Review (Self-Assessment) Question Answer Key

Course Title:	**ITG250: Cybersecurity Audit School**
CPE Requirement:	**32**
Total Questions Needed:	**96**

Episode	Topic Area		Question	Answer A	Answer B	Answer C	Answer D	Correct Answer			Explanations
1.1	Cybersecurity Key Concepts	1	This US Federal Agency defines Cybersecurity as the "Prevention of damage to, protection of, and restoration of computers, electronic communications systems, electronic communications services, wire communication, and electronic communication, including information contained therein, to ensure its availability, integrity, authentication, confidentiality, and nonrepudiation":	**National Institute of Star**	National Initiative for Security and Terminology (NIST).	ACI Learning.	International Standards Organization (ISO).	A	**A**	**Correct**	NIST is the US agency responsible for establishing Cybersecurity Standards.
									B	Incorrect	NIST is the US agency responsible for establishing Cybersecurity Standards.
									C	Incorrect	NIST is the US agency responsible for establishing Cybersecurity Standards.
									D	Incorrect	NIST is the US agency responsible for establishing Cybersecurity Standards.
1.1	Cybersecurity Key Concepts	2	Which of the following is not one of Saltzer and Schroeder's Design Principles?	Economy of mechanism	Fail-safe defaults	**Multi-factor authentication**	Least privilege	C	**A**	Incorrect	While multi-factor authentication is a good security practice today, it's not explicitly contained in the article.
									B	Incorrect	While multi-factor authentication is a good security practice today, it's not explicitly contained in the article.
									C	**Correct**	While multi-factor authentication is a good security practice today, it's not explicitly contained in the article.
									D	Incorrect	While multi-factor authentication is a good security practice today, it's not explicitly contained in the article.
1.2	Cybersecurity History and Breaches	3	What was the name of the malicious worm that infected many corporations on the internet in 2000?	Brain	Morris the cat	**ILOVEYOU**	Stuxnet	C	**A**	Incorrect	The ILOVEYOU Worm traveled across the internet through email.
									B	Incorrect	The ILOVEYOU Worm traveled across the internet through email.
									C	**Correct**	The ILOVEYOU Worm traveled across the internet through email.
									D	Incorrect	The ILOVEYOU Worm traveled across the internet through email.
1.2	Cybersecurity History and Breaches	4	In what year was the Advanced Encryption Standard (AES) published by NIST?	1983	1990	**2001**	2010		**A**	Incorrect	AES was established as the symmetric encryption standard by NIST in 2001, replacing DES.
									B	Incorrect	AES was established as the symmetric encryption standard by NIST in 2001, replacing DES.
									C	**Correct**	AES was established as the symmetric encryption standard by NIST in 2001, replacing DES.
									D	Incorrect	AES was established as the symmetric encryption standard by NIST in 2001, replacing DES.
1.2	Cybersecurity History and Breaches	5	This organization's data breach in 2018 impacted over 1.1 billion records and is considered one of the top five data breaches in history.	MySpace	**Aadhaar**	OxyData	Microsoft	B	**A**	Incorrect	The Aadhaar data breach impacted approx. 1.1 billion Indian citizens, as shown on the Informationisbeautiful website. The other answers had less impact or occurred at a different time.
									B	**Correct**	The Aadhaar data breach impacted approx. 1.1 billion Indian citizens, as shown on the Informationisbeautiful website. The other answers had less impact or occurred at a different time.
									C	Incorrect	The Aadhaar data breach impacted approx. 1.1 billion Indian citizens, as shown on the Informationisbeautiful website. The other answers had less impact or occurred at a different time.

									D	Incorrect	The Aadhaar data breach impacted approx. 1.1 billion Indian citizens, as shown on the Informationisbeautiful website. The other answers had less impact or occurred at a different time.
1.3	Types of Cyber Attacks - Human	6	This form of cybercrime uses email fraud to attack commercial, government, and non-profit organizations:	**Business Email Compromise (BEC).**	Business-to-Business Phishing (B2BP).	Internet worms.	Adware.	A	A	**Correct**	BEC is a top concern for the US FBI and is one of the most financially damaging online crimes.
									B	Incorrect	BEC is a top concern for the US FBI and is one of the most financially damaging online crimes.
									C	Incorrect	BEC is a top concern for the US FBI and is one of the most financially damaging online crimes.
									D	Incorrect	BEC is a top concern for the US FBI and is one of the most financially damaging online crimes.
1.3	Types of Cyber Attacks - Human	7	This form of phishing uses smartphone text messages to proliferate:	Whaling.	**SMSishing.**	Spear Phishing.	Vishing.	B	A	Incorrect	SMSishing uses SMS or text messages to send fraudulent messages via cell/smartphones.
									B	**Correct**	SMSishing uses SMS or text messages to send fraudulent messages via cell/smartphones.
									C	Incorrect	SMSishing uses SMS or text messages to send fraudulent messages via cell/smartphones.
									D	Incorrect	SMSishing uses SMS or text messages to send fraudulent messages via cell/smartphones.
1.4	Types of Cyber Attacks - Technical	8	This is a type of malicious software designed to block access to a computer system until a sum of money is paid:	**Ransomware.**	Business Account Compromise (BAC).	Botnet.	Malware.	A	A	**Correct**	This is the definition of ransomware, a form of malware that locks computers requiring a ransom.
									B	Incorrect	This is the definition of ransomware, a form of malware that locks computers requiring a ransom.
									C	Incorrect	This is the definition of ransomware, a form of malware that locks computers requiring a ransom.
									D	Incorrect	This is the definition of ransomware, a form of malware that locks computers requiring a ransom.
1.4	Types of Cyber Attacks - Technical	9	A _____ attack uses multiple systems (network IP addresses, web servers, etc.) to flood the bandwidth or resources of a targeted system.	Zombie	Phishing	**Distributed Denial-of-Service (DDoS)**	Botnet	C	A	Incorrect	This is a standard definition for a distributed denial-of-service (DDoS) attack. It may use "zombie" computers as part of a larger botnet.
									B	Incorrect	This is a standard definition for a distributed denial-of-service (DDoS) attack. It may use "zombie" computers as part of a larger botnet.
									C	**Correct**	This is a standard definition for a distributed denial-of-service (DDoS) attack. It may use "zombie" computers as part of a larger botnet.
									D	Incorrect	This is a standard definition for a distributed denial-of-service (DDoS) attack. It may use "zombie" computers as part of a larger botnet.
1.4	Types of Cyber Attacks - Technical	10	This type of technical attack is typically perpetrated by a nation-state or state-sponsored group, which gains unauthorized access to a computer network and remains undetected for an extended period.	Distributed Denial-of-Service (DDoS)	**Advanced Persistent Threat (APT)**	Ransomware	Zero-Day	B	A	Incorrect	This is a standard definition for an APT attack where the attackers are from one nation attacking the resources in another by using stealthy tactics for long-term access.
									B	**Correct**	This is a standard definition for an APT attack where the attackers are from one nation attacking the resources in another by using stealthy tactics for long-term access.
									C	Incorrect	This is a standard definition for an APT attack where the attackers are from one nation attacking the resources in another by using stealthy tactics for long-term access.
									D	Incorrect	This is a standard definition for an APT attack where the attackers are from one nation attacking the resources in another by using stealthy tactics for long-term access.

1.5	Cybersecurity Frameworks, Standards, and Regulations Overview	11	Which company is not part of the Payment Card Industry (PCI) Security Standards Council (SSC)?	Visa	Mastercard	Discover	**Microsoft**	D	A	Incorrect	Microsoft is not included in setting security standards for payment cards (credit and debit cards). The other three companies listed created a joint standard in 2004.
									B	Incorrect	Microsoft is not included in setting security standards for payment cards (credit and debit cards). The other three companies listed created a joint standard in 2004.
									C	Incorrect	Microsoft is not included in setting security standards for payment cards (credit and debit cards). The other three companies listed created a joint standard in 2004.
									D	**Correct**	Microsoft is not included in setting security standards for payment cards (credit and debit cards). The other three companies listed created a joint standard in 2004.
1.5	Cybersecurity Frameworks, Standards, and Regulations Overview	12	This international standard provides requirements for information security management systems (ISMS):	NIST Cybersecurity Framework.	Center for Internet Security (CIS) Controls.	Payment Card Industry Data Security Standard (PCI DSS).	**ISO/IEC 27001.**	D	A	Incorrect	The ISO/IEC 27000 family provides more than a dozen standards for cybersecurity and information system security. NIST is not international, and the Center for Internet Security provides security guides
									B	Incorrect	The ISO/IEC 27000 family provides more than a dozen standards for cybersecurity and information system security. NIST is not international, and the Center for Internet Security provides security guides
									C	Incorrect	The ISO/IEC 27000 family provides more than a dozen standards for cybersecurity and information system security. NIST is not international, and the Center for Internet Security provides security guides
									D	**Correct**	The ISO/IEC 27000 family provides more than a dozen standards for cybersecurity and information system security. NIST is not international, and the Center for Internet Security provides security guides
1.5	Cybersecurity Frameworks, Standards, and Regulations Overview	13	This is a suite of service offerings CPAs may provide in connection with system-level controls of a service organization:	Statements on Standards for Attestation Engagements (SSAE).	**System and Organization Controls (SOC).**	ISO/IEC 27000 Security Control Family.	Center for Internet Security (CIS) Controls.	B	A	Incorrect	SOC provides a suite of services provided by the AICPA to establish security control standards for auditors.
									B	**Correct**	SOC provides a suite of services provided by the AICPA to establish security control standards for auditors.
									C	Incorrect	SOC provides a suite of services provided by the AICPA to establish security control standards for auditors.
									D	Incorrect	SOC provides a suite of services provided by the AICPA to establish security control standards for auditors.
1.6	NIST Frameworks and Standards	14	This NIST document series contains computer/cyber/information and security guidelines, recommendations, and reference materials:	**Special Publication (SP) 800.**	Security Policy (SP).	Computer Security Resource Center (CSRC) Directives.	Federal Information Processing Standard (FIPS) 199.	A	A	**Correct**	NIST uses the Special Publication (SP) 800 subseries for its cybersecurity directives. The CSRC is responsible for the development of SPs.
									B	Incorrect	NIST uses the Special Publication (SP) 800 subseries for its cybersecurity directives. The CSRC is responsible for the development of SPs.
									C	Incorrect	NIST uses the Special Publication (SP) 800 subseries for its cybersecurity directives. The CSRC is responsible for the development of SPs.

											D	Incorrect	NIST uses the Special Publication (SP) 800 subseries for its cybersecurity directives. The CSRC is responsible for the development of SPs.
1.6	NIST Frameworks and Standards	15	This NIST Framework consists of five functions for protecting information technology assets in any sized organization:	Risk Management Framework (RMF).	Special Publication Standards.	**Cybersecurity Framework (CSF).**	Security and Privacy Controls Framework (SPCF).	C			A	Incorrect	The NIST Cybersecurity Framework has five functions for managing IT security programs. It is voluntary and based on existing NIST cybersecurity Standards.
											B	Incorrect	The NIST Cybersecurity Framework has five functions for managing IT security programs. It is voluntary and based on existing NIST cybersecurity Standards.
											C	**Correct**	The NIST Cybersecurity Framework has five functions for managing IT security programs. It is voluntary and based on existing NIST cybersecurity Standards.
											D	Incorrect	The NIST Cybersecurity Framework has five functions for managing IT security programs. It is voluntary and based on existing NIST cybersecurity Standards.
1.6	NIST Frameworks and Standards	16	Which of the following is not a goal of the NIST Risk and Cybersecurity Frameworks?	**Standard operating instructions for all organizations**	Consistent and cost-effective application of security controls	Repeatable processes	A technology-neutral and flexible approach	A			**A**	**Correct**	NIST focuses on strategic directions and processes rather than industry or area-specific operations. The others are listed goals of the NIST RMF and CSF.
											B	Incorrect	NIST focuses on strategic directions and processes rather than industry or area-specific operations. The others are listed goals of the NIST RMF and CSF.
											C	Incorrect	NIST focuses on strategic directions and processes rather than industry or area-specific operations. The others are listed goals of the NIST RMF and CSF.
											D	Incorrect	NIST focuses on strategic directions and processes rather than industry or area-specific operations. The others are listed goals of the NIST RMF and CSF.
1.7	Industry Frameworks (PCI, HIPAA. CIS CSC, ISO/IEC)	17	This International Standard contains over 110 specific cybersecurity controls:	ISO/IEC 27001.	**ISO/IEC 27002.**	ISO/IEC 27005.	NIST SP800-53r5.	B			A	Incorrect	ISO/IEC 27002:2013, The Code of Practice for Information Security Management provides direction on 14 security control groups and addresses 35 control objectives and more than 110 individual controls.
											B	**Correct**	ISO/IEC 27002:2013, The Code of Practice for Information Security Management provides direction on 14 security control groups and addresses 35 control objectives and more than 110 individual controls.
											C	Incorrect	ISO/IEC 27002:2013, The Code of Practice for Information Security Management provides direction on 14 security control groups and addresses 35 control objectives and more than 110 individual controls.
											D	Incorrect	ISO/IEC 27002:2013, The Code of Practice for Information Security Management provides direction on 14 security control groups and addresses 35 control objectives and more than 110 individual controls.
1.7	Industry Frameworks (PCI, HIPAA. CIS CSC, ISO/IEC)	18	How many domains are included in the PCI Data Security Standard (DSS)?	5	10	**12**	24	C			A	Incorrect	The PCI Data Security Standard (DSS) is composed of 12 domains with more than 300 controls, each of which includes testing procedures and corresponding guidance on how to implement them.
											B	Incorrect	The PCI Data Security Standard (DSS) is composed of 12 domains with more than 300 controls, each of which includes testing procedures and corresponding guidance on how to implement them.
											C	**Correct**	The PCI Data Security Standard (DSS) is composed of 12 domains with more than 300 controls, each of which includes testing procedures and corresponding guidance on how to implement them.
											D	Incorrect	The PCI Data Security Standard (DSS) is composed of 12 domains with more than 300 controls, each of which includes testing procedures and corresponding guidance on how to implement them.

1.7	Industry Frameworks (PCI, HIPAA. CIS CSC, ISO/IEC)	19	In the United States, this term relates to an individual's past, present, or future physical or mental health or condition and to the provision of health care to an individual:	Personal Health Data (PHD).	Personally Identifiable Information (PII).	HIPAA.	**Protected Health Information (PHI).**	D	**A**	Incorrect	This is the standard definition for Protected Health Information (PHI) as defined in the US HIPAA regulation.
									B	Incorrect	This is the standard definition for Protected Health Information (PHI) as defined in the US HIPAA regulation.
									C	Incorrect	This is the standard definition for Protected Health Information (PHI) as defined in the US HIPAA regulation.
									D	**Correct**	This is the standard definition for Protected Health Information (PHI) as defined in the US HIPAA regulation.
1.8	Cybersecurity Oversight, Governance, and Compliance	20	This is a strategic planning responsibility providing organizational oversight that sets policies and establishes practices for enforcement:	Leadership.	Compliance.	Audit.	**Governance.**	D	**A**	Incorrect	This is the standard definition of Governance.
									B	Incorrect	This is the standard definition of Governance.
									C	Incorrect	This is the standard definition of Governance.
									D	**Correct**	This is the standard definition of Governance.
1.8	Cybersecurity Oversight, Governance, and Compliance	21	Which of the following is not a standard strategic security control relative to the timing of security incidents?	**Administrative**	Preventive	Detective	Corrective	A	**A**	**Correct**	Administrative controls can include the other three types of controls listed.
									B	Incorrect	Before the event, preventive controls are intended to prevent an incident from occurring.
									C	Incorrect	During the event, detective controls are intended to identify and characterize an incident in progress.
									D	Incorrect	After the event, corrective controls are intended to limit the extent of any damage caused by the incident.
1.8	Cybersecurity Oversight, Governance, and Compliance	22	This level of management communicates the mission priorities, available resources, and overall risk tolerance to the layers below as a part of governance:	Chief Security Officer.	**Corporate Executives.**	IT Operations.	Audit Director.	B	**A**	Incorrect	The executive level communicates the mission priorities, available resources, and overall risk tolerance to the business/process level.
									B	**Correct**	The executive level communicates the mission priorities, available resources, and overall risk tolerance to the business/process level.
									C	Incorrect	The executive level communicates the mission priorities, available resources, and overall risk tolerance to the business/process level.
									D	Incorrect	The executive level communicates the mission priorities, available resources, and overall risk tolerance to the business/process level.
1.9	Security Polices	23	These are formal statements or rules that specify correct or expected behavior in companies:	**Policies.**	Standards.	Controls.	Regulations.	A	**A**	**Correct**	Policies are formal corporate statements or rules that specify correct or expected behavior.
									B	Incorrect	Standards are mandatory actions or rules that provide support or direction on how to comply with policies.
									C	Incorrect	Controls are specifications for implementing policy.
									D	Incorrect	Regulations are specific rules for a government body, not a company.
1.9	Security Polices	24	This ensures that tasks are completed in the same way each time:	Policies.	Standards.	**Procedures.**	Guidelines.	C	**A**	Incorrect	Procedures are written processes that provide step-by-step details and are required by policy.
									B	Incorrect	Procedures are written processes that provide step-by-step details and are required by policy.
									C	**Correct**	Procedures are written processes that provide step-by-step details and are required by policy.

1.9	Security Polices	25	Which of the following should be included in a corporate policy document?	Purpose	Audience	**Both A and B**	Neither A nor B	C	**D**	Incorrect	Procedures are written processes that provide step-by-step details and are required by policy.
									A	Incorrect	All of these items should be included in corporate policies.
									B	Incorrect	All of these items should be included in corporate policies.
									C	**Correct**	All of these items should be included in corporate policies.
									D	Incorrect	All of these items should be included in corporate policies.
1.1	Security Risk Management Overview	26	This is the level of risk an entity is willing to assume in order to achieve a potential desired result:	**Risk Tolerance.**	Risk Score.	Risk Analysis.	Threat Allowance.	A	**A**	**Correct**	Risk tolerance or appetite is the number of risks organizations or people are willing to take.
									B	Incorrect	Risk tolerance or appetite is the number of risks organizations or people are willing to take.
									C	Incorrect	Risk tolerance or appetite is the number of risks organizations or people are willing to take.
									D	Incorrect	Risk tolerance or appetite is the number of risks organizations or people are willing to take.
1.1	Security Risk Management Overview	27	Non-compliance with laws, standards, or requirements is considered which type of risk?	Technical	Procedural	**Management**	Operational	C	**A**	Incorrect	Non-compliance with control requirements is a management risk.
									B	Incorrect	Non-compliance with control requirements is a management risk.
									C	**Correct**	Non-compliance with control requirements is a management risk.
									D	Incorrect	Non-compliance with control requirements is a management risk.
1.1	Security Risk Management Overview	28	Which of the following is not considered a normal part of the strategic risk management process?	Conducting a risk assessment	Implementing risk mitigation	Continuous monitoring of risks	**Transferring risk**	D	**A**	Incorrect	Transferring risk is a type of risk mitigation and is considered at the tactical level.
									B	Incorrect	Transferring risk is a type of risk mitigation and is considered at the tactical level.
									C	Incorrect	Transferring risk is a type of risk mitigation and is considered at the tactical level.
									D	**Correct**	Transferring risk is a type of risk mitigation and is considered at the tactical level.
1.11	Threat Analysis	29	_____ is the method or path a threat will use to access a real or potential target.	Threat source	**Threat vector**	Threat modeling	Risk vector	B	**A**	Incorrect	The threat vector is the way a threat will gain access to a target to incur a loss.
									B	**Correct**	The threat vector is the way a threat will gain access to a target to incur a loss.
									C	Incorrect	The threat vector is the way a threat will gain access to a target to incur a loss.
									D	Incorrect	The threat vector is the way a threat will gain access to a target to incur a loss.
1.11	Threat Analysis	30	This is the process for identifying real or potential threats using multiple sources to proactively prevent or mitigate attacks.	Risk Management.	Vulnerability Assessments.	**Threat intelligence.**	Threat analysis.	C	**A**	Incorrect	Cyber threat intelligence is what cyber threat information becomes once it has been collected, evaluated in the context of its source and reliability, and analyzed through rigorous and structured tradecraft techniques by those with substantive expertise and access to all-source information.
									B	Incorrect	Cyber threat intelligence is what cyber threat information becomes once it has been collected, evaluated in the context of its source and reliability, and analyzed through rigorous and structured tradecraft techniques by those with substantive expertise and access to all-source information.
									C	**Correct**	Cyber threat intelligence is what cyber threat information becomes once it has been collected, evaluated in the context of its source and reliability, and analyzed through rigorous and structured tradecraft techniques by those with substantive expertise and access to all-source information.

									D	Incorrect	Cyber threat intelligence is what cyber threat information becomes once it has been collected, evaluated in the context of its source and reliability, and analyzed through rigorous and structured tradecraft techniques by those with substantive expertise and access to all-source information.
1.11	Threat Analysis	31	What website provides a matrix that catalogs types of threats based on their threat vector?	NIST CSRC	MITRE Common Vulnerability Enumeration (CVE)	**MITRE ATT&CK® Framework**	Staysafeonline.org	C	A	Incorrect	MITRE ATT&CK® is a globally-accessible knowledge base of adversary tactics and techniques based on real-world observations.
									B	Incorrect	MITRE ATT&CK® is a globally-accessible knowledge base of adversary tactics and techniques based on real-world observations.
									C	**Correct**	MITRE ATT&CK® is a globally-accessible knowledge base of adversary tactics and techniques based on real-world observations.
									D	Incorrect	MITRE ATT&CK® is a globally-accessible knowledge base of adversary tactics and techniques based on real-world observations.
1.12	Security Risk Management in Practice	32	This is a measure of the extent to which an entity is threatened by a potential circumstance or event:	**Risk.**	Threat.	Vulnerability.	Control.	A	A	**Correct**	Risk is defined as "a measure of the extent to which an entity is threatened by a potential circumstance or event."
									B	Incorrect	Risk is defined as "a measure of the extent to which an entity is threatened by a potential circumstance or event."
									C	Incorrect	Risk is defined as "a measure of the extent to which an entity is threatened by a potential circumstance or event."
									D	Incorrect	Risk is defined as "a measure of the extent to which an entity is threatened by a potential circumstance or event."
1.12	Security Risk Management in Practice	33	This type of risk analysis uses numeric values to calculate actual risk measures:	Threat modeling.	Qualitative.	**Quantitative.**	Vulnerability assessments.	C	A	Incorrect	Quantitative risk analysis uses specific frequency and impact values to define specific risk amounts.
									B	Incorrect	Quantitative risk analysis uses specific frequency and impact values to define specific risk amounts.
									C	**Correct**	Quantitative risk analysis uses specific frequency and impact values to define specific risk amounts.
									D	Incorrect	Quantitative risk analysis uses specific frequency and impact values to define specific risk amounts.
1.12	Security Risk Management in Practice	34	Risk _____ is making the decision not to engage in the actions associated with that risk.	Mitigation	**Avoidance**	Acceptance	Transfer	B	A	Incorrect	Avoiding the risk removes it from the environment, for example, turning off a vulnerable system.
									B	**Correct**	Avoiding the risk removes it from the environment, for example, turning off a vulnerable system.
									C	Incorrect	Avoiding the risk removes it from the environment, for example, turning off a vulnerable system.
									D	Incorrect	Avoiding the risk removes it from the environment, for example, turning off a vulnerable system.
2.1	Asset Identification and Inventory	35	This is a list of your most important systems, devices, software, services, and data:	**Asset Inventory.**	System Security Plan	Systems database.	Business Impact Analysis (BIA).	A	A	**Correct**	Creating and maintaining an Asset Inventory is the first step in the Identify Category.
									B	Incorrect	A System Security Plan contains information about the security of specific assets.
									C	Incorrect	While your asset inventory may be contained in a systems database, the correct name is an asset inventory.
									D	Incorrect	Your BIA prioritizes systems and operations.
2.1	Asset Identification and Inventory	36	These are graphical charts that depict the layout of your computer or telecommunications network:	Network Charts.	Data Flow Diagram.	**Network Diagrams.**	Bit Map.	C	A	Incorrect	The correct name is a network diagram.

									B	Incorrect	A data flow diagram uses a network diagram to show how data traverses a network.
									C	**Correct**	This is the definition of a network diagram.
									D	Incorrect	Bitmap is used in computer graphics.
2.2	Third-Party/Service Provider Management	**37**	This external role owns or manages assets under contract for the benefit of an organization:	Internal Server Farm Administrators.	Infrastructure as a Service (IaaS).	**Third-Party Service Providers.**	Cloud Service Providers.	C	A	Incorrect	This is an internal asset.
									B	Incorrect	This is a type of service.
									C	**Correct**	Third-party service providers manage and/or own assets for use by the organization.
									D	Incorrect	Cloud Service Providers are a type of third-party service provider. They generally own all of the equipment.
2.2	Third-Party/Service Provider Management	**38**	This organization is a world leader dedicated to defining and raising awareness of best practices to ensure a secure cloud computing environment:	FedRAMP.	NIST CSRC.	PCI SSC.	**Cloud Security Alliance (CSA).**	D	A	Incorrect	FedRAMP is a US cloud provider certification.
									B	Incorrect	NIST CSRC providers general standards and guidelines for information technology and security.
									C	Incorrect	The PCI SSC provides standards and certification for card service providers.
									D	**Correct**	The CSA provides guidance, training, and certification in cloud security.
2.3	Business Impact Assessment	**39**	This is used to survey organizational leaders to identify the potential impacts if a business function or process is interrupted:	**Business Impact Assessment (BIA) Questionnaire.**	Business Risk Survey.	Threat Analysis.	Vulnerability Assessment.	A	A	**Correct**	A BIA Questionnaire is used to capture information on business impacts.
									B	Incorrect	The standard name is a Business Impact Assessment rather than Risk Survey.
									C	Incorrect	Threat analysis is a part of the risk assessment process.
									D	Incorrect	Vulnerabilities assessments capture real or potential weaknesses.
2.3	Business Impact Assessment	**40**	Which of the following is not determined in the BIA process?	MTD - Maximum Tolerable Downtime	RTO - Recovery Time Objective	**SLA - Service Level Agreement**	RPO - Recovery Point Objective	C	A	Incorrect	The SLA is an agreement between the client and service provider for a level of service requirements.
									B	Incorrect	The SLA is an agreement between the client and service provider for a level of service requirements.
									C	**Correct**	The SLA is an agreement between the client and service provider for a level of service requirements.
									D	Incorrect	The SLA is an agreement between the client and service provider for a level of service requirements.
2.4	Configuration Management and Change Control	**41**	This is a repository that stores specific configuration information for systems, services, and technical assets:	Data Flow Diagram.	**Configuration Management Data Base (CMDB).**	Software inventory list.	Active Directory Users and Computers.	B	A	Incorrect	The CMDB documents systems settings and management information.
									B	**Correct**	The CMDB documents systems settings and management information.
									C	Incorrect	The CMDB documents systems settings and management information.
									D	Incorrect	The CMDB documents systems settings and management information.
2.4	Configuration Management and Change Control	**42**	This is the formal process to identify, analyze, approve, and document changes to assets:	Configuration Management.	**Change Management.**	Inventory Management.	Baselining.	B	A	Incorrect	This is the definition of change management.
									B	**Correct**	This is the definition of change management.
									C	Incorrect	This is the definition of change management.
									D	Incorrect	This is the definition of change management.

3.1	Defending Business Assets Overview	43	A _____ is a defense or countermeasure put in place to manage risk.	Firewall	Threat protection	Deterrent	**Control**	D	**A**	Incorrect	A firewall is a specific type of control.
									B	Incorrect	This is a fabricated term.
									C	Incorrect	Deterrent is a type of control.
									D	**Correct**	This is the general definition of a control.
3.1	Defending Business Assets Overview	44	This is the software that supports a computer's basic functions and provides an additional layer of protection; examples include Windows and macOS:	**Operating system.**	Antivirus.	Systems administration.	Kernel.	A	**A**	**Correct**	The operating system is the layer between hardware and applications.
									B	incorrect	The operating system is the layer between hardware and applications.
									C	incorrect	The operating system is the layer between hardware and applications.
									D	incorrect	The operating system is the layer between hardware and applications.
3.2	Identity and Access Management	45	In this process, the subject provides a unique and distinguishing name, account number, or user-id:	**Identification.**	Authentication.	Authorization.	Accounting.	A	**A**	**Correct**	Identification can be a unique and distinguishing name, account number, or user-id.
									B	incorrect	Identification can be a unique and distinguishing name, account number, or user-id.
									C	incorrect	Identification can be a unique and distinguishing name, account number, or user-id.
									D	incorrect	Identification can be a unique and distinguishing name, account number, or user-id.
3.2	Identity and Access Management	46	This is a repository of an organization's network resources, assets, and users that usually follows a hierarchical database standard format:	Configuration Management Data Base (CMDB).	Server Inventory System.	Kerberos.	**Directory Service.**	D	**A**	incorrect	A CMDB is used by management to store configuration and asset inventory information.
									B	incorrect	This is a fabricated term.
									C	incorrect	Kerberos is a method for authentication.
									D	**Correct**	Directory services are software systems that store, organize, and provide access to directory information to unify network resources.
3.3	Authentication and Authorization	47	A smartcard, token, or device is an example of which form of authentication?	**Something you have**	Something you know	Something you wear	Something you are	A	**A**	**Correct**	These are examples of something you have.
									B	Incorrect	These are examples of something you have.
									C	Incorrect	These are examples of something you have.
									D	Incorrect	These are examples of something you have.
3.3	Authentication and Authorization	48	This form of authentication can be a physical device or software application that contains a digital certificate to verify identity:	Biometrics.	**Tokens.**	Passwords.	Fingerprint Scanner.	B	**A**	Incorrect	Tokens can be a physical device or software that contains the subject's identification verification, usually in the form of a digital certificate.
									B	**Correct**	Tokens can be a physical device or software that contains the subject's identification verification, usually in the form of a digital certificate.
									C	Incorrect	Tokens can be a physical device or software that contains the subject's identification verification, usually in the form of a digital certificate.
									D	Incorrect	Tokens can be a physical device or software that contains the subject's identification verification, usually in the form of a digital certificate.
3.4	Vulnerability and Patch Management	49	A _____ is a flaw or weakness in an information system, system security procedures, internal controls, or implementation that could be exploited or triggered by a threat like a cybercriminal.	Software bug	**Vulnerability**	Threat	Risk	B	**A**	Incorrect	This is the NIST definition of vulnerability.
									B	**Correct**	This is the NIST definition of vulnerability.
									C	Incorrect	This is the NIST definition of vulnerability.
									D	Incorrect	This is the NIST definition of vulnerability.

3.4	Vulnerability and Patch Management	50	This form of vulnerability remediation applies a software update to fix a bug or improve the application:	Upgrade.	Configuration setting.	Policy.	**Patch.**	D	**A**	Incorrect	A software patch fixes known security or functionality issues.
									B	Incorrect	A software patch fixes known security or functionality issues.
									C	Incorrect	A software patch fixes known security or functionality issues.
									D	**Correct**	A software patch fixes known security or functionality issues.
3.5	Security Awareness	51	What is the root cause of most security breaches?	Malicious hackers	**Human failure**	Computer viruses	Poor passwords	B	**A**	Incorrect	Human failure is the root cause of most security failures.
									B	**Correct**	Human failure is the root cause of most security failures.
									C	Incorrect	Human failure is the root cause of most security failures.
									D	Incorrect	Human failure is the root cause of most security failures.
3.5	Security Awareness	52	When should users receive security awareness training?	Continually	At employee orientation	**Both A and B**	Neither A nor B	C	**A**	Incorrect	Users should receive security awareness training continually and at employee orientation.
									B	Incorrect	Users should receive security awareness training continually and at employee orientation.
									C	**Correct**	Users should receive security awareness training continually and at employee orientation.
									D	Incorrect	Users should receive security awareness training continually and at employee orientation.
3.6	Physical Security	53	What is always the top priority for security?	**Human life safety**	Online safety	Crime prevention	Compliance with regulations	A	**A**	**Correct**	The safety of humans and preservation of life is always the number one priority.
									B	Incorrect	The safety of humans and preservation of life is always the number one priority.
									C	Incorrect	The safety of humans and preservation of life is always the number one priority.
									D	Incorrect	The safety of humans and preservation of life is always the number one priority.
3.6	Physical Security	54	This is a multi-disciplinary approach that uses urban and architectural design and the management of built and natural environments to reduce the potential for crime:	Criminal Derrance Using Natural Terrain (CDUNT).	Barrier and Detection Installation and Management (BDIM).	**Crime Prevention Through Environmental Design (CPTED).**	Man traps.	C	**A**	Incorrect	This is the definition of CPTED, a standard approach to designing facilities to reduce crime.
									B	Incorrect	This is the definition of CPTED, a standard approach to designing facilities to reduce crime.
									C	**Correct**	This is the definition of CPTED, a standard approach to designing facilities to reduce crime.
									D	Incorrect	This is the definition of CPTED, a standard approach to designing facilities to reduce crime.
3.7	Personnel Security	55	Performing pre-employment screening and background checks is the responsibility of which function?	Executive Management	**Human Resources**	Cybersecurity	IT Audit	B	**A**	Incorrect	HR is responsible for conducting employee checks, both before and during employment.
									B	**Correct**	HR is responsible for conducting employee checks, both before and during employment.
									C	Incorrect	HR is responsible for conducting employee checks, both before and during employment.
									D	Incorrect	HR is responsible for conducting employee checks, both before and during employment.
3.7	Personnel Security	56	Which are potential indicators of an insider threat that may harm the organization?	Excess access to corporate systems	Financial gains	**Both A and B**	Neither A nor B	C	**A**	Incorrect	Both of these and more are ways to detect the potential an insider may threaten an organization.
									B	Incorrect	Both of these and more are ways to detect the potential an insider may threaten an organization.
									C	**Correct**	Both of these and more are ways to detect the potential an insider may threaten an organization.
									D	Incorrect	Both of these and more are ways to detect the potential an insider may threaten an organization.

3.8	Computer Networking Fundamentals	**57**	This is not a layer in the OSI networking model:	**Operating system.**	Transport.	Network.	Physical.	A	**A**	**Correct**	The OSI 7-Layer model is Application, Presentation, Session, Transport, Network, Data, and Physical.
									B	Incorrect	The OSI 7-Layer model is Application, Presentation, Session, Transport, Network, Data, and Physical.
									C	Incorrect	The OSI 7-Layer model is Application, Presentation, Session, Transport, Network, Data, and Physical.
									D	Incorrect	The OSI 7-Layer model is Application, Presentation, Session, Transport, Network, Data, and Physical.
3.8	Computer Networking Fundamentals	**58**	This form of network address consists of four "octets" using numbers between 0 and 255:	MAC.	**IPv4.**	IPv6.	TCP Port number.	B	**A**	Incorrect	The MAC address is a hexadecimal number assigned to a network interface card.
									B	**Correct**	IP version 4 uses four numbers from 0-255, with a period separating them.
									C	Incorrect	IP version 6 uses a 128-bit hexadecimal address.
									D	Incorrect	A TCP port is a number from 1-65,535 that's associated with a service.
3.9	Network Defenses	**59**	A core principle of a network firewall that any traffic that isn't explicitly permitted by a rule should be automatically denied is known as a(n):	Access Control List.	**Default Deny Rule.**	Explicit Access Rule.	Whitelisting.	B	**A**	Incorrect	One of the core principles of a firewall, known as the default deny rule, is that any traffic that isn't explicitly permitted by a rule should be automatically denied.
									B	**Correct**	One of the core principles of a firewall, known as the default deny rule, is that any traffic that isn't explicitly permitted by a rule should be automatically denied.
									C	Incorrect	One of the core principles of a firewall, known as the default deny rule, is that any traffic that isn't explicitly permitted by a rule should be automatically denied.
									D	Incorrect	One of the core principles of a firewall, known as the default deny rule, is that any traffic that isn't explicitly permitted by a rule should be automatically denied.
3.9	Network Defenses	**60**	This type of network device has enhanced abilities to watch for attacks and make changes to your network security as they occur:	VPN Concentrators.	Unified Threat Management .	**IDS/IPS.**	Proxy Server.	C	**A**	Incorrect	Intrusion Detection System or Intrusion Protection System, known as an IDS/IPS, is a network device that has enhanced abilities to watch for attacks and make changes to your security as they occur.
									B	Incorrect	Intrusion Detection System or Intrusion Protection System, known as an IDS/IPS, is a network device that has enhanced abilities to watch for attacks and make changes to your security as they occur.
									C	**Correct**	Intrusion Detection System or Intrusion Protection System, known as an IDS/IPS, is a network device that has enhanced abilities to watch for attacks and make changes to your security as they occur.
									D	Incorrect	Intrusion Detection System or Intrusion Protection System, known as an IDS/IPS, is a network device that has enhanced abilities to watch for attacks and make changes to your security as they occur.
3.1	Network Security Access Controls	**61**	A _____ is a widely used Internet record listing that identifies who owns a domain.	Firewall rule	IP address	Internet Identifying Record (IIR)	**Whois**	D	**A**	Incorrect	The whois record lists the owner of internet domains assigned by official organizations such as ARIN and ICANN.
									B	Incorrect	The whois record lists the owner of internet domains assigned by official organizations such as ARIN and ICANN.
									C	Incorrect	The whois record lists the owner of internet domains assigned by official organizations such as ARIN and ICANN.
									D	**Correct**	The whois record lists the owner of internet domains assigned by official organizations such as ARIN and ICANN.
3.1	Network Security Access Controls	**62**	This common practice divides a network into zones based on business or security needs:	**Segmentation.**	Firewalling.	Virtual Private Network (VPN).	Co-location.	A	**A**	**Correct**	Network segmentation separates the network into specific areas based on business needs; it can be logical, virtual, or physical.
									B	Incorrect	Network segmentation separates the network into specific areas based on business needs; it can be logical, virtual, or physical.

									C	Incorrect	Network segmentation separates the network into specific areas based on business needs; it can be logical, virtual, or physical.
									D	Incorrect	Network segmentation separates the network into specific areas based on business needs; it can be logical, virtual, or physical.
3.11	Endpoint and System Security Configuration	**63**	This is a concept about using the minimal number of applications or services needed for the system to work. This is a common function of system hardening:	System simplification.	Separation of duties.	**Least Functionality.**	Least Authorization.	C	**A**	Incorrect	Least functionality is running the minimal number of applications or services needed for the system to work.
									B	Incorrect	Least functionality is running the minimal number of applications or services needed for the system to work.
									C	**Correct**	Least functionality is running the minimal number of applications or services needed for the system to work.
									D	Incorrect	Least functionality is running the minimal number of applications or services needed for the system to work.
3.11	Endpoint and System Security Configuration	**64**	This security capability sets the internal system policies on Microsoft Windows Operating Systems:	Security Policy Administration (SPA).	**Local /Group Policies.**	Windows Policy Administrator (WPA).	Windows Security Configuration Manager (WSCM).	B	**A**	Incorrect	Local and group policies are the function of establishing and managing the specific security and functionality settings in a Windows environment.
									B	**Correct**	Local and group policies are the function of establishing and managing the specific security and functionality settings in a Windows environment.
									C	Incorrect	Local and group policies are the function of establishing and managing the specific security and functionality settings in a Windows environment.
									D	Incorrect	Local and group policies are the function of establishing and managing the specific security and functionality settings in a Windows environment.
3.12	Endpoint and System Security Protection	**65**	Which is not a typical detection method for antivirus programs?	**User identification**	Signature	Behavior	Heuristic	A	**A**	**Correct**	Signatures, Behavior, and Heuristics are common methods for automating malware detection. User identification is not effective.
									B	Incorrect	Signatures, Behavior, and Heuristics are common methods for automating malware detection. User identification is not effective.
									C	Incorrect	Signatures, Behavior, and Heuristics are common methods for automating malware detection. User identification is not effective.
									D	Incorrect	Signatures, Behavior, and Heuristics are common methods for automating malware detection. User identification is not effective.
3.12	Endpoint and System Security Protection	**66**	What should set the rules for using removable media within an organization?	End-user decision	**Corporate policy**	IT administrators	Internal Audit	B	**A**	Incorrect	Corporate policies should establish requirements and security controls for using any type of removable media (e.g., USB drives).
									B	**Correct**	Corporate policies should establish requirements and security controls for using any type of removable media (e.g., USB drives).
									C	Incorrect	Corporate policies should establish requirements and security controls for using any type of removable media (e.g., USB drives).
									D	Incorrect	Corporate policies should establish requirements and security controls for using any type of removable media (e.g., USB drives).
3.13	Application Security	**67**	Which programming language uses a runtime interpreter?	Java	.NET	Python	**C++**	D	**A**	Incorrect	The C languages (C, C#, C++) all use a compiler to create executable code. An interpreter executes code when it is run.

									B	Incorrect	The C languages (C, C#, C++) all use a compiler to create executable code. An interpreter executes code when it is run.
									C	Incorrect	The C languages (C, C#, C++) all use a compiler to create executable code. An interpreter executes code when it is run.
									D	**Correct**	The C languages (C, C#, C++) all use a compiler to create executable code. An interpreter executes code when it is run.
3.13	Application Security	**68**	What's the project that provides standards and directions on secure development/coding techniques?	NIST CSRC	**OWASP**	Software Assurance Maturity Model	Software Technical Implementation Guide	B	A	Incorrect	OWASP (www.owasp.org) is a worldwide organization providing guides on secure development.
									B	**Correct**	OWASP (www.owasp.org) is a worldwide organization providing guides on secure development.
									C	Incorrect	OWASP (www.owasp.org) is a worldwide organization providing guides on secure development.
									D	Incorrect	OWASP (www.owasp.org) is a worldwide organization providing guides on secure development.
3.14	Cloud and Virtualization Security	**69**	_____ is a model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction.	Virtualization	Server Farms	**Cloud Computing**	Co-location Data Centers	C	A	Incorrect	This is the NIST definition of Cloud Computing.
									B	Incorrect	This is the NIST definition of Cloud Computing.
									C	**Correct**	This is the NIST definition of Cloud Computing.
									D	Incorrect	This is the NIST definition of Cloud Computing.
3.14	Cloud and Virtualization Security	**70**	What is the underlying technology that creates and runs virtual machines?	**Hypervisor**	Virtual Machine Manager (VMM)	Virtual Desktop Infrastructure (VDI)	Cloud Access Security Broker (CASB)	A	A	**Correct**	A hypervisor is used with virtualization to manage and run virtual machines and operating systems.
									B	Incorrect	A hypervisor is used with virtualization to manage and run virtual machines and operating systems.
									C	Incorrect	A hypervisor is used with virtualization to manage and run virtual machines and operating systems.
									D	Incorrect	A hypervisor is used with virtualization to manage and run virtual machines and operating systems.
4.1	Encryption Concepts	**71**	What term is a process or set of rules to be followed in calculations or other problem-solving operations and doesn't need to be kept secret?	Encryption Key	**Algorithm**	Steganography	Encoding	B	A	Incorrect	This is the secret value used with an algorithm to encrypt and decrypt messages.
									B	**Correct**	This is the definition of an algorithm.
									C	Incorrect	Steganography is "hidden writing," hiding messages in other media.
									D	Incorrect	Encoding transforms human text into machine text.
4.1	Encryption Concepts	**72**	This is the act of making something difficult to understand and should rely on something not known or widely discovered:	Encryption.	Steganography.	**Obfuscation.**	Data hiding.	C	A	Incorrect	This is the definition of obfuscation.
									B	Incorrect	This is the definition of obfuscation.
									C	**Correct**	This is the definition of obfuscation.
									D	Incorrect	This is the definition of obfuscation.
4.2	Cryptographic Algorithms	**73**	In cybersecurity, this is the most common symmetric encryption algorithm today and is a NIST Standard:	**Advanced Encryption Standard (AES).**	Data Encryption Standard (DES).	Public Key Infrastructure (PKI).	Multi-factor authentication.	A	A	**Correct**	AES is the symmetric encryption standard.
									B	Incorrect	DES is an old NIST encryption standard.
									C	Incorrect	This uses asymmetric encryption for managing keys.
									D	Incorrect	This is a form of authentication, not cryptography.
4.2	Cryptographic Algorithms	**74**	What are the types of keys used for asymmetric encryption?	Symmetric key pairs	Keychains	Digital signatures	**Public/Private Keys**	D	A	Incorrect	Symmetric encryption uses a single key to encrypt and decrypt.
									B	Incorrect	A keychain holds public keys as a part of PKI.
									C	Incorrect	A digital signature contains a subject's encrypted private key to prove identity.
									D	**Correct**	Asymmetric encryption uses public/private keys.

4.3	Encryption - Public Key Infrastructure	75	This standard is the process of creating, managing, distributing, storing, using, and revoking keys and digital certificates:	Advanced Encryption Standard (AES).	**Public Key Infrastructure (PKI).**	Digital Key Management System (DKMS).	Key escrow.	B	**A** Incorrect	AES is the NIST symmetric encryption standard.
									B **Correct**	PKI is a set of roles, policies, and procedures needed to manage public-key (asymmetric) encryption.
									C Incorrect	This is a fabricated term.
									D Incorrect	Key escrow is a form of having a backup or backdoor encryption key.
4.3	Encryption - Public Key Infrastructure	76	In PKI, this entity issues digital certificates ensuring the certificate holder's identity:	Certificate Manager (CM).	**Certificate Authority (CA).**	Registration Authority (RA).	Key Registrar.	B	**A** Incorrect	This is a fabricated term.
									B **Correct**	The CA verifies the owner/holder of a certificate.
									C Incorrect	The RA validates the user's or endpoint's identity.
									D Incorrect	This is a fabricated term.
4.4	Data Protection Techniques	77	This process takes a string of any length and produces a fixed-length string for output:	Asymmetric encryption.	Symmetric encryption.	Obfuscation.	**Hashing.**	D	**A** Incorrect	This is the definition of hashing.
									B Incorrect	This is the definition of hashing.
									C Incorrect	This is the definition of hashing.
									D **Correct**	This is the definition of hashing.
4.4	Data Protection Techniques	78	You can use this control for notification if files have changed within a system:	**File Integrity Management (FIM).**	Asymmetric encryption.	Certificate Authority (CA).	Public Key Infrastructure (PKI).	A	**A** **Correct**	FIM uses hashing to ensure the integrity of files.
									B Incorrect	FIM uses hashing to ensure the integrity of files.
									C Incorrect	FIM uses hashing to ensure the integrity of files.
									D Incorrect	FIM uses hashing to ensure the integrity of files.
4.5	Data Privacy Controls	79	This is a voluntary tool used by organizations to create or improve privacy programs:	NIST Cybersecurity Framework.	**NIST Privacy Framework.**	ISO/IEC 27001.	General Data Protection Regulation (GDPR).	B	**A** Incorrect	This is a cybersecurity, not a privacy, framework.
									B **Correct**	The NIST Privacy Framework is a guideline to help organizations manage privacy programs.
									C Incorrect	This is an international information security standard.
									D Incorrect	This is the EU's privacy law.
4.5	Data Privacy Controls	80	A _____ is a decision tool to identify, document, manage, and mitigate privacy risks.	**Privacy Impact Assessment (PIA)**	Business Impact Assessment (BIA)	Vulnerability Assessment	Privacy Risk Management (PRM)	A	**A** **Correct**	A PIA is used to evaluate privacy risks.
									B Incorrect	A BIA manages business impact risks.
									C Incorrect	This assesses system vulnerabilities.
									D Incorrect	This is a fabricated term.
5.1	Logging, Monitoring and Alerting	81	Logging and monitoring is part of which NIST Cybersecurity Framework category?	Identification	Protection	**Detection**	Response	C	**A** Incorrect	Detection (event capture) is the third category in the NIST CSF.
									B Incorrect	Detection (event capture) is the third category in the NIST CSF.
									C **Correct**	Detection (event capture) is the third category in the NIST CSF.
									D Incorrect	Detection (event capture) is the third category in the NIST CSF.
5.1	Logging, Monitoring and Alerting	82	This type of security device provides centralized log management allowing for log integrity, correlation, and backup:	Virtualized logging.	Unified Threat Management (UTM).	Information Security Continuous Monitoring (ISCM).	**Security Incident and Event Management (SIEM).**	D	**A** Incorrect	A SIEM is a centralized system or service that provides real-time analysis of security alerts generated by applications and network hardware.
									B Incorrect	A SIEM is a centralized system or service that provides real-time analysis of security alerts generated by applications and network hardware.
									C Incorrect	A SIEM is a centralized system or service that provides real-time analysis of security alerts generated by applications and network hardware.
									D **Correct**	A SIEM is a centralized system or service that provides real-time analysis of security alerts generated by applications and network hardware.

5.2	Incident Response (IR) Planning	83	Which of the following is not one of the four high-level steps listed in the NIST Publication on Incident Response (SP800-61)?	Preparation	**Notify affected parties**	Detection & Analysis	Post-incident activity	B	A	Incorrect	This is included in the Containment, Eradication, and Recovery step.
									B	**Correct**	This is not included in the Containment, Eradication, and Recovery step.
									C	Incorrect	This is included in the Containment, Eradication, and Recovery step.
									D	Incorrect	This is included in the Containment, Eradication, and Recovery step.
5.2	Incident Response (IR) Planning	84	A violation or imminent threat of violation of computer security policies, acceptable use policies, or standard security practices is known as a:	**Computer Security Incident.**	Risk Event.	Penetration Test.	Hacking Incident.	A	A	**Correct**	A computer security incident is a violation or imminent threat of violation of computer security policies, acceptable use policies, or standard security practices.
									B	Incorrect	A computer security incident is a violation or imminent threat of violation of computer security policies, acceptable use policies, or standard security practices.
									C	Incorrect	A computer security incident is a violation or imminent threat of violation of computer security policies, acceptable use policies, or standard security practices.
									D	Incorrect	A computer security incident is a violation or imminent threat of violation of computer security policies, acceptable use policies, or standard security practices.
5.3	Incident Response (IR) Testing	85	Which is a typical way to test an organization's Incident Response Plan (IRP)?	**Tabletop exercise**	Penetration Test	Vulnerability Assessment	Disaster Recovery failover	A	A	**Correct**	Incident response testing includes, for example, the use of checklists, walk-through or tabletop exercises, simulations, and comprehensive real-life exercises.
									B	Incorrect	Incident response testing includes, for example, the use of checklists, walk-through or tabletop exercises, simulations, and comprehensive real-life exercises.
									C	Incorrect	Incident response testing includes, for example, the use of checklists, walk-through or tabletop exercises, simulations, and comprehensive real-life exercises.
									D	Incorrect	Incident response testing includes, for example, the use of checklists, walk-through or tabletop exercises, simulations, and comprehensive real-life exercises.
5.3	Incident Response (IR) Testing	86	Who is typically not included in incident response testing and training?	Internal users	Systems administrators	Incident response team	**External end-users**	D	A	Incorrect	External end-users are generally not included in IR testing and training.
									B	Incorrect	External end-users are generally not included in IR testing and training.
									C	Incorrect	External end-users are generally not included in IR testing and training.
									D	**Correct**	External end-users are generally not included in IR testing and training.
5.4	Digital Forensics	87	This function's purpose is to recover data from computers used as evidence during criminal, civil, or intellectual property investigations:	Incident Response.	Disaster Recovery.	**Digital Forensics.**	Cybersecurity.	C	A	Incorrect	Digital forensics is a part of Incident Response and is the technical capability to recover and investigate materials found on digital devices.
									B	Incorrect	Digital forensics is a part of Incident Response and is the technical capability to recover and investigate materials found on digital devices.
									C	**Correct**	Digital forensics is a part of Incident Response and is the technical capability to recover and investigate materials found on digital devices.
									D	Incorrect	Digital forensics is a part of Incident Response and is the technical capability to recover and investigate materials found on digital devices.
5.4	Digital Forensics	88	Use this when securing evidence to detail who is involved and how and when it was obtained:	Faraday bag.	Forensics toolkit.	**A Chain of Evidence custody form.**	Incident Response Plan.	C	A	Incorrect	A Faraday bag is used to ensure any digital evidence is protected from electronic emissions.
									B	Incorrect	Forensic examiners may use a toolkit as part of their investigation, but it may not document who is involved and the evidence obtained.
									C	**Correct**	When securing evidence, use a Chain of Evidence custody form to detail who is involved and how and when it was obtained.

									D	Incorrect	Your incident response plan is your procedure for conducting a security investigation.
5.5	Recovering Systems	**89**	This document is designed to ensure that an organization can recover from a potentially destructive incident and resume operations as quickly as possible following that event:	Incident Response Plan (IRP).	Risk Management Plan (RMP).	**Continuity of Operations Plan (COOP).**	Business Resumption Plan (BRP).	C	**A**	Incorrect	The COOP is a fundamental part of a system and business recovery.
									B	Incorrect	The COOP is a fundamental part of a system and business recovery.
									C	**Correct**	The COOP is a fundamental part of a system and business recovery.
									D	Incorrect	The COOP is a fundamental part of a system and business recovery.
5.5	Recovering Systems	**90**	The organization's order of restoration should be based on a(n):	**Business Impact Assessment (BIA).**	Order of Restoration Plan (ORP).	Server Risk Assessment (SRA).	Service Level Agreement (SLA).	A	**A**	**Correct**	Your BIA should establish what systems and services are recovered in a specific order based on business needs.
									B	Incorrect	Your BIA should establish what systems and services are recovered in a specific order based on business needs.
									C	Incorrect	Your BIA should establish what systems and services are recovered in a specific order based on business needs.
									D	Incorrect	Your BIA should establish what systems and services are recovered in a specific order based on business needs.
5.6	Business Continuity and recovery	**91**	Which of the following is not a step in the development of a business continuity plan according to the Ready.gov website?	Business impact analysis (BIA)	**Failover Site Determination**	Recovery Strategies	Testing & Exercises	B	**A**	Incorrect	Failover Site Determination may be conducted in the Recovery Strategy step based on the business needed.
									B	**Correct**	Failover Site Determination may be conducted in the Recovery Strategy step based on the business needed.
									C	Incorrect	Failover Site Determination may be conducted in the Recovery Strategy step based on the business needed.
									D	Incorrect	Failover Site Determination may be conducted in the Recovery Strategy step based on the business needed.
5.6	Business Continuity and recovery	**92**	Which of the following should be included in an organization's Business Continuity Plan?	Recovery objectives	Roles and responsibilities	**Both A and B**	Neither A nor B	C	**A**	Incorrect	Recovery objectives and roles and responsibilities should be included in a standard BCP.
									B	Incorrect	Recovery objectives and roles and responsibilities should be included in a standard BCP.
									C	**Correct**	Recovery objectives and roles and responsibilities should be included in a standard BCP.
									D	Incorrect	Recovery objectives and roles and responsibilities should be included in a standard BCP.
6.1	The Auditor's Role	**93**	This is a practice of having more than one person required to complete a task and is used to prevent fraud and error:	**Segregation of Duties.**	Least Privilege.	Single Sign-On.	Independence.	A	**A**	**Correct**	The principle of SOD is based on shared responsibilities of a key process that disperses the critical functions of that process to more than one person or department.
									B	Incorrect	The principle of SOD is based on shared responsibilities of a key process that disperses the critical functions of that process to more than one person or department.
									C	Incorrect	The principle of SOD is based on shared responsibilities of a key process that disperses the critical functions of that process to more than one person or department.
									D	Incorrect	The principle of SOD is based on shared responsibilities of a key process that disperses the critical functions of that process to more than one person or department.
6.2	CISO's Role	**94**	This corporate executive creates the strategic information security plan and manages organization-wide system and data protection initiatives:	IT Audit Director.	**Chief Information Security Officer (CISO).**	Chief Financial Officer.	Chief Information Officer.	B	**A**	Incorrect	The CISO is responsible for both the strategic direction and the operational aspects of an organization's information security program.
									B	**Correct**	The CISO is responsible for both the strategic direction and the operational aspects of an organization's information security program.
									C	Incorrect	The CISO is responsible for both the strategic direction and the operational aspects of an organization's information security program.

									D	Incorrect	The CISO is responsible for both the strategic direction and the operational aspects of an organization's information security program.
6.3	Establishing Audit Scope	**95**	Which of the following is a typical method for limiting the scope of a cybersecurity audit?	Multi-factor authentication	Centralizing management functions	**Network separation/segmentation**	All of the above	C	**A**	Incorrect	Separating systems/servers on their own network segment limits the audit to just that area.
									B	Incorrect	Separating systems/servers on their own network segment limits the audit to just that area.
									C	**Correct**	Separating systems/servers on their own network segment limits the audit to just that area.
									D	Incorrect	Separating systems/servers on their own network segment limits the audit to just that area.
6.4	Building the Audit Plan	**96**	Which step is not typically part of planning a cybersecurity audit?	Gain management support	Establish the audit timeline	Gather information	**Implement cybersecurity controls**	D	**A**	Incorrect	Implementing controls is outside of planning a cybersecurity audit.
									B	Incorrect	Implementing controls is outside of planning a cybersecurity audit.
									C	Incorrect	Implementing controls is outside of planning a cybersecurity audit.
									D	**Correct**	Implementing controls is outside of planning a cybersecurity audit.
6.5	Cybersecurity Evaluation Methods	**97**	Which of the following is not an assessment method as stated in NIST SP 800-53A?	**Scan**	Interview	Examine	Test	A	**A**	**Correct**	NIST lists three types of standard assessment methods: Interview, Examine, and Test. A scan is a type of testing.
									B	Incorrect	NIST lists three types of standard assessment methods: Interview, Examine, and Test. A scan is a type of testing.
									C	Incorrect	NIST lists three types of standard assessment methods: Interview, Examine, and Test. A scan is a type of testing.
									D	Incorrect	NIST lists three types of standard assessment methods: Interview, Examine, and Test. A scan is a type of testing.
6.6	Vulnerability Assessments, Scanning, and Testing	**98**	This application is used to scan networks for IP addresses and open ports or services:	Microsoft Defender.	OWASP ZAP.	**Nmap.**	Wireshark.	C	**A**	Incorrect	Nmap is a tool for scanning networks for open IPs and ports. Zenmap is the GUI front-end.
									B	Incorrect	Nmap is a tool for scanning networks for open IPs and ports. Zenmap is the GUI front-end.
									C	**Correct**	Nmap is a tool for scanning networks for open IPs and ports. Zenmap is the GUI front-end.
									D	Incorrect	Nmap is a tool for scanning networks for open IPs and ports. Zenmap is the GUI front-end.
6.6	Vulnerability Assessments, Scanning, and Testing	**99**	According to the Payment Card Industry (PCI), how often do scans need to be conducted for a cardholder data environment?	Continually	**Quarterly**	Annually	As determined by management	B	**A**	Incorrect	Quarterly Scans are required in accordance with PCI DSS Requirement 11.2.
									B	**Correct**	Quarterly Scans are required in accordance with PCI DSS Requirement 11.2.
									C	Incorrect	Quarterly Scans are required in accordance with PCI DSS Requirement 11.2.
									D	Incorrect	Quarterly Scans are required in accordance with PCI DSS Requirement 11.2.
6.7	Penetration testing	**100**	This is a live test of the effectiveness of security defenses through mimicking the actions of real-life attackers:	Vulnerability Assessment.	**Penetration (Pen) Test.**	Red Team Exercise.	Threat Modeling.	B	**A**	Incorrect	This is the ISACA definition of a Penetration Test.
									B	**Correct**	This is the ISACA definition of a Penetration Test.
									C	Incorrect	This is the ISACA definition of a Penetration Test.
									D	Incorrect	This is the ISACA definition of a Penetration Test.
6.7	Penetration testing	**101**	Reconnaissance is a part of which phase of penetration testing?	Planning	**Discovery**	Access	Attack	B	**A**	Incorrect	Reconnaissance is a step in the discovery phase.

									B	**Correct**	Reconnaissance is a step in the discovery phase.
									C	Incorrect	Reconnaissance is a step in the discovery phase.
									D	Incorrect	Reconnaissance is a step in the discovery phase.
6.8	Security Maturity Models (Capability Maturity Model [CMM])	**102**	This is the Capability Maturity Model (CMM) level, where processes are documented, and the organization is usually reactive:	Level 1 - Initial.	**Level 2 - Repeatable.**	Level 3 - Defined.	Level 4 - Quantitatively Managed.	B	A	Incorrect	Level 2, Repeatable, is characteristic of this level of maturity that some processes are repeatable, possibly with consistent results. Process discipline is unlikely to be rigorous.
									B	**Correct**	Level 2, Repeatable, is characteristic of this level of maturity that some processes are repeatable, possibly with consistent results. Process discipline is unlikely to be rigorous.
									C	Incorrect	Level 2, Repeatable, is characteristic of this level of maturity that some processes are repeatable, possibly with consistent results. Process discipline is unlikely to be rigorous.
									D	Incorrect	Level 2, Repeatable, is characteristic of this level of maturity that some processes are repeatable, possibly with consistent results. Process discipline is unlikely to be rigorous.
6.9	Audit Using NIST Frameworks	**103**	Which of the following is not a goal of the NIST Cybersecurity Framework?	Consistent and cost-effective application of security controls	Repeatable processes	**Standard operating instructions for all organizations**	A technology-neutral and flexible approach	C	A	Incorrect	NIST focuses on strategic directions and processes rather than industry or area-specific operations.
									B	Incorrect	NIST focuses on strategic directions and processes rather than industry or area-specific operations.
									C	**Correct**	NIST focuses on strategic directions and processes rather than industry or area-specific operations.
									D	Incorrect	NIST focuses on strategic directions and processes rather than industry or area-specific operations.
6.1	Audit With Other Security Frameworks and Standards (ISO)	**104**	This reference provides 20 control areas separated into basic, foundational, and organizational functions:	ISO/IEC 27001:2013.	**Center for Internet Security (CIS) Controls.**	NIST CSF.	PCI DSS.	B	A	Incorrect	The CIS Controls provides an implementation path for establishing a cybersecurity program.
									B	**Correct**	The CIS Controls provides an implementation path for establishing a cybersecurity program.
									C	Incorrect	The CIS Controls provides an implementation path for establishing a cybersecurity program.
									D	Incorrect	The CIS Controls provides an implementation path for establishing a cybersecurity program.
6.11	Auditing PCI DSS	**105**	This is comprised of people, processes, and technology that store, process, or transmit credit/debit card data or sensitive authentication data:	Data Flow Diagram (DFD).	Virtualized Data Environment (VDE).	**Cardholder Data Environment (CDE).**	Credit Card Database (CCDB).	C	A	Incorrect	This is the PCI definition for a CDE.
									B	Incorrect	This is the PCI definition for a CDE.
									C	**Correct**	This is the PCI definition for a CDE.
									D	Incorrect	This is the PCI definition for a CDE.
6.11	Auditing PCI DSS	**106**	A _____ is the final report for a PCI Assessment/Audit.	**Report on Compliance (RoC)**	Compliance Standardization Report (CSR)	Self-Assessment Questionnaire (SAQ)	PCI Assessment Report (PAR)	A	A	**Correct**	The Report on Compliance (RoC) is the official report demonstrating compliance with DSS.
									B	Incorrect	The Report on Compliance (RoC) is the official report demonstrating compliance with DSS.
									C	Incorrect	The Report on Compliance (RoC) is the official report demonstrating compliance with DSS.
									D	Incorrect	The Report on Compliance (RoC) is the official report demonstrating compliance with DSS.
7.1	Collecting and Organizing Cybersecurity Evidence	**107**	A _____ is a document used as a risk management tool and to fulfill regulatory compliance acting as a repository for identified risks and including additional information about each one.	Business Impact Assessment (BIA)	**Risk Register**	Vulnerability Scanner	Audit log	B	A	Incorrect	A risk register is a tool for documenting risks and can be used for collecting cybersecurity audit evidence.

										B	**Correct**	A risk register is a tool for documenting risks and can be used for collecting cybersecurity audit evidence.
										C	Incorrect	A risk register is a tool for documenting risks and can be used for collecting cybersecurity audit evidence.
										D	Incorrect	A risk register is a tool for documenting risks and can be used for collecting cybersecurity audit evidence.
7.2	NIST Reporting Requirements	**108**	The _____ is the corrective action plan (document or tool) for tracking and planning the resolution of the weaknesses.	Business Impact Assessment (BIA)	System Security Plan (SSP)	Risk Comliance Report (RCR)	**Plan of Action and Milestones (POAM)**	D		A	Incorrect	The POAM is a document that identifies tasks needing to be accomplished. It details resources required to accomplish the elements of the plan, any milestones in meeting the tasks, and scheduled completion dates for the milestones.
										B	Incorrect	The POAM is a document that identifies tasks needing to be accomplished. It details resources required to accomplish the elements of the plan, any milestones in meeting the tasks, and scheduled completion dates for the milestones.
										C	Incorrect	The POAM is a document that identifies tasks needing to be accomplished. It details resources required to accomplish the elements of the plan, any milestones in meeting the tasks, and scheduled completion dates for the milestones.
										D	**Correct**	The POAM is a document that identifies tasks needing to be accomplished. It details resources required to accomplish the elements of the plan, any milestones in meeting the tasks, and scheduled completion dates for the milestones.
7.3	Prioritizing Risks and Influencing Decisions	**109**	In the NIST Risk Management Framework (RMF), this role makes the final risk decisions before a system is allowed in production:	IT Audit Directory.	Chief Information Security Officer (CISO).	**Authorizing Official (AO).**	Chief Risk Officer (CRO).	C		A	Incorrect	According to NIST, the AO is a senior official or executive with the authority to formally assume responsibility for operating an information system at an acceptable level of risk to organizational operations.
										B	Incorrect	According to NIST, the AO is a senior official or executive with the authority to formally assume responsibility for operating an information system at an acceptable level of risk to organizational operations.
										C	**Correct**	According to NIST, the AO is a senior official or executive with the authority to formally assume responsibility for operating an information system at an acceptable level of risk to organizational operations.
										D	Incorrect	According to NIST, the AO is a senior official or executive with the authority to formally assume responsibility for operating an information system at an acceptable level of risk to organizational operations.