# ISC2

## Exam Questions CC

Certified in Cybersecurity (CC)

**NEW QUESTION 1**
Structured way to align IT with business goals while managing risks and meeting all industry and government regulations

A. GRC
B. Policies
C. Law
D. Stanfard

**Answer:** A

**NEW QUESTION 2**
In the context of cybersecurity, typical threat actors include the following:

A. Insiders (either deliberately, by simple human error, or by gross incompetence).
B. Outside individuals or informal groups (either planned or opportunistic, discovering vulnerability).
C. Technology (such as free-running bots and artificial intelligence
D. All

**Answer:** D

**NEW QUESTION 3**
What is multi-factor authentication (MFA)?

A. A type of authentication that uses only one method
B. A type of authentication that uses only two methods
C. A type of authentication that uses more than two methods (Correct)
D. A type of authentication that uses only one factor

**Answer:** C

**NEW QUESTION 4**
How do you distinguish Authentication and Identification

A. Both Same
B. Authentication is the process of verifying user identity and a user of a system or an application
C. Authentication is the process of verifying user identity and Identification is the ability to identify uniquely quely Identification is the process to allow resource access
D. Identification is the process of verifying user identity and Authentication is the process to allow resource access

**Answer:** B

**NEW QUESTION 5**
4 Embedded systems and network-enabled devices that communicate with the internet are considered as

A. Endpoint
B. Node
C. IOT
D. router

**Answer:** C

**NEW QUESTION 6**
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 7**
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 8**

Part of a zero-trust strategy that breaks LANs into very small and highly localized zones using firewalls.

A. Zero Trust
B. DMZ
C. VPN
D. Micro Segmentation

**Answer:** D

**NEW QUESTION 9**
In Which of the following access control models can the creator of an object delegate permission

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

**Answer:** C

**NEW QUESTION 10**
An entity that acts to exploit a target organizations system vulnerabilities is a

A. Attacker
B. Threat vector
C. Threat
D. Threat Actor

**Answer:** D

**NEW QUESTION 10**
255.255.255.0 Address represents

A. Broadcast
B. Unicast
C. Subnet mask
D. Global Address

**Answer:** C

**NEW QUESTION 15**
Example of Token based Authentication

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

**Answer:** C

**NEW QUESTION 20**
Which OSI layer VPN works

A. Layer 5
B. Layer 6
C. Layer 1
D. Layer 3

**Answer:** D

**NEW QUESTION 22**
System capabilities designed to detect and prevent the unauthorized use and transmission of information.

A. SOC
B. SIEM solutions
C. Data Loss Prevention
D. Crytography

**Answer:** C

**NEW QUESTION 26**
A popular way of implementing "least privilege"

A. MAC
B. DAC
C. RBAC

D. ABAC

**Answer:** C

**NEW QUESTION 30**
What is the primary goal of incident management

A. To potect life health and safety
B. To reduce the impacrt of an incident
C. To prepare for any incident
D. To resume interrupted operations as soon as possible

**Answer:** C

**NEW QUESTION 31**
What is meant by non-repudiation?

A. If a user does something, they can't later claim that they didn't do it.
B. Controls to protect the organization's reputation from harm due to inappropriate social media postings by employees, even if on their private accounts and personal time.
C. It is part of the rules set by administrative controls.
D. It is a security feature that prevents session replay attacks.

**Answer:** A

**NEW QUESTION 33**
Which drives for the IPv6 introduction

A. IPv4 was not secured
B. IPv4 not combatible with new devices
C. Because IPv4 was projected to be exhausted
D. IPV6 support WiFi

**Answer:** C

**NEW QUESTION 37**
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 42**
A company wants to ensure that its employees can evacuate the building in case of an emergency which physical control is best suited for this scenario

A. Fire Alarms
B. Exit signs
C. Emergency lighting
D. Emergency exit doors

**Answer:** D

**NEW QUESTION 47**
IDS can be described in terms of what fundamental functional components?

A. Response
B. Information Sources
C. Analysis
D. All of the choices.

**Answer:** D

**NEW QUESTION 51**
Timiting access to resources based on the sensitivity of the information that the resource contains and the authorization of the user to access information with that level of sensitivity.

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

**Answer:** B

**NEW QUESTION 53**
A cybercrime in which the attacker floods a server with internet traffic to prevent users from accessing connected online services and sites

A. Phising
B. Virus
C. Spoofing
D. DDOS

**Answer:** D

**NEW QUESTION 54**
Which type of attack takes advantage of vulnerabilities in validation?

A. ARP spoofing
B. Pharming attacks
C. Cross-site scripting (XSS)
D. DNS poisoning

**Answer:** C

**NEW QUESTION 59**
A _____ creates an encrypted tunnel to protect your personal data and communications

A. HTTPS
B. VPN
C. Anti-virus
D. IDS

**Answer:** B

**NEW QUESTION 60**
The common term used to describe the mechanisms that control the temperature and humidity in a data center

A. VLAN (virtual local area network)
B. STAT (system temperature and timing)
C. TAWC (temperature and water control)
D. HVAC (heating, ventilation and air conditioning)

**Answer:** D

**NEW QUESTION 61**
Finance Server and Transactions Server has restored its original facility after a disaster, what should be moved in FIRST?

A. Management
B. Most critical systems
C. Most critical functions
D. Least critical functions

**Answer:** D

**NEW QUESTION 63**
What is the range of well known ports

A. 0 - 1023
B. 1023-49151
C. 49152 - 65535
D. None

**Answer:** A

**NEW QUESTION 67**
After an Earthquake disrupting business operations, which documents contains the reactive procedures required to return business to normal operations

A. The Business Impact Analysis
B. The Business Continuity Plan
C. The Disaster Recovery plan
D. The Business Impact Plan

**Answer:** C

**NEW QUESTION 68**
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 71**
Which of the following is a subject?

A. file
B. fence
C. filename
D. user

**Answer:** D

**NEW QUESTION 73**
Which layer does VLAN hopping belong to?

A. Layer 3
B. Layer 4
C. Layer 7
D. Layer 2

**Answer:** D

**NEW QUESTION 76**
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 79**
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 80**
What is the difference between business continuity planning and disaster recovery planning?

A. Business continuity planning is abount restoring IT and communincations back to full operations after a dustruption, while disaster recovery planning is about maintaining criticla business functions
B. Disaster recovery planning is about restoring IT and communications back to full operations after a disruption, while business continuity planning is about maintaining critical business functions
C. Business continuity planning and disaster recovery planning are the same thisg
D. Business continuity planning is about maintainig criticla business funtions before disasteroccurs

**Answer:** B

**NEW QUESTION 81**
Is a way to prevent unwanted devices from connecting to a network.

A. DMZ
B. VPN
C. VLAN
D. NAC

**Answer:** D

**NEW QUESTION 84**
The prevention of authorized access to resources or the delaying of time-critical operations. (Time-critical may be milliseconds or it may be hours, depending upon the service provided.)

A. DDOS
B. Authetication

C. Authentication
D. Availablity

**Answer:** A

**NEW QUESTION 88**
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 91**
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 96**
Difference between Sniffing and Snooping

A. Sniffing is the process of intercepting and collecting network traffic as it passes over a digital networ
B. Spoofing is the act of disguising a communication from an unknown source as being trustworthy.
C. Snooping is the process of intercepting and collecting network traffic as it passes over a digital networ
D. Sniffing is the act of disguising a communication from an unknown source as being trustworthy.
E. Both are same
F. Sniffing is not thread and snoofing is a thread

**Answer:** A

**NEW QUESTION 98**
While taking the certification exam for ISC2 CC, You notice another candidate for the certification cheating. What should you do?

A. Yell at the other candidate for violating test security.
B. Nothing—each person is responsible for their own actions.
C. Report the candidate to ISC2.
D. Call local law enforcement.

**Answer:** C

**NEW QUESTION 101**
What does Criticality represents?

A. The need for consultation with the involved business ensure critical systems are identified and available
B. The importance an organization gives to data or an information system in performing its operations or achieving its mission
C. The need for security professional to ensure the appropriate levels of availavility are provided
D. All of the above

**Answer:** B

**NEW QUESTION 104**
Which component of the incident response plan involves identifying critical data and systems?

A. Detection and Analysis
B. Preparation
C. Cantainment
D. Eradication

**Answer:** B

**NEW QUESTION 106**
The primary functionality of PAM is?

A. Validate the level of access a user have to a file
B. Prevent unauthorized access to organizational assets
C. Provide just-in-time access to critical resources
D. Manage centralized access control

**Answer:** C

**NEW QUESTION 111**
Information should be consistently and readily accessible for authorized parties ?

A. Confidentiality
B. Authentication
C. Availability
D. Non-repudiation

**Answer:** C

**NEW QUESTION 113**
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 118**
What is the purpose of non-repudiation in information security?

A. To ensure data is always accessible when needed
B. To protect data from unauthorized access
C. To prevent the sender or recipient of a message from denying having sent or received the message
D. To ensure data is accurate and unchanged

**Answer:** C

**NEW QUESTION 119**
In what way do a victim's files get affected by ransomware?

A. By destroying them
B. By encrypting them
C. By stealing them
D. By selling them

**Answer:** B

**NEW QUESTION 121**
Which threats are directly associated with malware? Select that apply.

A. APT
B. Ransomeware
C. Trojan
D. DDOS

**Answer:** C

**NEW QUESTION 124**
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 127**
Which of the following is a type of risk that involves the unauthorized use or disclosure of confidential information such as passwords, financial data or personal information?

A. Compliance risk
B. Reputatuinal risk
C. Operational risk
D. Information risk

**Answer:** D

**NEW QUESTION 128**
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 130**
When is the Business Continuity Plan Enacted?

A. When there is a event
B. When there is a incident
C. When there is a loss of business operations
D. When there is a natural disaster

**Answer:** C

**NEW QUESTION 135**
What is the primary purpose of a firewall in network security?

A. Encrypt data transmissions
B. Prevent unauthorized access
C. Monitor network traffic
D. Backup critical data

**Answer:** B

**NEW QUESTION 140**
Which of the following uses registered port

A. HTTP
B. SMB
C. TCP
D. MS Sql server

**Answer:** D

**NEW QUESTION 145**
Which of the following is a characteristic of cloud

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

**Answer:** B

**NEW QUESTION 146**
The magnitude of the harm expected as a result of the consequences of an unauthorized disclosure, modification, destruction or loss of information is known as

A. Threat
B. Vulnerability
C. Impact
D. Likelihood

**Answer:** C

**NEW QUESTION 148**
Which of the following is not a source of redundant power

A. Generator
B. Utility
C. UPS
D. HVAC

**Answer:** D

**NEW QUESTION 152**
Which of these tool is commonly used to crack passwords

A. Bup Suite
B. Nslookup

C. Wireshark
D. John the ripper

**Answer:** D

**NEW QUESTION 155**
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 157**
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 162**
How many bits represent the organization unique identifier (oui) in mac addresses?

A. 16 Bits
B. 48 Bits
C. 24 Bits
D. 32 Bits

**Answer:** C

**NEW QUESTION 164**
What does a breach refer to in the context of cybersecurity

A. An unauthorized access to a system or system recours
B. Any observable occurance in a network or system
C. A deiberate security incident
D. A previously know system vulnerablity

**Answer:** A

**NEW QUESTION 165**
Removing the design belief that the network has any trusted space. Security is managed at eachpossible level, representing the most granular asset. Micro segmentation of workloads is a tool of the model.

A. Zero Trust
B. DMZ
C. VLAN
D. Micro Segmentation

**Answer:** A

**NEW QUESTION 169**
Who should participate in creating a BCP

A. Only members from the IT department
B. Only members from the management team
C. Members from across the organization
D. Only members from the finanace department

**Answer:** C

**NEW QUESTION 170**
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 173**
Some Employee of his organization launched a privilege escalation attack to gain root access on one of the organization's database serversiThe employee does have an authorized user account on the server. What log file would be MOST likely to contain relevant information??

A. Database application log
B. Firewall log
C. Operating system log
D. IDS log

**Answer:** C

**NEW QUESTION 174**
Type of cyber attack carried out over a LAN that involves sending malicious packets to a default gateway on a LAN

A. ARP Poisoning
B. Syn Flood
C. Ping of death
D. Trojan

**Answer:** A

**NEW QUESTION 178**
What goal of security is enhanced by a strong business continuity program?

A. non-repudiation
B. Availability
C. Confidentiality
D. Integrity

**Answer:** B

**NEW QUESTION 182**
What is the primary factor in the reliability of information and system

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

**Answer:** C

**NEW QUESTION 183**
Which maintains that a user or entity should only have access to the spec data, resources and applications needed to complete a required task.

A. Zero Trust
B. Defence in Depth
C. Least Privileges
D. AII

**Answer:** C

**NEW QUESTION 184**
When responding to a security incident, your team determines that the vulnerability that was exploited was not widely known to the security community, and that there are no currently known definitions/listings in common vulnerability databases or collections. This vulnerability and exploit might be called _____

A. Malware
B. Zero-day
C. Event
D. Attack

**Answer:** B

**NEW QUESTION 189**
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 193**
The internet standards organization, made up of network designers, operators, vendors and researchers, that defines protocol standards

A. ISO
B. NIST
C. IETF
D. GDPR

**Answer:** C

**NEW QUESTION 194**
The process of running a simulated instances of a computer system in a layer abstracted from the underlying hardware server or workstation

A. Containerization
B. Simulation
C. Emulation
D. Virtualization

**Answer:** D

**NEW QUESTION 195**
Organization experiences a security event that does not affect the confidentiality integrity and availability of its information system. What term BEST describes this situation?

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

**Answer:** D

**NEW QUESTION 198**
What is the main purpose of creating baseline in ensuring system integrity

A. To compare the baseline with the current state of the systems
B. To protect the information
C. To understand the current state of the system
D. AII

**Answer:** A

**NEW QUESTION 201**
A portion of the organization's network that interfaces directly with the outside world; typically, this exposed area has more security controls and restrictions than the rest of the internal IT environment.

A. Virtual private network (VPN)
B. Virtual local area network (VLAN)
C. Zero Trust
D. Demilitarized zone (DMZ)

**Answer:** D

**NEW QUESTION 204**
What is the range of private ports

A. 0 - 1023
B. 1023-49151
C. 49152 - 65535
D. None

**Answer:** C

**NEW QUESTION 206**
Which Prevent crime by designing a physical environment that positively influences human behavior.

A. DMZ
B. Security Alarm
C. CPTED
D. CCTV

**Answer:** C

**NEW QUESTION 210**
A _____ is a distributed denial-of-service (DDoS) attack in which an attacker attempts to flood a targeted server with Internet Control Message Protocol (ICMP) packets.

A. DOS
B. Syn flood
C. Smurf attack
D. Phishing attack

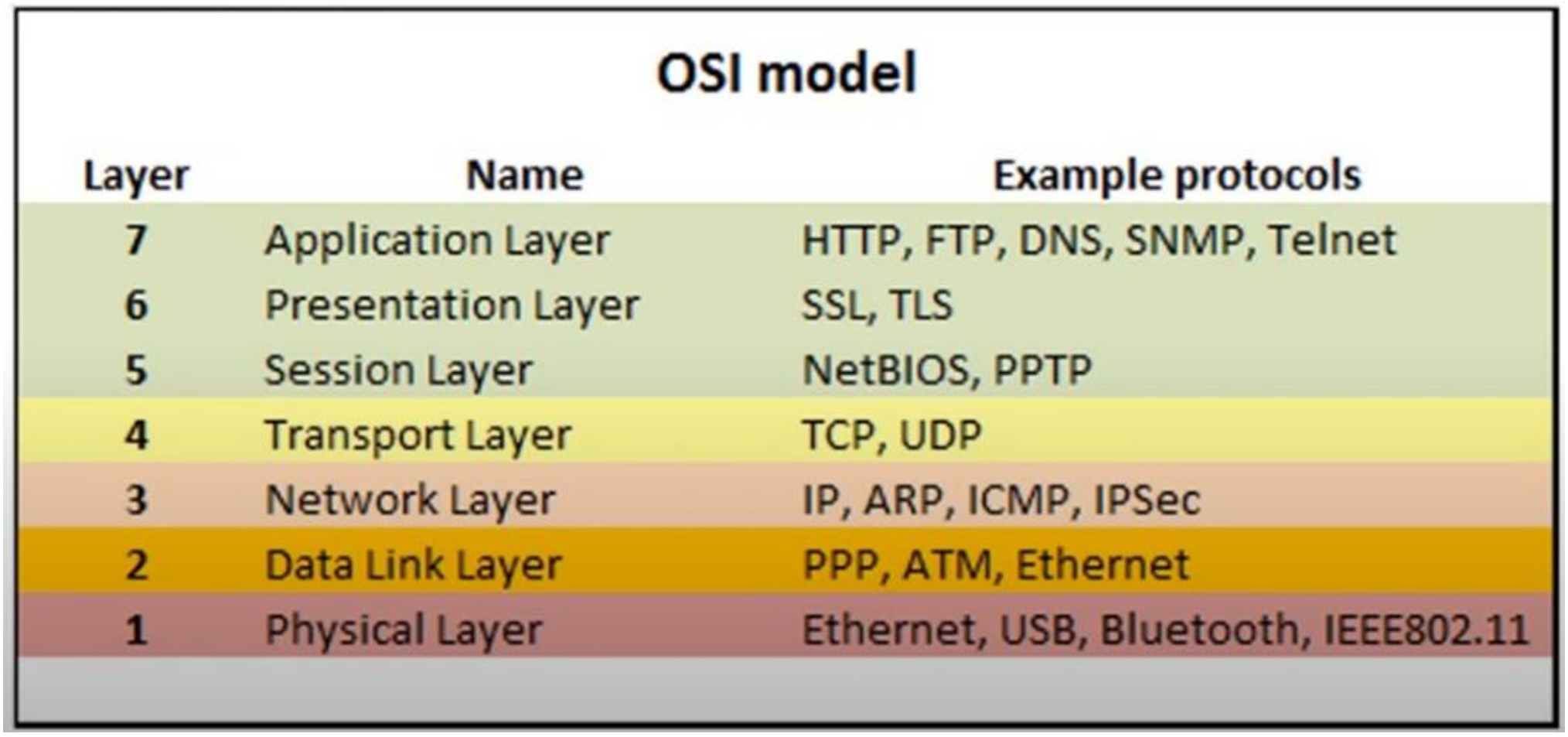
**Answer:** C

**NEW QUESTION 215**
Which of the following cloud service models provides the most suitable environment for customers to build and operate their own software?

A. SaaS
B. laaS
C. PaaS

**Answer:** A

**NEW QUESTION 220**
Exhibit.




IPSec works in which layer of OSI Model

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

**Answer:** C

**NEW QUESTION 221**
A logical group of workstations, servers and network devices that appear to be on the same LAN despite their geographical distribution.

A. LAN
B. VPN
C. WLAN
D. VLAN

**Answer:** D

**NEW QUESTION 224**
A company performs an analysis of its information systems requirements functions and interdependences in order to prioritize contingency requirement. What is this process called?

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

**Answer:** D

**NEW QUESTION 228**

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 229**
A method for risk analysis that is based on the assignment of a descriptor such as low, medium or high.

A. Quantitative Risk Analysis
B. Risk Assessment
C. Risk Mitigation
D. Qualitative Risk Analys

**Answer:** D

**NEW QUESTION 234**
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 238**
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 240**
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 243**
Which penetration testing technique requires the team to do the MOST work and effort?

A. White box
B. Blue box
C. Gray box
D. Black box

**Answer:** D

**NEW QUESTION 244**
An agreement between a cloud service provider and a cloud service customer based on a taxonomy of cloud computing- specific terms

A. Memorandum of Understanding
B. Memorandam on Agreement
C. SLA
D. AII

**Answer:** C

**NEW QUESTION 249**
A type of malware that downloads onto a computer disguised as a legitimate program

A. Worm
B. Trojan
C. virus

D. Ransomware

**Answer:** B

**NEW QUESTION 253**
John was recently offered a consulting opportunity as a side job. He is concerned that this might constitute a conflict of interest. Which one of the following sources that he needs to refer to take an appropriate decision?

A. ISC2 Code of ethics
B. Organizational code of ethics
C. Country code of ethics
D. Organizational security policy

**Answer:** B

**NEW QUESTION 254**
Derrick logs on to a system in order to read a file. In this example. Derrick is the _____?

A. Subject
B. Object
C. Process
D. Predicate

**Answer:** A

**NEW QUESTION 258**
Which of the following documents contains elements that are NOT mandatory

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

**Answer:** D

**NEW QUESTION 263**
What is the benefit of subnet

A. By increasing network bandwidth
B. By improving network security
C. By reducing network congestion
D. By simplifying network management

**Answer:** C

**NEW QUESTION 264**
DevOps team has updated the application source code, Tom has discovered that many unauthorized changes have been made. What is the BEST control Tom can implement to prevent a recurrence of this problem?

A. Backup
B. File labels
C. Security audit
D. Hashing

**Answer:** D

**NEW QUESTION 267**
The testing or evaluation of security controls to determine the extent to which the controls are implemented correctly, operating as intended, and producing the desired outcome with respect to meeting the security requirements for an information system or organization.

A. Security Assessment
B. Risk Assessment
C. DRP
D. IRP

**Answer:** A

**NEW QUESTION 269**
The Bell and LaPadula access control model is a form of

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

**Answer:** B

**NEW QUESTION 271**
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 continuty plan
B. Incident response plan
C. Disaster recvoery plan
D. Security operation plan

**Answer:** B

**NEW QUESTION 275**
A company wants to ensure that its employees cannot bring unauthorized electronic devices into the workspace which physical control is best suited for this

A. Metal Detectors
B. Security gaurds
C. RFID scanners
D. Baggage X-ray machinces

**Answer:** A

**NEW QUESTION 279**
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 284**
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 286**
A Company wants to ensure that its employees can access the network resources from anywhere in the world which access control model is best suited for this scenario

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

**Answer:** D

**NEW QUESTION 288**
Which is related to Privacy

A. GDPR
B. FIPS
C. MOU
D. AII

**Answer:** D

**NEW QUESTION 292**
What is the process of verifying a users identity called?

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

**Answer:** B

**NEW QUESTION 297**

Why is the recovery of IT often crucial to the recovery and sustainment of business operations

A. IT is not important to business operation
B. IT often the cause for the disaster
C. IT can be easily recovers without any impact of business operations
D. Many business rely heavily on IT for their operations

**Answer:** D

**NEW QUESTION 300**
What is privacy in the context of Information Security?

A. Protecting data from unauthorized access
B. Ensuring data is accurate and unchanged
C. Making sure data is always accessible when needed.
D. Disclosed without their consent

**Answer:** A

**NEW QUESTION 303**
Which document serve as specifications for the implementation of policy and dictates mandatory requirements

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

**Answer:** C

**NEW QUESTION 306**
Which security control mostly used to prevent data breach

A. Physical control
B. Logical Control
C. Adminstrative Control
D. RBAC

**Answer:** B

**NEW QUESTION 311**
Exhibit.

| Symmetric Encryption | Asymmetric Encryption |
|---|---|
| • Symmetric encryption consists of one key for encryption and decryption. | • Asymmetric Encryption consists of two cryptographic keys known as **Public Key** and **Private Key**. |
| • Symmetric Encryption is a lot quicker compared to the Asymmetric method. | • As Asymmetric Encryption incorporates two separate keys, the process is slowed down considerably. |
| • RC4<br>• AES<br>• DES<br>• 3DES<br>• QUAD | • RSA<br>• Diffie-Hellman<br>• ECC<br>• El Gamal<br>• DSA |

How many keys would be required to support 50 users in an asymmetric cryptography system?

A. 100
B. 200
C. 50
D. 1225

**Answer:** A

**NEW QUESTION 315**
A Company IT system experienced a system crash that result in a loss of data. What term best describes this event?

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

**Answer:** A

**NEW QUESTION 316**
Devid's team recently implemented a new system that gathers information from a variety of different log sources, analyses that information, and then triggers automated playbooks in response to security events, what term BEST describes this technology?

A. SIEM
B. Log Repository
C. IPS
D. SOAR

**Answer:** D

**NEW QUESTION 319**
WF attack in which a subscriber currently authenticated to an Server and connected through a secure session browses to an attacker's website, causing the subscriber to unknowingly invoke unwanted actions at the Server

A. XSS
B. CSRF
C. Spoofing
D. ALL

**Answer:** B

**NEW QUESTION 323**
The purpose of risk identification:

A. Employees at all levels of the organization are responsible for identifying risk.
B. Identify risk to communicate it clearly.
C. Identify risk to protect against it.
D. ALL

**Answer:** D

**NEW QUESTION 328**
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 332**
A company experiences a major IT outage and cannot perform its critical business functions. What type of plan will hep the company recover from this event?

A. BCP
B. IRP C DRP
C. BIA

**Answer:** C

**NEW QUESTION 334**
What is the purpose of multi-factor authentication (MFA) in 1AM?

A. To simplify user access
B. To eliminate the need for authentication
C. To add an additional layer of security by requiring multiple forms of verification
D. To grant unrestricted access to all users

**Answer:** C

**NEW QUESTION 336**
Which of these activities is often associated with DR efforts?

A. Running anti-malware solutions

B. Scanning the IT environment for vulnerabilities
C. Zero-day exploits
D. Employees returning to the primary production location

**Answer:** D

**NEW QUESTION 338**
A set of instructions to help IT staff detect, respond to, and recover from network security incidents?

A. BCP
B. IRP
C. DRP
D. None

**Answer:** B

**NEW QUESTION 343**
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 348**
Permitting authorized access to information while protecting it from improper disclosure

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

**Answer:** B

**NEW QUESTION 352**
Example of Type 1 Authentication

A. Password
B. Smart Card
C. Finger Print
D. RSA Token

**Answer:** A

**NEW QUESTION 356**
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 360**
What is the main challenge in achieving non repudiation in electronic transactions

A. Ensuring the identity of the sender and recipient is verified
B. Ensuring the authenticity and integrity of the message
C. Making sure the message is not tampered with during transmission
D. All of the above

**Answer:** D

**NEW QUESTION 361**
Which of the following documents identifies the principles and rules governing an organization's protection of information systems and data

A. Procudure
B. Guideline
C. Policy
D. Standard

**Answer:** C

**NEW QUESTION 366**
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 368**
In incident terminology the Zero day is

A. Days with a cybersecurity incident
B. A previously unknown system vulnerability
C. Days without a cybersecurity incident
D. Days to solve a previously unknown system vulnerability

**Answer:** B

**NEW QUESTION 371**
What are the primary responsibilities of a computer incident response team (CIRT) during an incident?

A. To determine the difference between minor and major incident
B. To troubleshoot network and system issues
C. To provide medical assistance at accident scenes
D. To asses the amount and scope of damage caused by the incident

**Answer:** D

**NEW QUESTION 373**
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 377**
Walmart has large ecommerce presence in world. Which of these solutions would ensure the LOWEST possible latency for their customers using their services?

A. CDN
B. SaaS
C. Load Balancing
D. Decentralized Data Centers

**Answer:** A

**NEW QUESTION 378**
What is the primary purpose of a honeytoken in cybersecurity?

A. To lure and detect attackers
B. To encrypt sensitive data
C. To enhance network performance
D. To manage user access

**Answer:** A

**NEW QUESTION 383**
A one-way spinning door or barrier that allows only one person at a time to enter a building or pass through an area.

A. Turnstile
B. ManTrap
C. Bollard
D. Gate

**Answer:** A

**NEW QUESTION 384**
allows for extremely granular restrictions within the IT environment, to the point where rules can be applied to individual machines and/or users,

A. DMZ

B. Microsegmentation
C. VLAN
D. NAC

**Answer:** B

**NEW QUESTION 388**
Can be considered to be a fingerprint of the file or message

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

**Answer:** A

**NEW QUESTION 391**
A common network device used to filter traffic?

A. Server
B. Endpoint
C. Ethernet
D. Firewa

**Answer:** D

**NEW QUESTION 395**
Example of Technical controls

A. Security Guard
B. GPS installed in vehicle to track location
C. Door Lock
D. None

**Answer:** B

**NEW QUESTION 397**
An external entity has tried to gain access to your organization's IT environment without proper authorization. This is an example of a(n)

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

**Answer:** B

**NEW QUESTION 399**
Government can imposes financial penalties as a consequence of breaking a

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

**Answer:** B

**NEW QUESTION 402**
Which of the following properties is not guaranteed by Digital signatures

A. Authentication
B. Confidentiality
C. Non-Repudiation
D. Integrity

**Answer:** B

**NEW QUESTION 407**
Which of the following is not a feature of a cryptographic hash function

A. Deterministic
B. Unique
C. Useful
D. Reversible

**Answer:** D

**NEW QUESTION 409**
A company's governing board may agree that legal services will examine any third-party contracts, so they create a _____ stating that aside from legal services, no other department in the companvhahppn pivpn nprmkcinn to review third-party contracts

A. Procedure
B. Policy
C. Standard
D. Law

**Answer:** B

**NEW QUESTION 411**
What principle states that individuals should only have the minimum set of permissions necessary to carry out their job functions?

A. Least privilege
B. Two person control
C. Job rotation
D. Separation of privileges

**Answer:** A

**NEW QUESTION 413**
Which ensure maintaining business operations during or after an incident

A. Incident Response
B. Business Continuity
C. Disaster Recovery
D. AII

**Answer:** C

**NEW QUESTION 416**
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 417**
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 422**
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 425**
Risk tolerance also known as

A. Risk threshold
B. Risk appetite
C. Acceptable risk
D. AII

**Answer:** D

**NEW QUESTION 430**
Which of these is the most efficient and effective way to test a business continuity plan

A. Simulations
B. Discussions
C. Walkthroughs
D. Reviews

**Answer:** A

**NEW QUESTION 434**
Port scanning attack target which OSI layer

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

**Answer:** A

**NEW QUESTION 437**
Which of the following is unlikely to be a member of the disaster recovery team

A. Executive Management
B. Public Relations
C. Billing Clerk
D. IT personnel

**Answer:** C

**NEW QUESTION 438**
EKristal is the security administrator for a large online service provider. Kristal learns that the company is harvesting personal data of its customers and sharing the data with local governments where the company operates, without the knowledge of the users, to allow the governments to persecute users on the basis of their political and philosophical beliefs. The published user agreement states that the company will not share personal user data with any entities without the users' explicit permission. According to the ISC2 Code of Ethics, to whom does Kristal ultimately report in this situation?

A. The company Kristal works for
B. The governments of the countries where the company operates
C. ISC2
D. The users

**Answer:** D

**NEW QUESTION 442**
Methods or mechanisms cybercriminals use to gain illegal, unauthorized access to computer systems and networks.

A. Attacker
B. Threat Vector
C. Threat
D. Threat actor

**Answer:** B

**NEW QUESTION 444**
Which device is used to control traffic flow in network

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

**Answer:** D

**NEW QUESTION 448**
.....

# Thank You for Trying Our Product

## We offer two products:

1st - We have Practice Tests Software with Actual Exam Questions

2nd - Questons and Answers in PDF Format

## CC Practice Exam Features:

* CC Questions and Answers Updated Frequently

* CC Practice Questions Verified by Expert Senior Certified Staff

* CC Most Realistic Questions that Guarantee you a Pass on Your FirstTry

* CC Practice Test Questions in Multiple Choice Formats and Updatesfor 1 Year