CyberRookie CSX Fundamentals - Quiz questions

1. **Three common controls used to protect the availability of information are**	Redundancy, backups and access controls
2. **Governance has several goals, including**	Providing strategic direction, Ensuring that objectives are achieved, Verifying that organizational resources are being used appropriately, Ascertaining whether risk is being managed properly.
3. **According to the NIST framework, which of the following are considered key functions necessary for the protection of digital assets?**	Protect, Recover, Identify
4. **The best definition for cybersecurity?**	Protecting information assets by addressing threats to information that is processed, stored or transported by interworked information systems
5. **Cybersecurity role that is charged with the duty of managing incidents and remediation?**	Cybersecurity management
6. **The core duty of cybersecurity is to identify, respond and manage**	risk to an organization's digital assets.
7. **A threat**	is anything capable of acting against an asset in a manner that can cause harm.
8. **A asset**	is something of value worth protecting.
9. **A vulnerability**	is a weakness in the design, implementation, operation or internal controls in a process that could be exploited to violate the system security
10. **The path or route used to gain access to the target asset is known as a**	attack vector
11. **In an attack, the container that delivers the exploit to the target is called**	payload
12. **Policies**	communicate required and prohibited activities and behaviors.
13. **Rootkit**	is a class of malware that hides the existence of other malware by modifying the underlying operating system.
14. **Procedures**	provide details on how to comply with policies and standards.
15. **Guidelines**	contain step-by-step instructions to carry out procedures.
16. **Malware**	also called malicious code, is software designed to gain access to targeted computer systems, steal information or disrupt computer operations.
17. **Standards**	are used to interpret policies in specific situations.
18. **Patches**	are solutions to software programming and coding errors.
19. **Identity Management**	includes many components such as directory services, authentication and authorization services, and user management capabilities such as provisioning and deprovisioning.
20. **The Internet perimeter should**	Detect and block traffic from infected internal end points, Eliminate threats such as email spam, viruses and worms, Control user traffic bound toward the Internet, Monitor and detect network ports for rogue activity.
21. **Transport layer of the OSI**	ensures that data are transferred reliably in the correct sequence
22. **Session layer of the OSI**	coordinates and manages user connections
23. **There key benefits of the DMZ system are**	An intruder must penetrate three separate devices, Private network addresses are not disclosed to the Internet, Internal systems do not have direct access to the Internet
24. **best states the role of encryption within an overall cybersecurity program**	Encryption is an essential but incomplete form of access control

25. **The number and types of layers needed for defense in depth are a function of**	Asset value, criticality, reliability of each control and degree of exposure.
26. **Put the steps of the penetration testing phase into the correct order**	Planning, Discovery, Attack, Reporting
27. **System hardening should implement the principle of**	Least privilege or access control
28. **Which of the following are considered functional areas of network management as defined by ISO?**	Accounting management, Fault management, Performance management, Security management
29. **Virtualization involves**	Multiple guests coexisting on the same server in isolation of one another
30. **Vulnerability management begins with an understanding of cybersecurity assets and their locations, which can be accomplished by**	Maintaining an asset inventory.
31. **Arrange the steps of the incident response process into the correct order**	Preparation, Detection and analysis, Investigation, Mitigation and recovery, Postincident analysis
32. **Which element of an incident response plan involves obtaining and preserving evidence**	Containment
33. **Select three. The chain of custody contains information regarding**	Who had access to the evidence, in chronological order, Proof that the analysis is based on copies identical to the original evidence, The procedures followed in working with the evidence
34. **NIST defines a Threat as a**	"violation or imminent threat of violation of computer security policies, acceptable use policies, or standard security practices."
35. **Select all that apply. A business impact analysis (BIA) should identify**	The estimated probability of the identified threats actually occurring, The efficiency and effectiveness of existing risk mitigation controls, A list of potential vulnerabilities, dangers and/or threats.
36. **Cloud computing**	is defined as "a model for enabling convenient, on-demand network access to a shared pool of configurable resources (e.g., networks, servers, storage, applications and services) that can be rapidly provisioned and released with minimal management or service provider interaction
37. **Select all that apply. Which of the following statements about advanced persistent threats (APTs) are true?**	APTs typically originate from sources such as organized crime groups, activists or governments, APTs use obfuscation techniques that help them remain undiscovered for months or even years, APTs are often long-term, multi-phase projects with a focus on reconnaissance
38. **Smart devices, BYOD strategies and freely available applications and services are all examples of:**	The reorientation of technologies and services designed around the individual end user.
39. **Choose three. Which types of risk are typically associated with mobile devices?**	Organizational risk, Technical risk, Physical risk
40. **Which three elements of the current threat landscape have provided increased levels of access and connectivity, and therefore increased opportunities for cybercrime**	Cloud computing, social media and mobile computing
41. **To which of the following layers of the Open Systems Interconnect (OSI) model would one map Ethernet?**	Data Link
42. **Which of the following interpret requirements and apply them to specific situations?**	Standards

43. **Business continuity plans (BCPs) associated with organizational information systems should be developed primarily on the basis of:**	Business needs
44. **A segmented network**	Consists of two or more security zones
45. **Which cybersecurity principle is most important when attempting to trace the source of malicious activity?**	Nonrepudiation
46. **Which of the following offers the strongest protection for wireless network traffic?**	Wireless Protected Access 2 (WPA2)
47. **Outsourcing poses the greatest risk to an organization when it involves:**	Core business functions
48. **Risk assessments should be performed**	On a regular basis
49. **Maintaining a high degree of confidence regarding the integrity of evidence requires a(n):**	Chain of custody
50. **A firewall that tracks open connection-oriented protocol sessions is said to be:**	Stateful
51. **During which phase of the system development lifecycle (SDLC) should security first be considered?**	Planning
52. **A cybersecurity architecture designed around the concept of a perimeter is said to be:**	System-centric
53. **A passive network hub operates at which layer of the OSI model?**	Physical
54. **Updates in cloud-computing environments can be rolled out quickly because the environment is:**	Homogeneous
55. **During which phase of the six-phase incident response model is the root cause determined?**	Eradication
56. **The attack mechanism directed against a system is commonly called a(n):**	Payload
57. **Where should an organization's network terminate virtual private network (VPN) tunnels?**	At the perimeter, to allow for effective internal monitoring
58. **In practical applications:**	Asymmetric key encryption is used to securely obtain symmetric keys
59. **Which two factors are used to calculate the likelihood of an event?**	Threat and vulnerability
60. **What is one advantage of a firewall implemented in software over a firewall appliance?**	Flexibility
61. **A business continuity plan (BCP) is not complete unless it includes:**	Detailed procedures
62. **Under the US-CERT model for incident categorization, a CAT-3 incident refers to which of the following?**	Malicious code
63. **An interoperability error is what type of vulnerability?**	Emergent
64. **Securing Supervisory Control and Data Acquisition (SCADA) systems can be challenging because they**	Operate in specialized environments and often have non-standard design elements
65. **Virtual systems should be managed using a dedicated virtual local area network (VLAN) because**	Insecure protocols could result in a compromise of privileged user credentials
66. **Describes the activities required to identify the occurrence of a cybersecurity incident**	Security continuous monitoring, detection and evaluating anomalies/incidents
67. **This key function ensures that organizational objectives and stakeholder needs are aligned with desired outcomes through effective decision making and prioritization.**	Governance
68. **The primary objective of cybersecurity is**	Protecting a company's digital assets
69. **The activity that ensures business processes continue after a security incident**	Recovery
70. **Which is associated with identifying digital assets**	Asset management

71. **Responsibilities and/or duties of Governance, Risk Management and Compliance (GRC)**	Adherence to required laws and regulations, Implementation of required procedures, Development of internal controls to mitigate risk, Adherence to voluntary contractual requirements.
72. **In most information security organizations, which role sets the overall strategic direction**	Board of Directors
73. **Governance involves all of the following except**	Implement contractual obligations
74. **Governance involves all of the following**	Provide strategic direction, Ensure responsible use of company resources, Evaluate whether risk is managed appropriately
75. **Which role is generally responsible for the design, implementation, management processes and technical controls within a security organization**	Cybersecurity practitioners
76. **Which of the following falls within the scope of risk management**	Cyber risk, investment risk and financial risk
77. **Which term describes the overall structure designed to protect an organization from disclosure of information to unauthorized users, improper modification of data, and non-access to systems**	Information security
78. **The following statement is false:**	Cybersecurity includes protection of paper documents
79. **All of the following statements are true:**	Cybersecurity is a component of information security, Cybersecurity deals with the protection of digital assets, Cybersecurity should align with enterprise information security objectives
80. **Risk management involves which of the following activities**	Recognizing risk, Assessing impact and likelihood of risk, Developing strategies to mitigate risk
81. **Risk management does not involve**	Ensuring information security objectives are achieved
82. **Cybersecurity involves the protection of the following digital assets**	Information that is processed, stored or transported within internetworked information systems
83. **Which terms describe the overall concept of information security?**	Ongoing, Evolving, Systemic
84. **Potential consequences of lack of confidentiality except**	Fraud
85. **Potential consequences of lack of confidentiality**	Disclosure of information protected by privacy laws, Legal action against the enterprise, Interference with national security
86. **The degree to which a user or program can create, modify, read, or write to a file is called**	File permission
87. **Which information security component considers the level of sensitivity and legal requirements and is subject to change over time**	Confidentiality
88. **Authentication is defined as**	The act of verifying identity, The act of verifying a user's eligibility to access computerized information
89. **Establishment and maintenance of user profiles that define the authentication, authorization and access controls for each user is called**	Identity management
90. **A cryptology tool used to prove message integrity using algorithms to create unique numeric values**	Hashes
91. **Potential consequences of lack of integrity**	Inaccuracy, Erroneous decisions, Fraud
92. **Integrity is described as**	Protection of information from unauthorized modification
93. **Methods of control can help protect integrity**	Logging, Digital Signatures, Hashes, Encryption

94.	**Which type of documentation records details of information or events in an organized record-keeping system, usually sequenced in the order in which they occurred**	Log
95.	**A week of severe rainstorms has flooded your company's building. All servers have been ruined. It is estimated that business will be down for 3 weeks. This is an example of**	Lack of availability
96.	**When two or more controls work in parallel to protect an asset, it is called**	Redundancy
97.	**Types of backups**	Full, incremental and differential
98.	**A differential backup**	Only copies files that have changed since last full backup
99.	**Potential consequences resulting from lack of availability include**	Loss of functionality and operational effectiveness, Loss of productive time, Interference with enterprise's objectives
100.	**The concept that a message or other piece of information is genuine is called**	Nonrepudiation
101.	**Describe authentication**	The act of verifying identity, Verification of the correctness of a piece of data, Designed to protect against fraudulent logon activity, Verifying a user's eligibility to access computerized information
102.	**Nonrepudiation is implemented through which methods**	Transactional logs, Digital signatures
103.	**The process of converting plaintext messages, applying a mathematical function to them and producing ciphertext messages is called:**	Encryption
104.	**What control mechanism defines authentication and authorization protocols for users?**	Access controls