

ISC2

Exam Questions CC

Certified in Cybersecurity (CC)



NEW QUESTION 1

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 2

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 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

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 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

A set of security controls or system settings used to ensure uniformity of configuration through the IT environment?

- A. Patches
- B. Inventory
- C. Baseline
- D. Policy

Answer: C

NEW QUESTION 7

Ping flood attack target which OSI layer

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

Answer: B

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 of the following is not a Social engineering technique

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

Answer: D

NEW QUESTION 10

A organization's security system which involves in preventing, detecting, analyzing, and responding to cybersecurity incidents.

- A. Business continuity team
- B. Disaster recovery team
- C. Incident response team
- D. Security operations center

Answer: D

NEW QUESTION 10

TCP and UDP reside at which layer of the osi model?

- A. Session
- B. Transport
- C. Data link
- D. Presentation

Answer: D

NEW QUESTION 12

Mark has purchased a MAC LAPTOP. He is scared of losing his screen and planning to buy an insurance policy. So, which risk management strategy is?

- A. Risk acceptance
- B. Risk deterrence
- C. Risk transference
- D. Risk mitigation

Answer: C

NEW QUESTION 17

Which OSI layer VPN works

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

Answer: D

NEW QUESTION 19

A hacker gains access to a company 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 layer

Answer: D

NEW QUESTION 23

System capabilities designed to detect and prevent the unauthorized use and transmission of information.

- A. SOC
- B. SIEM solutions
- C. Data Loss Prevention
- D. Cryptography

Answer: C

NEW QUESTION 27

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 30

Which of the following is a systematic approach to protecting against cyber threats that involves a continuous cycle of identifying, assessing and prioritizing risks and implementing measures to reduce or eliminate those risks?

- A. Security Assessment
- B. Incident response
- C. Penetration testing
- D. Risk Management

Answer: D

NEW QUESTION 32

Are a measure of an organization's baseline of security performance

- A. Security Assessment
- B. Security Audit
- C. Security Benchmark
- D. Security Management

Answer: C

NEW QUESTION 37

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 40

What is the difference between BCP and DRP

- A. BCP is about restoring IT and communications back to full operations after a disruption, while DRP is about maintaining critical business functions
- B. DRP is about restoring IT and communications back to full operations after a disruption, while BCP is about maintaining critical business functions
- C. DRP and BCP are the same
- D. BCP is about maintaining critical business functions before a disaster occurs

Answer: B

NEW QUESTION 42

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 disruption, while disaster recovery planning is about maintaining critical 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 thing
- D. Business continuity planning is about maintaining critical business functions before disaster occurs

Answer: B

NEW QUESTION 45

Is a way to prevent unwanted devices from connecting to a network.

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

Answer: D

NEW QUESTION 48

In information systems terms, the activities necessary to restore IT and communications services of an organization during and after an outage

- A. IR
- B. BC
- C. Risk Management
- D. DR

Answer: D

NEW QUESTION 50

What security feature used in HTTPS

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

Answer: D

NEW QUESTION 52

which is the short form of IPv6 address 2001:0db8:0000:0000:0000:ffff:0000:0001

- A. 2001:db8::ffff:0:1
- B. 2001:db8:0000:ffff:0:1
- C. 2001:db80::ffff:0000:1
- D. 2001:db8::ffff:0000:0001

Answer: A

NEW QUESTION 53

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

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

Answer: A

NEW QUESTION 54

Which Regulation addresses personal privacy

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

Answer: B

NEW QUESTION 55

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 58

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 63

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 65

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 67

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 68

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. Reputational risk
- C. Operational risk
- D. Information risk

Answer: D

NEW QUESTION 71

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 75

Which of these is WEAKEST form of authentication we can implement?

- A. Something you know
- B. Something you are
- C. Something you have
- D. Biometric authentications

Answer: A

NEW QUESTION 80

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 81

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 83

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 86

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 88

What is knowledge based authentication

- A. Authentication based on a passphrase or secret code
- B. Authentication based on a token or memory card
- C. Authentication based on biometrics or measurable characteristics
- D. Authentication based on something you do

Answer: A

NEW QUESTION 93

Which phase of the access control process(AAA) does a user prove his/her identity?

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

Answer: A

NEW QUESTION 94

What is IPSEC replay 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 session

Answer: D

NEW QUESTION 99

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 101

A company network experience a sudden flood of network packets that causes major slowdown in internet traffic. What type of event is this?

- A. Security incident
- B. Natural disaster
- C. Exploit
- D. Adverse event

Answer: D

NEW QUESTION 103

How does IPSec protect against reply attacks

- A. By using sequence numbers
- B. By limiting access to the network
- C. By using digital signatures
- D. By encryption all network traffic

Answer: A

NEW QUESTION 108

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 110

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 113

How often should an organization test its business continuity plan

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

Answer: C

NEW QUESTION 114

Selvaa presents a userid and a password to a system in order to log on. Which of the following characteristics must the userid have?

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

Answer: D

NEW QUESTION 116

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 119

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 122

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 125

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 128

Mark is configuring an automated data transfer between two hosts and is choosing an authentication technique for one host to connect to the other host. What approach would be best-suited for this scenario?

- A. Biometric
- B. Smart Card
- C. SSH Key
- D. Hard Coded Password

Answer: C

NEW QUESTION 132

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 137

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 138

Which of the following documents contains elements that are NOT mandatory

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

Answer: D

NEW QUESTION 143

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 148

The Bell and LaPadula access control model is a form of

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

Answer: B

NEW QUESTION 152

Who must follow HIPAA Compliance

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

Answer: B

NEW QUESTION 153

_____ 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 154

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 156

Which of the following best describes the type of technology the team should implement to increase the work effort of buffer overflow attacks?

- A. Address space layout randomization
- B. Memory induction application
- C. Input memory isolation
- D. Read-only memory integrity checks

Answer: A

NEW QUESTION 158

Which of these is WEAKEST form of authentication we can implement?

- A. Something you know
- B. Something you are
- C. Something you have
- D. Biometric authentications

Answer: A

NEW QUESTION 159

Which type of authentication is something which you

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

Answer: C

NEW QUESTION 160

What is the process of verifying a users identity called?

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

Answer: B

NEW QUESTION 163

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 165

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 166

Why is security training important?

- A. Because it fulfills regulatory requirements.
- B. Because it helps people to perform their job duties more efficiently.
- C. Because it reduces the risk of certain types of attacks, like social engineering.
- D. All

Answer: C

NEW QUESTION 171

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 174

Granting a user access to services or the system

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

Answer: C

NEW QUESTION 177

What is sensitivity in the context of confidentiality

- A. The harm caused to external stakeholders if information is disclosed or modified
- B. The ability of information to be accessed only by authorized individuals
- C. The need for protection assigned to information by its owner
- D. The Health status of the individuals

Answer: C

NEW QUESTION 178

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 179

Which layer of the OSI Layer model is the target of a buffer overflow attack

- A. Layer 7
- B. Layer 3
- C. Layer 5
- D. Layer 4

Answer: A

NEW QUESTION 180

Which type of attack attempts to gain information by observing the devices power consumption

- A. DOS
- B. Side Channles
- C. XSS
- D. XSRF

Answer: B

NEW QUESTION 183

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 187

Which of the following is the least secure communications protocol?

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

Answer: C

NEW QUESTION 190

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 191

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 195

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 198

A security event, or combination of security events, that constitutes a secu incident in which an intruder gains, or attempts to gain, access to a system or system resource without authorization

- A. Intrusion
- B. Exploit
- C. Threat
- D. Attack

Answer: A

NEW QUESTION 199

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 201

What is Remanence

- A. The ability of retaining magnetization in storage disk after deletion
- B. Files or pieces of files get scattered throughout your disks.
- C. Data corruption due to disk failure
- D. All

Answer: A

NEW QUESTION 205

Who is responsible for publishing and signing the organization s policies?

- A. The security office
- B. Human resources
- C. Senior management
- D. The legal department

Answer: C

NEW QUESTION 208

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 209

Which layer provides the services to user?

- A. Application layers
- B. Session Layers
- C. Presentation Layer
- D. Physical Layer

Answer: A

NEW QUESTION 212

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 214

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 217

A new BYOD policy has been enforced in NEW Corp which type of control is used to enforce this security policies

- A. Physical control
- B. Logical Control

- C. Administrative Control
- D. Technical Control

Answer: C

NEW QUESTION 220

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 223

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 226

Which protocol is used for secure email

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

Answer: D

NEW QUESTION 229

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 233

Dani is an ISC2 member and an employee of New Corporation. One of Dani's colleagues offers to share a file that contains an illicit copy of a newly released movie. What should Dani do

- A. Inform ISC2
- B. Inform law enforcement
- C. Accept the movie
- D. Refuse to accept

Answer: D

NEW QUESTION 238

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 241

Example of Technical controls

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

Answer: B

NEW QUESTION 243

Set of rules that everyone must comply with and usually carry monetary penalties for noncompliance

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

Answer: A

NEW QUESTION 248

Provides confidentiality by hiding or obscuring a message so that it cannot be understood by anyone except the intended recipient.

- A. Hashing
- B. Encoding
- C. Cryptography
- D. All

Answer: C

NEW QUESTION 249

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 250

Which is not the function of IPS

- A. To encrypt network traffic
- B. To monitor network traffic
- C. To filter network traffic
- D. To detect and prevent attacks

Answer: A

NEW QUESTION 255

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 257

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 261

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 265

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 269

Why Red book is important in BCP

- A. To have hard copy for easy access
- B. Easy to carry and transfer
- C. A hurricane hits, the power is out and all the facilities are compromised and there is no access to electronic backups
- D. All

Answer: C

NEW QUESTION 274

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 275

Load balancing safe guard which CIA triad

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

Answer: B

NEW QUESTION 280

Protection against an individual falsely denying having performed a particular action

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

Answer: D

NEW QUESTION 283

What is the BEST defense against dumpster diving attacks?

- A. Anti-malware software
- B. Clean desk policy
- C. Data loss prevention tools
- D. Shredding

Answer: D

NEW QUESTION 287

Which one of the following groups is NOT normally part of an organization's cybersecurity incident response team?

- A. Technical Subject Matter Experts
- B. Cybersecurity Experts
- C. Management
- D. Law Enforcement

Answer: D

NEW QUESTION 290

Devid is worried about distributed denial of service attacks against his company's primary web application, which of the following options will provide the MOST resilience against large-scale ddos attacks?

- A. Implement a CDN
- B. Increase the number of servers in the web application server cluster
- C. Contract for DDoS mitigation services via the company's IPS
- D. Increase the amount of bandwidth available from one or more ISPs

Answer: A

NEW QUESTION 293

The prevention of authorized access to resources or the delaying of time critical operations.

- A. ARP Poisoning
- B. Syn Flood
- C. Denial-of-Service (DoS)
- D. All

Answer: C

NEW QUESTION 296

Which is not possible models for an Incident Response Team (IRT):

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

Answer: D

NEW QUESTION 300

You experienced a power outage that disrupted access to your data center. What type of security concern occurred?

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

Answer: A

NEW QUESTION 305

What is the purpose of the post incident phase of incident response?

- A. To detect and analyze incidents
- B. To prepare for future incidents
- C. To document lessons learned and improve future incident response effectiveness
- D. To containment and eradicate incidents

Answer: C

NEW QUESTION 306

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 310

The harmonization of automated computing tasks, providing a consolidated and reusable workflow

- A. Cloud Orchestration
- B. Cloud Manager
- C. Cloud broker
- D. Cloud Controller

Answer: A

NEW QUESTION 311

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 315

.....

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](#)