that provides reliable, ordered, and error-checked delivery of a stream of octets. 73. b) Translate human-readable domain names (e.g., www.google.com (http://www.google.com)) into machine-readable IP addresses. 74. c) Distributed Denial of Service (DDoS) 75. b) Attract and trap attackers, diverting them from legitimate targets and allowing their activities to be studied. 76. b) To resolve IP addresses to MAC addresses on a local network. 77. b) Data transmitted over them is typically not encrypted by default, making it susceptible to eavesdropping. 78. c) Network segmentation or subnetting 79. b) To automatically assign IP addresses and other network configuration parameters to devices on a network. 80. a) Layer 1 (Physical Layer) 81. b) IP spoofing 82. b) Securing end-user devices such as laptops, desktops, and mobile devices.

Domain 5: Security Operations 83. b) To record events occurring in an organization's IT systems and networks, and to detect and respond to security incidents. 84. c) Collect, correlate, and analyze log data from various sources to detect and respond to security threats. 85. b) An automated process of proactively identifying security weaknesses in systems and networks. 86. b) A simulated cyberattack against your computer system to check for exploitable vulnerabilities, often involving manual exploitation attempts. 87. b) To identify, acquire, test, and install software updates (patches) to fix vulnerabilities and improve functionality. 88. c) Reviewing and approving proposed changes, testing them, and having a rollback plan. 89. b) Collecting, preserving, analyzing, and presenting digital evidence in a legally admissible manner. 90. b) A chronological documentation trail showing the seizure, custody, control, transfer, analysis, and disposition of physical or electronic evidence. 91. b) Unusual outbound network traffic or logins from unexpected geographic locations. 92. b) To establish and maintain a consistent and secure configuration for all systems and software. 93. b) Identify, monitor, and protect sensitive data from being exfiltrated or used in an unauthorized manner. 94. b) Any observable occurrence in a system or network. 95. b) To independently assess the effectiveness of an organization's security controls, policies, and procedures against a defined standard. 96. b) Incorporating security considerations and testing throughout the entire software development lifecycle (SDLC). 97. b) Users are often

the first line of defense and can be targets for social engineering attacks. 98. b) To test the organization's detection and response capabilities by mimicking real-world attackers' tactics, techniques, and procedures (TTPs). 99. b) To defend against real or simulated attacks, test incident response plans, and identify areas for security improvement. 100. b) To know what assets (hardware, software, data) the organization has, where they are located, and their value or criticality, in order to effectively protect them.