

Actual exam question from ISC's CISSP

Question #: 8

Topic #: 1

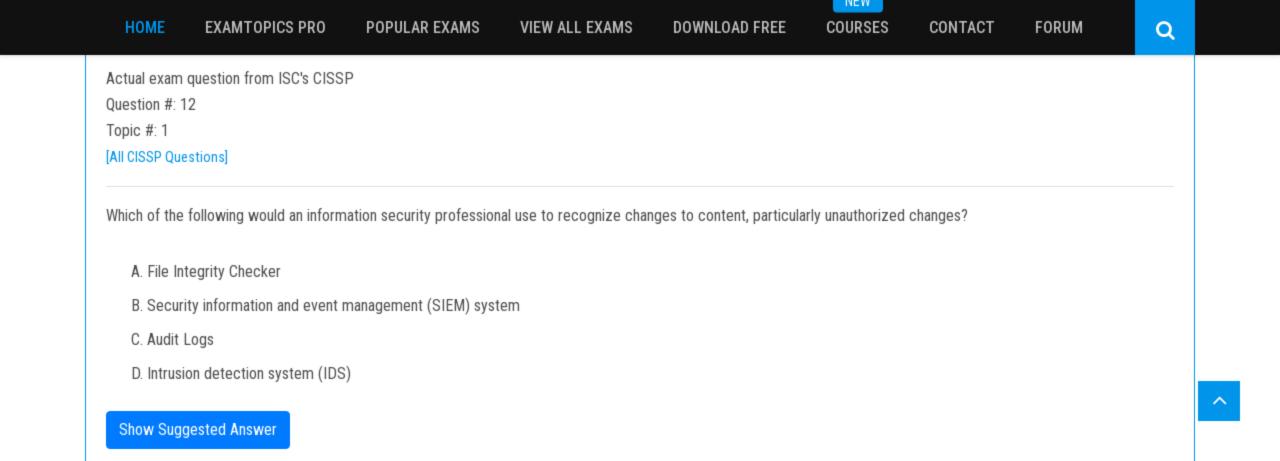
[All CISSP Questions]

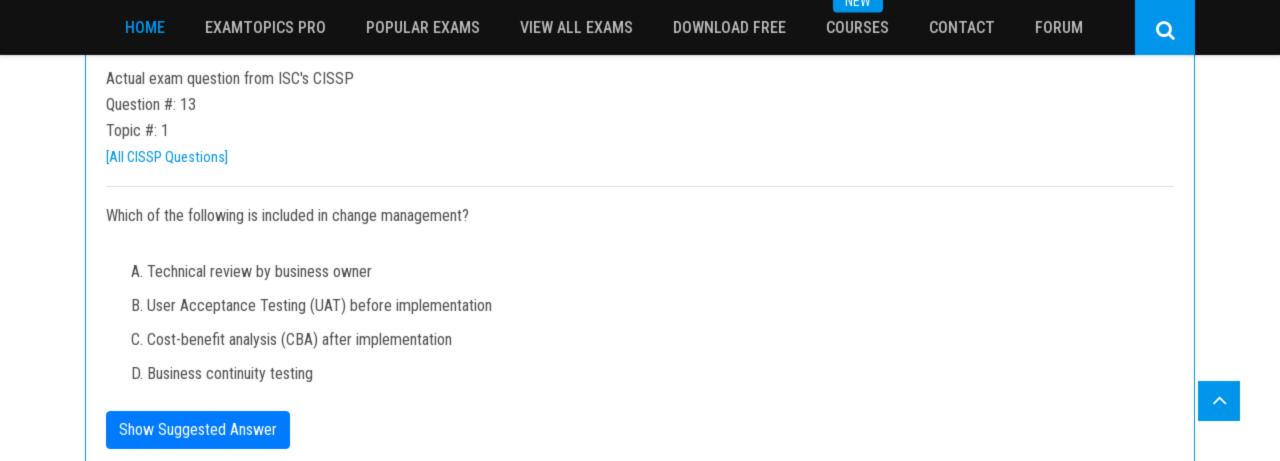
Clothing retailer employees are provisioned with user accounts that provide access to resources at partner businesses. All partner businesses use common identity and access management (IAM) protocols and differing technologies. Under the Extended Identity principle, what is the process flow between partner businesses to allow this IAM action?

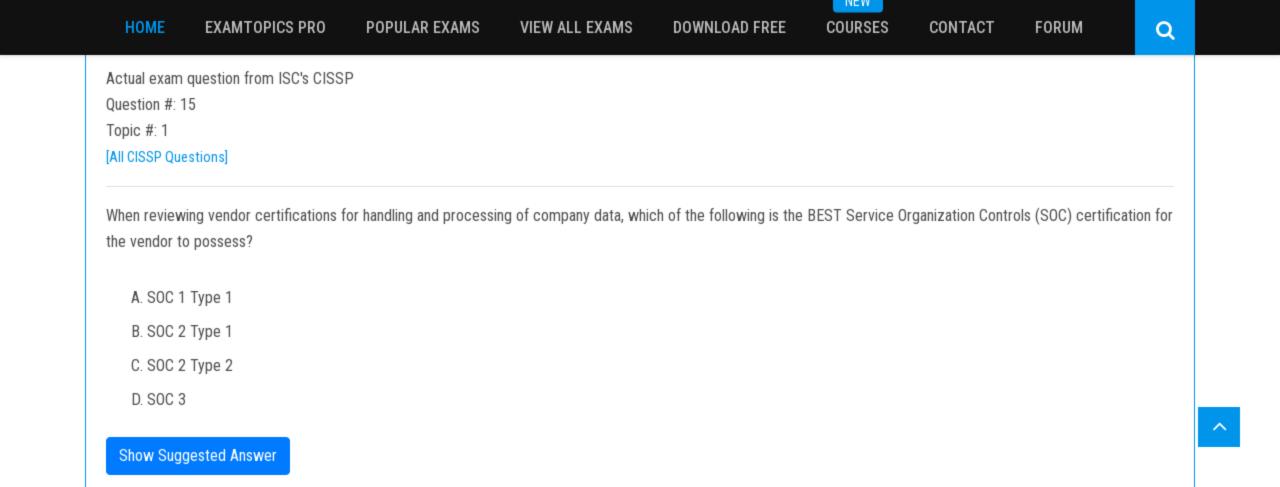
- A. Clothing retailer acts as User Self Service, confirms identity of user using industry standards, then sends credentials to partner businesses that act as a Service Provider and allows access to services.
- B. Clothing retailer acts as identity provider (IdP), confirms identity of user using industry standards, then sends credentials to partner businesses that act as a Service Provider and allows access to services.
- C. Clothing retailer acts as Service Provider, confirms identity of user using industry standards, then sends credentials to partner businesses that act as an identity provider (IdP) and allows access to resources.
- D. Clothing retailer acts as Access Control Provider, confirms access of user using industry standards, then sends credentials to partner businesses that act as a Service Provider and allows access to resources.

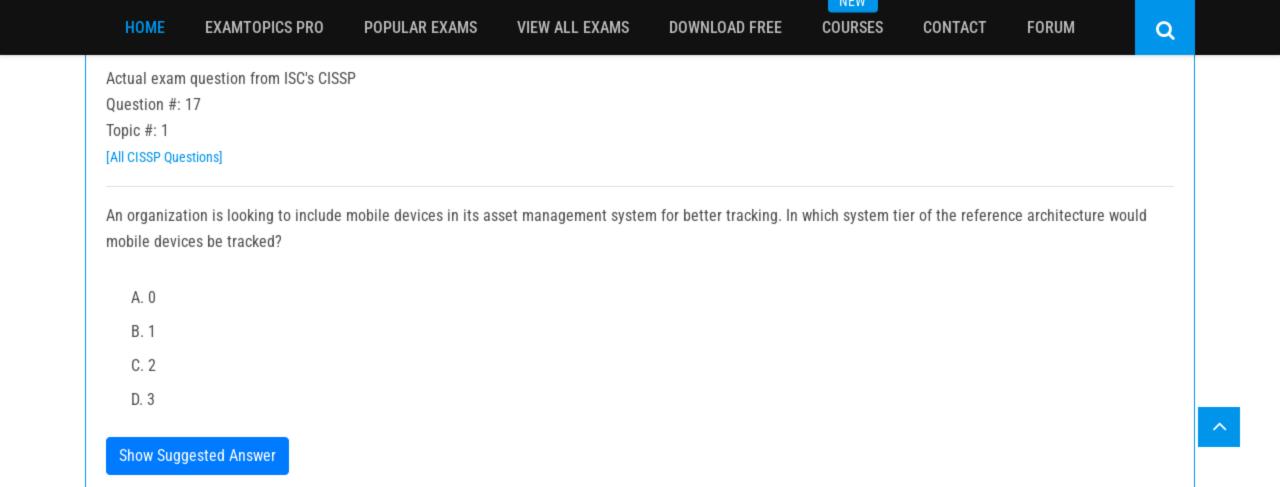
Show Suggested Answer

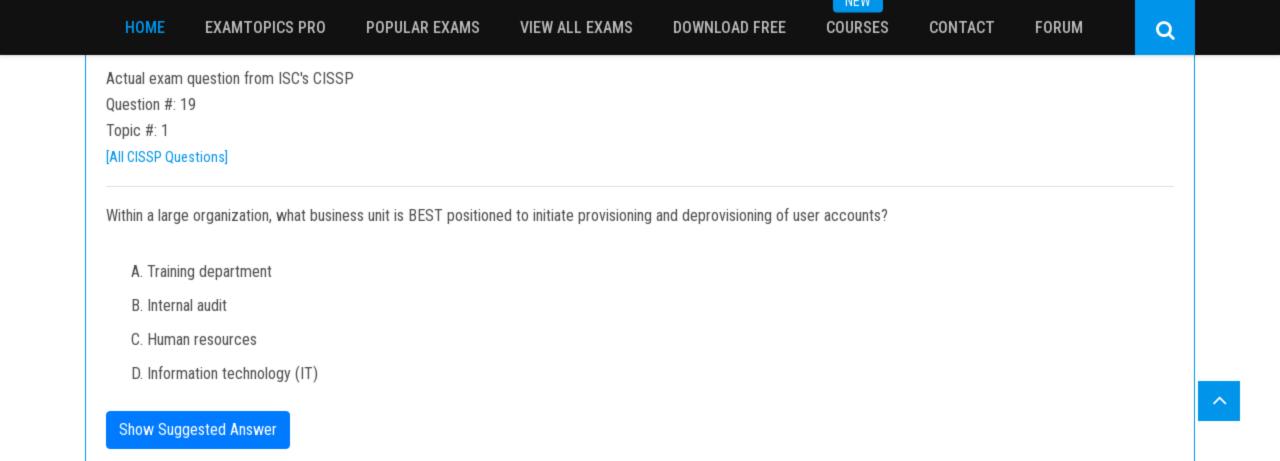
^

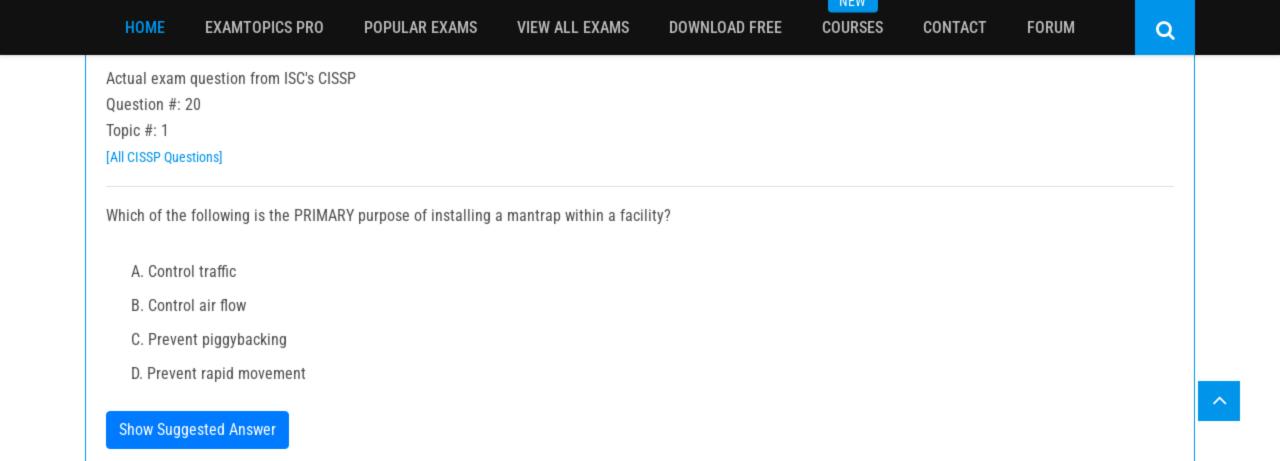










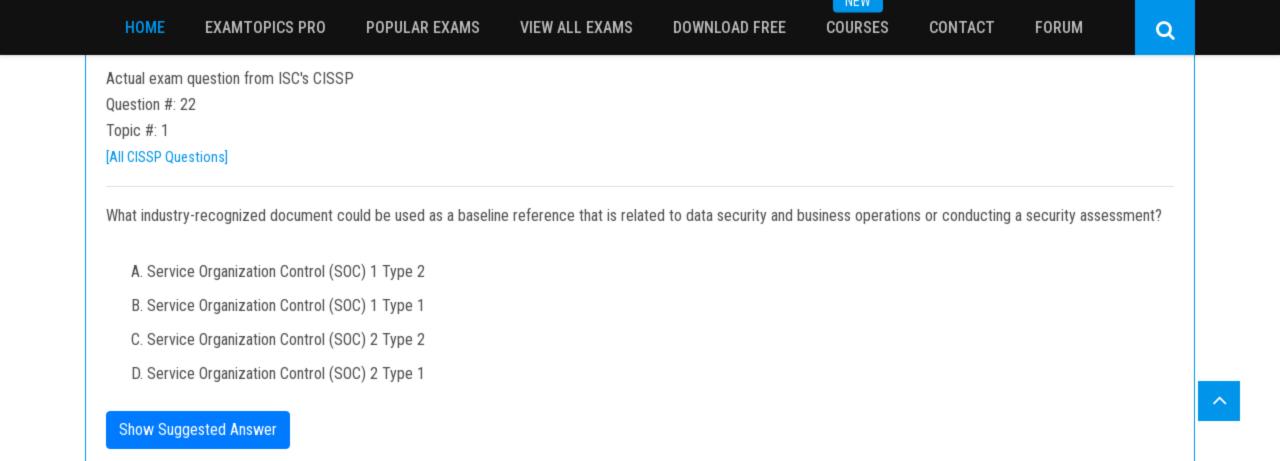


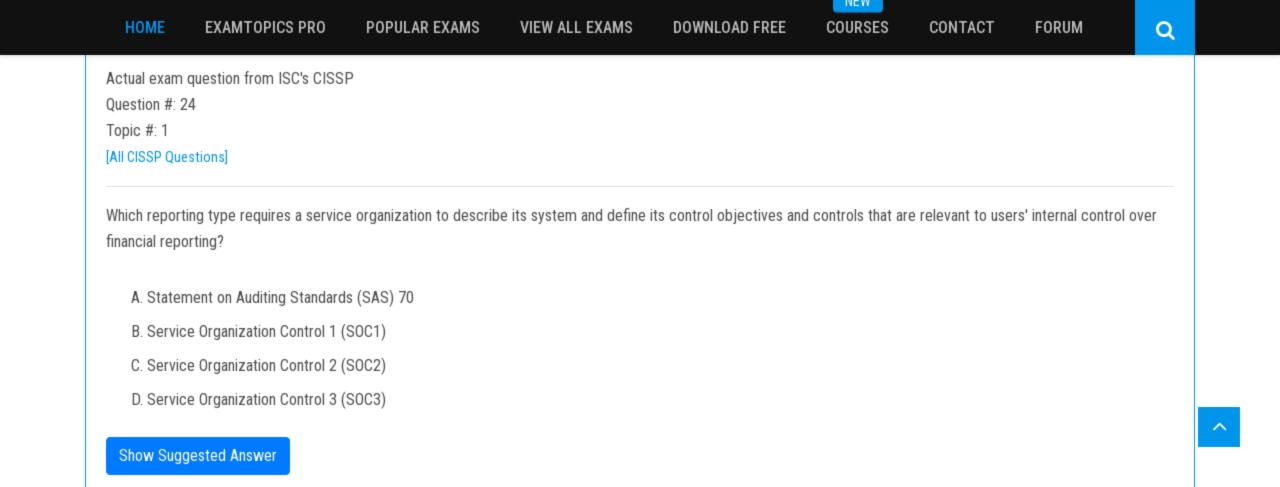
[All CISSP Questions]

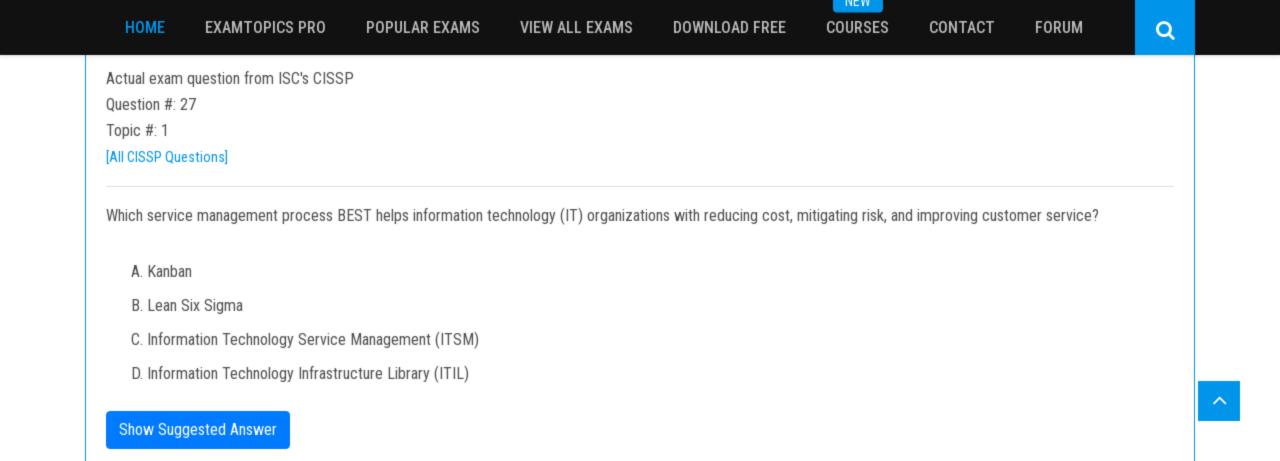
In the "Do" phase of the Plan-Do-Check-Act model, which of the following is performed?

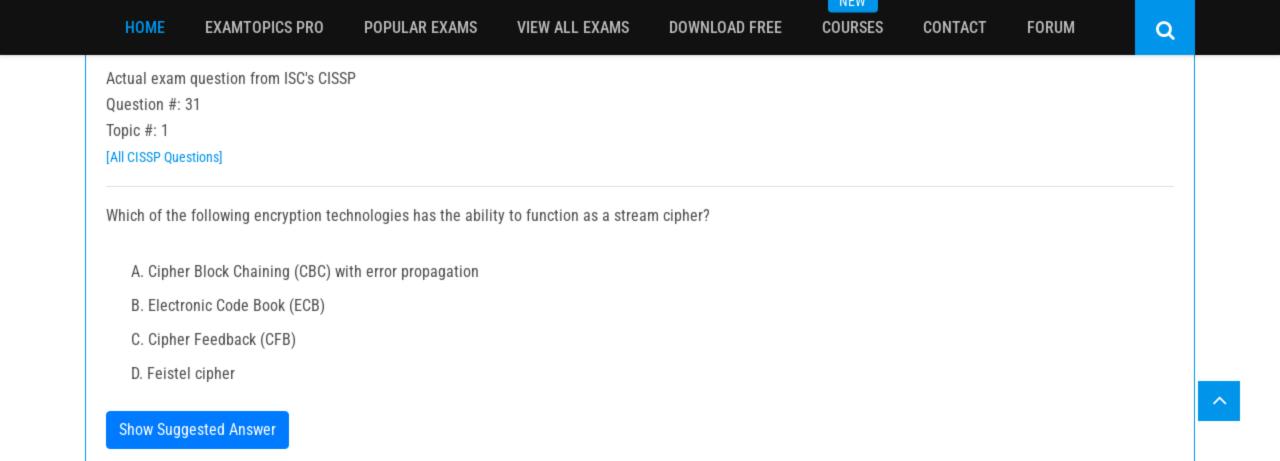
- A. Maintain and improve the Business Continuity Management (BCM) system by taking corrective action, based on the results of management review.
- B. Monitor and review performance against business continuity policy and objectives, report the results to management for review, and determine and authorize actions for remediation and improvement.
- C. Ensure the business continuity policy, controls, processes, and procedures have been implemented.
- D. Ensure that business continuity policy, objectives, targets, controls, processes and procedures relevant to improving business continuity have been established.

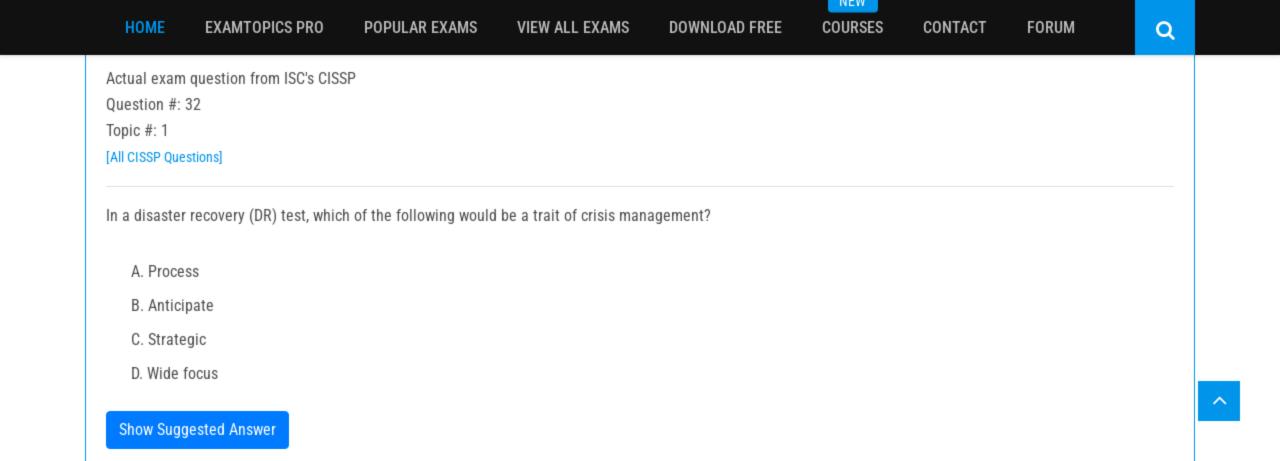
Show Suggested Answer

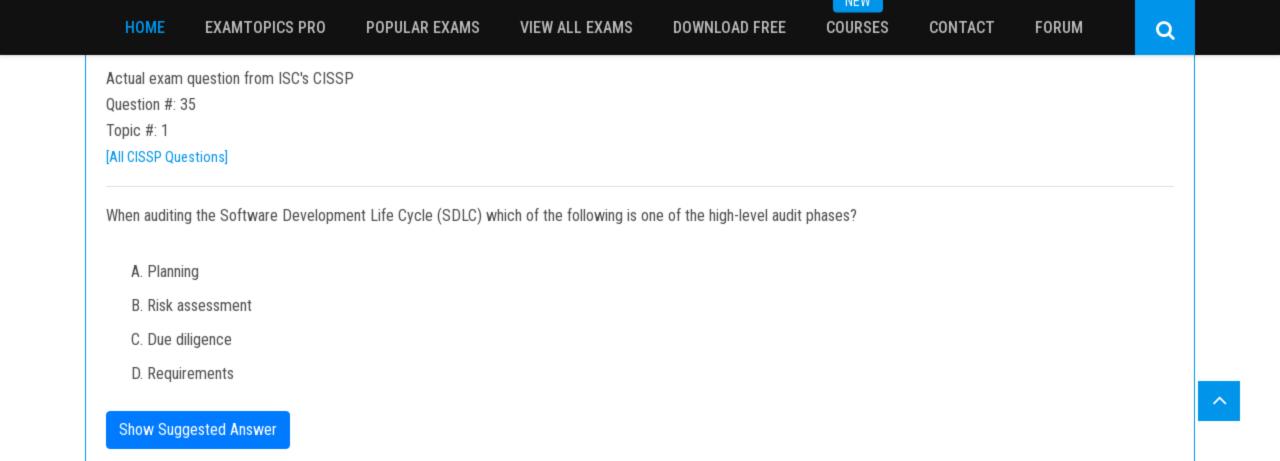


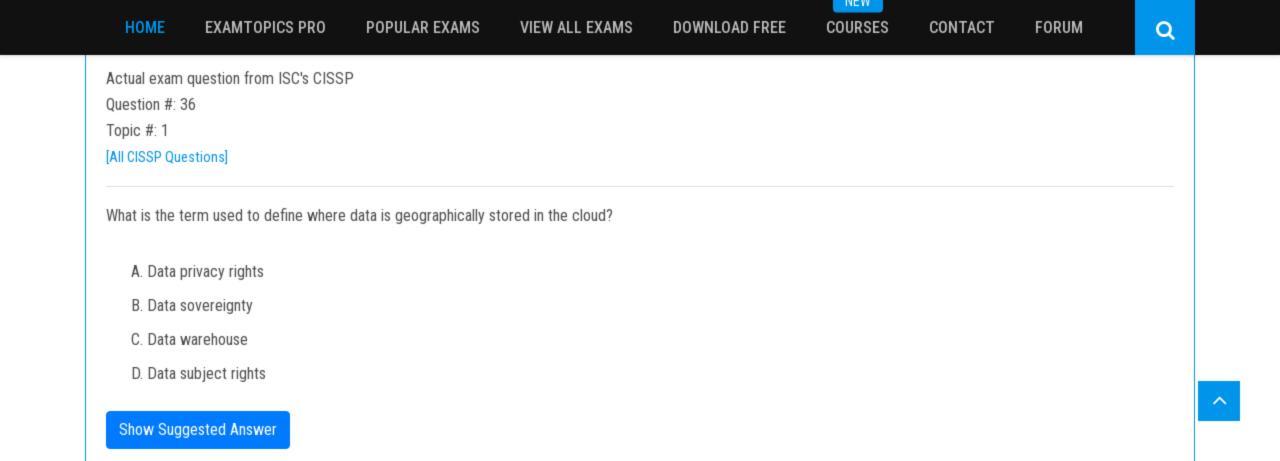


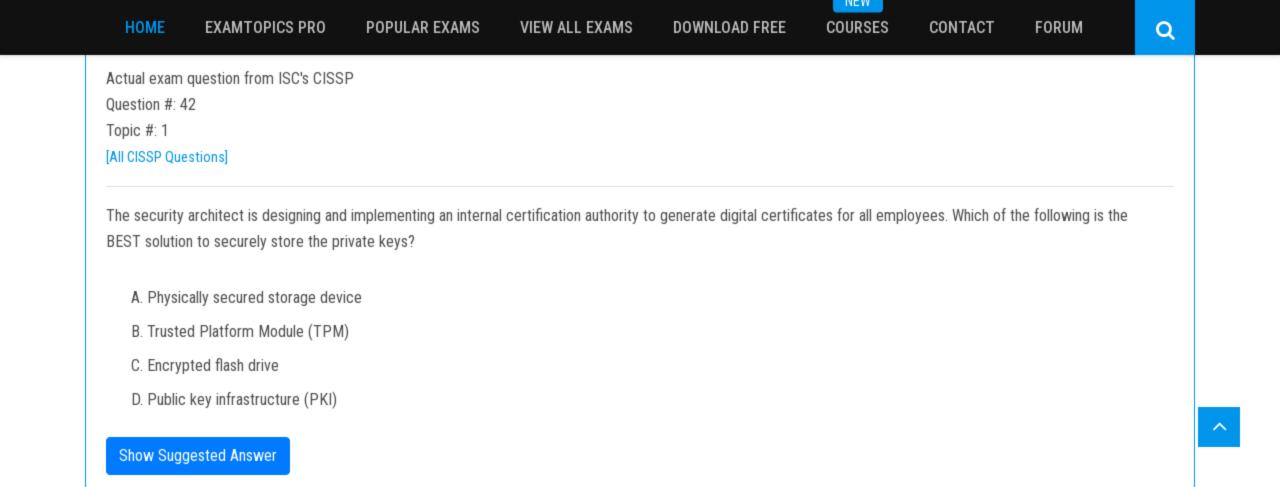


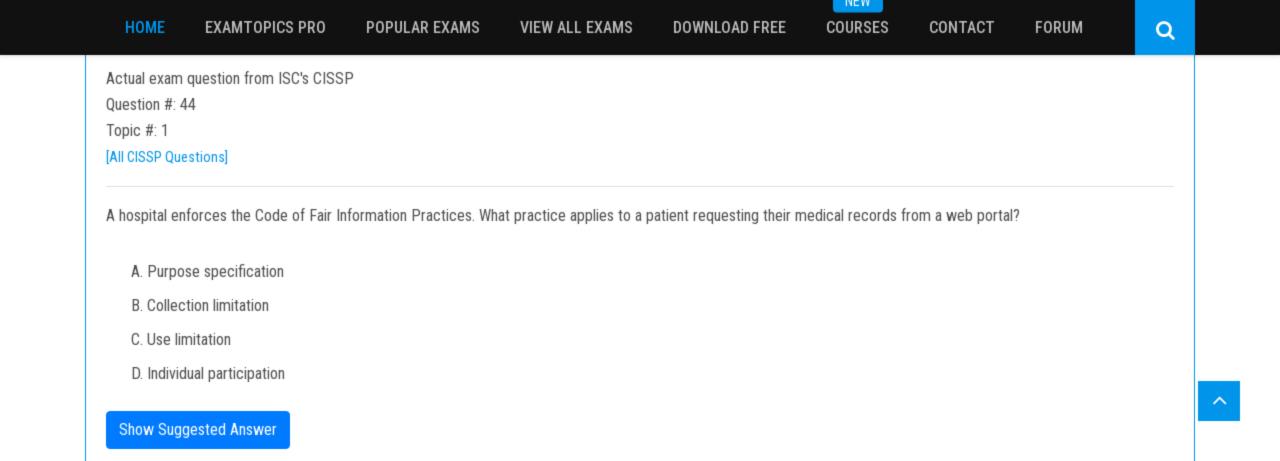


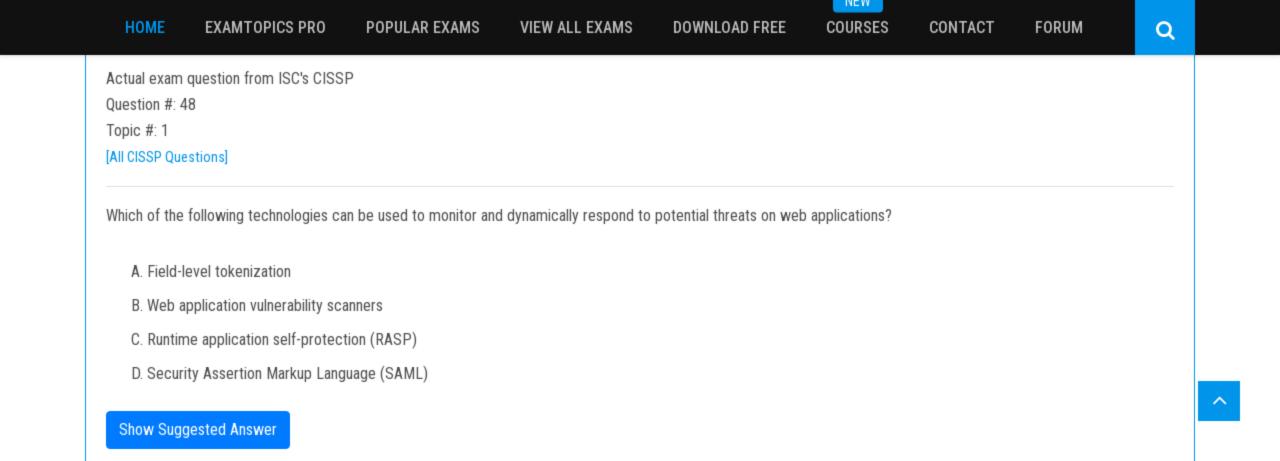


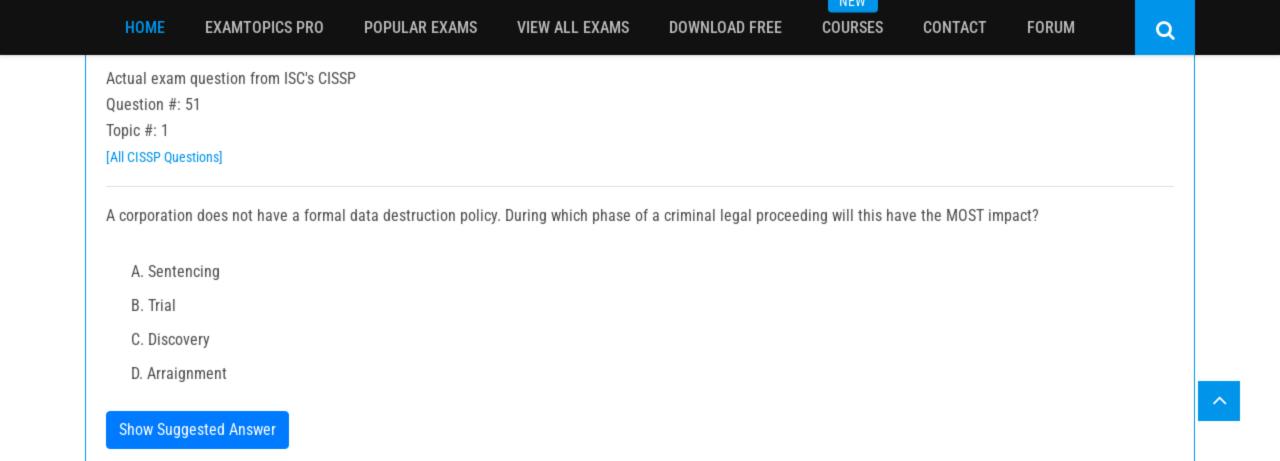


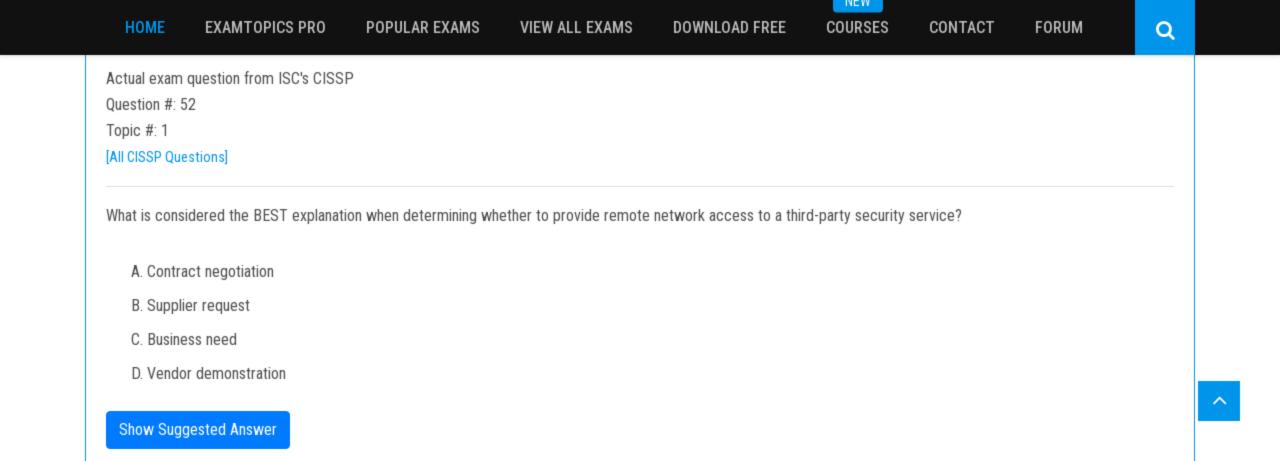


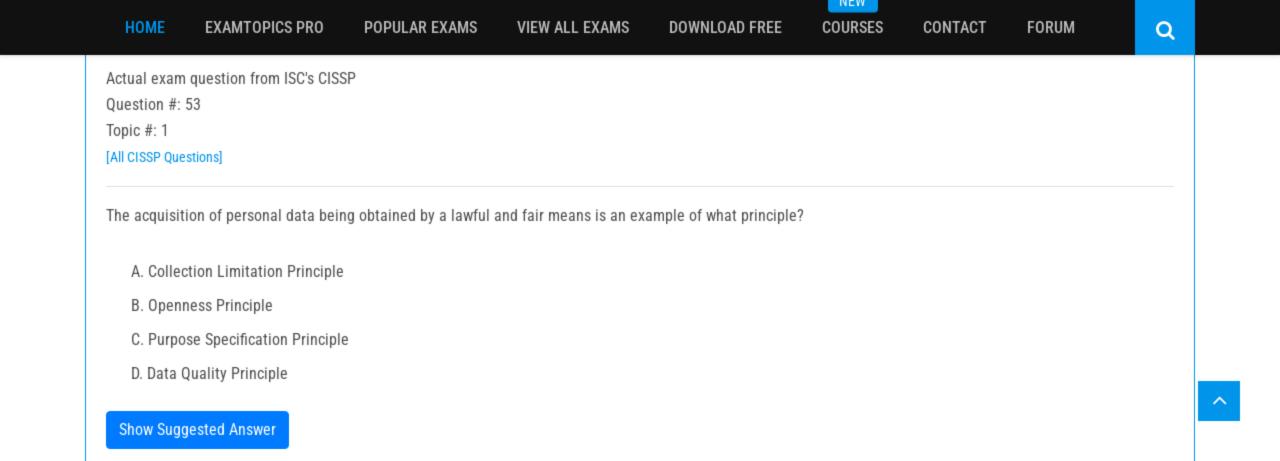


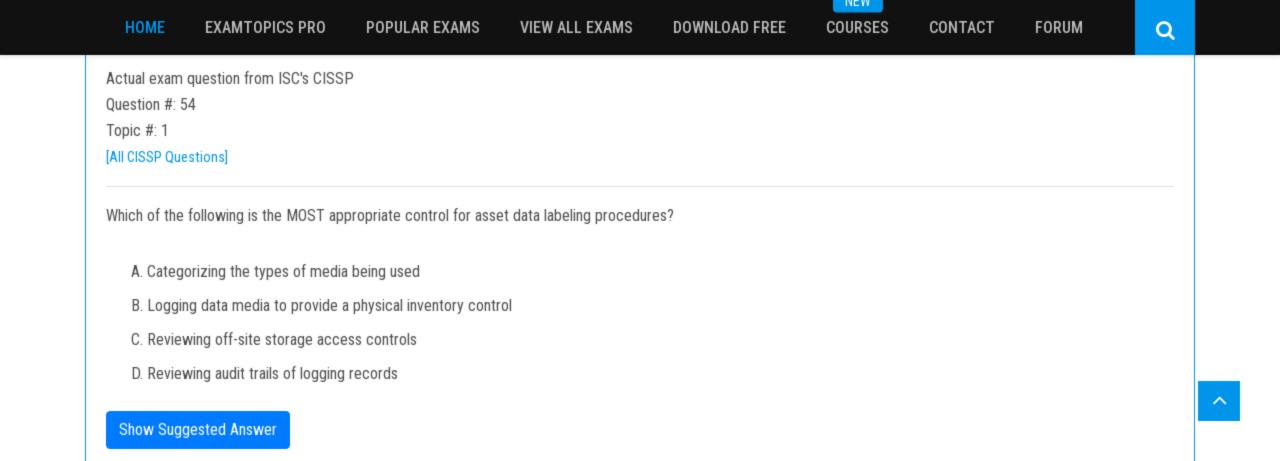


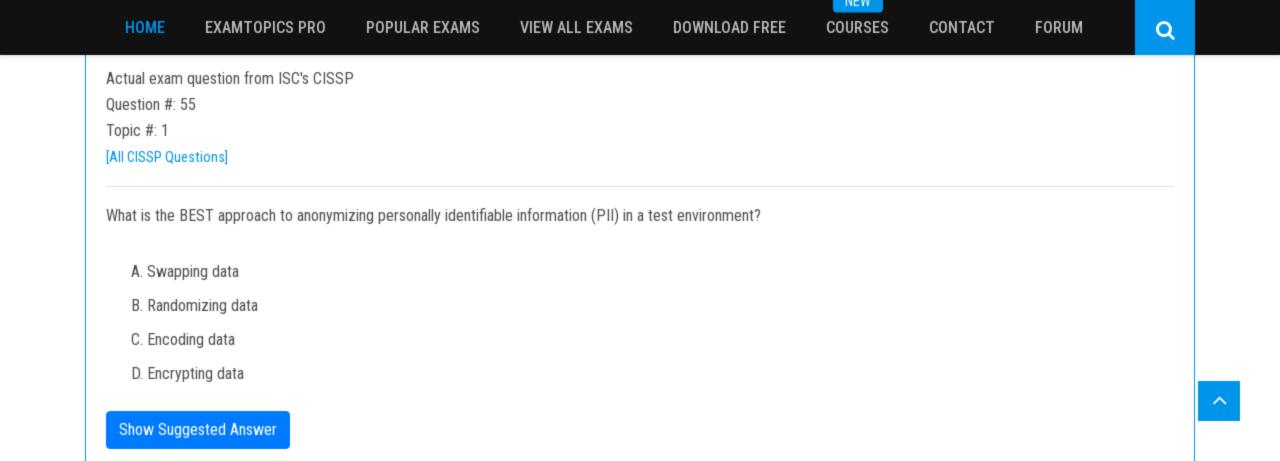


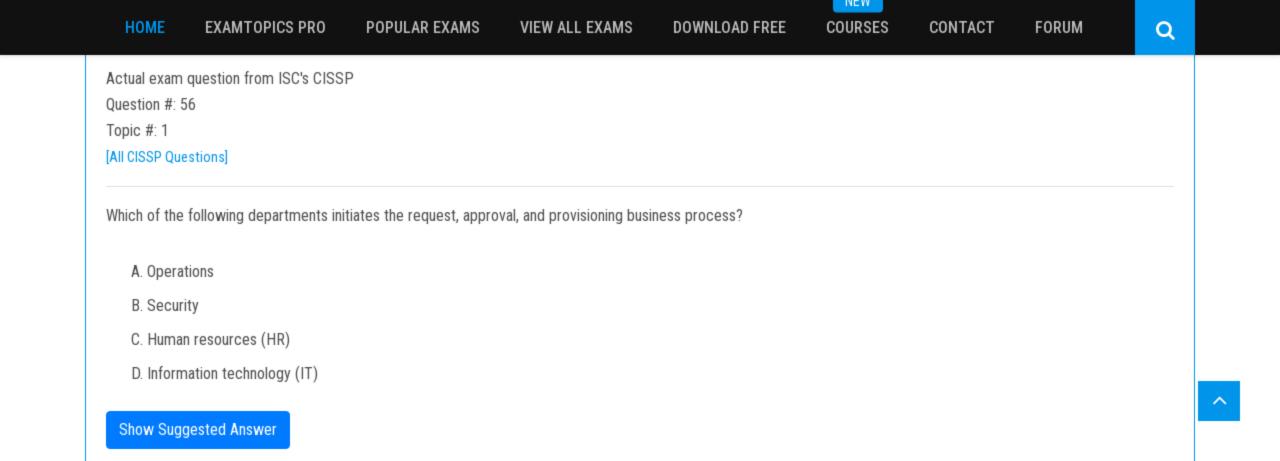


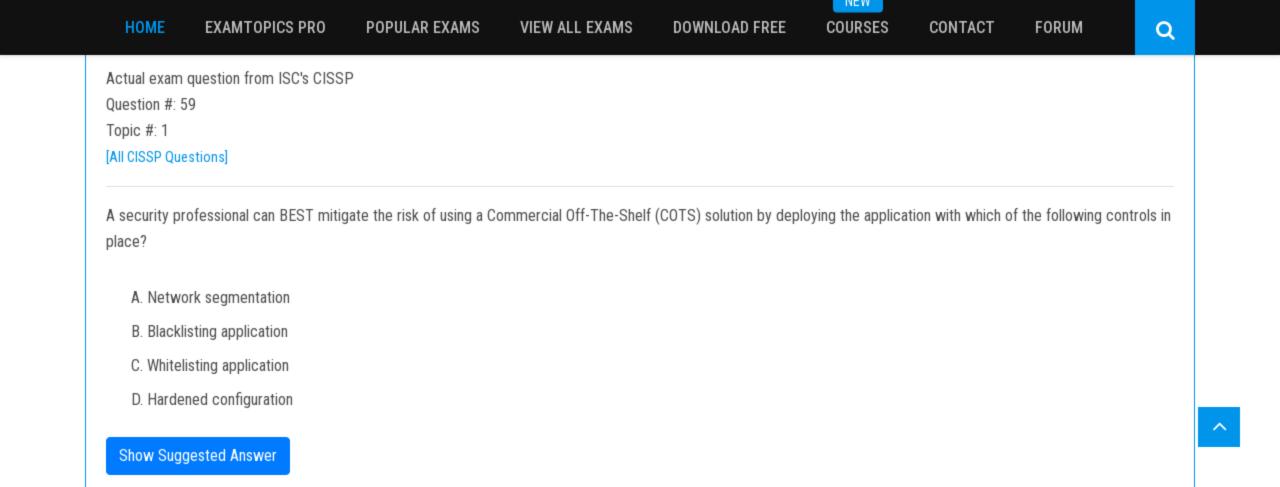


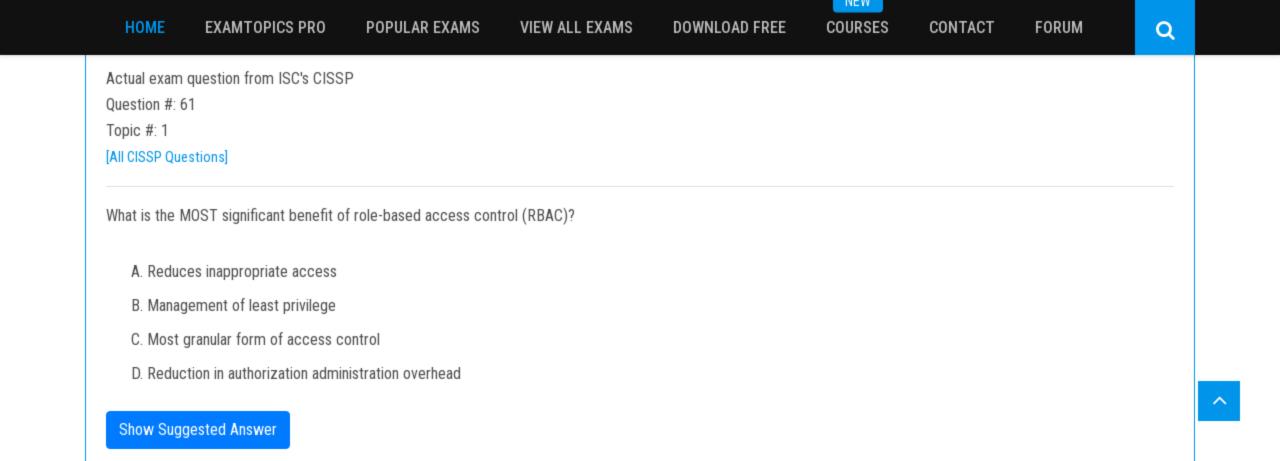


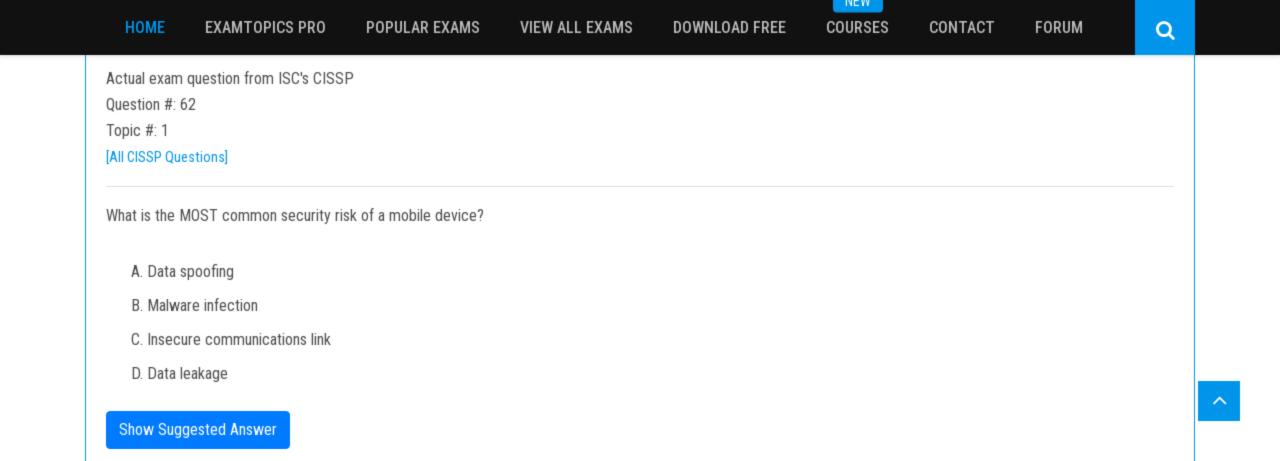


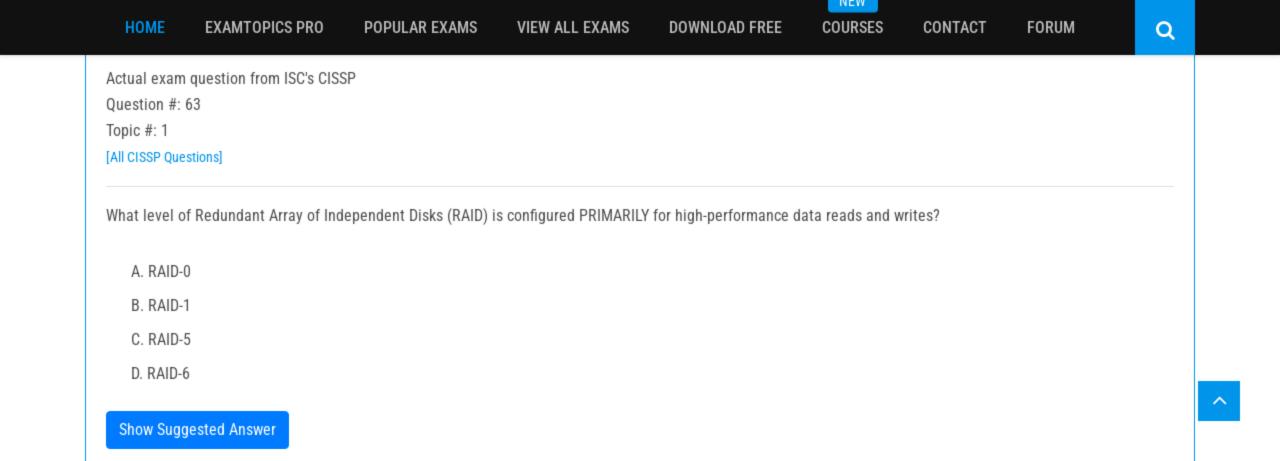


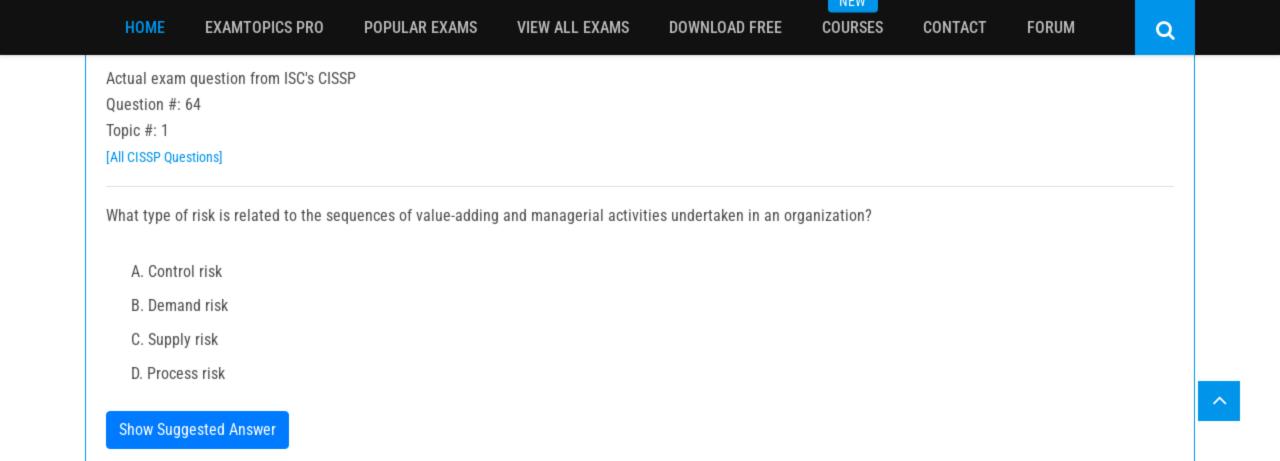


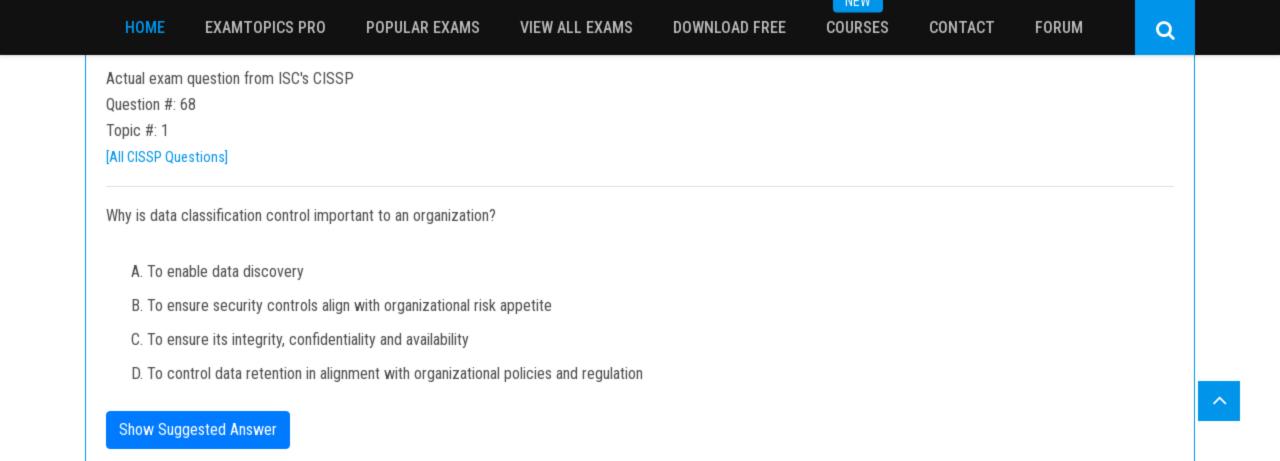


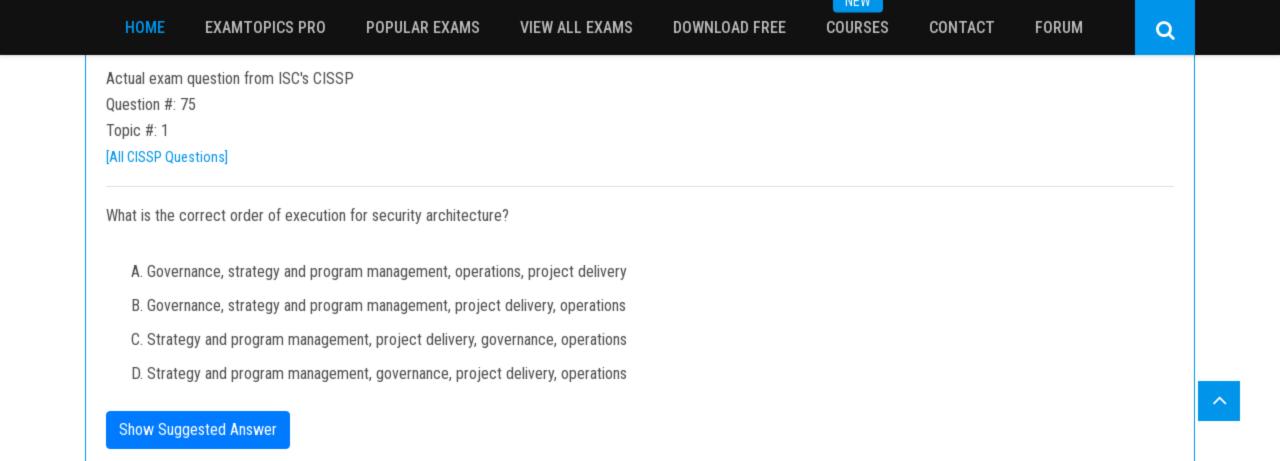


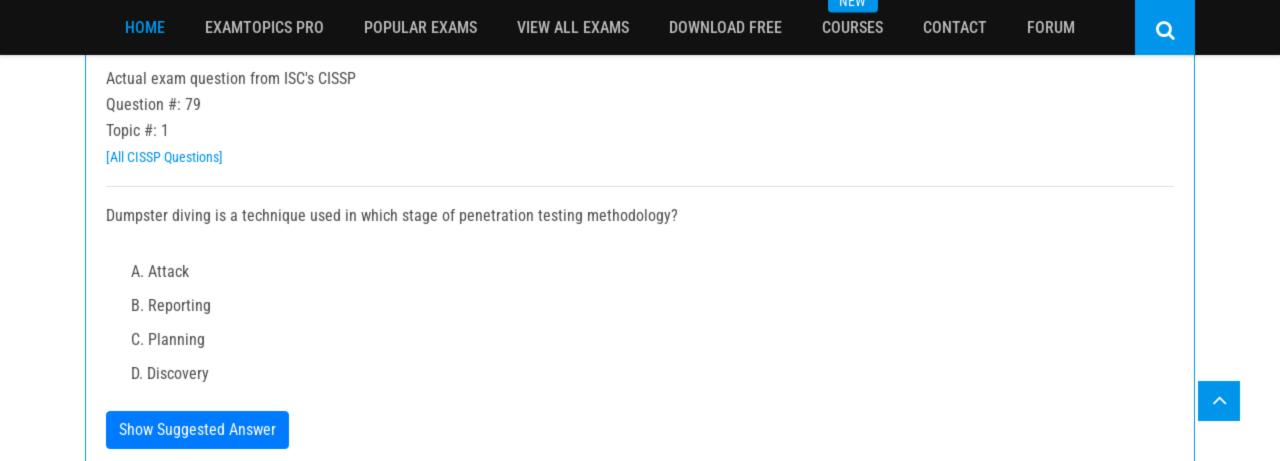


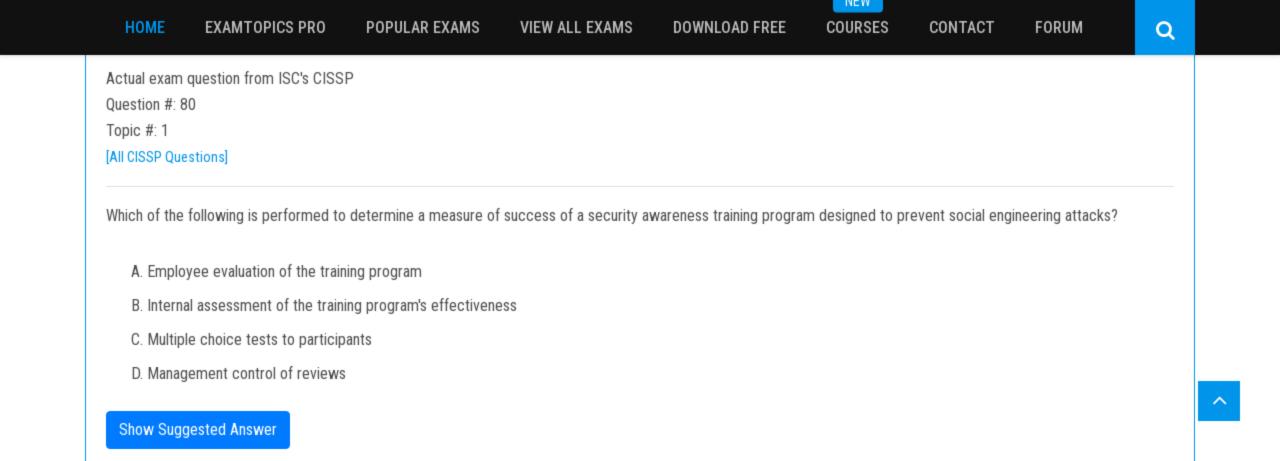


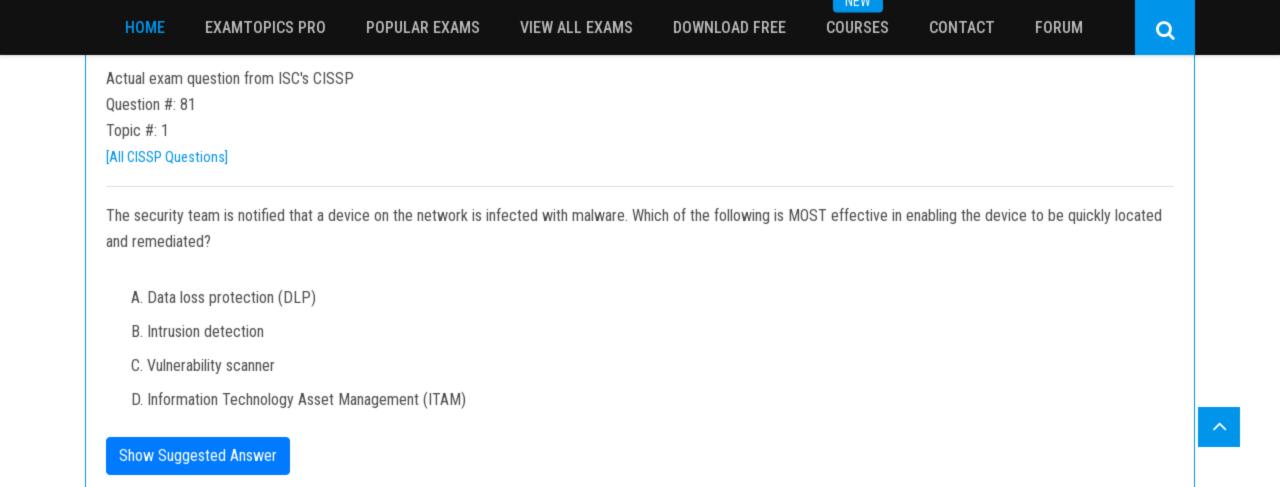


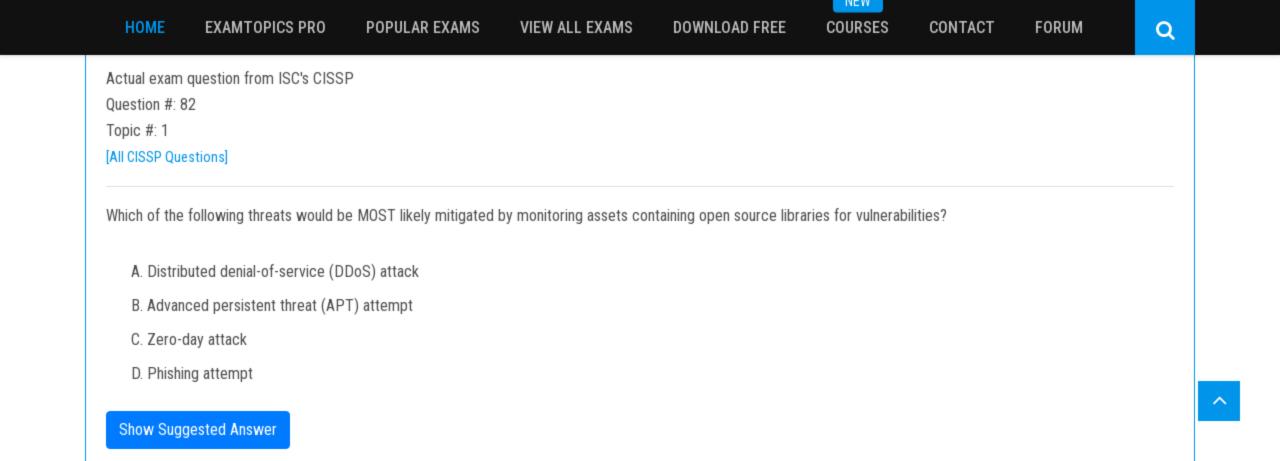


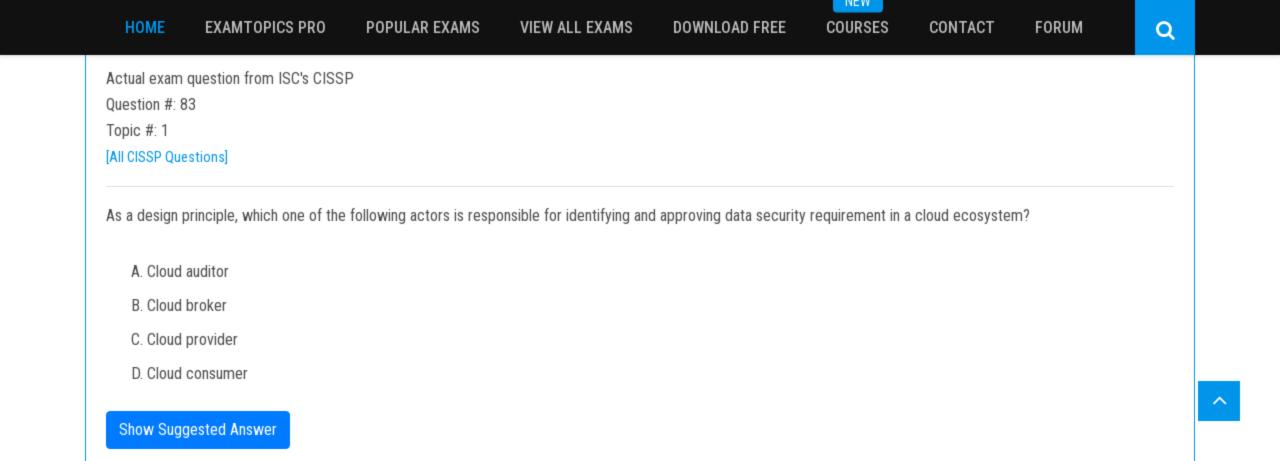


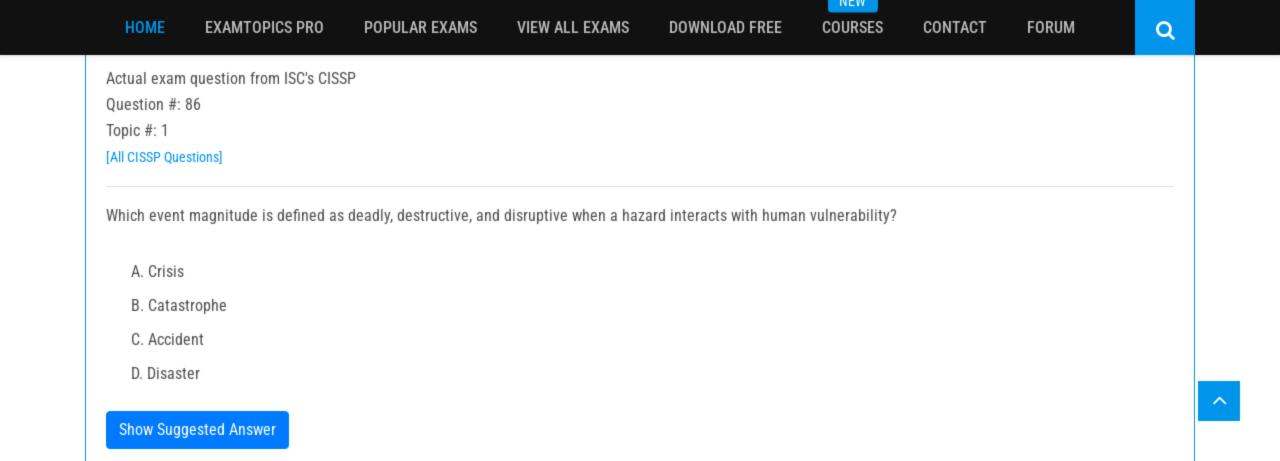


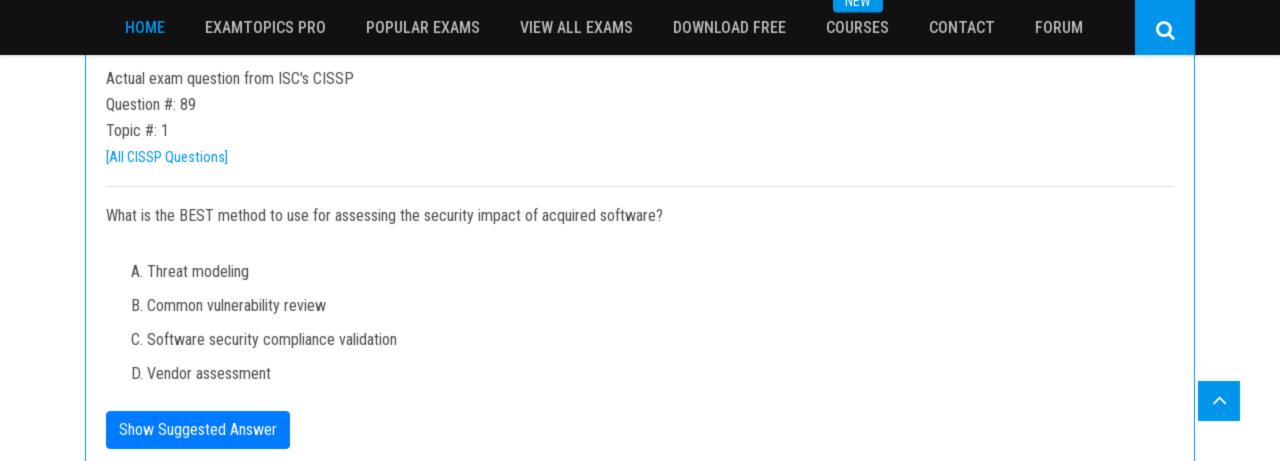


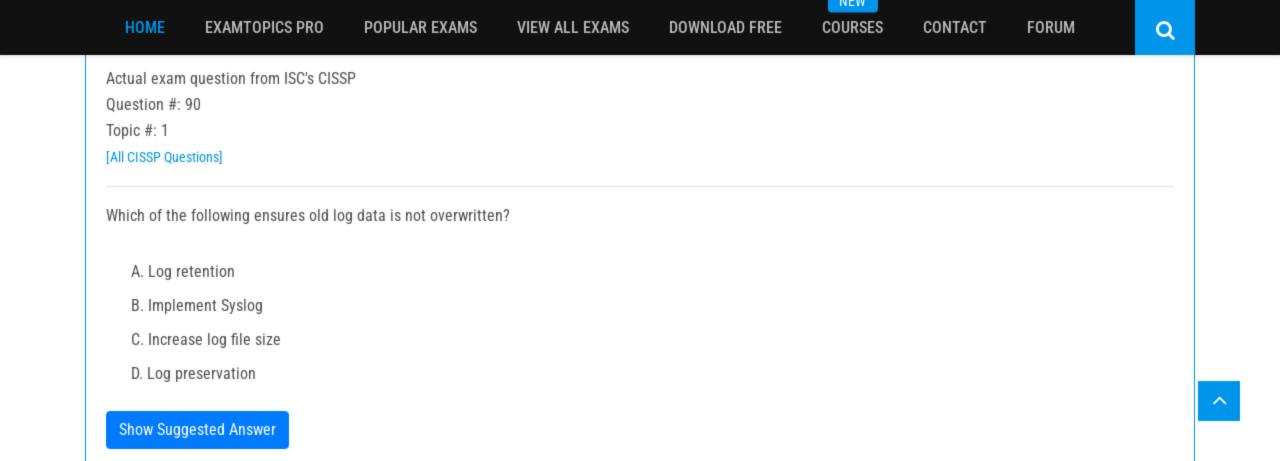


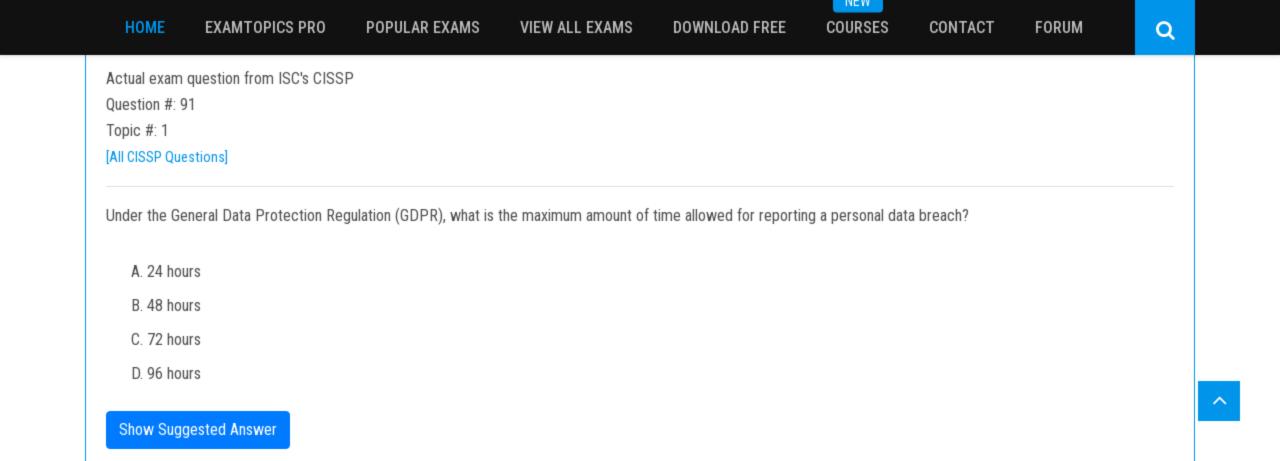


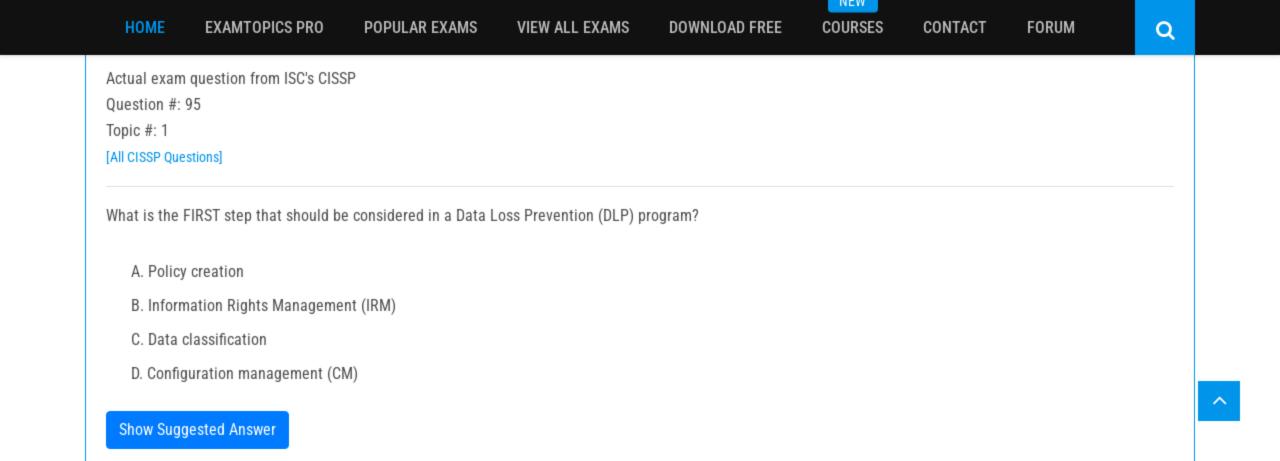


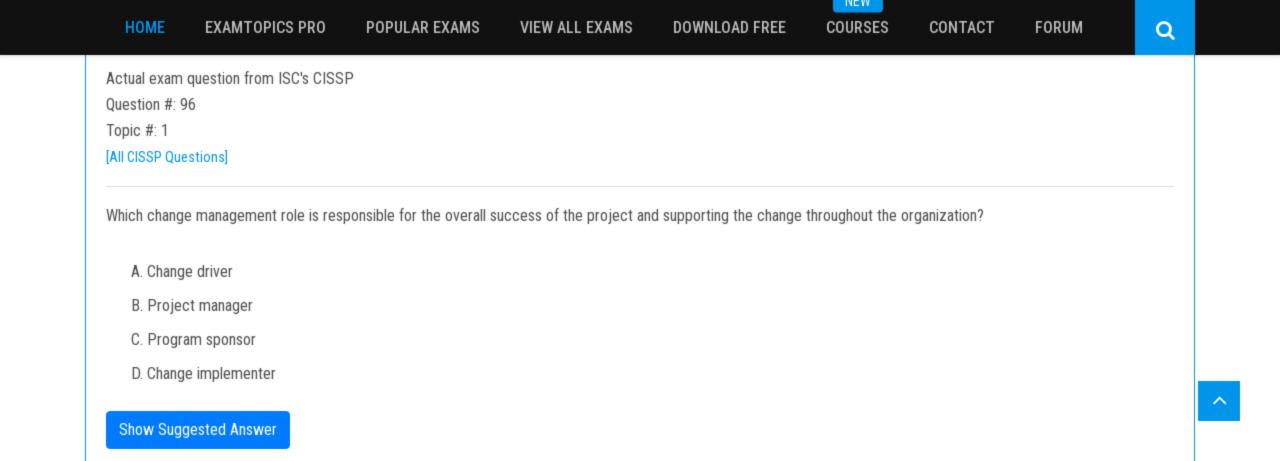


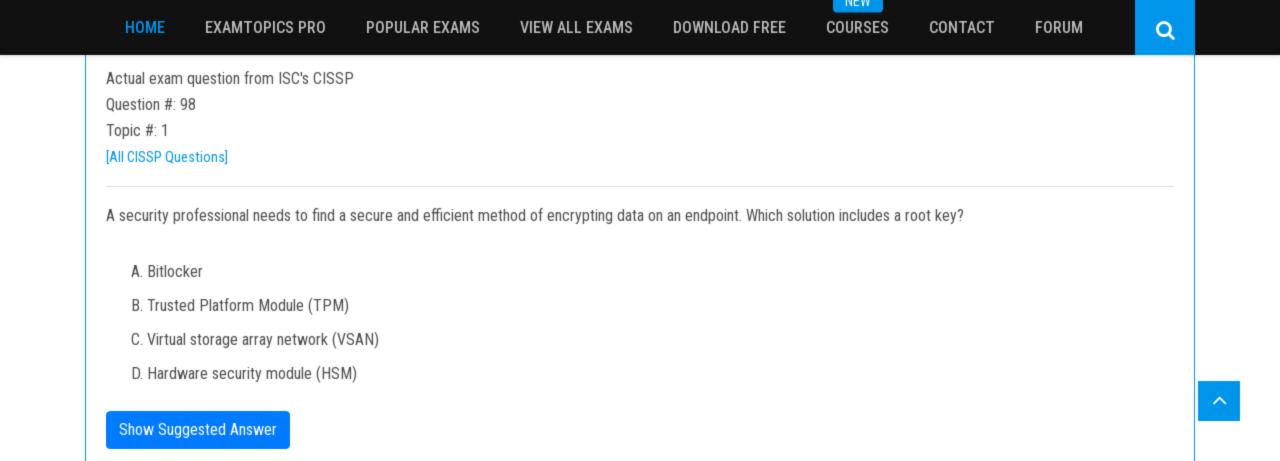












Actual exam question from ISC's CISSP

Question #: 99

Topic #: 1

[All CISSP Questions]

Which combination of cryptographic algorithms are compliant with Federal Information Processing Standard (FIPS) Publication 140-2 for non-legacy systems?

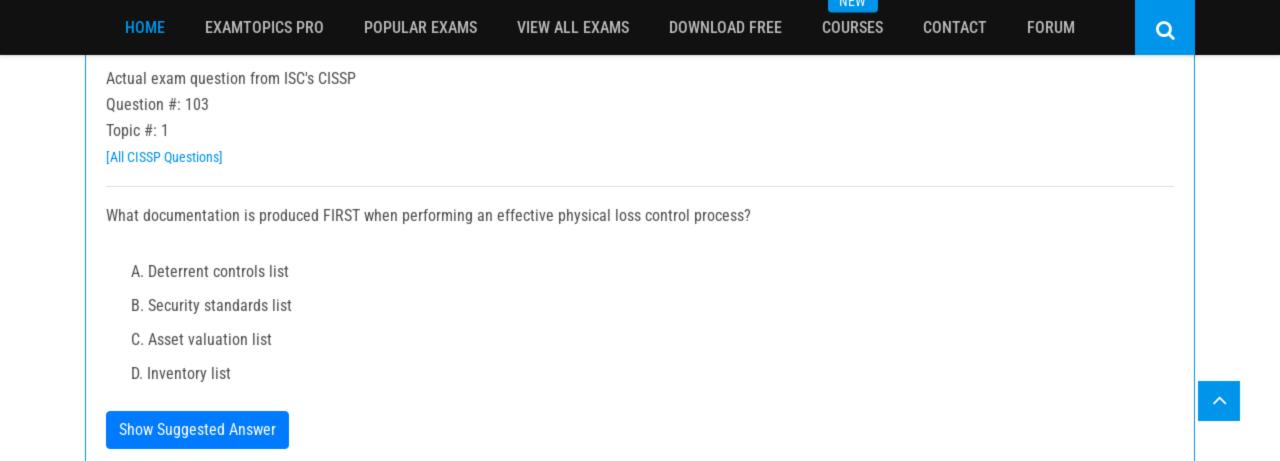
- A. Diffie-hellman (DH) key exchange: DH (>=2048 bits) Symmetric Key: Advanced Encryption Standard (AES) > 128 bits Digital Signature: Digital Signature Algorithm (DSA) (>=2048 bits)
- B. Diffie-hellman (DH) key exchange: DH (>=2048 bits) Symmetric Key: Advanced Encryption Standard (AES) > 128 bits Digital Signature: Rivest-Shamir-Adleman (RSA) (1024 bits)
- C. Diffie-hellman (DH) key exchange: DH (<=1024 bits) Symmetric Key: Blowfish Digital Signature: Rivest-Shamir-Adleman (RSA) (>=2048 bits)
- D. Diffie-hellman (DH) key exchange: DH (>=2048 bits) Symmetric Key: Advanced Encryption Standard (AES) < 128 bits Digital Signature: Elliptic Curve Digital Signature Algorithm (ECDSA) (>=256 bits)

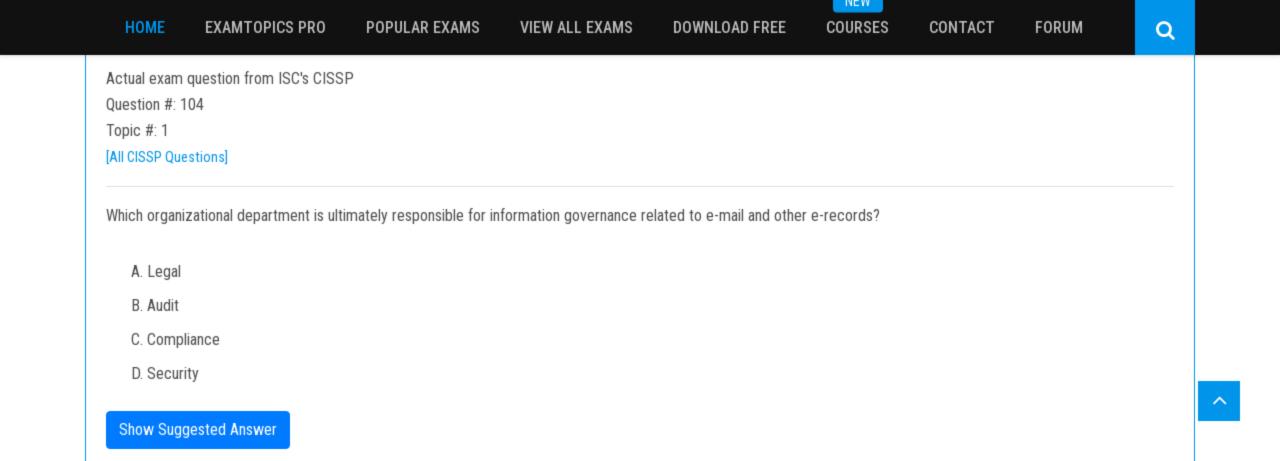
Show Suggested Answer

^

FORUM

Q





Question #: 112

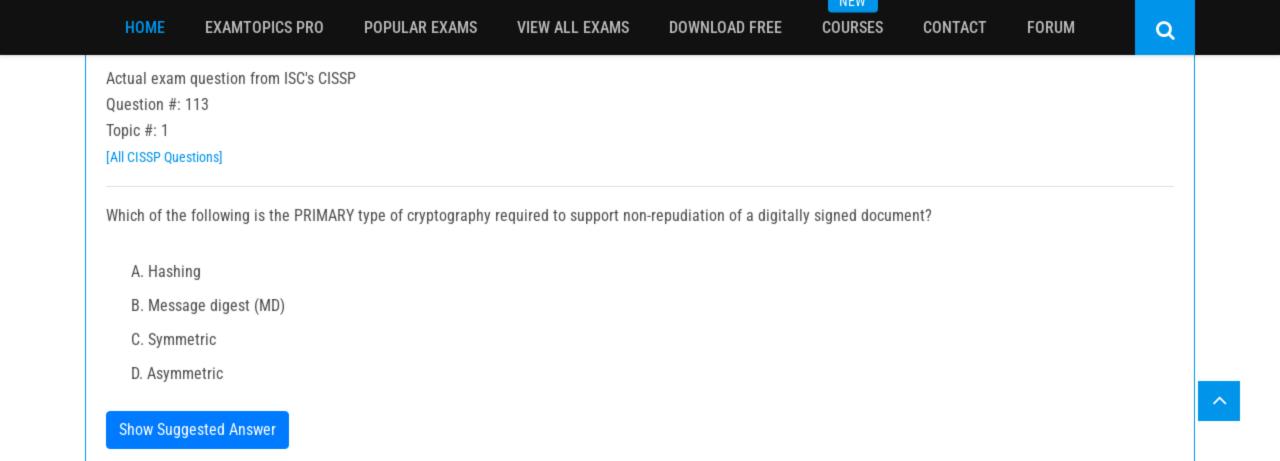
Topic #: 1

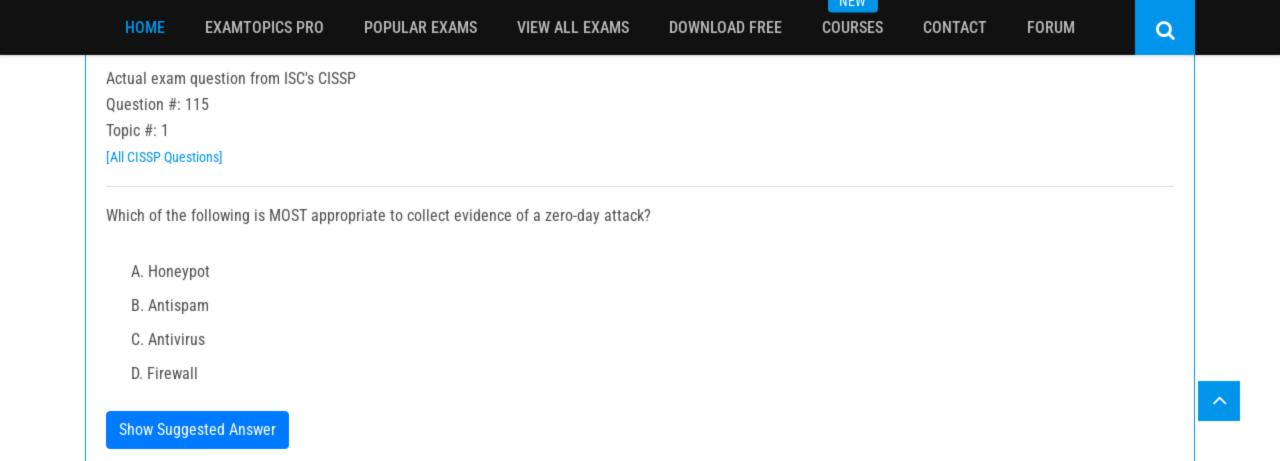
[All CISSP Questions]

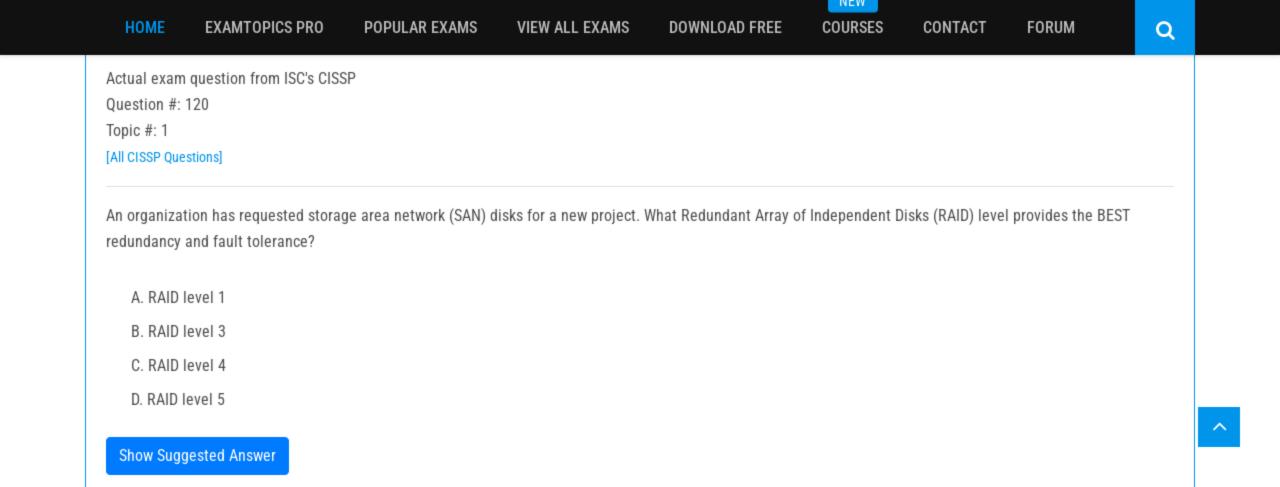
An international trading organization that holds an International Organization for Standardization (ISO) 27001 certification is seeking to outsource their security monitoring to a managed security service provider (MSSP). The trading organization's security officer is tasked with drafting the requirements that need to be included in the outsourcing contract. Which of the following MUST be included in the contract?

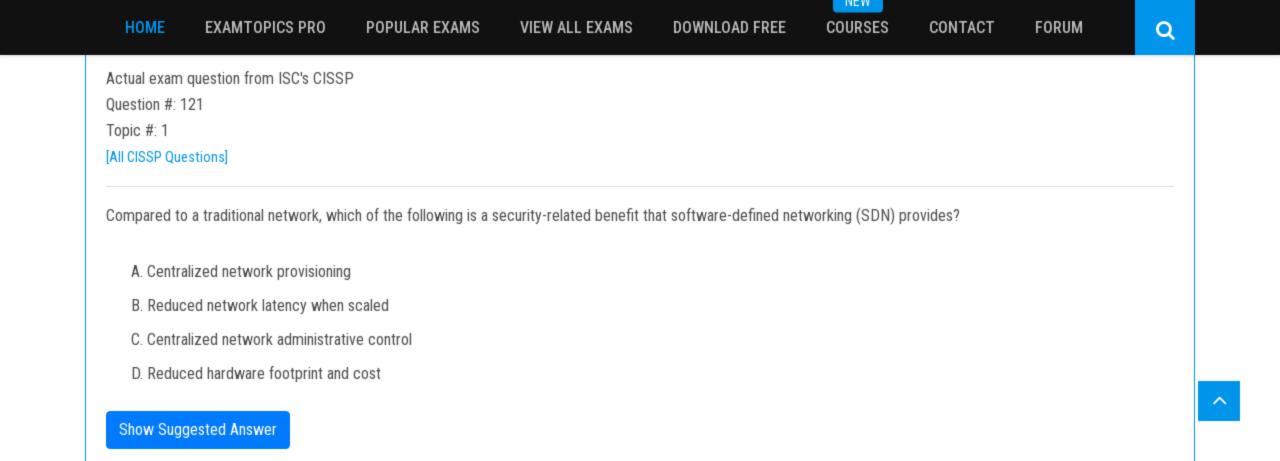
Q

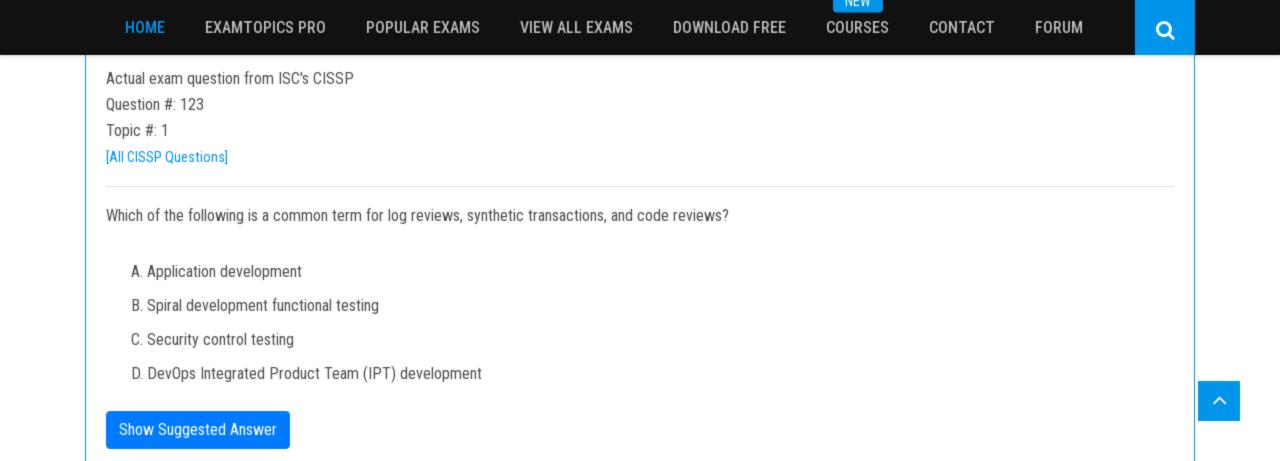
- A. A detailed overview of all equipment involved in the outsourcing contract
- B. The right to perform security compliance tests on the MSSP's equipment
- C. The MSSP having an executive manager responsible for information security
- D. The right to audit the MSSP's security process

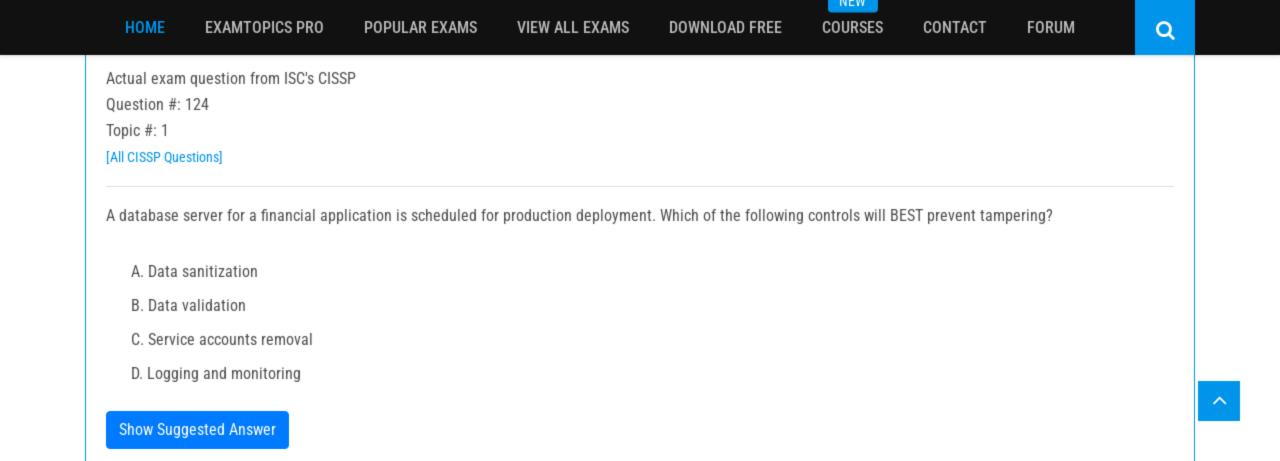












IA C AA

Actual exam question from ISC's CISSP

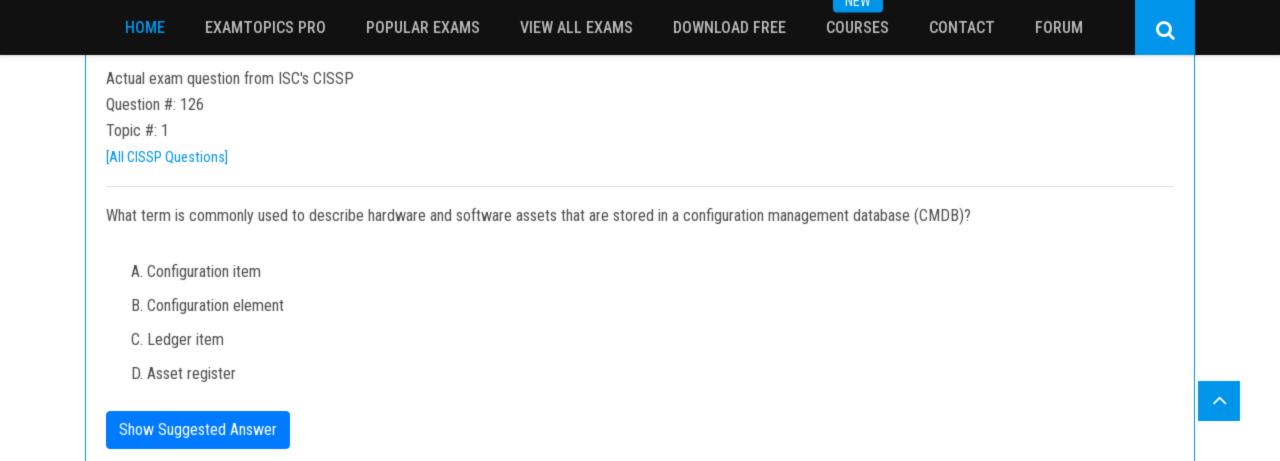
Question #: 125

Topic #: 1

[All CISSP Questions]

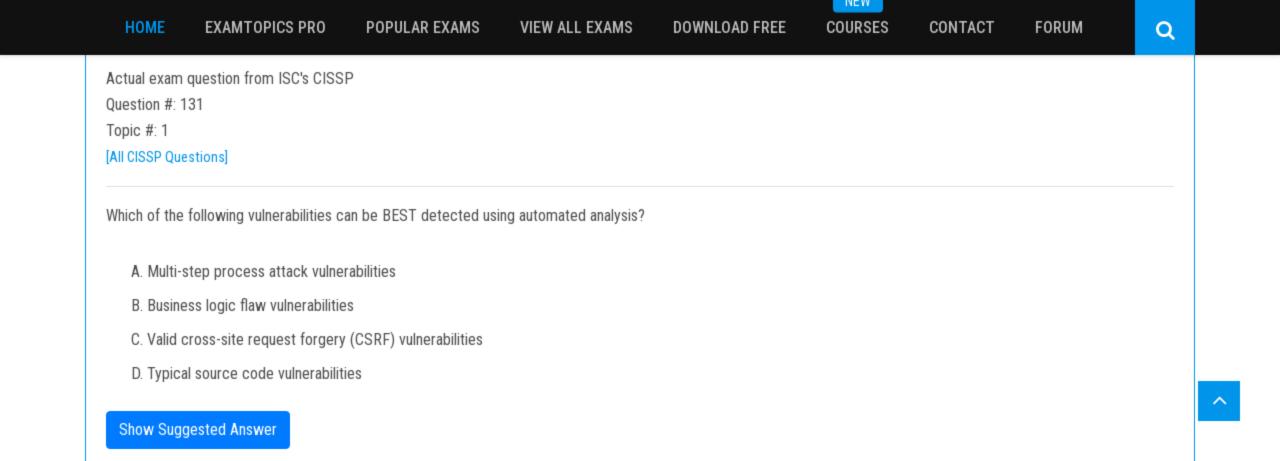
The Industrial Control System (ICS) Computer Emergency Response Team (CERT) has released an alert regarding ICS-focused malware specifically propagating through Windows-based business networks. Technicians at a local water utility note that their dams, canals, and locks controlled by an internal Supervisory Control and Data Acquisition (SCADA) system have been malfunctioning. A digital forensics professional is consulted in the Incident Response (IR) and recovery. Which of the following is the MOST challenging aspect of this investigation?

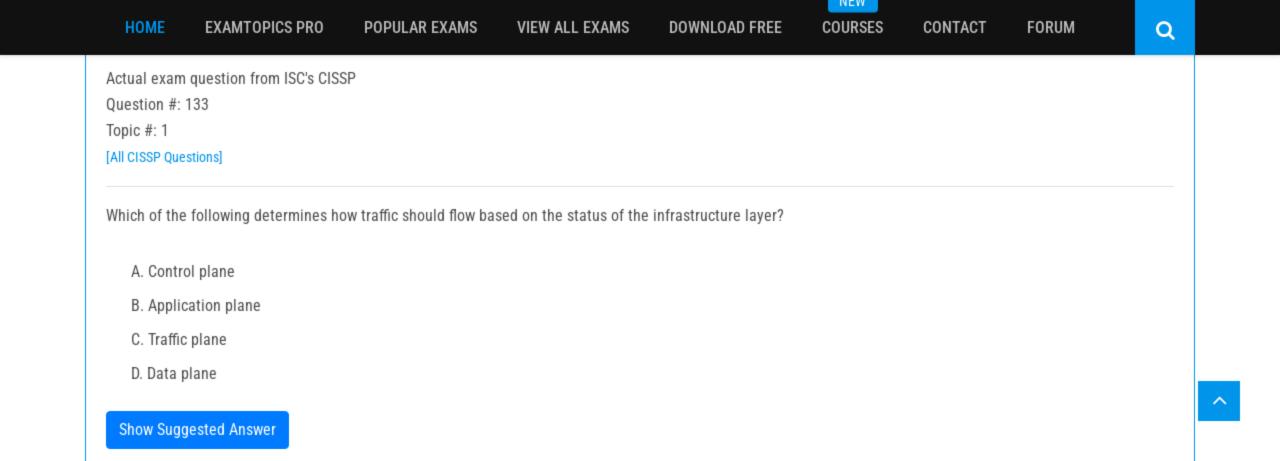
- A. Group policy implementation
- B. SCADA network latency
- C. Physical access to the system
- D. Volatility of data

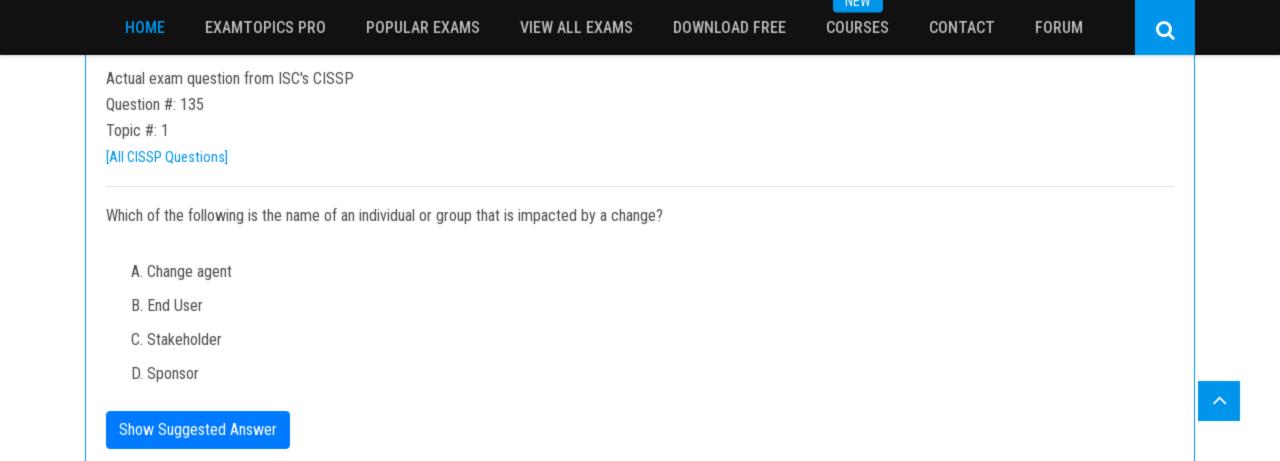


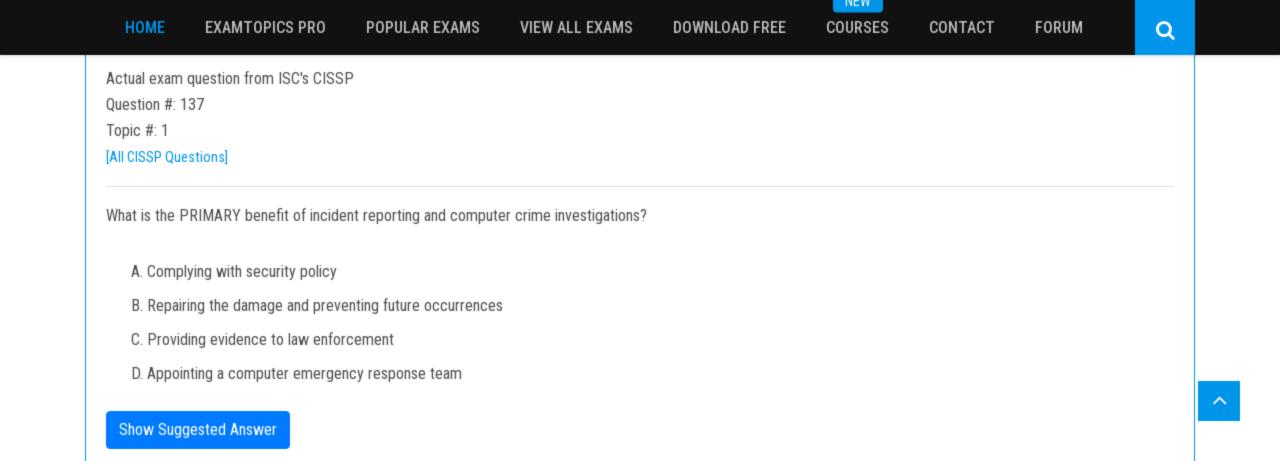
A company hired an external vendor to perform a penetration test of a new payroll system. The company's internal test team had already performed an in-depth application and security test of the system and determined that it met security requirements. However, the external vendor uncovered significant security weaknesses where sensitive personal data was being sent unencrypted to the tax processing systems. What is the MOST likely cause of the security issues?

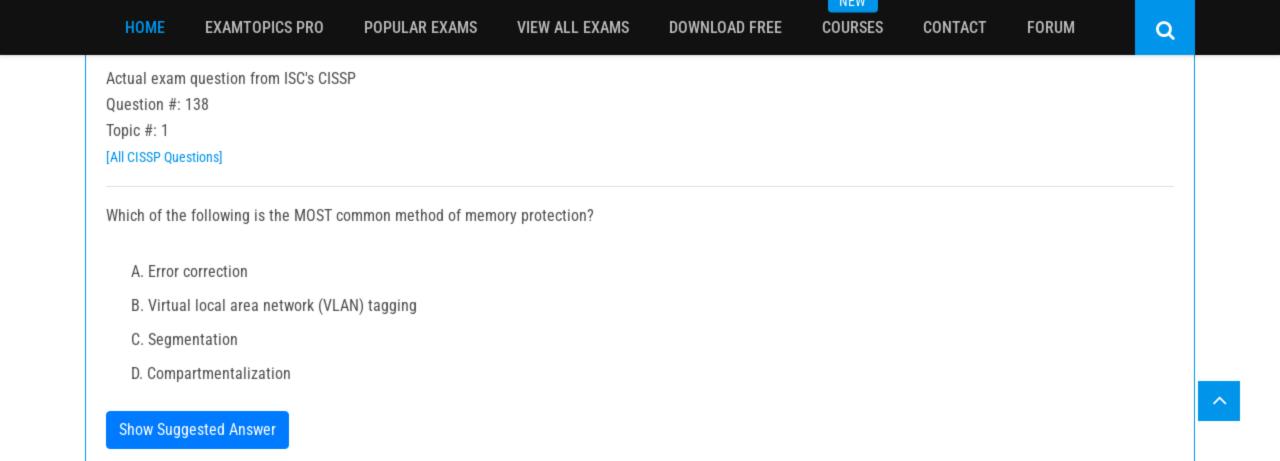
- A. Inadequate performance testing
- B. Inadequate application level testing
- C. Failure to perform negative testing
- D. Failure to perform interface testing

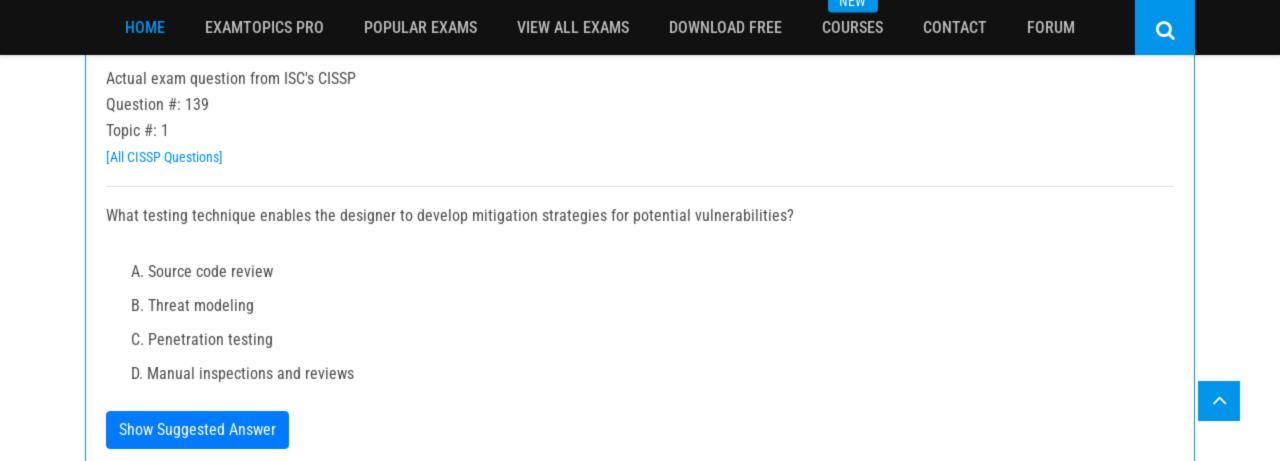


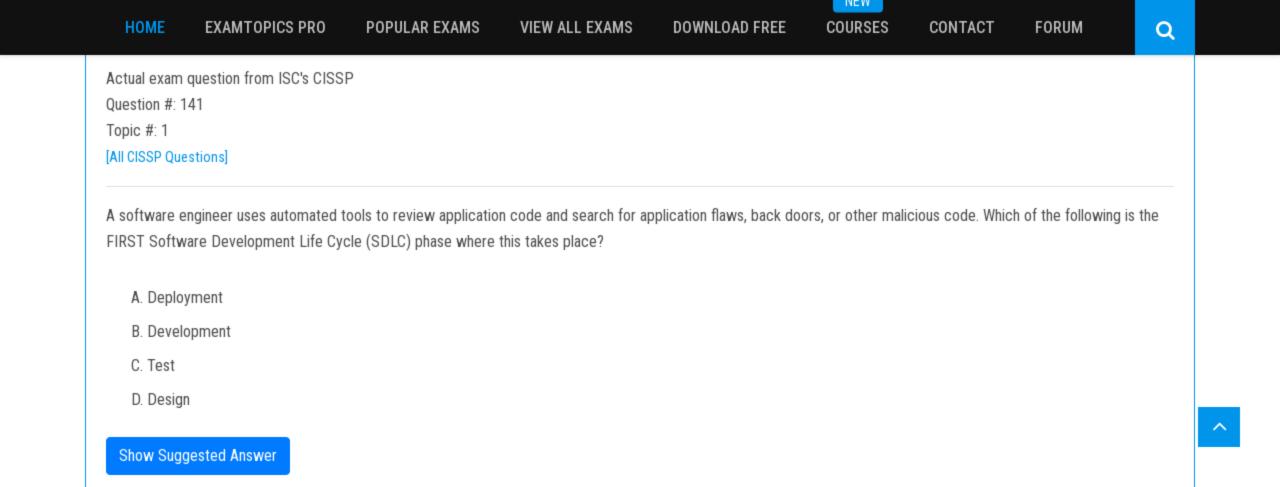












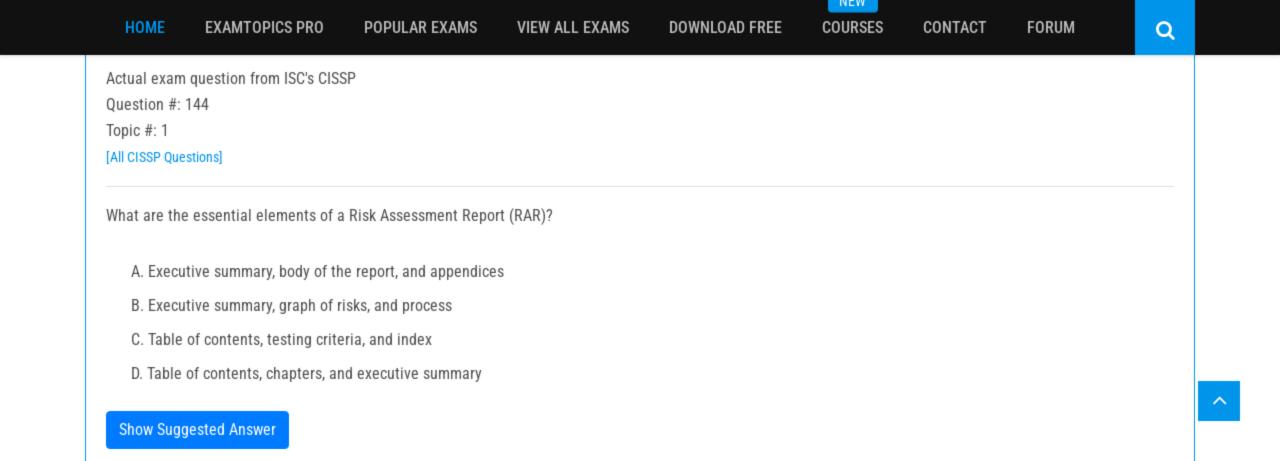
Topic #: 1

[All CISSP Questions]

A company developed a web application which is sold as a Software as a Service (SaaS) solution to the customer. The application is hosted by a web server running on a specific operating system (OS) on a virtual machine (VM). During the transition phase of the service, it is determined that the support team will need access to the application logs. Which of the following privileges would be the MOST suitable?

Q

- A. Administrative privileges on the hypervisor
- B. Administrative privileges on the application folders
- C. Administrative privileges on the web server
- D. Administrative privileges on the OS



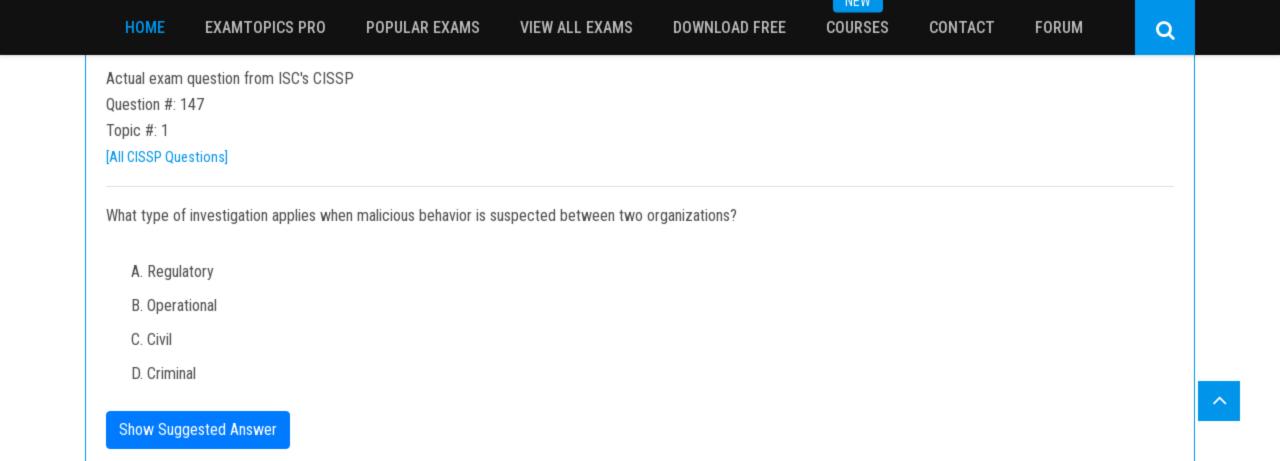
Topic #: 1

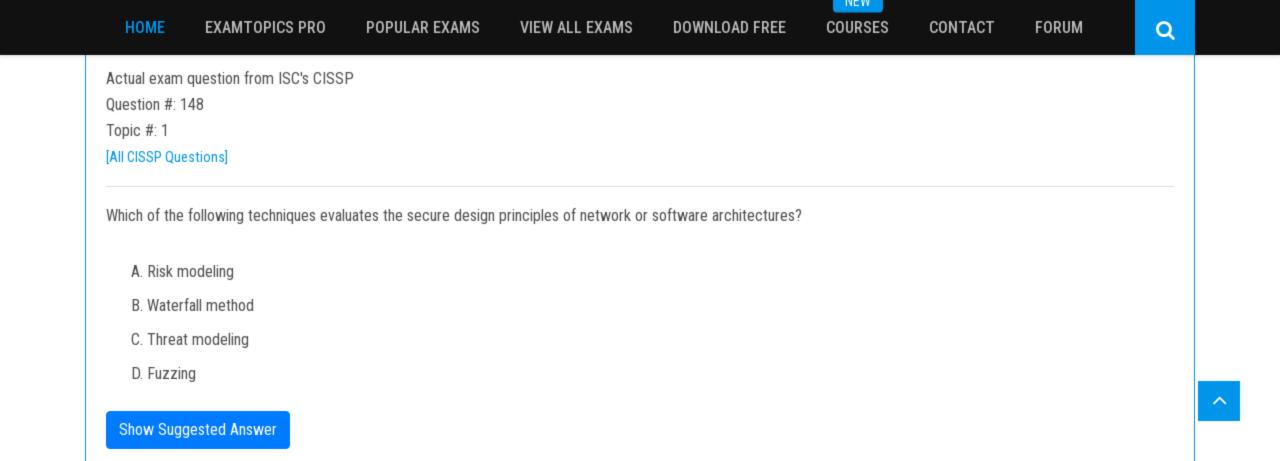
[All CISSP Questions]

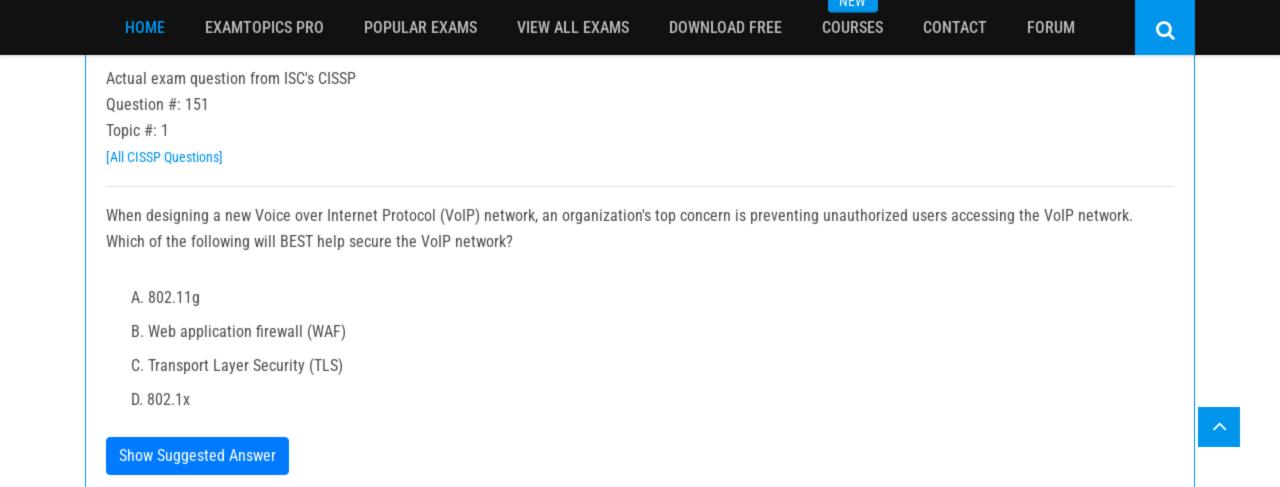
The security operations center (SOC) has received credible intelligence that a threat actor is planning to attack with multiple variants of a destructive virus. After obtaining a sample set of this virus' variants and reverse engineering them to understand how they work, a commonality was found. All variants are coded to write to a specific memory location. It is determined this virus is of no threat to the organization because they had the foresight to enable what feature on all endpoints?

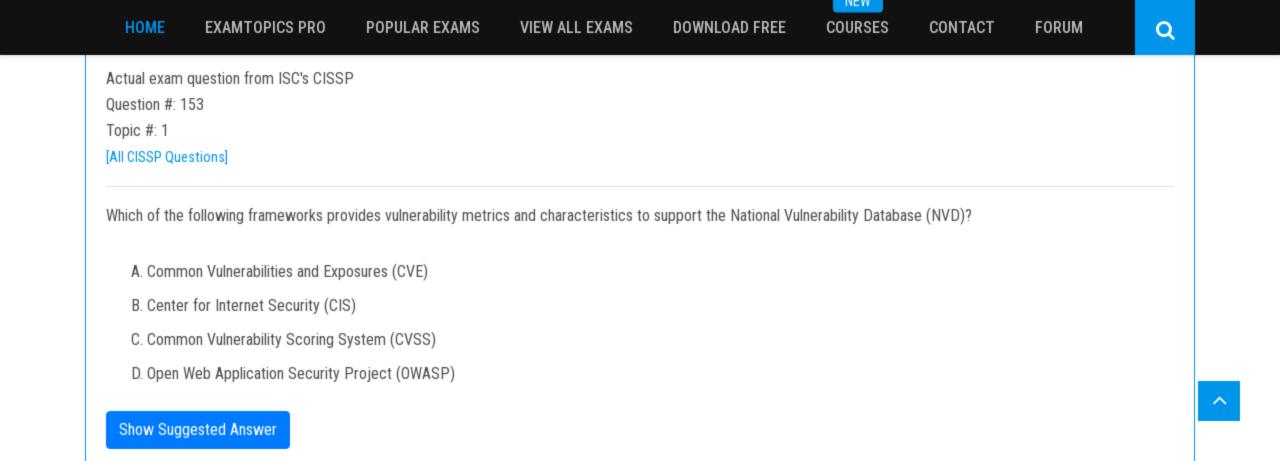
- A. Address Space Layout Randomization (ASLR)
- B. Trusted Platform Module (TPM)
- C. Virtualization
- D. Process isolation

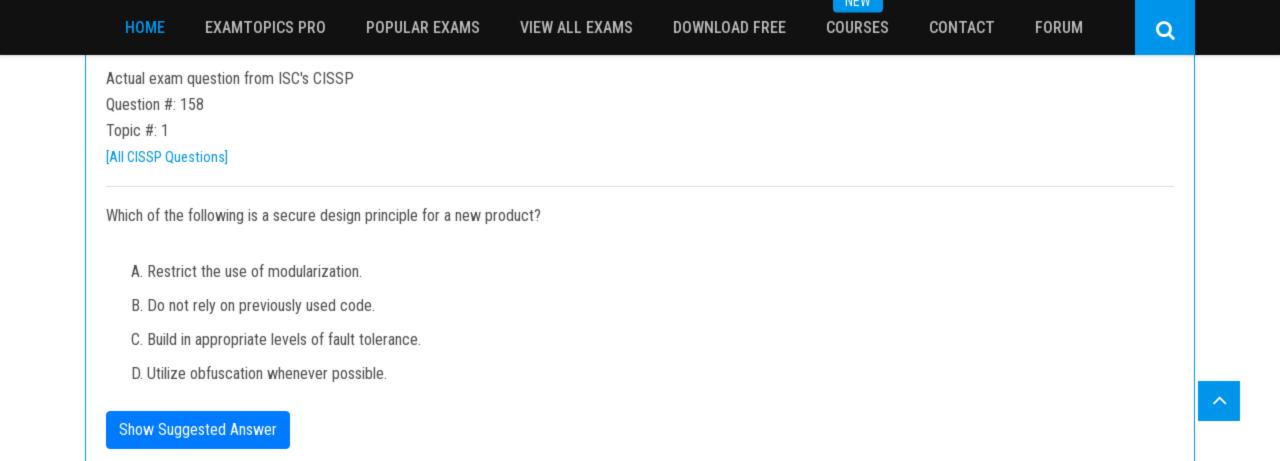
Show Suggested Answer

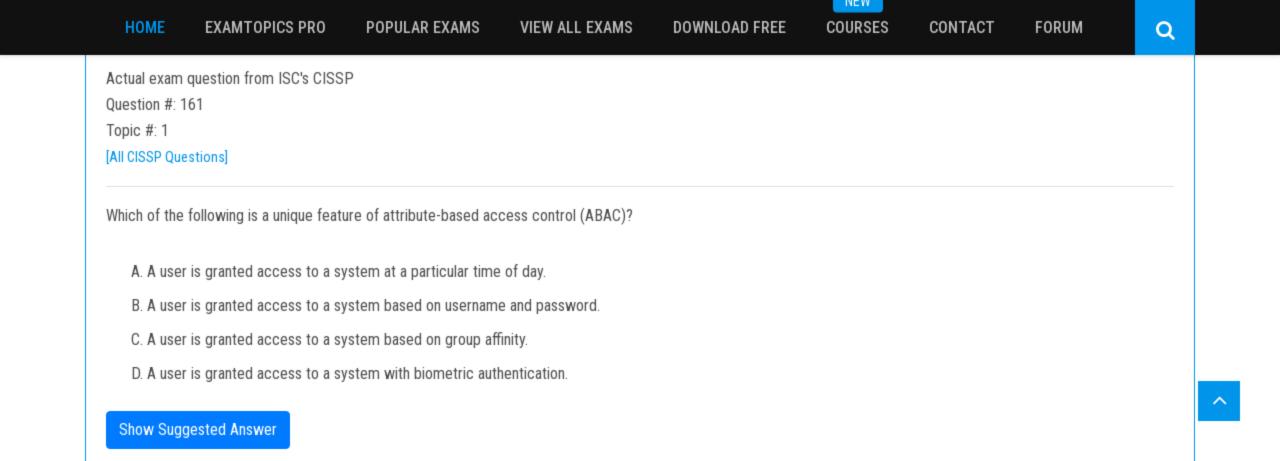


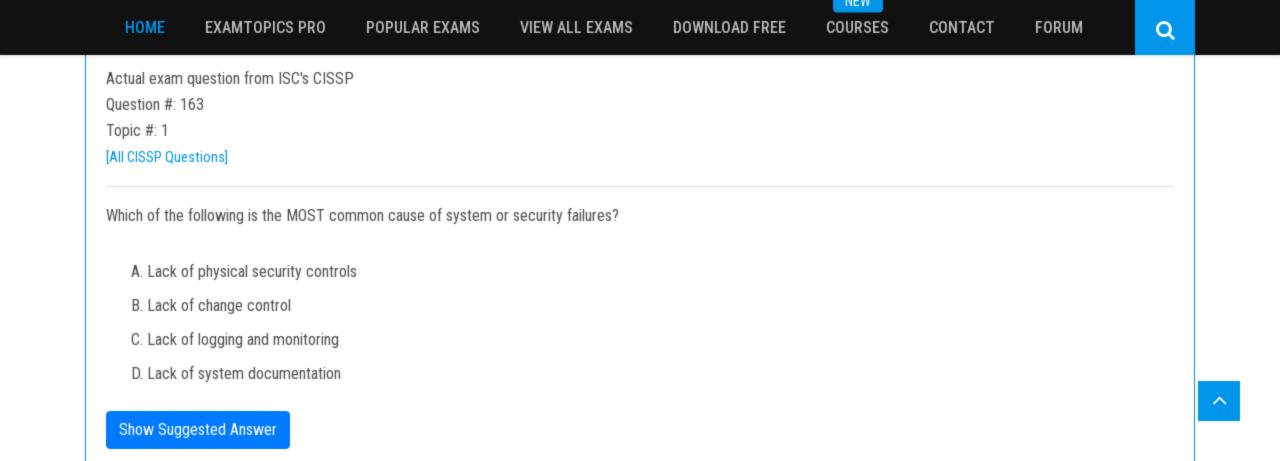


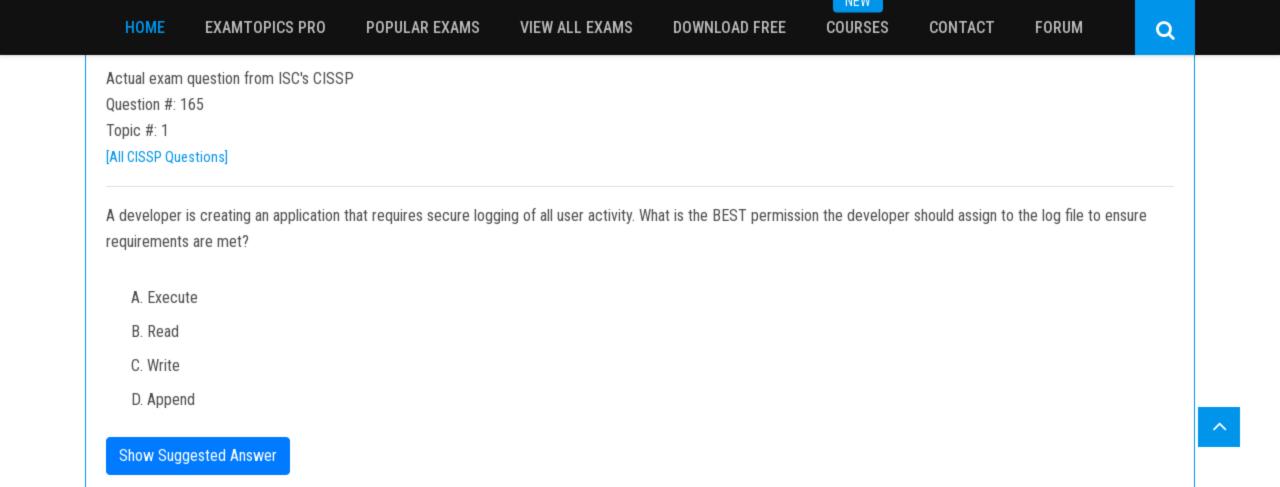


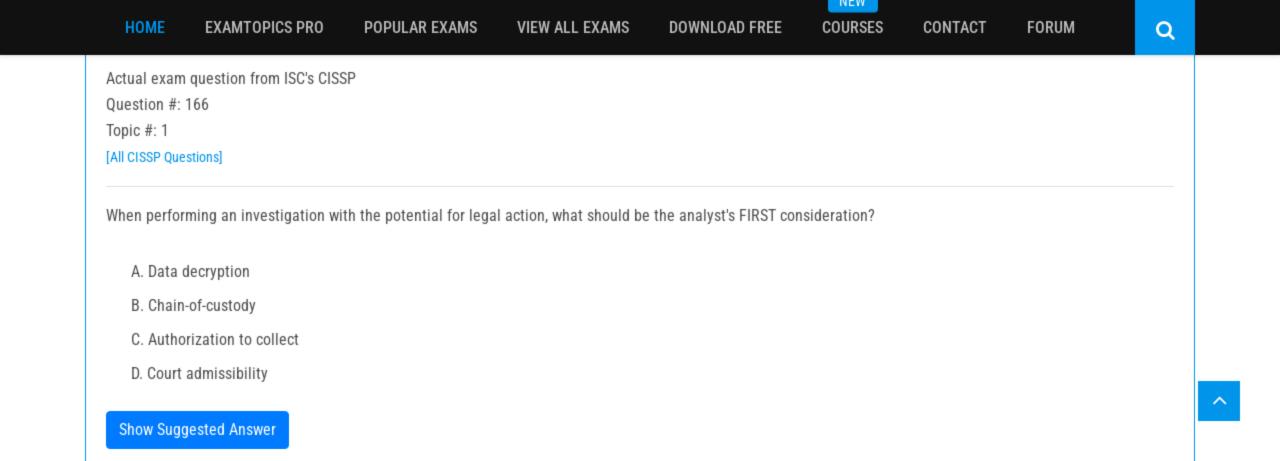


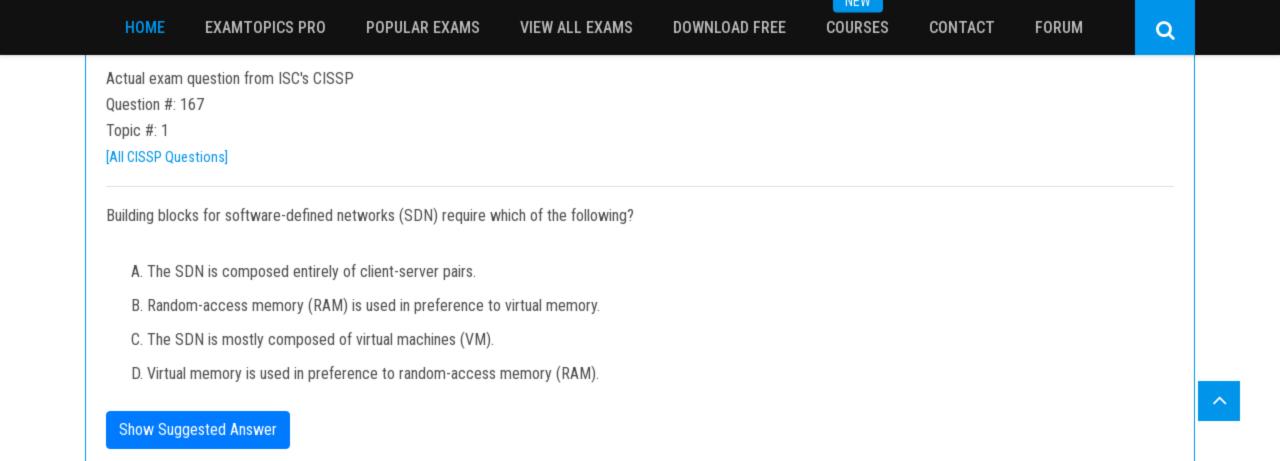


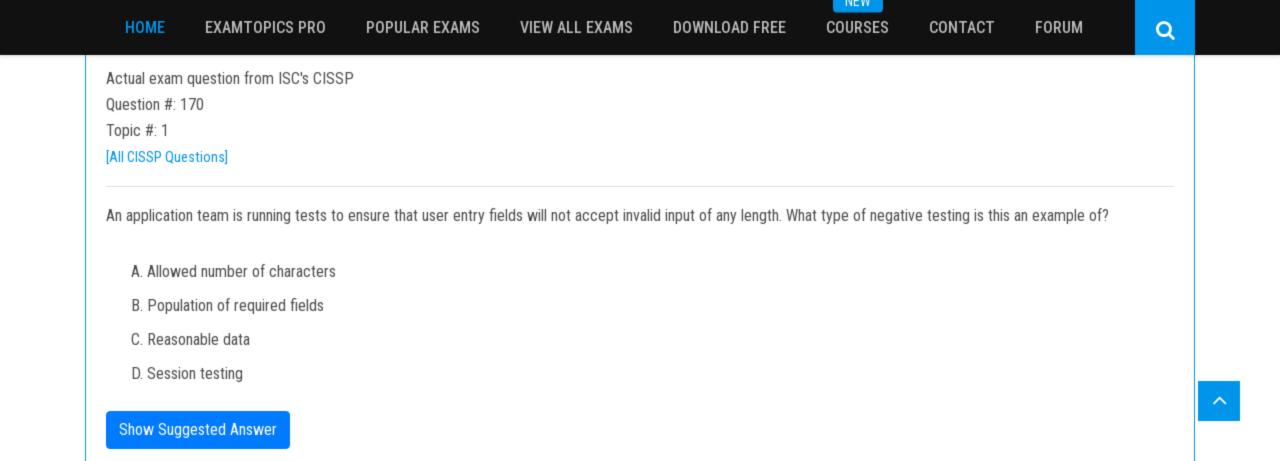












Actual exam question from ISC's CISSP

Question #: 174

Topic #: 1

[All CISSP Questions]

Systems Security Professional (CISSP) with identity and access management (IAM) responsibilities is asked by the Chief Information Security Officer (CISO) to perform a vulnerability assessment on a web application to pass a Payment Card Industry (PCI) audit. The CISSP has never performed this before. According to the (ISC)

Code of Professional Ethics, which of the following should the CISSP do?

- A. Inform the CISO that they are unable to perform the task because they should render only those services for which they are fully competent and qualified
- B. Since they are CISSP certified, they have enough knowledge to assist with the request, but will need assistance in order to complete it in a timely manner
- C. Review the CISSP guidelines for performing a vulnerability assessment before proceeding to complete it
- D. Review the PCI requirements before performing the vulnerability assessment

Show Suggested Answer

Actual exam question from ISC's CISSP

Question #: 175

Topic #: 1

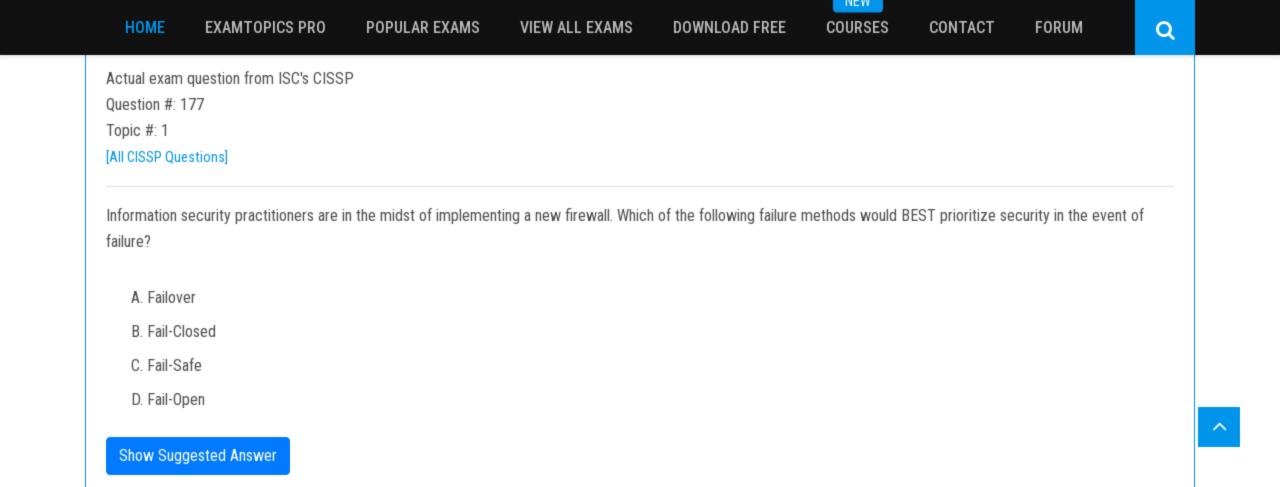
[All CISSP Questions]

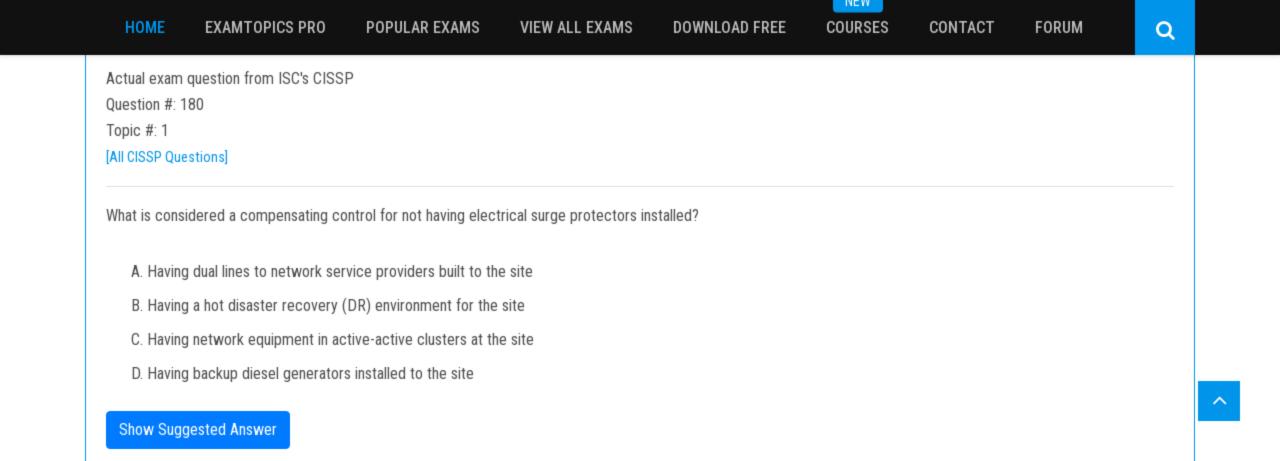
While performing a security review for a new product, an information security professional discovers that the organization's product development team is proposing to collect government-issued identification (ID) numbers from customers to use as unique customer identifiers. Which of the following recommendations should be made to the product development team?

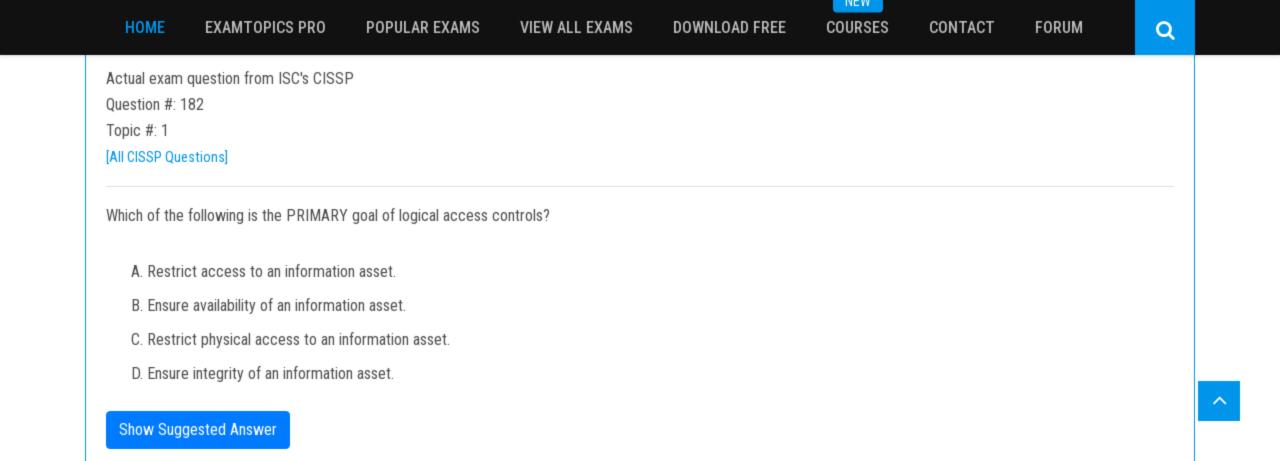
Q

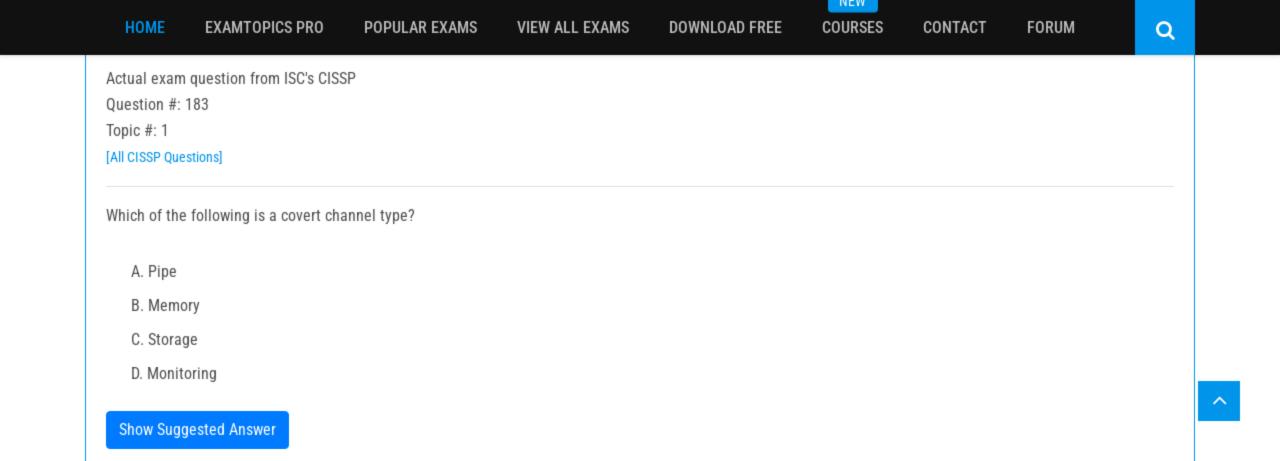
- A. Customer identifiers should be a variant of the user's government-issued ID number.
- B. Customer identifiers should be a cryptographic hash of the user's government-issued ID number.
- C. Customer identifiers that do not resemble the user's government-issued ID number should be used.
- D. Customer identifiers should be a variant of the user's name, for example, "jdoe" or "john.doe."

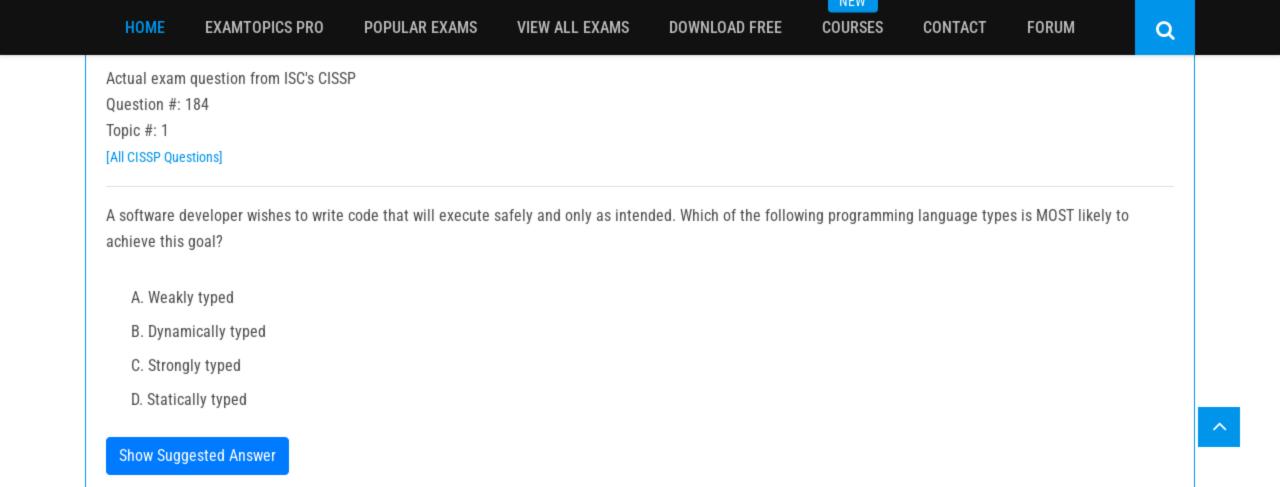
Show Suggested Answer

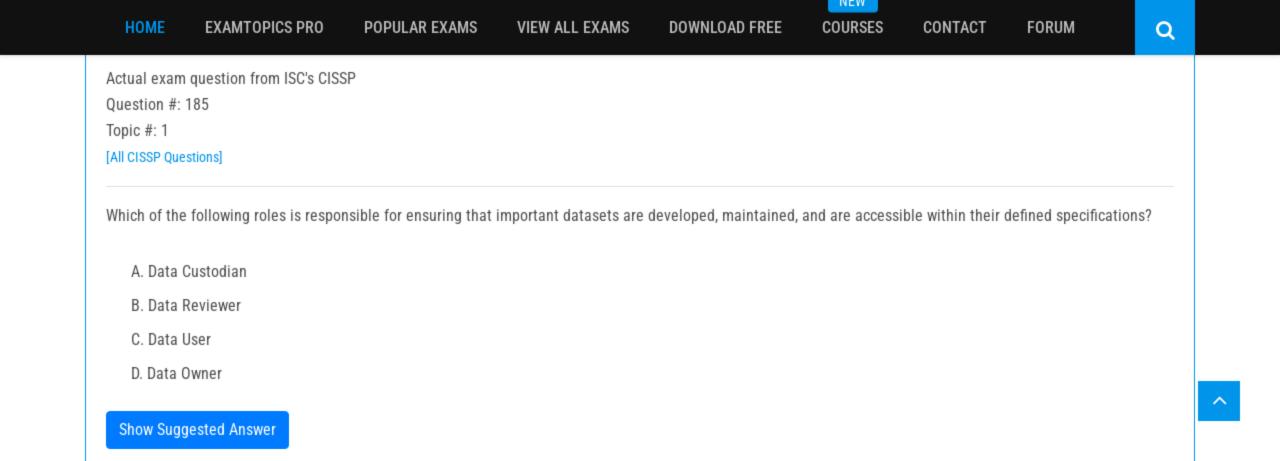


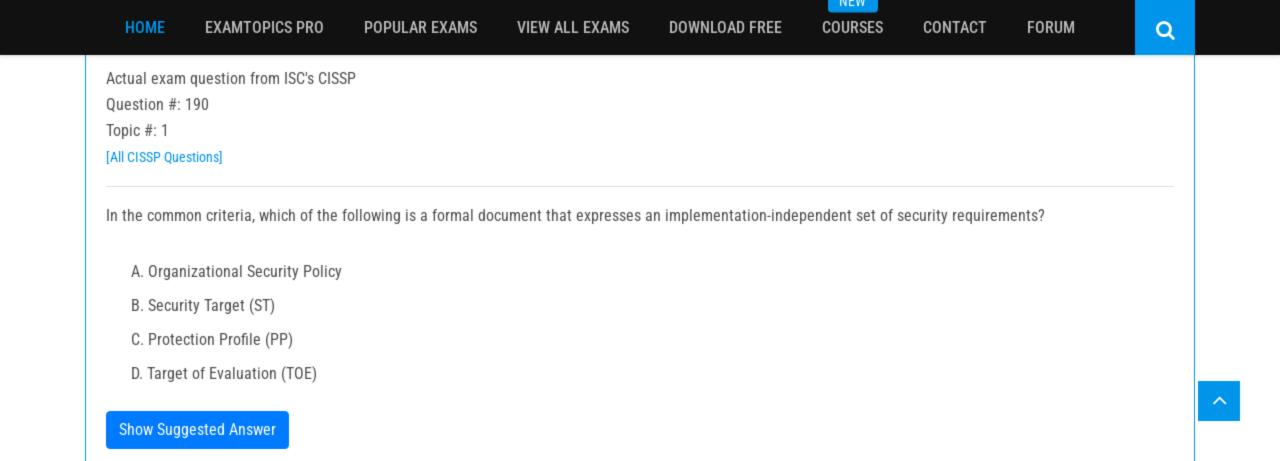


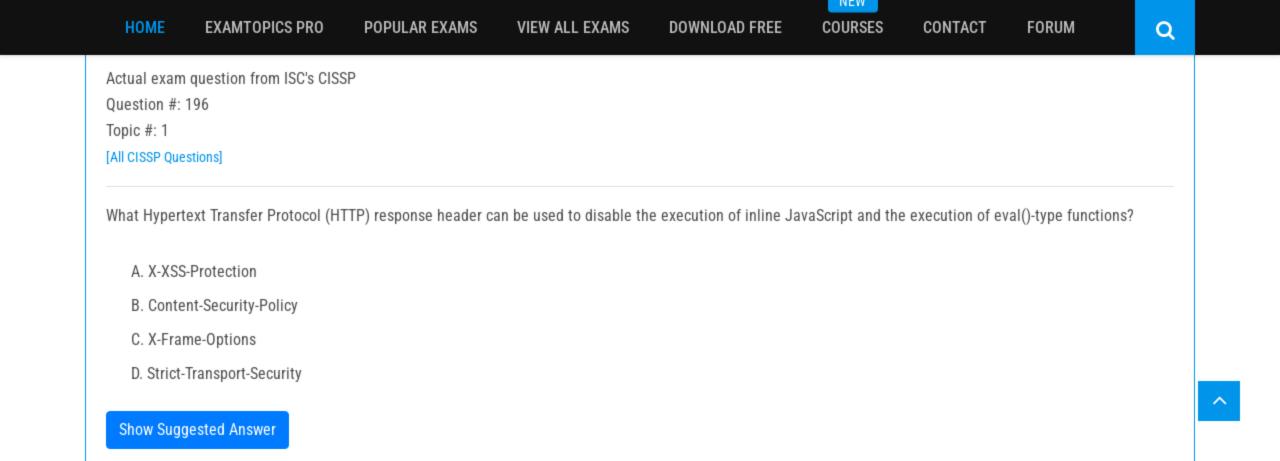


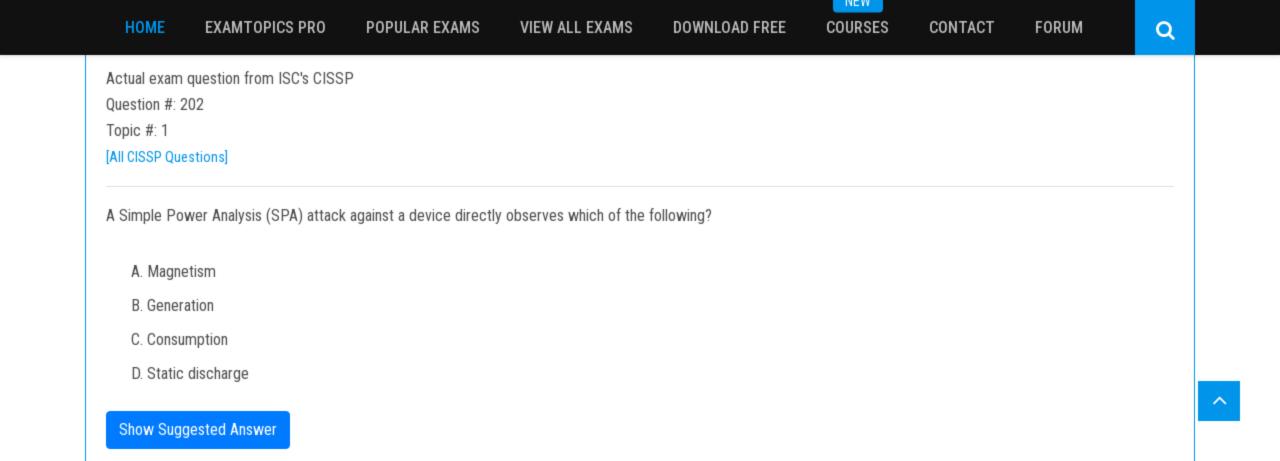


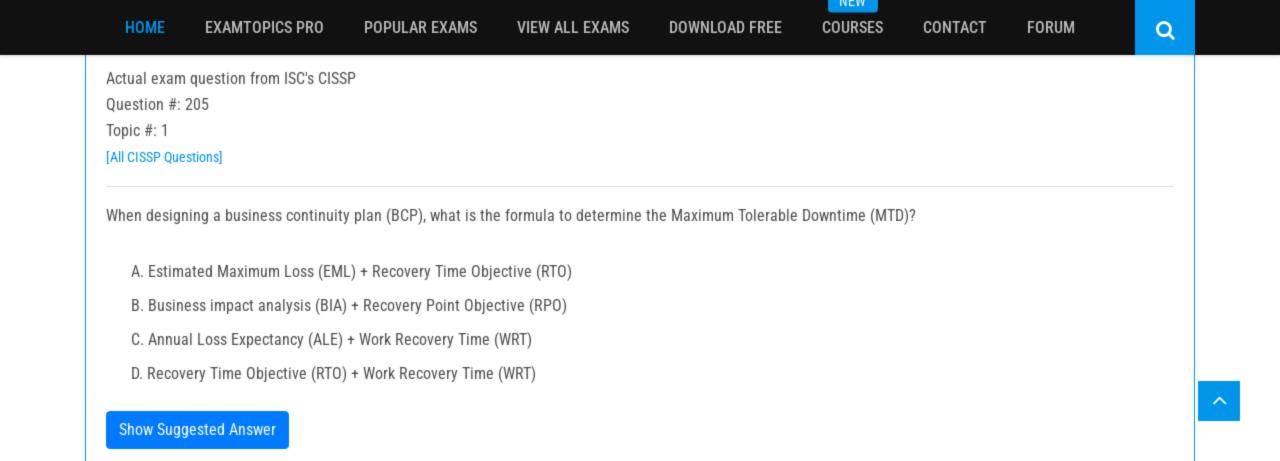


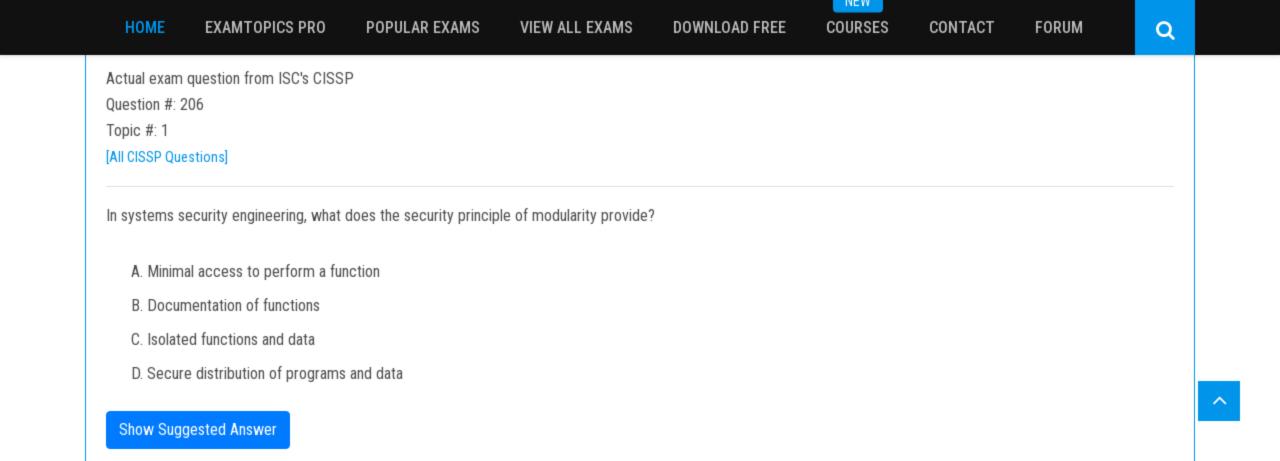


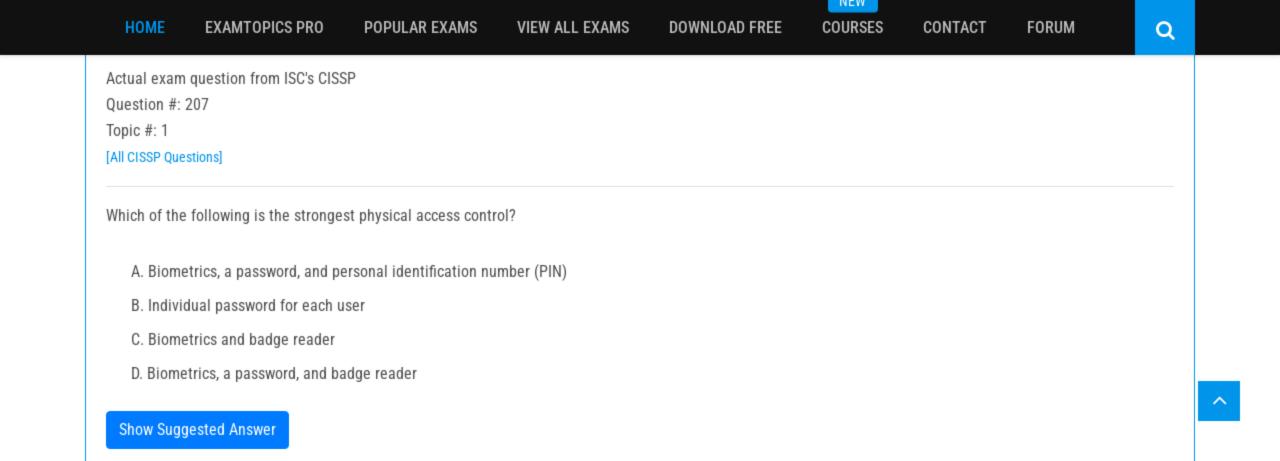


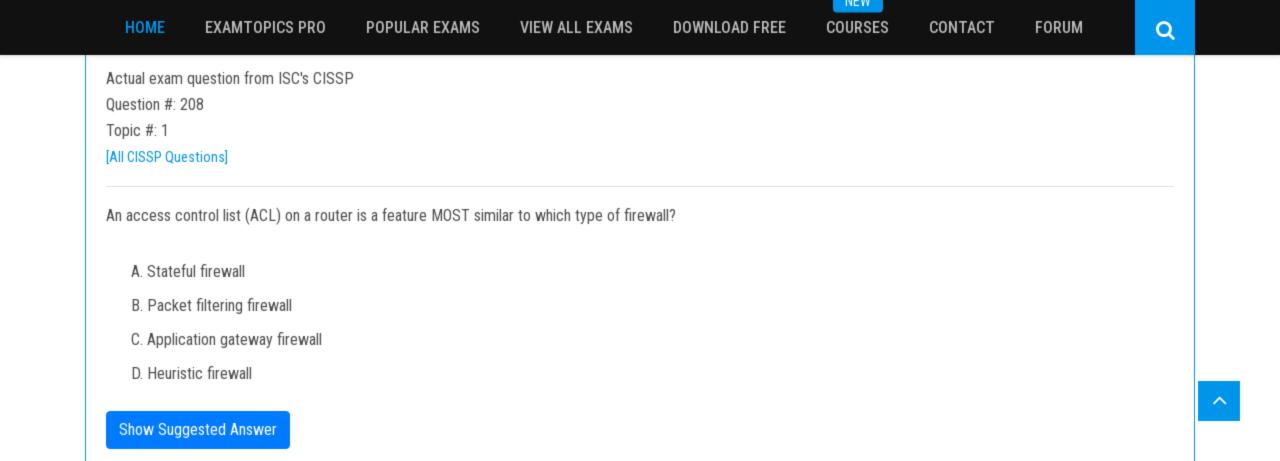


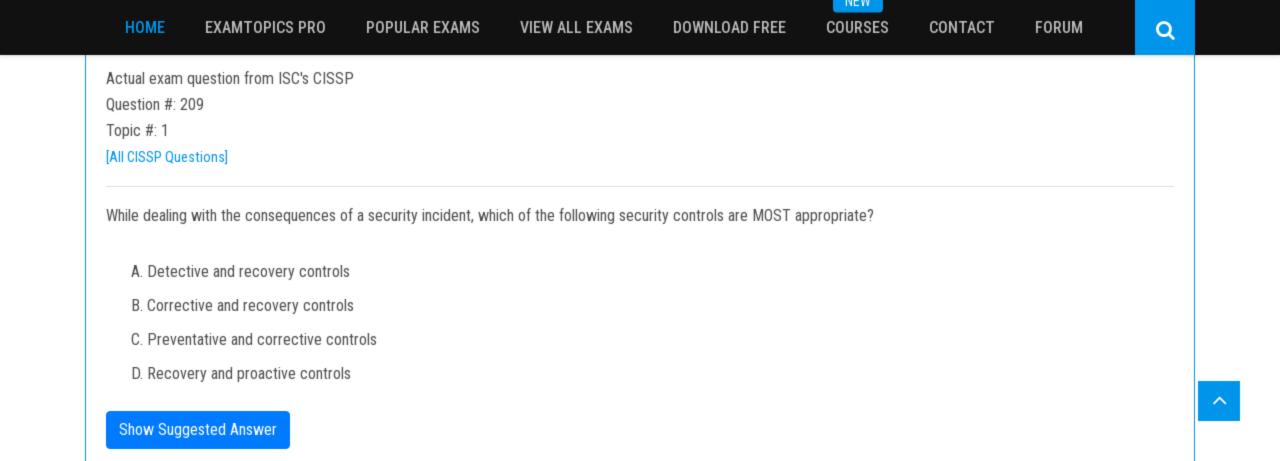


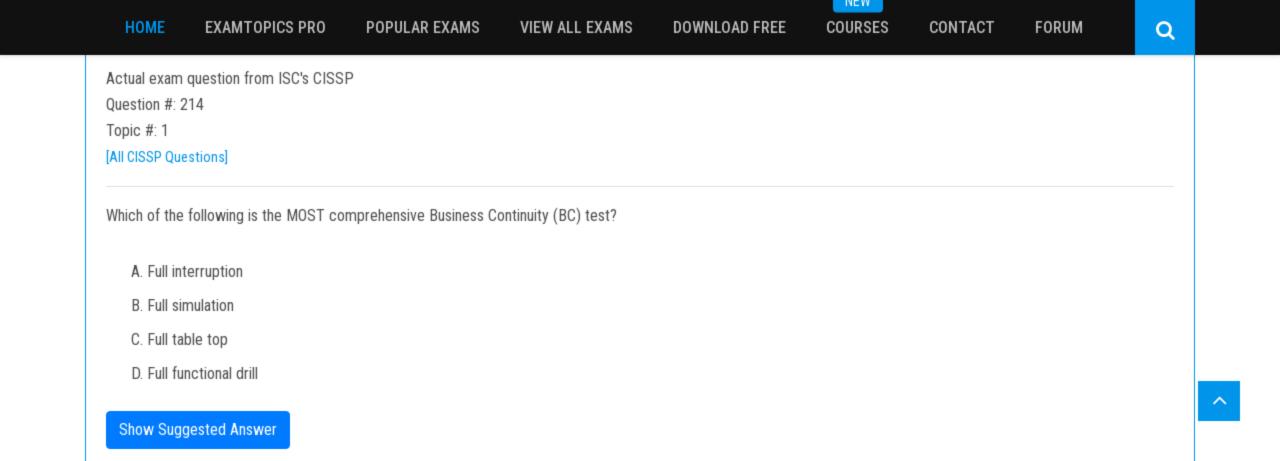


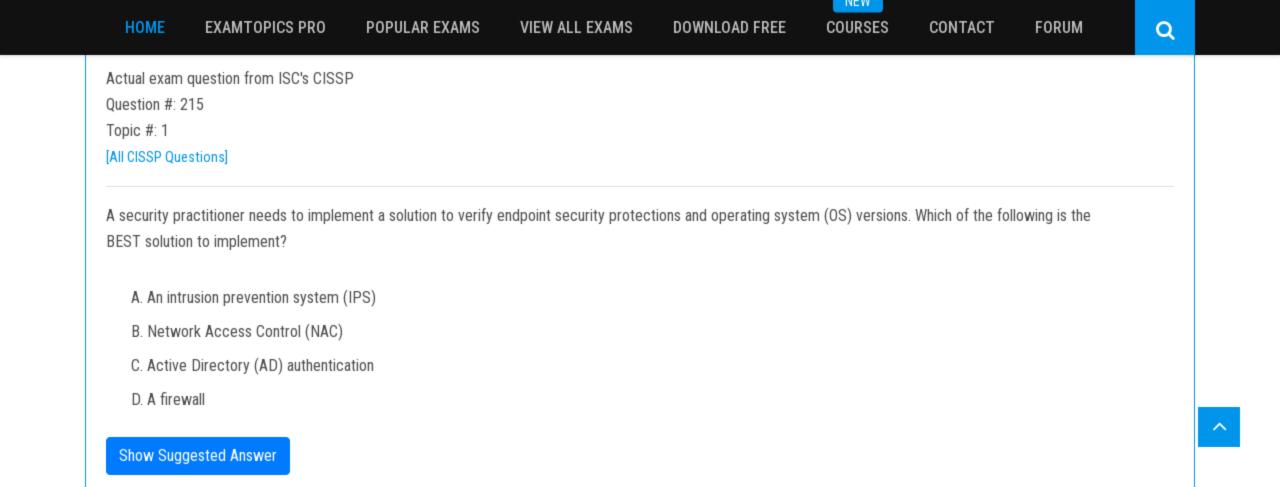


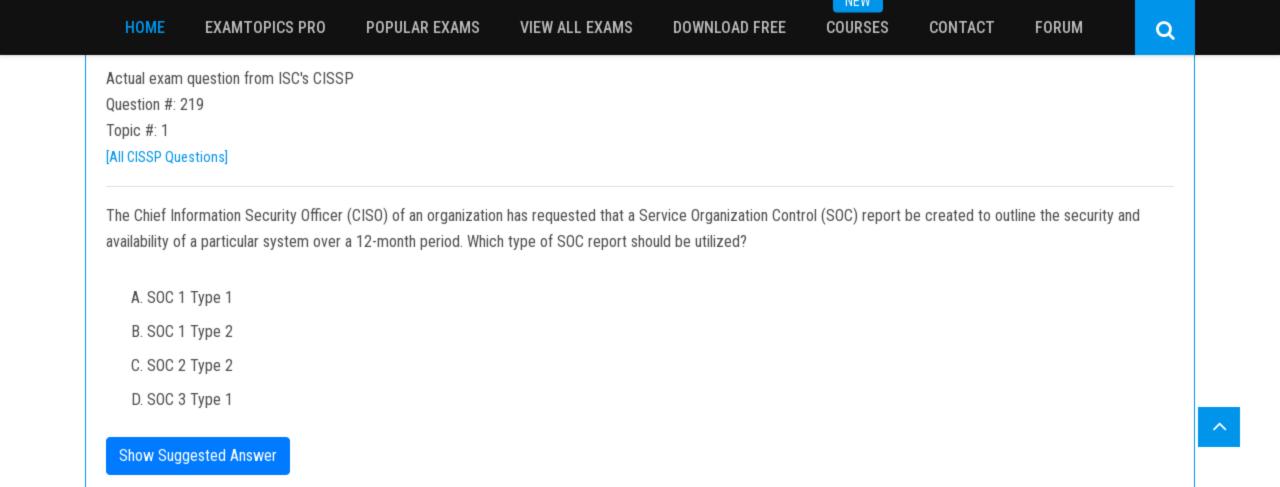












Actual exam question from ISC's CISSP

Question #: 220

Topic #: 1

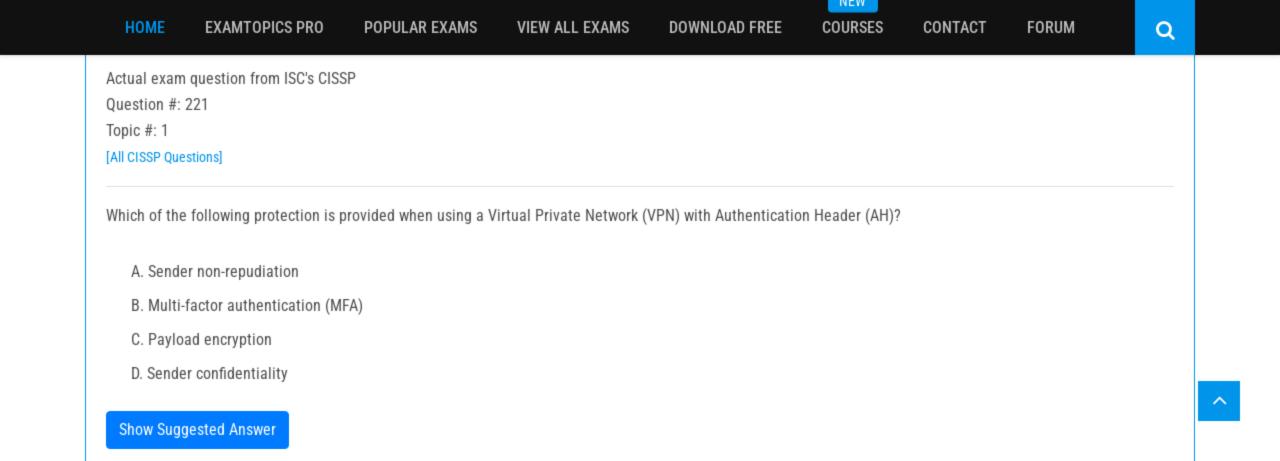
[All CISSP Questions]

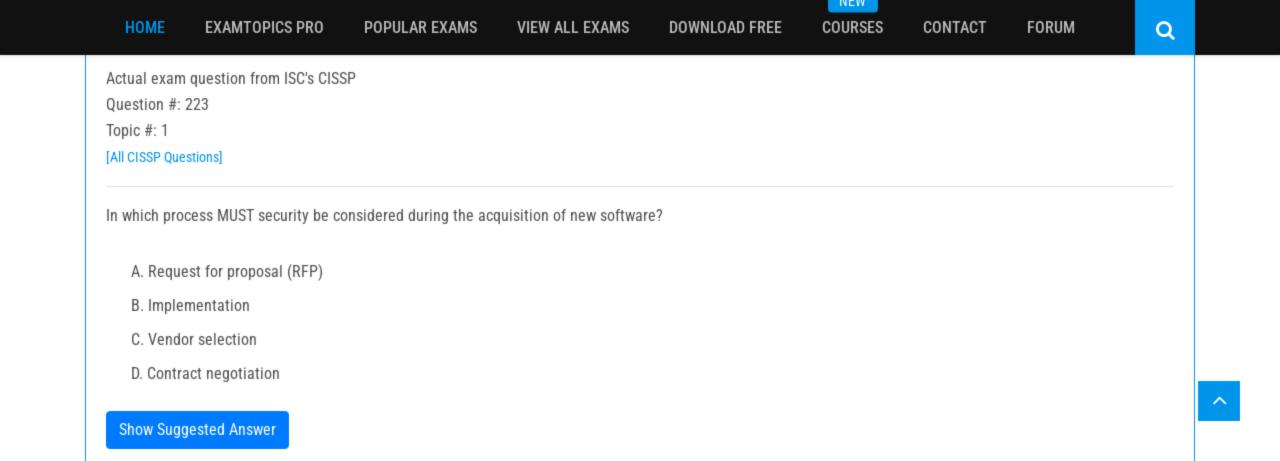
An organization recently upgraded to a Voice over Internet Protocol (VoIP) phone system. Management is concerned with unauthorized phone usage. The security consultant is responsible for putting together a plan to secure these phones. Administrators have assigned unique personal identification number (PIN) codes for each person in the organization. What is the BEST solution?

- A. Have the administrator enforce a policy to change the PIN regularly. Implement call detail records (CDR) reports to track usage.
- B. Have the administrator change the PIN regularly. Implement call detail records (CDR) reports to track usage.
- C. Use phone locking software to enforce usage and PIN policies. Inform the user to change the PIN regularly.
- D. Implement call detail records (CDR) reports to track usage.

Show Suggested Answer

Q





Actual exam question from ISC's CISSP

Question #: 225

Topic #: 1

[All CISSP Questions]

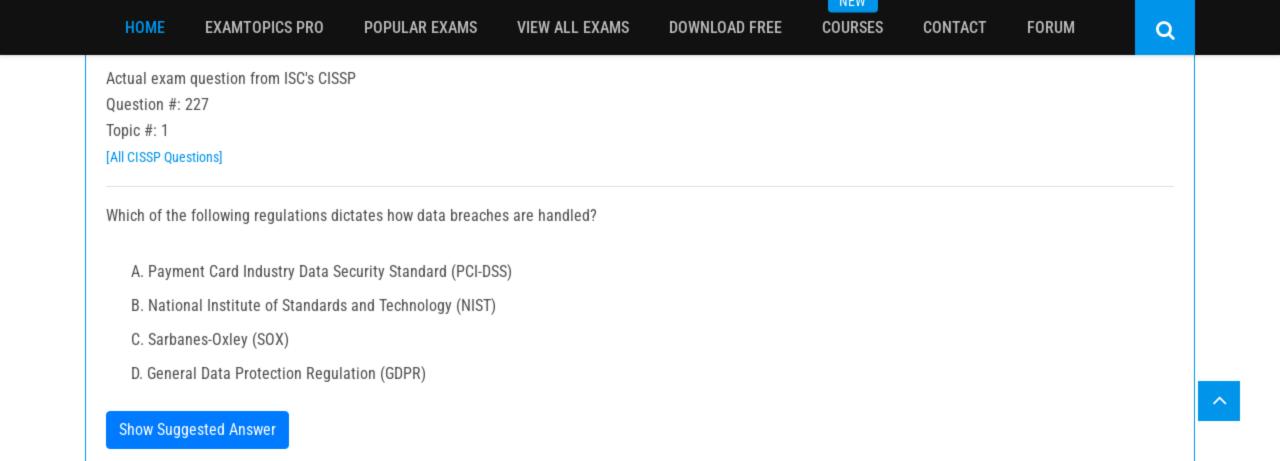
Which of the following measures serves as the BEST means for protecting data on computers, smartphones, and external storage devices when traveling to high-risk countries?

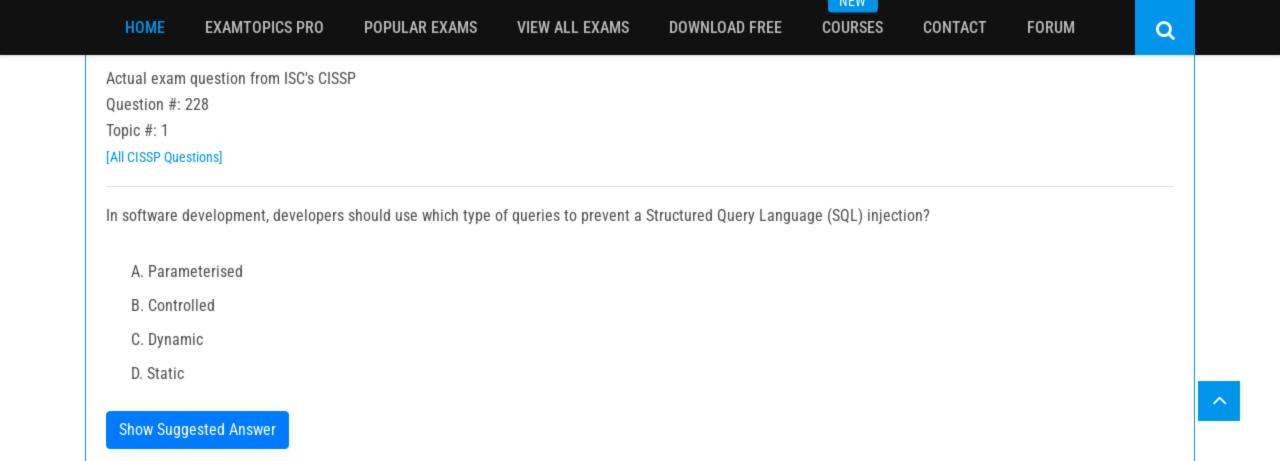
- A. Review applicable destination country laws, forensically clean devices prior to travel, and only download sensitive data over a virtual private network (VPN) upon arriving at the destination.
- B. Leverage a Secure Socket Layer (SSL) connection over a virtual private network (VPN) to download sensitive data upon arriving at the destination.
- C. Keep laptops, external storage devices, and smartphones in the hotel room when not in use.
- D. Use multi-factor authentication (MFA) to gain access to data stored on laptops or external storage devices and biometric fingerprint access control mechanisms to unlock smartphones.

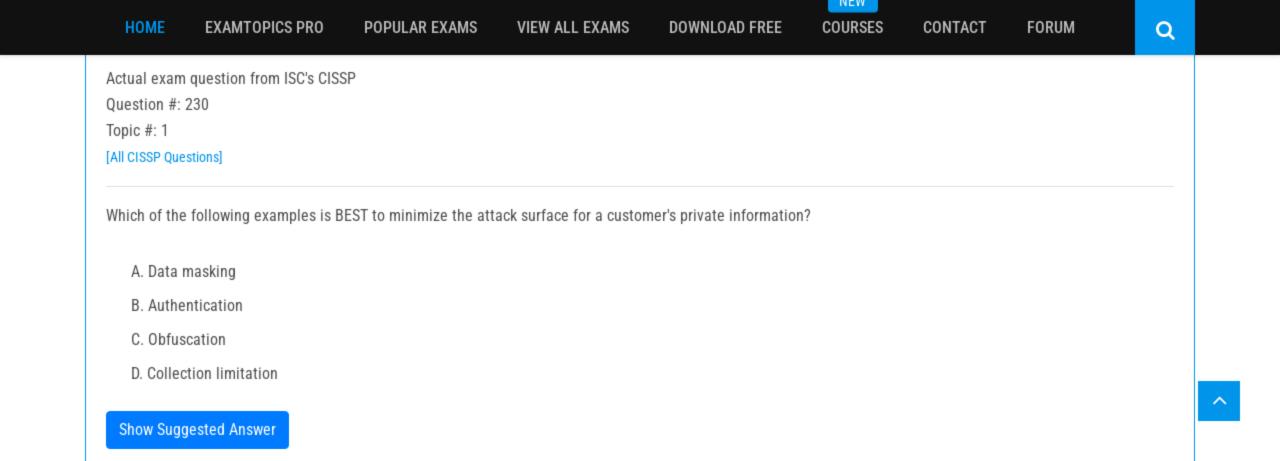
Show Suggested Answer

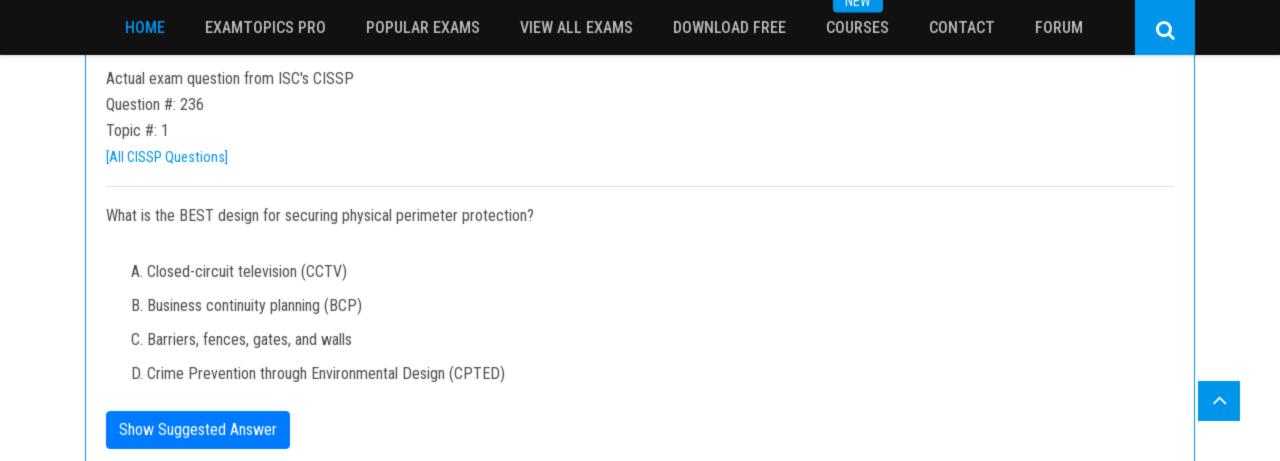
 $\hat{}$

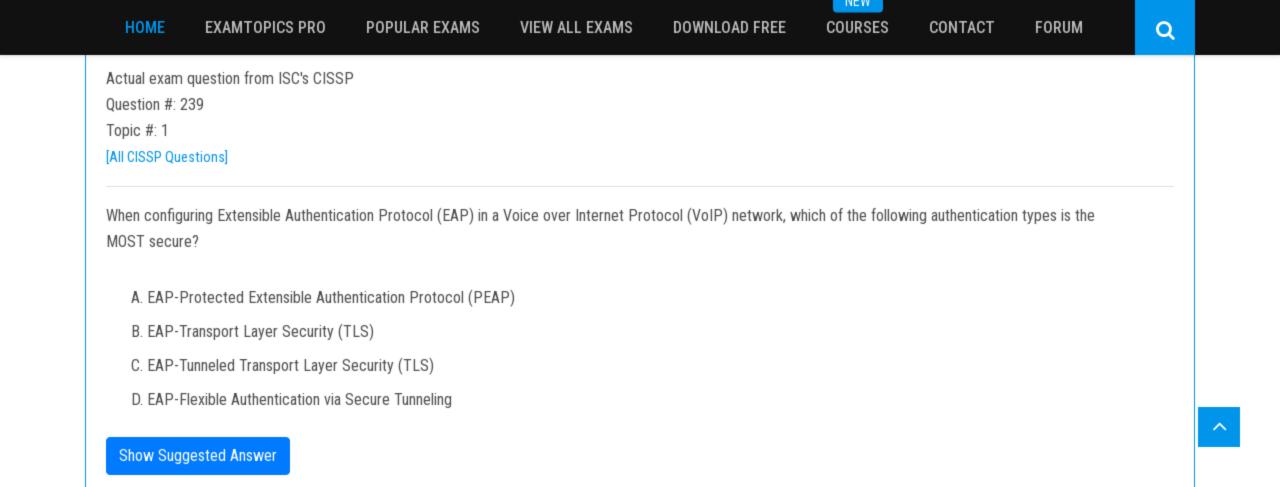
Q

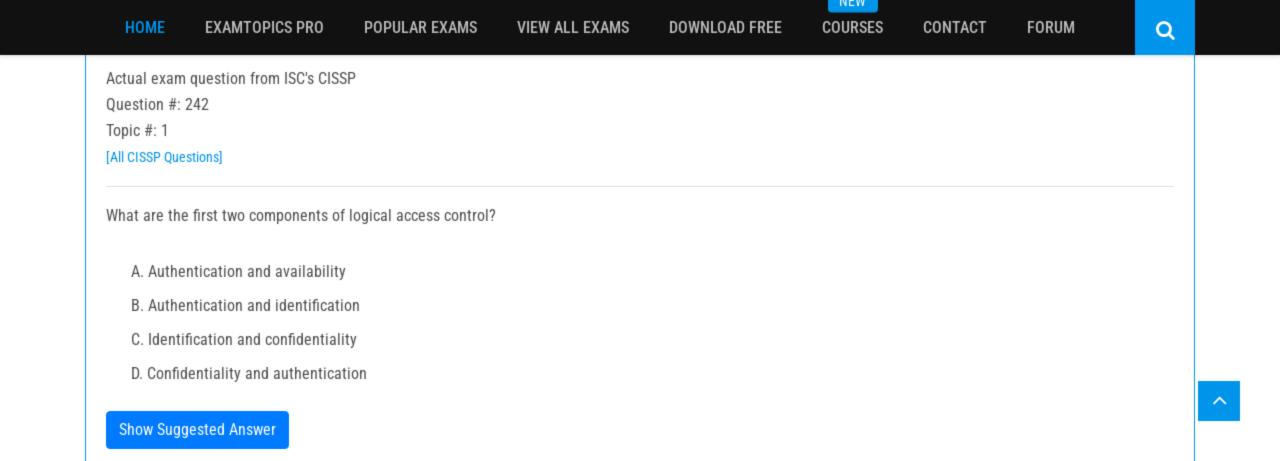


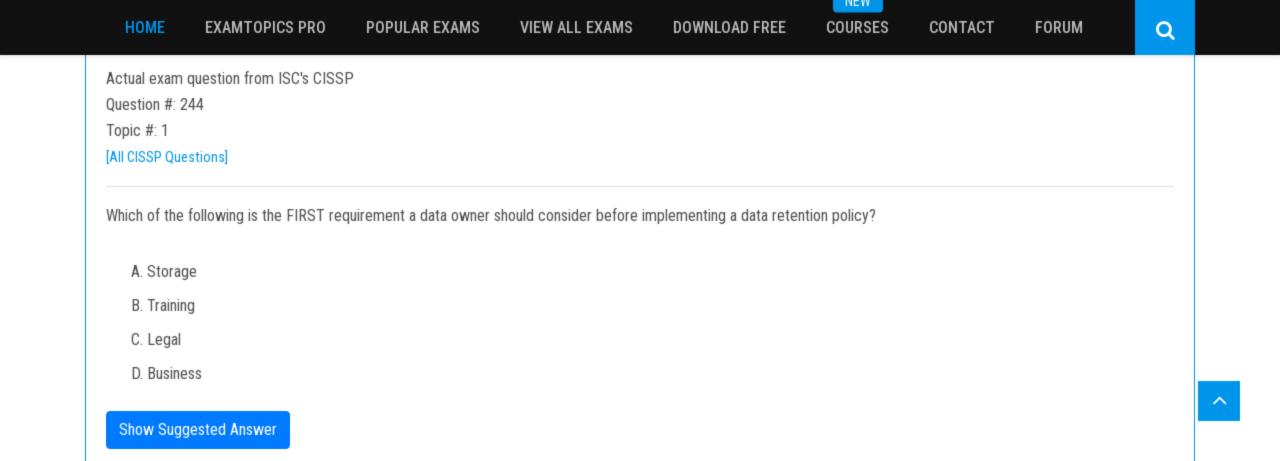


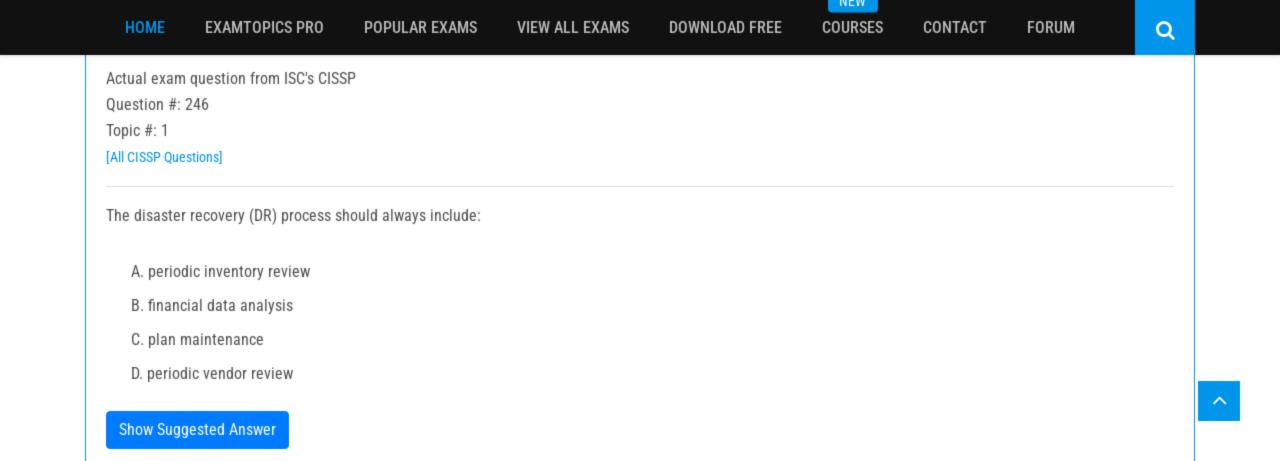


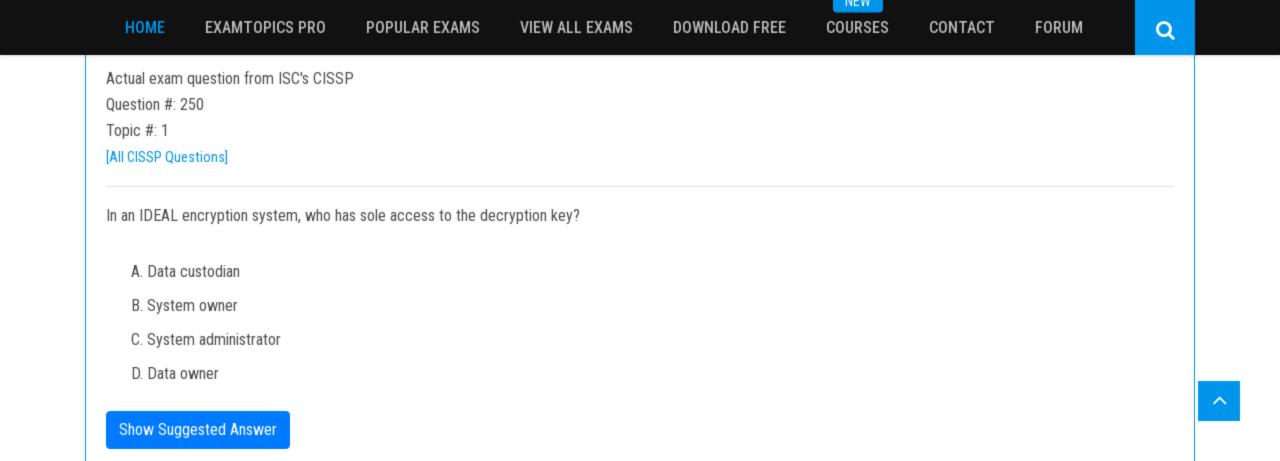


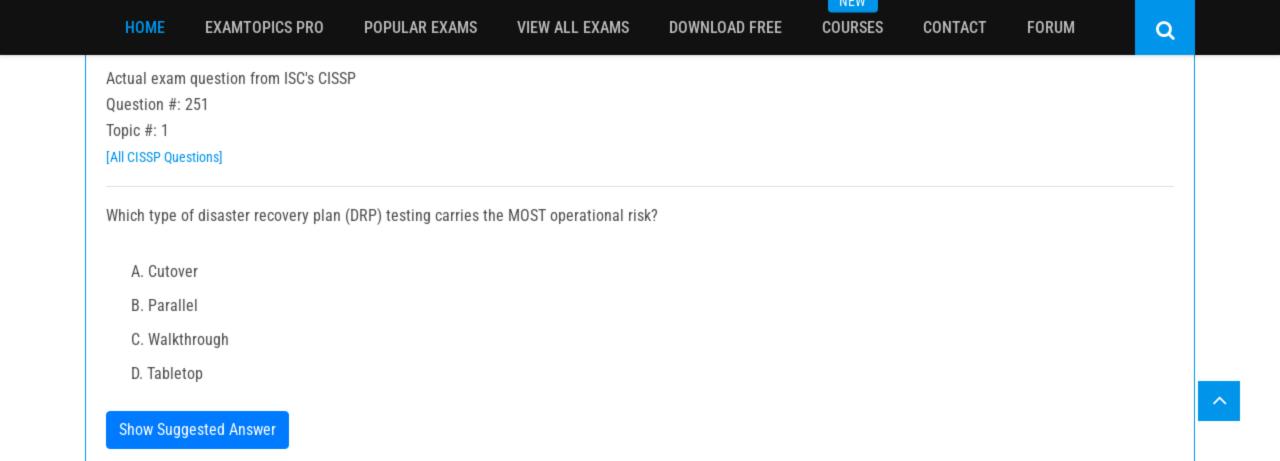


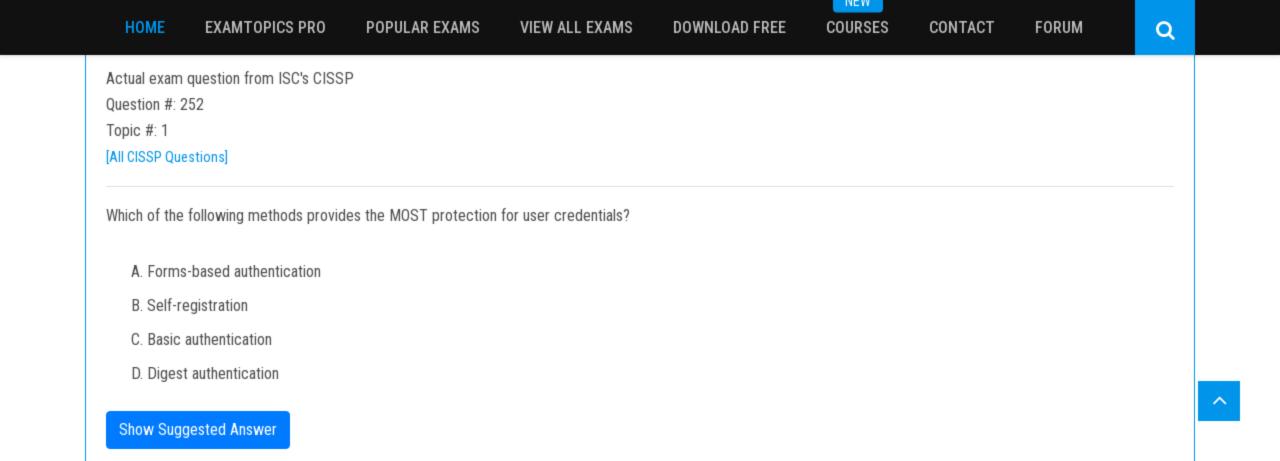


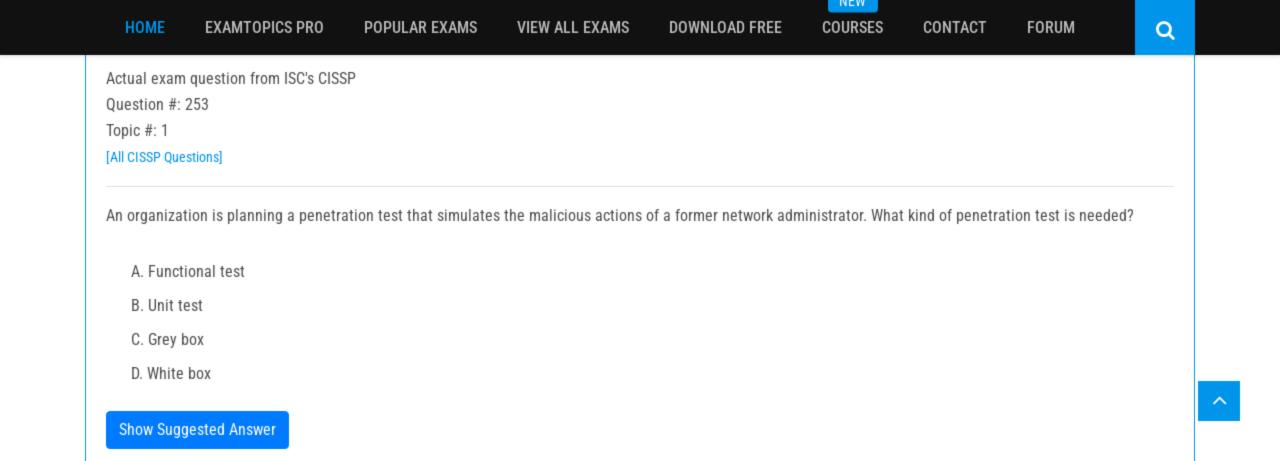












IA C AA

Actual exam question from ISC's CISSP

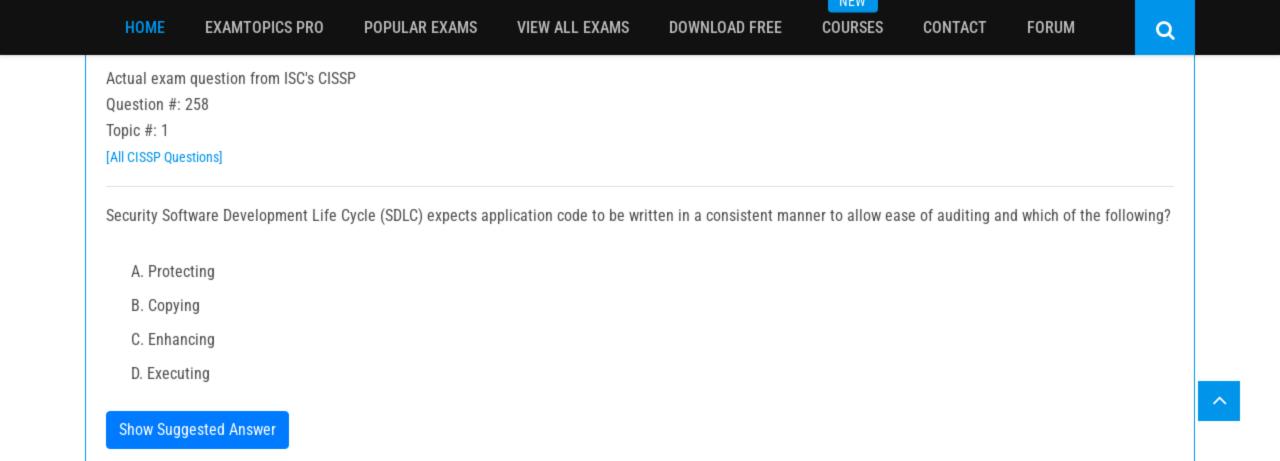
Question #: 257

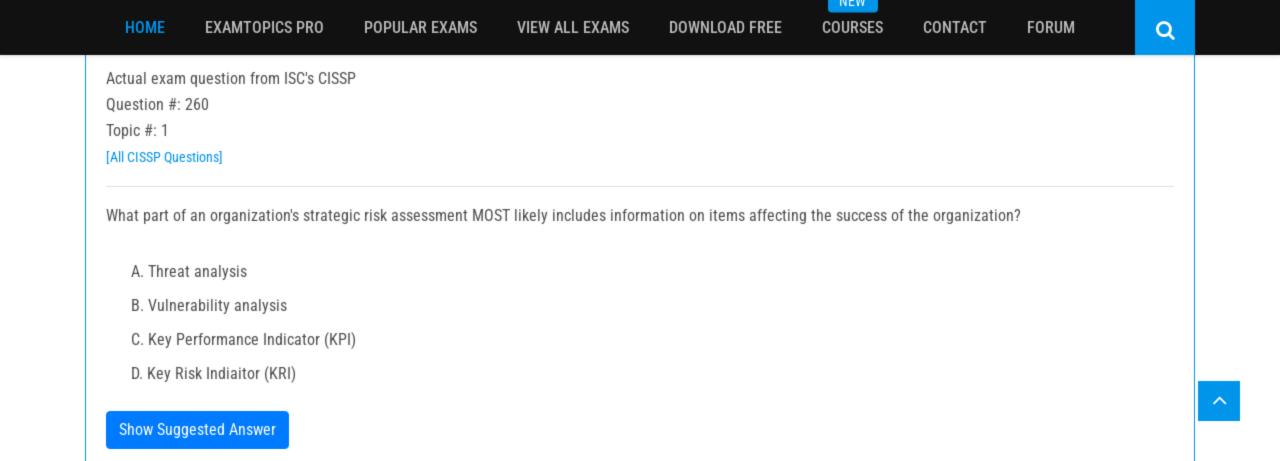
Topic #: 1

[All CISSP Questions]

Two computers, each with a single connection on the same physical 10 gigabit Ethernet network segment, need to communicate with each other. The first machine has a single Internet Protocol (IP) Classless Inter-Domain Routing (CIDR) address of 192.168.1.3/30 and the second machine has an IP/CIDR address 192.168.1.6/30. Which of the following is correct?

- A. Since each computer is on a different layer 3 network, traffic between the computers must be processed by a network bridge in order to communicate
- B. Since each computer is on the same layer 3 network, traffic between the computers may be processed by a network router in order to communicate
- C. Since each computer is on the same layer 3 network, traffic between the computers may be processed by a network bridge in order to communicate
- D. Since each computer is on a different layer 3 network, traffic between the computers must be processed by a network router in order to communicate





COURSES

IAC AA

CONTACT

FORUM

Q

Actual exam question from ISC's CISSP

Question #: 262

Topic #: 1

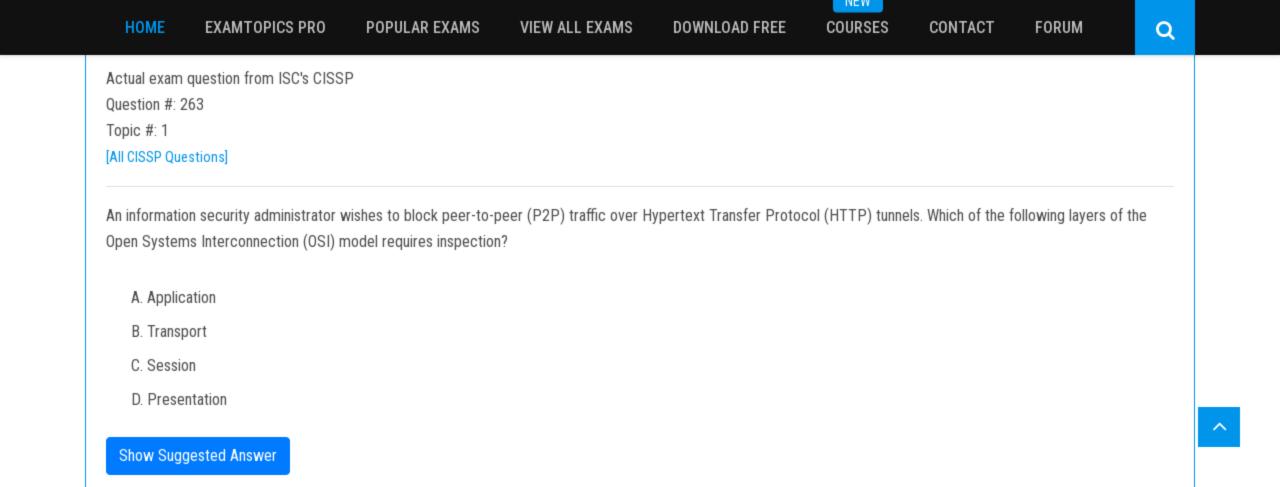
[All CISSP Questions]

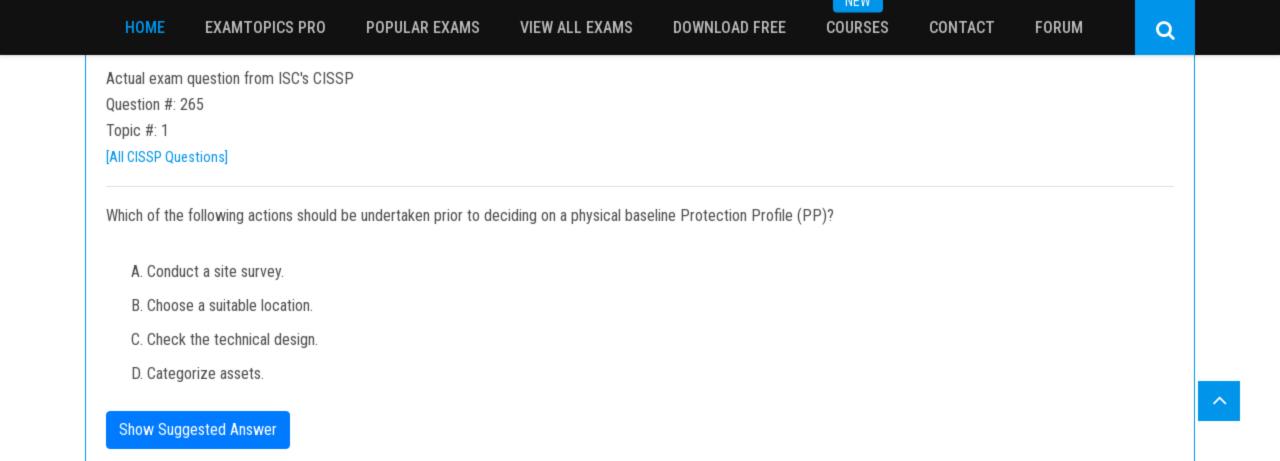
The Chief Executive Officer (CEO) wants to implement an internal audit of the company's information security posture. The CEO wants to avoid any bias in the audit process; therefore, has assigned the Sales Director to conduct the audit. After significant interaction over a period of weeks the audit concludes that the company's policies and procedures are sufficient, robust and well established. The CEO then moves on to engage an external penetration testing company in order to showcase the organization's robust information security stance. This exercise reveals significant failings in several critical security controls and shows that the incident response processes remain undocumented. What is the MOST likely reason for this disparity in the results of the audit and the external penetration test?

- A. The audit team lacked the technical experience and training to make insightful and objective assessments of the data provided to them.
- B. The scope of the penetration test exercise and the internal audit were significantly different.
- C. The external penetration testing company used custom zero-day attacks that could not have been predicted.
- D. The information technology (IT) and governance teams have failed to disclose relevant information to the internal audit team leading to an incomplete assessment being formulated.

Show Suggested Answer

^





IA C AA

Actual exam question from ISC's CISSP

Question #: 266

Topic #: 1

[All CISSP Questions]

Management has decided that a core application will be used on personal cellular phones. As an implementation requirement, regularly scheduled analysis of the security posture needs to be conducted. Management has also directed that continuous monitoring be implemented. Which of the following is required to accomplish management's directive?

- A. Routine reports generated by the user's cellular phone provider that detail security events
- B. Strict integration of application management, configuration management (CM), and phone management
- C. Management application installed on user phones that tracks all application events and cellular traffic
- D. Enterprise-level security information and event management (SIEM) dashboard that provides full visibility of cellular phone activity

Q

Actual exam question from ISC's CISSP

Question #: 267

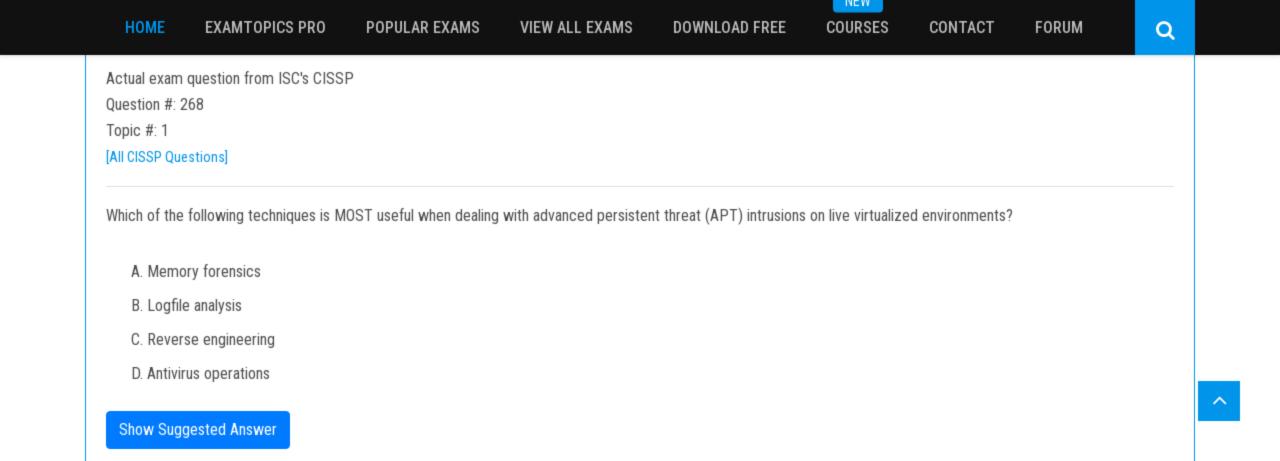
Topic #: 1

[All CISSP Questions]

A systems engineer is designing a wide area network (WAN) environment for a new organization. The WAN will connect sites holding information at various levels of sensitivity, from publicly available to highly confidential. The organization requires a high degree of interconnectedness to support existing business processes.

What is the BEST design approach to securing this environment?

- A. Use reverse proxies to create a secondary "shadow" environment for critical systems.
- B. Place firewalls around critical devices, isolating them from the rest of the environment.
- C. Layer multiple detective and preventative technologies at the environment perimeter.
- D. Align risk across all interconnected elements to ensure critical threats are detected and handled.



Actual exam question from ISC's CISSP

Question #: 271

Topic #: 1

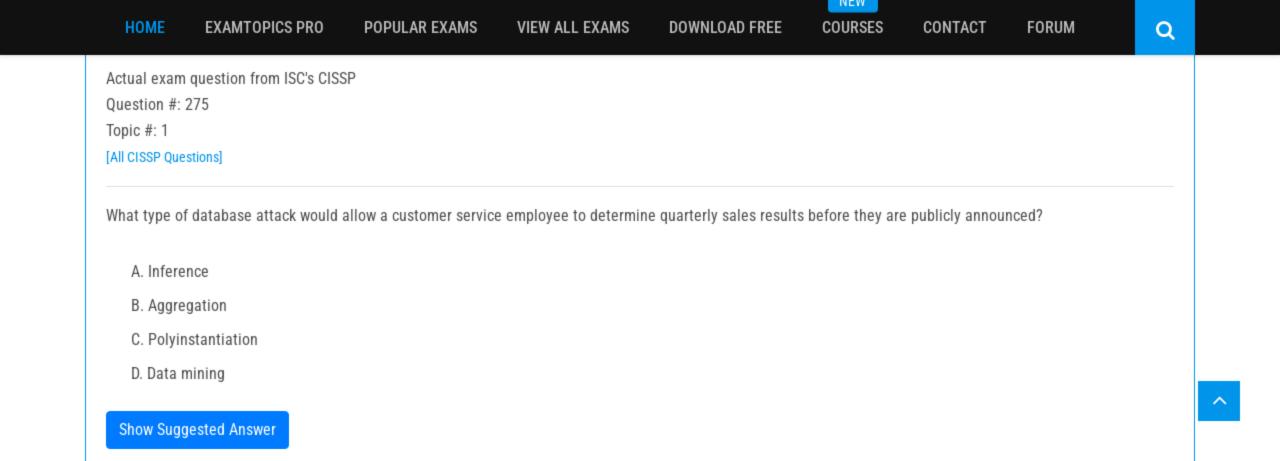
[All CISSP Questions]

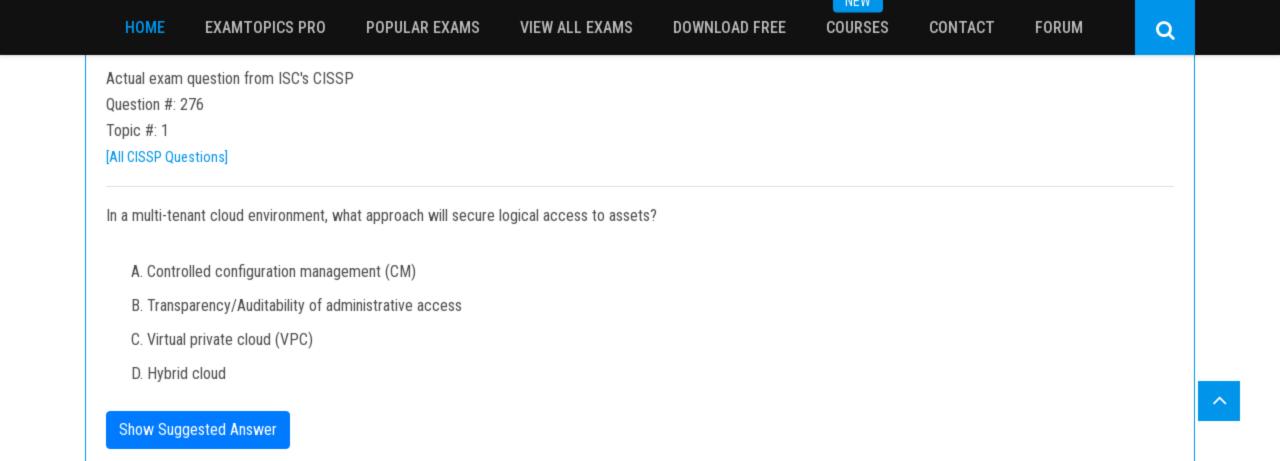
A security professional has reviewed a recent site assessment and has noted that a server room on the second floor of a building has Heating, Ventilation, and Air Conditioning (HVAC) intakes on the ground level that have ultraviolet light fi Iters installed, Aero-K Fire suppression in the server room, and pre-action fire suppression on floors above the server room. Which of the following changes can the security professional recommend to reduce risk associated with these conditions?

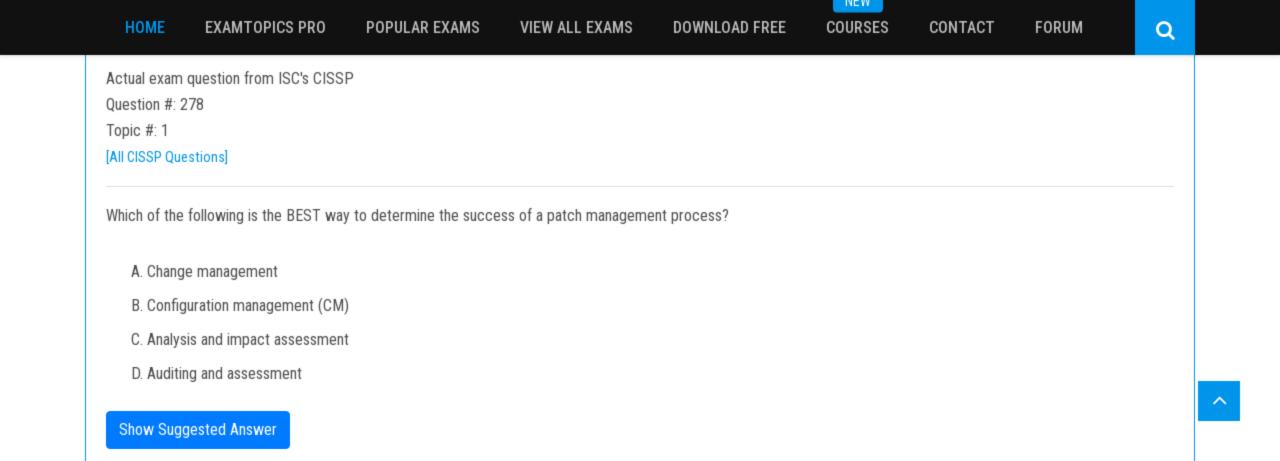
FORUM

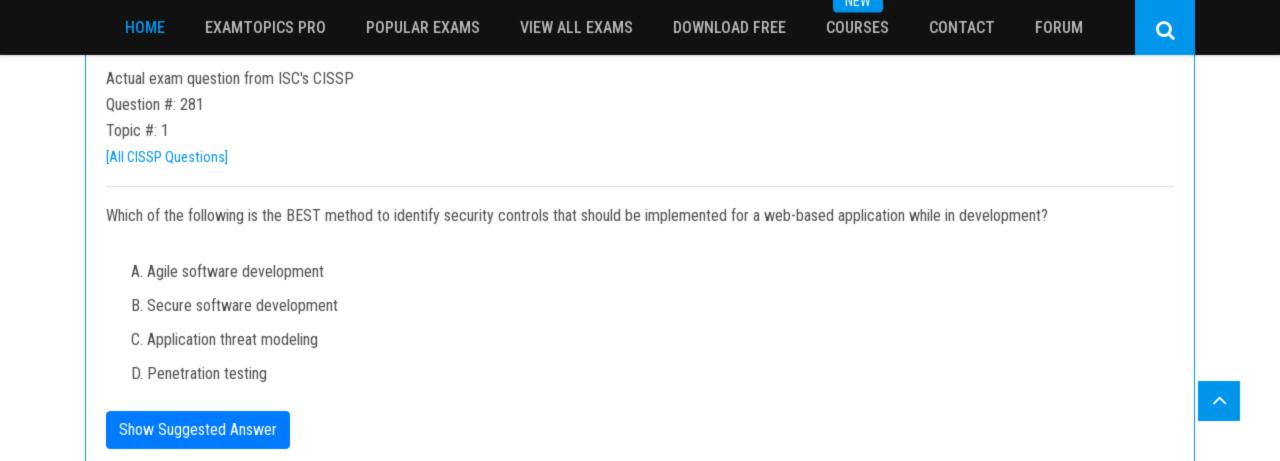
Q

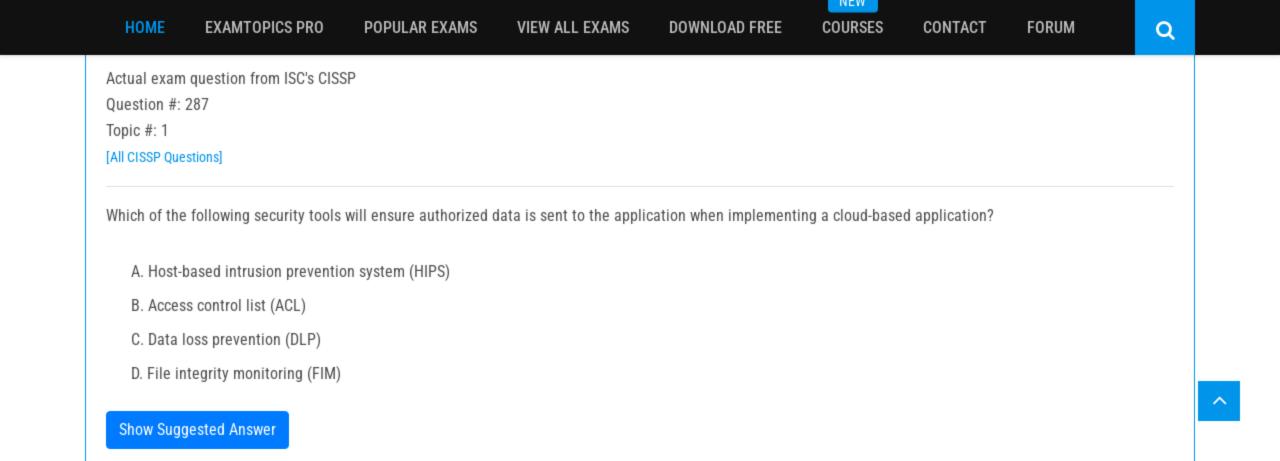
- A. Remove the ultraviolet light filters on the HVAC intake and replace the fire suppression system on the upper floors with a dry system
- B. Elevate the HVAC intake by constructing a plenum or external shaft over it and convert the server room fire suppression to a pre-action system
- C. Add additional ultraviolet light fi Iters to the HVAC intake supply and return ducts and change server room fire suppression to FM-200
- D. Apply additional physical security around the HVAC intakes and update upper floor fire suppression to FM-200

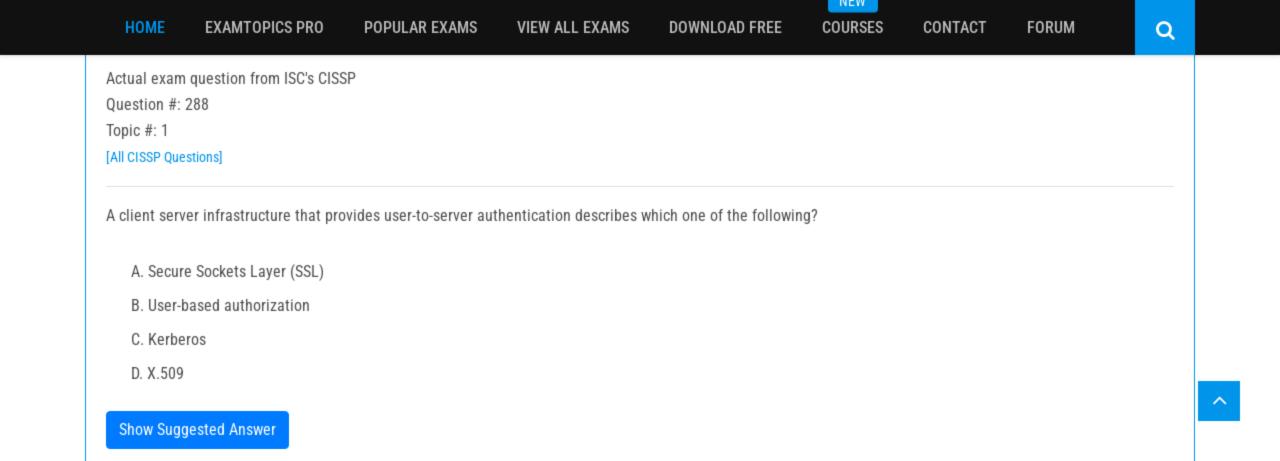


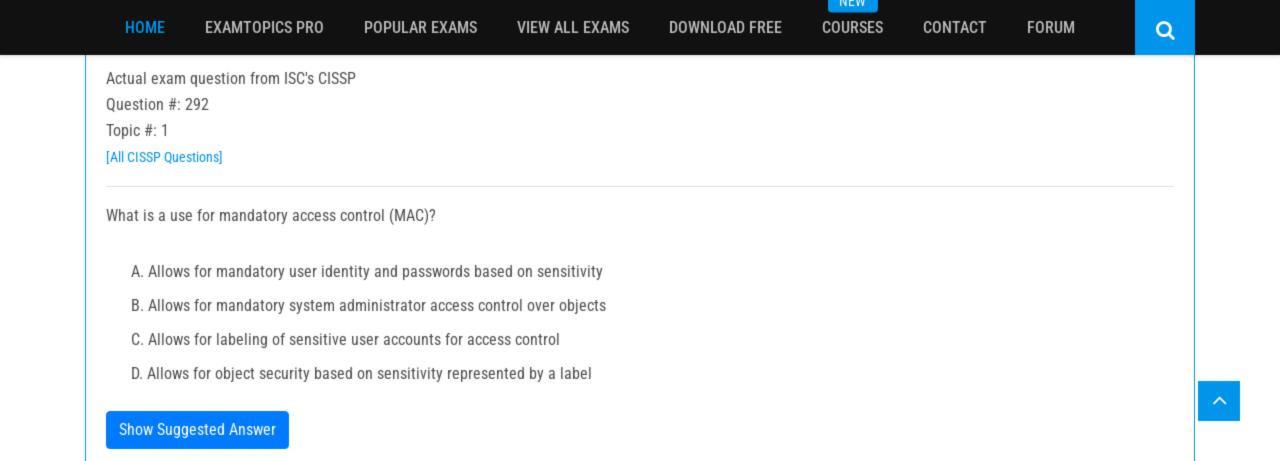












Question #: 293

Topic #: 1

[All CISSP Questions]

An organization has developed a way for customers to share information from their wearable devices with each other. Unfortunately, the users were not informed as to what information collected would be shared. What technical controls should be put in place to remedy the privacy issue while still trying to accomplish the organization's business goals?

Q

- A. Share only what the organization decides is best.
- B. Stop sharing data with the other users.
- C. Default the user to not share any information.
- D. Inform the user of the sharing feature changes after implemented.

Show Suggested Answer

