

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. Stanford

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 the recommended fire suppression system for server rooms

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

Answer: D

NEW QUESTION 4

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 5

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 6

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 7

255.255.255.0 Address represents

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

Answer: C

NEW QUESTION 8

Which is an approach to networking that uses software-based controllers or application programming interfaces (APIs) to communicate with underlying hardware infrastructure and direct traffic on a network.

- A. VLAN
- B. SDN
- C. VPN
- D. SAN

Answer: B

NEW QUESTION 9

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 10

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 10

The last phase in the data security cycle is

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

Answer: B

NEW QUESTION 12

Scans networks to determine everything that is connected as well as other information.

- A. Burbsuite
- B. Wireshark
- C. Fiddler
- D. Zen Mao

Answer: D

NEW QUESTION 15

Port forwarding is also known as

- A. Port mapping
- B. Tunneling
- C. Punch through
- D. ALL

Answer: D

NEW QUESTION 17

Which layer does VLAN hopping belong to?

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

Answer: D

NEW QUESTION 21

What is the difference between business continuity planning and disaster recovery planning?

- A. Business continuity planning is about restoring IT and communications 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 critica business funtions before disasteroccurs

Answer: B

NEW QUESTION 25

What does Personally Identifiable Information (PII) 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 30

Which Regulation addresses personal privacy

- A. HIPAA
- B. GDPR
- C. NIST
- D. ISO

Answer: B

NEW QUESTION 35

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 38

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 41

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 44

Which threats are directly associated with malware? Select that apply.

- A. APT
- B. Ransomware
- C. Trojan
- D. DDOS

Answer: C

NEW QUESTION 46

A structured approach used to oversee and manage risk for an enterprise

- A. Risk Assessment
- B. Risk threshold
- C. Risk Management Framework
- D. Risk appetite

Answer: C

NEW QUESTION 48

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 52

Which of the following is not a source of redundant power

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

Answer: D

NEW QUESTION 54

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 58

What is a threat in the context of cybersecurity

- A. An inherent weakness or flaw in a system
- B. Something in need of protection
- C. The means by which a threat actor carries out their objectives
- D. A person or thing that takes action to exploit a target organizations system vulnerabilities

Answer: D

NEW QUESTION 60

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 65

What is IPSEC reply attack

- A. An attack where an attacker modifies packets in transit
- B. An attack where an attacker eavesdrops on network traffic
- C. An attack where an attacker overloads a network with traffic
- D. An attack where an attacker attempts to inject packets in an existing sessio

Answer: D

NEW QUESTION 67

What is the end goal of DRP

- A. All System backup restored
- B. DR site activated
- C. Shifting the Infrastructure to new place
- D. Business restored to full last-known reliable operations.

Answer: D

NEW QUESTION 71

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 73

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. All

Answer: A

NEW QUESTION 76

How often should an organization test its business continuity plan

- A. Continually
- B. Annually
- C. Routinely
- D. Daily

Answer: C

NEW QUESTION 80

What is the first step in incident response planning

- A. Develop a policy approved by management
- B. Identify critical data and systems
- C. Train staff on incident response
- D. implement an incident response team

Answer: A

NEW QUESTION 83

What is the range of private ports

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

Answer: C

NEW QUESTION 84

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 88

A type of malware that is capable of self propagation and can infect multiple systems on network without the need for human intervention

- A. Worm
- B. Spy ware
- C. Adwre
- D. Virus

Answer: A

NEW QUESTION 93

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

- A. SaaS
- B. IaaS
- C. PaaS

Answer: A

NEW QUESTION 95

What is the recommended range of temperature for optimized maximum uptime and hardware life in a data center?

- A. 62 F to 69 F
- B. 64 F to 81 F
- C. 82 F to 90 F
- D. 91 F to 100 F

Answer: B

NEW QUESTION 98

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 contingency
- 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 103

Which type of control is used to identify that an attack has occurred or is currently occurring

- A. Preventive control
- B. Detective control
- C. Corrective control
- D. Recovery control

Answer: B

NEW QUESTION 106

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 111

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 113

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. All

Answer: C

NEW QUESTION 117

The mitigation of violations of security policies and recommended practices

- A. DR
- B. IR
- C. Threat hunting
- D. Incident response

Answer: D

NEW QUESTION 122

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 127

What is a security token used to authenticate a user to a web application, typically after they log in?

- A. Captcha
- B. API key
- C. CSRF token
- D. Session token

Answer: D

NEW QUESTION 130

Which type of malware encrypts a users file system and demands payment in exchange of decrypting key

- A. Worm
- B. Trojan
- C. virus
- D. Ransomware

Answer: D

NEW QUESTION 131

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 136

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 138

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 143

_____ are virtual separations within a switch and are used mainly to limit broadcast traffic

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

Answer: C

NEW QUESTION 146

What does internal consistency of information refer to

- A. Data being accurate, usefull and complete
- B. Data being protected from errors or loss of information
- C. All instances of data being identical in form content and meaning
- D. Data being displayed and stored the same way on all system

Answer: C

NEW QUESTION 149

What is the primary goal of Identity and Access Management (IAM) in cybersecurity?

- A. To ensure 100% security against all threats
- B. To provide secure and controlled access to resources
- C. To eliminate the need for user authentication
- D. To monitor network traffic for performance optimization

Answer: A

NEW QUESTION 151

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 152

Which is related to Privacy

- A. GDPR
- B. FIPS
- C. MOU
- D. All

Answer: D

NEW QUESTION 154

What is the process of verifying a users identity called?

- A. Confidentiality
- B. Authentication
- C. Authorization
- D. Identification

Answer: B

NEW QUESTION 157

Which of these is an example of deterrent control

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

Answer: B

NEW QUESTION 161

An organization develops a set of procedures to restore critical business processes after a significant disruption. What type of plan is this?

- A. bcp
- B. IRP
- C. DRP
- D. None

Answer: A

NEW QUESTION 165

Which is strongly used for Securing Wi-Fi

- A. WPA2
- B. WEP
- C. WPA
- D. SSL

Answer: A

NEW QUESTION 166

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 168

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 172

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 177

Which of the following is the least secure communications protocol?

- A. CHAP
- B. Ipsec
- C. PAP
- D. EAP

Answer: C

NEW QUESTION 178

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 180

John joined the ISC2 Organizations, his manager asked to check the authentications in security module. What would John use to ensure a certain control is working as he want and expect it to?

- A. Security Testing
- B. Security assessment
- C. Security audit
- D. Security walkthrough

Answer: A

NEW QUESTION 182

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 187

organization experiences a security event that potentially jeopardizes the confidentiality, integrity or availability of its information system. What term best describes this situation?

- A. Breach

- B. Event
- C. Incident
- D. Exploit

Answer: C

NEW QUESTION 188

The practice of ensuring that an organizational process cannot be completed by a single person; forces collusion as a means to reduce insider threats.

- A. Segregation of Duties
- B. Principle of Least Privilege
- C. Privileged Account
- D. Rule-based access control

Answer: A

NEW QUESTION 189

What should been done to limit the damage caused by the ransomware attack

- A. Use a different email client to prevent malicious attachments
- B. Add more Administrative users to the Domain Admins group
- C. Delete all emails with attachments
- D. Limit the use of administrative privileges to only when required

Answer: D

NEW QUESTION 192

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 194

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 195

Which type of control is used to restore systems or processes to their normal state after an attack has occurred

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

Answer: D

NEW QUESTION 199

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 204

Which of the following physical controls is used to protect against eavesdropping and data theft through electromagnetic radiation

- A. EMI Shielding
- B. Screening rooms
- C. White noise generators
- D. ALL

Answer: A

NEW QUESTION 206

Which type of network is set up similar to the internet but is private to an organization. Select the MOST appropriate?

- A. Extranet
- B. VLAN
- C. Intranet
- D. VPN

Answer: B

NEW QUESTION 207

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 211

Which is a curated knowledge base and model for cyber adversary behavior, reflecting the various phases of an adversary's attack lifecycle and the platforms they are known to target

- A. MITRE ATT&CK
- B. CVE
- C. Risk Management framework
- D. Security Management

Answer: A

NEW QUESTION 216

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 220

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 222

A common network device used to filter traffic?

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

Answer: D

NEW QUESTION 225

Example of Technical controls

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

Answer: B

NEW QUESTION 230

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 235

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 236

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 240

Incident management is also known as

- A. Risk Management
- B. Business Continuity management
- C. Incident management
- D. Crisis management

Answer: D

NEW QUESTION 244

The practice of sending fraudulent communications that appear to come from a reputable source

- A. DOS
- B. Virus
- C. Spoofing
- D. Phishing

Answer: D

NEW QUESTION 245

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 247

Protection against an individual falsely denying having performed a particular action

- A. Authentication
- B. Identification
- C. Verification
- D. Non repudiation

Answer: D

NEW QUESTION 251

Risk tolerance also known as

- A. Risk threshold
- B. Risk appetite
- C. Acceptable risk
- D. All

Answer: D

NEW QUESTION 255

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 257

How do IT professionals differentiate between typical IT problems and security incidents?

- A. By providing medical assistance at accident scenes
- B. By collection evidence and reposting the incident
- C. By receiving specific training on incident response
- D. By participating in remediation and lessons learns stages

Answer: C

NEW QUESTION 259

Uses multiple types of access controls in literal or theoretical layers to help an organization avoid a monolithic security

- A. DMZ
- B. VLAN
- C. Defence in Depth
- D. VPN

Answer: C

NEW QUESTION 262

What is the potential impact of an IPSec reply attack

- A. Modification of network traffic
- B. Disruption of network communication
- C. Unauthorized access to network resources
- D. ALL

Answer: A

NEW QUESTION 266

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 268

A Company critical functions were disrupted due to a system outage. What plan should the organization have in place to sustain these operations during and after a significant disruptions?

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

Answer: B

NEW QUESTION 272

A backup is which type for security control

- A. Preventive
- B. Deterrent
- C. Recovery
- D. Corrective

Answer: C

NEW QUESTION 276

.....

Thank You for Trying Our Product

We offer two products:

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

2nd - Questions 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 First Try
- * CC Practice Test Questions in Multiple Choice Formats and Updates for 1 Year

100% Actual & Verified — Instant Download, Please Click
[Order The CC Practice Test Here](#)