# ISC2

## Exam Questions CC

Certified in Cybersecurity (CC)

**NEW QUESTION 1**
What federal law requires the use of vulnerability scanning on information systems operated by federal government agencies?

A. FISMA
B. HIPAA
C. GLBA
D. FERPA

**Answer:** A

**NEW QUESTION 2**
Faking the sender address in a transmission to gain illegal entry into a secure system

A. Phishing
B. ARP
C. Spoofing
D. ALL

**Answer:** C

**NEW QUESTION 3**
What are registered port used for

A. Common protocols at the core of TCP/IP model
B. Used for web servers
C. Used for in housed or opensource applications
D. Proprietary applications from vendors and develope

**Answer:** D

**NEW QUESTION 4**
What is the recommended fire suppression system for server rooms

A. Foam based
B. Water based
C. Powder based
D. ftac hacorl

**Answer:** D

**NEW QUESTION 5**
A chief information security officer (CISO) at a large organization documented a policy that establishes the acceptable use of cloud environments for all staff. This is an example of

A. Technical control
B. Physical control
C. Cloud control
D. Management/Administrative control

**Answer:** D

**NEW QUESTION 6**
Common network device used to connect networks?

A. Server
B. Endpoint
C. Router
D. Switch

**Answer:** C

**NEW QUESTION 7**
What is the importance of non-repudiation in todays world of ecommerce

A. It ensures that people are not held responsible for transaction that did not conduct
B. It ensures that people are held responsible for transactions they conducted
C. It ensures that transactions are not conducted online
D. It ensures that transactions are conducted online

**Answer:** B

**NEW QUESTION 8**
Ping flood attack target which OSI layer

A. Layer 4
B. Layer 3
C. Layer 5
D. Layer 6

**Answer:** B

**NEW QUESTION 9**
Which is related to Standard

A. NIST
B. GDPR
C. HIPAA
D. ALL

**Answer:** A

**NEW QUESTION 10**
Requires that all instances of the data be identical in form,

A. Confidentiality
B. Availability
C. Consistency
D. ALL

**Answer:** C

**NEW QUESTION 10**
Which of the following is not a Social engineering technique

A. Pretexting
B. Baiting
C. Quid pro quo
D. Double Dealing

**Answer:** D

**NEW QUESTION 14**
Example of Token based Authentication

A. Kerberos
B. Basic
C. OAuth
D. NTLN

**Answer:** C

**NEW QUESTION 19**
A hacker gains access to a compony network and begins to intercept network traffic in order to steal login credentials which OSI layer is being attacked

A. Data Link layer
B. Physical layer
C. Network Layer
D. Application laver

**Answer:** D

**NEW QUESTION 23**
Which of the following is not a protocol of the OSI layer 3

A. IGMP
B. IP
C. ICMP
D. SSH

**Answer:** D

**NEW QUESTION 25**
Which type of control is used to minimize the impact of an attack and to restore normal operations as quick as possible

A. Compensatory Control
B. Corrective Control
C. Recovery control
D. Detective Control

**Answer:** C

**NEW QUESTION 27**
What type of attack does the attacker store and reuse login information. Select the BEST answer?

A. Man-in-the-middle attack
B. Smurf attack
C. DDoS attack
D. Replay attack

**Answer:** D

**NEW QUESTION 28**
Which is the Not the component of a Business Continuity (BC) plan

A. Immediate response procedures and checklists
B. Notification systems and call trees for alerting personnel
C. Guidance for management, including designation of authority for specific managers
D. Manacomont

**Answer:** D

**NEW QUESTION 32**
What is the importance of identifying roles and responsibilities in incident response planning?

A. To prevent incidents from happening
B. To ensure that everyone knows their job in the incident response process
C. To reduce the impact of the incident
D. To choose an appropriate containment strategy

**Answer:** B

**NEW QUESTION 33**
What is an incident in the context of cybersecurity

A. Any observable occurrence in a network or system
B. A deliberate security incident in which an intruder gains access to a system or system resource without authorization
C. A particular attack that exploits system vulnerabilities
D. An event that actually or potentially jeopardizes the confidentiality integrity or availability of an information system.

**Answer:** D

**NEW QUESTION 35**
Which element of the security policy framework includes recommendation that are NOT bindings?

A. Procedures
B. Guidelines
C. Standards
D. Policies

**Answer:** C

**NEW QUESTION 38**
The last phase in the data security cycle is

A. Encryption
B. Destruction
C. Archival
D. Backup

**Answer:** B

**NEW QUESTION 39**
The documentation of a predetermined set of instructions or procedures to detect, respond to andlimit consequences of a malicious cyberattack against an organization's information systems(s).

A. IR
B. IRP
C. BCP
D. DRP

**Answer:** B

**NEW QUESTION 44**

COVID-19 is one of the perfect example of a situation, where a ______ plan is enacted to sustain the business

A. IRP
B. DRP
C. BCP
D. ALL

**Answer:** C

**NEW QUESTION 47**
What is the purpose of defense in depth in information security

A. To Implement only technical controls to prevent a cyber attack
B. To provide unrestricted access to organization assets
C. To establish variable barriers across multiple layers and mission of the organization
D. To guarantee that a cyber attack will not occur

**Answer:** C

**NEW QUESTION 52**
What does Personally Identifiable Information (Pll) pertain to?

A. Information about an individual's health status
B. Data about an individual that could be used to identify them (Correct)
C. Trade secrets, research, business plans and intellectual property
D. The importance assigned to information by its owner

**Answer:** B

**NEW QUESTION 54**
A tool used to inspect outbound traffic to reduce threats

A. Anti-ma I ware
B. NIDC
C. DLP
D. Firewall

**Answer:** C

**NEW QUESTION 58**
What security feature used in HTTPS

A. IPSec
B. SSH
C. ICMP
D. SSL/TLS

**Answer:** D

**NEW QUESTION 61**
A cyber security professional observes an unusual occurrence in the network or system. What term best describes this situations

A. Breach
B. Exploit
C. Event
D. Intrusion

**Answer:** C

**NEW QUESTION 63**
What is the difference between hub and switch

A. A hub is less likely to be used in home network
B. A hub can create separate broad cast domains when used to create Vlan
C. A hub retransmits traffic to all devices, while a switch route traffic to a specific devices
D. A switch retransmits traffic to all devices, while a hub route traffic to a specific devices

**Answer:** C

**NEW QUESTION 65**
A company needs to protect its confidential data from unauthorized access which logical control is best suited for this scenario

A. Encryption
B. Firewall
C. Antivirus

D. Hashing

**Answer:** A

**NEW QUESTION 68**
6 Which access control method uses attributes and rules to define access policies that are evaluate by a central Policy Decision Point (PDP)

A. DAC
B. RBAC
C. MAC
D. ABAC

**Answer:** D

**NEW QUESTION 73**
Which Prevents Threat

A. Antivirus
B. IDS
C. SIEM
D. HIDS

**Answer:** A

**NEW QUESTION 75**
A security practitioner who needs step-by-step instructions to complete a provisioning task

A. Standard
B. Policy
C. Procedure
D. Laws or Regulations

**Answer:** C

**NEW QUESTION 76**
When Operating in A Cloud Environment, What Cloud Deployment Model Provides Security Teams With The Greatest Access To Forensic Information?

A. FaaS
B. SaaS
C. PaaS
D. laaS

**Answer:** D

**NEW QUESTION 80**
Dylan is creating a cloud architecture that requires connections between systems in two different private VPCs. What would be the best way for Dylan to enable this access?

A. VPN Connection
B. Internet Gateway
C. Public IP Address
D. VPC Endpoint

**Answer:** D

**NEW QUESTION 85**
Which is the component of a Business Continuity (BC) plan

A. Immediate response procedures and checklists
B. Notification systems and call trees for alerting personnel
C. Guidance for management, including designation of authority for specific managers
D. ALL

**Answer:** D

**NEW QUESTION 89**
Which type of database combines related records and fields into a logical tree structure?

A. Relational
B. Hierarchical
C. Object-oriented
D. Network

**Answer:** B

**NEW QUESTION 93**
Which of the following is a characteristic of cloud

A. Broad Network Access
B. Rapid Elasticity
C. Measured Service
D. All

**Answer:** B

**NEW QUESTION 97**
Which is the loopback address

A. ::1
B. 127.0.0.1
C. 255.255.255.0
D. Both A and B

**Answer:** D

**NEW QUESTION 100**
Which type of software testing focuses on examining the source code for vulnerabilities and security issues?

A. Black-box testing
B. White-box testing
C. Functional testing
D. User acceptance testing

**Answer:** B

**NEW QUESTION 102**
The method of distributing network traffic equally across a pool of resources that support an application

A. Vlan
B. DNS
C. VPN
D. Load Balancing

**Answer:** D

**NEW QUESTION 104**
Which of the following security controls is designed to prevent unauthorized access to sensitive information by ensuring that it is only accessible to authorized users?

A. Encryption
B. Firewall
C. Antivirus
D. Access control

**Answer:** D

**NEW QUESTION 108**
Created by switches to logically segment a network without altering its physical topology.

A. LAN
B. WAN
C. VLAN
D. MAN

**Answer:** C

**NEW QUESTION 112**
A company primary data center goes down due to a hardware failure causing a major disruption to the IT and communications systems. What is the focus of disaster recovery planning in this scenario

A. Maintaining critical business functions during the disruption
B. Fixing the hardware failure
C. Restoring IT and communications back to full operations after the disruptions
D. Guiding the actions of emergency response personnel during the disruption

**Answer:** C

**NEW QUESTION 116**
A company network has been infected with malware and all its servers are down. What is the first step that the Disaster Recovery team should take to restore the systems?

A. Disconnect the affected systems from the network
B. Conduct a risk assessment of determine the extent of the damage
C. Restore data from backup systems
D. Contact the enforcement to investigate the cyberattack

**Answer:** A

**NEW QUESTION 119**
Which addresses reserved for internal network use and are not routable on the internet.

A. acOO:: to adff:ffff:ffff:ffff:ffff:ffff:ffff:ffff
B. fcOO:: to fdff:ffff:ffff:ffff:ffff:ffff:ffff:ffff
C. bcOO:: to bdff:ffff:ffff:ffff:ffff:ffff:ffff:ffff
D. ccOO:: to cdff:ffff:ffff:ffff:ffff:ffff:ffff:ffff

**Answer:** B

**NEW QUESTION 122**
Hashing used to safe guard which CIA triad

A. Confidentiality
B. Availability
C. Integrity
D. All

**Answer:** C

**NEW QUESTION 126**
What is the primary factor in the reliability of information and system

A. Authenticity
B. Confidentiality
C. Integrity
D. Availability

**Answer:** C

**NEW QUESTION 128**
Configuration settings or parameters stored as data, managed through a software graphical user interface (GUI) is

A. Logical access control
B. Physical access control
C. Administrative Access control

**Answer:** A

**NEW QUESTION 131**
Which plan provides the team with immediate response procedures and check lists and guidance for management?

A. BCP
B. IRP
C. DRP
D. ALL

**Answer:** A

**NEW QUESTION 133**
Which of the following is not an element of system security configuration management

A. Baselines
B. Updates
C. Inventory
D. Audit logs

**Answer:** D

**NEW QUESTION 138**
Which is the SSH port

A. 21
B. 23
C. 24
D. 22

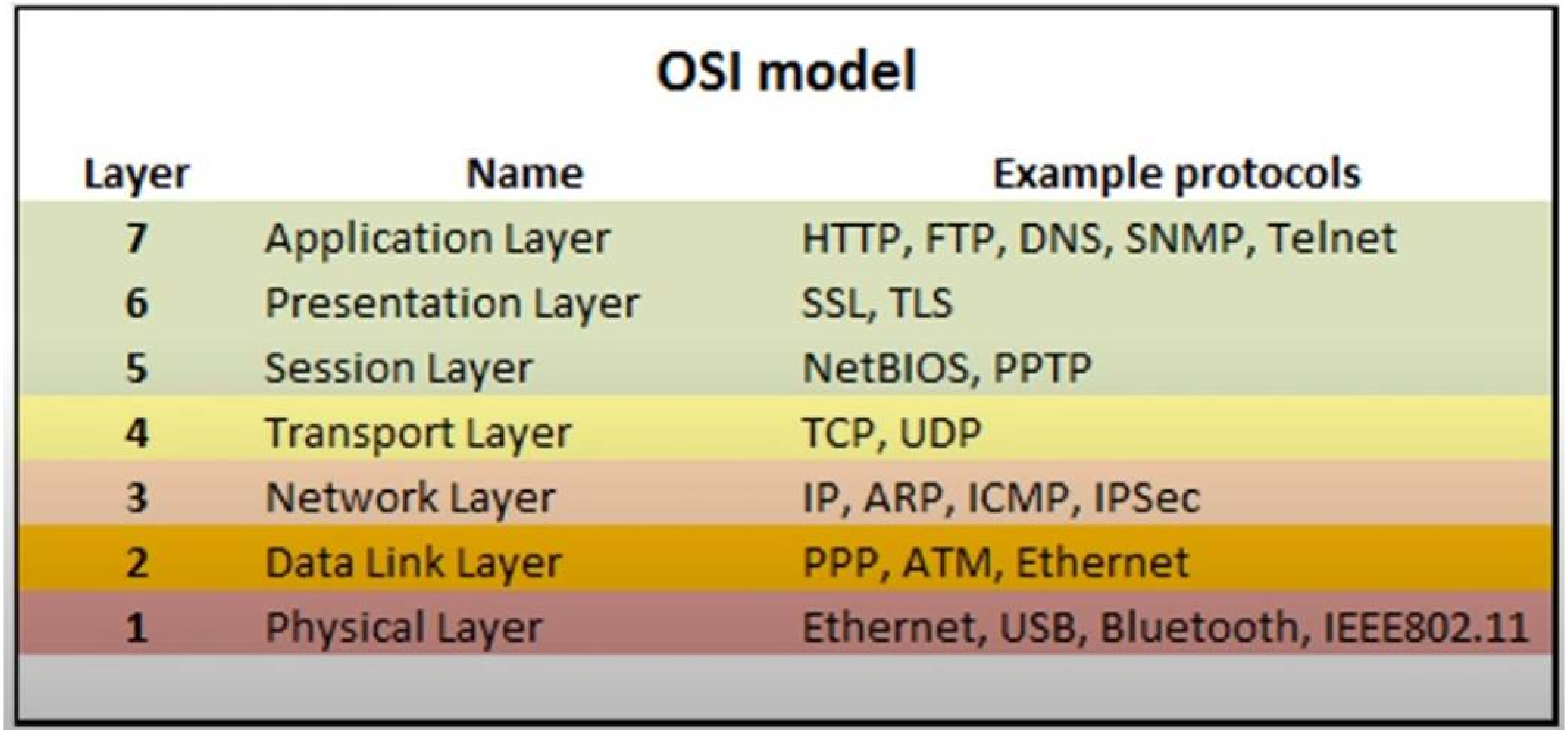
**Answer:** D

**NEW QUESTION 142**
Which access control model grants permission based on the sensitivity of the data and the user job functions

A. DAC
B. RBAC
C. MAC
D. RUBAC

**Answer:** B

**NEW QUESTION 146**
Exhibit.



OSI model

| Layer | Name | Example protocols |
|---|---|---|
| 7 | Application Layer | HTTP, FTP, DNS, SNMP, Telnet |
| 6 | Presentation Layer | SSL, TLS |
| 5 | Session Layer | NetBIOS, PPTP |
| 4 | Transport Layer | TCP, UDP |
| 3 | Network Layer | IP, ARP, ICMP, IPSec |
| 2 | Data Link Layer | PPP, ATM, Ethernet |
| 1 | Physical Layer | Ethernet, USB, Bluetooth, IEEE802.11 |

IPSec works in which layer of OSI Model

A. Layer 2
B. Layer 5
C. Layer 3
D. Layer 7

**Answer:** C

**NEW QUESTION 149**
Which of the following best describes the puposes of a business impact analysis?

A. To document a predetermined set of instructions or procedures for restoring IT and communications services after a disruption
B. To mitigate security violation and ensure that business operation can continue during a contigency
C. To provide a high level overview of the disaster recovery plan
D. To analyze an information systems requirements and functions in order to determine system contingency priorities

**Answer:** D

**NEW QUESTION 151**
A company has implemented Mandatory access control for its confidential data which of the following statement is true

A. The data can be accessed by users who possess a need to know
B. Access controls cannot be changed by anyone except the system administrato
C. The owner of the data can modify the access control
D. The system adminstrator can change the access contrls

**Answer:** B

**NEW QUESTION 155**
Which of the following is NOT one of the three main components of a sql database?

A. Views
B. Schemas
C. Tables
D. Object-oriented interfaces

**Answer:** D

**NEW QUESTION 157**
Which of these components is very likely to be instrumental to any disaster recovery (DR) effort?

A. Routers
B. Laptops
C. Firewalls
D. Backups

**Answer:** D

**NEW QUESTION 161**
What is the priority of incident response in the context of incident management

A. Protect the organization mission and objectives
B. Reduce the impact of the incident
C. Protect life health and safety
D. Resume interrupted operations as soon as possible

**Answer:** C

**NEW QUESTION 163**
Representation of data at Layer 3 of the Open Systems Interconnection (OSI) model.

A. Segment
B. Packet
C. Frame
D. None of the Above

**Answer:** B

**NEW QUESTION 164**
Which encryption type used in HTTPS communication

A. Symentric
B. Assymentric
C. None
D. Both A and B

**Answer:** D

**NEW QUESTION 166**
are events that may indicate that an organization's systems or data have been compromised or that measures put in place to protect them have failed

A. Exploit
B. Security Incident
C. Threat
D. Rreach

**Answer:** B

**NEW QUESTION 168**
Which type of attack will most effectively maintain remote access and control over the victims computer

A. Phising
B. Trojans
C. XSS
D. RootKits

**Answer:** D

**NEW QUESTION 169**
Actions, processes and tools for ensuring an organization can continue critical operations during a contingency.

A. BC
B. DR
C. IR
D. All

**Answer:** A

**NEW QUESTION 172**
The Bell and LaPadula access control model is a form of

A. RBAC
B. MAC
C. DAC
D. ABAC

**Answer:** B

**NEW QUESTION 173**
A measure of the degree to which an organization depends on the information or information system for the success of a mission or of a business function.

A. Availability
B. Criticality
C. Authorization
D. Confidentiality

**Answer:** B

**NEW QUESTION 174**
Shaun is planning to protect their data in all states(Rest, Motion, use), defending against data leakage. What would be the BEST solution to implement?

A. End to end encryption.
B. Hashing
C. DLP
D. Threat Modeling

**Answer:** C

**NEW QUESTION 177**
Who must follow HIPAA Compliance

A. Energy Sector
B. Health Care
C. Finance Sector
D. ALL

**Answer:** B

**NEW QUESTION 182**
A company security team detected a cyber attack against it information systems and activates a set of procedures to mitigate the attack., What type of plan is this?

A. Business continuity plan
B. Incident response plan
C. Disaster recvoery plan
D. Security operation plan

**Answer:** B

**NEW QUESTION 185**
Works via encapsulation and wrapping a packet inside another packet.

A. Network segmentation
B. Load balancing
C. Tunnelling
D. Data encryption

**Answer:** C

**NEW QUESTION 190**
Example of Deterrent controls

A. CCTV
B. BCP
C. DRP
D. IRP

**Answer:** A

**NEW QUESTION 195**
What is the term used to denote the inherent set of privileges assigned to a user upon the creation of a new account?

A. Aggregation
B. Transitivity
C. Baseline
D. Entitlement

**Answer:** C

**NEW QUESTION 197**
Which of the following types of vulnerabilities cannot be discovered in the course of a routine vulnerability assessment?

A. Zero-day vulnerability
B. Kernel flaw
C. Buffer overflow
D. File and directory permissions

**Answer:** A

**NEW QUESTION 201**
Which type of authentication is something which you

A. Type1
B. Type 2
C. Type 3
D. Type 4

**Answer:** C

**NEW QUESTION 203**
What is the process of verifying a users identity called?

A. Confidentiality
B. Autentication
C. Authorization
D. Identification

**Answer:** B

**NEW QUESTION 207**
Your organization is concerned about network security and wants to prevent unauthorized access to its resources by implementing a security model where the network has not
trusted space what type of security model is this

A. Zero trust
B. Trusted computing
C. Trusted platform modelus
D. Trusted execution environment

**Answer:** A

**NEW QUESTION 208**
Access control used in in high-security situations such as military and government organizations.

A. DAC
B. MAC
C. RBAC
D. ABAC

**Answer:** B

**NEW QUESTION 213**
Which of these is an example of deterrent control

A. Biometric
B. Guard Dog
C. Encryption
D. Trunstile

**Answer:** B

**NEW QUESTION 214**
True or False? The IT department is responsible for creating the organization's business continuity plan

A. True
B. False

**Answer:** B

**NEW QUESTION 219**
Which is the first step in the risk management process

A. Risk response
B. Risk mitigation
C. Risk identification
D. Risk assessment

**Answer:** C

**NEW QUESTION 221**
Which type of fire suppression system is more friendly to electronics

A. Carbon di Oxide based
B. Chemical based
C. Water based
D. Foam based

**Answer:** A

**NEW QUESTION 222**
Which protocol would be most suitable to fulfill the secure communication requirements between clients and the server for a company deploying a new application?

A. FTP
B. HTTP
C. HTTPS
D. SMTP

**Answer:** C

**NEW QUESTION 224**
When the ISC2 Mail server sends mail to other mail servers it becomes —?

A. SMTP Server
B. SMTP Peer
C. SMTP Master
D. SMTP Client

**Answer:** D

**NEW QUESTION 226**
What is the purpose of immediate response procedures and checklists in a BCP

A. To notify personnel that the BCP is being enacted
B. To provide guidance for management
C. To safeguard the confidentiality, integrity and availability of information
D. To ensure business operations are accounted for in the plan

**Answer:** A

**NEW QUESTION 228**
What cybersecurity principle focuses on granting users only the privileges necessary to perform their job functions?

A. Least privilege (Correct)
B. defense in depth
C. separation of duties
D. need-to-know basis

**Answer:** A

**NEW QUESTION 229**
1 ______ is a weighted factor based on a subjective analysis of the probability that a given threat or set of threats is capable of exploiting a given vulnerability or set of vulnerabilities.

A. Likelihood of occurrence
B. Threat Vector
C. Risk
D. Impact

**Answer:** A

**NEW QUESTION 234**
Malicious code that acts like a remotely controlled "robot" for an attacker, with other Trojan and worm capabilities.

A. Rootkit
B. Ma I ware
C. Bot

D. Virus

**Answer:** C

**NEW QUESTION 236**
A company experiences a power outage that causes a major disruption in its operations. What type of plan will help the company sustain operations?

A. DRP
B. IRP
C. BCP
D. ALL

**Answer:** C

**NEW QUESTION 239**
Which plan is activated when both the Incident response and BCP fails

A. Risk Management
B. BIA
C. DRP
D. None

**Answer:** C

**NEW QUESTION 240**
Which access control model can grant access to a given object based on complex rules

A. ABAC
B. DAC
C. MAC
D. RBAC

**Answer:** A

**NEW QUESTION 243**
Which one of the following cryptographic algorithms does not depend upon the prime factorization problem?

A. RSA - Rivest-Shamir-Adleman
B. GPG - GNU Privacy Guard
C. ECC - Elliptic curve cryptosystem
D. PGP - Pretty Good Privacy

**Answer:** C

**NEW QUESTION 244**
A company data center has been breached by hackers and all its systems have been taken down what is the main objective of the DRP in such a scenario?

A. To relocate the data center to another location
B. To ensure the physical safety of employees in the data center
C. To investigate and prosecute the hackers responsible of the attack
D. To restore the IT systems to their last known state

**Answer:** D

**NEW QUESTION 249**
An unknown person obtaining access to the company file system without authorization is example of

A. Intrusion
B. Breach
C. Exploit
D. Incident

**Answer:** B

**NEW QUESTION 253**
Which uses encrypted, machine-generated codes to verify a user's identity.

A. Basic Authentication
B. Form Based Authentication
C. Token Based Authentication
D. All

**Answer:** C

**NEW QUESTION 254**
A new BYOD policy has been enforced in NEW Corp which type of control is used to enforce thissecurity policies

A. Physical control
B. Logical Control
C. Administrative Control
D. Technical Control

**Answer:** C

**NEW QUESTION 258**
The process of applying secure configurations (to reduce the attack surface)

A. Security Assessment
B. Security Evaluation
C. Security Benchmark
D. Security Hardening

**Answer:** D

**NEW QUESTION 260**
What is the primary goal of implementing input validation in application security?

A. To ensure all inputs are stored in a secure database
B. To prevent unauthorized access to the application
C. To validate and sanitize user inputs to prevent code injection attacks (Correct)
D. To encrypt sensitive data transmitted between the client and server

**Answer:** C

**NEW QUESTION 265**
An outward-facing IP address used to access the Internet.

A. Global Address
B. Private Address
C. Public Address
D. DNS

**Answer:** C

**NEW QUESTION 268**
Which protocol is used for secure email

A. POP3S
B. IMAPS
C. SMTPS
D. All

**Answer:** D

**NEW QUESTION 271**
Port used in DNS

A. 53
B. 80
C. 45
D. 54

**Answer:** A

**NEW QUESTION 272**
Which of the following does not normally influence an organization's retention policy for logs?

A. Laws
B. Corporate governance
C. Regulations
D. Audits

**Answer:** D

**NEW QUESTION 275**
An analysis of an information system's requirements, functions, and interdependencies used to characterize system contingency requirements and priorities in the event of a significant disruption.

A. BIA

B. DR
C. BCP
D. IRP

**Answer:** A

**NEW QUESTION 277**
Can be considered to be a fingerprint of the file or message

A. Hashing .
B. encryption
C. decryption
D. encoding

**Answer:** A

**NEW QUESTION 279**
A large organization is planning to create a DRP. Which of the following is the BEST document to provide a high-level overview of the plan?

A. Technical guides for IT personnel
B. Department specific plans
C. Full copies of the plan for critical disaster recovery team members
D. Execute summary

**Answer:** D

**NEW QUESTION 281**
The primary goal of a risk assessment

A. Avoid Risk
B. Estimate and Prioritize Risk
C. Ignore risk
D. Evaluate the Impact

**Answer:** B

**NEW QUESTION 282**
Natalia is concerned about the security of his organization's domain name records and would like to adopt a technology that ensures their authenticity by adding digital signatures. Select the MOST appropriate technology to use?

A. DNSSIGN
B. DNSSEC
C. CERTDNS
D. DNS2

**Answer:** B

**NEW QUESTION 284**
Government can imposes financial penalties as a consequence of breaking a

A. Standard
B. Regulation
C. Policy
D. Procedures

**Answer:** B

**NEW QUESTION 287**
Which of the following is a common security measure to prevent Cross Site Scripting (XSS) attacks in web applications?

A. implementing strong password policies
B. using a firewall to block incoming traffic
C. validating and sanitizing user input (Correct)
D. encrypting data during transmission

**Answer:** C

**NEW QUESTION 290**
The DLP solution should be deployed so that it can inspect all forms of data leaving the organization, including:

A. Posting to web pages/websites
B. Applications/application programming interfaces (APIs)
C. Copy to portable media
D. All

**Answer:** D

**NEW QUESTION 292**
What is the most important aspect of security awareness/training?

A. Maximizing business capabilities
B. Protecting assets
C. Protecting health and human safety
D. Ensuring the confidentiality of data

**Answer:** C

**NEW QUESTION 297**
A company primary data center goes down due to a hardware failure causing a major disruption to the IT and communications systems. What is the focus of disaster recovery planning in this scenario

A. Maintaining critical business functions during the disruption
B. Fixing the hardware failure
C. Restoring IT and communication system back to full operations after the disruptions.
D. Guiding the actions of emergency response personnel during the disruption

**Answer:** C

**NEW QUESTION 301**
Duke would like to restrict users from accessing a list of prohibited websites while connected to his network. Which one of the following controls would BEST achieve his objective?

A. URL Filter
B. IP Address Block
C. DLP Solution
D. IPS Solution

**Answer:** A

**NEW QUESTION 302**
What does the concept of integrity applied to

A. Organization
B. Information system and processes for business operations
C. People
D. ALL

**Answer:** D

**NEW QUESTION 306**
Which authentication helps build relationships between different technology providers, enabling automatic identification and user access. Employees no longer need to enter separate usernames and passwords when visiting a new service provider

A. Basic
B. Kerberos
C. Token Based
D. Federated

**Answer:** D

**NEW QUESTION 310**
The Order of controls used in Defence in Depth

A. Assests, Physical control
B. Administrative Controls, Logical/Techincal Controls
C. Assests, Administrative Controls, Physical controls, Logical/Techincal Controls
D. Physical control
E. Administrative Controls, Logical/Techincal Controls, Assests
F. Assests, Administrative Controls, Logical/Techincal Controls, Physical controls

**Answer:** D

**NEW QUESTION 313**
Raj is considering a physical deterrent control to dissuade unauthorized people from entering the organization's property. Which of the following would serve this purpose?

A. A wall
B. Razor tape
C. A sign
D. A hidden camera

**Answer:** A

**NEW QUESTION 316**
Which is not possible models for an Incident Response Team (IRT):

A. Leveraged
B. Dedicated
C. Hybrid
D. Outsourced

**Answer:** D

**NEW QUESTION 317**
Why is an asset inventory much important?

A. It tells you what to encrypt
B. The law requires it
C. It contains a price list
D. You can't protect what you don't know you have

**Answer:** D

**NEW QUESTION 318**
A hacker is trying to gain access to a company network which of the following scenarios would be an example of defense in depth

A. The company relies solely on a firewall to block unauthorized access
B. The company stores all sensitive data on a single server
C. The hacker is required to enter a username and password
D. None

**Answer:** C

**NEW QUESTION 322**
Four main components of Incident Response are

A. Preparation, Detection and Analysis, Containment, Eradication a
B. Preparation, Detection, Analysis and Containment
C. Detection, Analysis, Containment, Eradication and Recovery
D. All

**Answer:** A

**NEW QUESTION 327**
Mark works in the security office. During research, Mark learns that a configuration change could better protect the organization's IT environment. Mark makes a proposal for this change, but the change cannot be implemented until it is approved, tested, and then cleared for deployment by the Change Control Board. This is an example of ______

A. Holistic security
B. Defense in depth
C. Threat intelligence
D. Segregation of duties

**Answer:** D

**NEW QUESTION 332**
Events with a negative consequence, such as system crashes, network packet floods, unauthorized use of system privileges, defacement of a web page or execution of malicious code that destroys data.

A. Breach
B. Incident
C. Adverse Event
D. Exploit

**Answer:** C

**NEW QUESTION 334**
Which device is used to control traffic flow in network

A. SDN
B. Switch
C. Hub
D. Router

**Answer:** D

**NEW QUESTION 339**

……