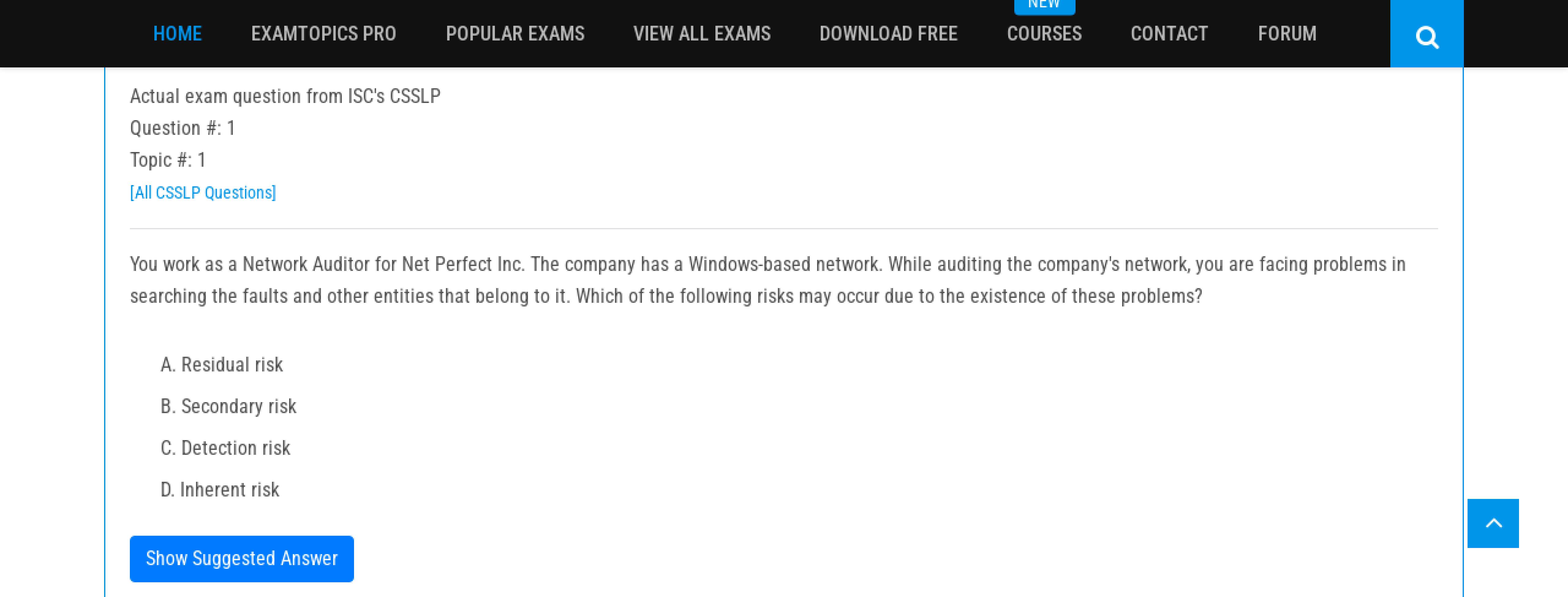


Actual exam question from ISC's CSSLP

Question #: 1

Topic #: 1

[All CSSLP Questions]

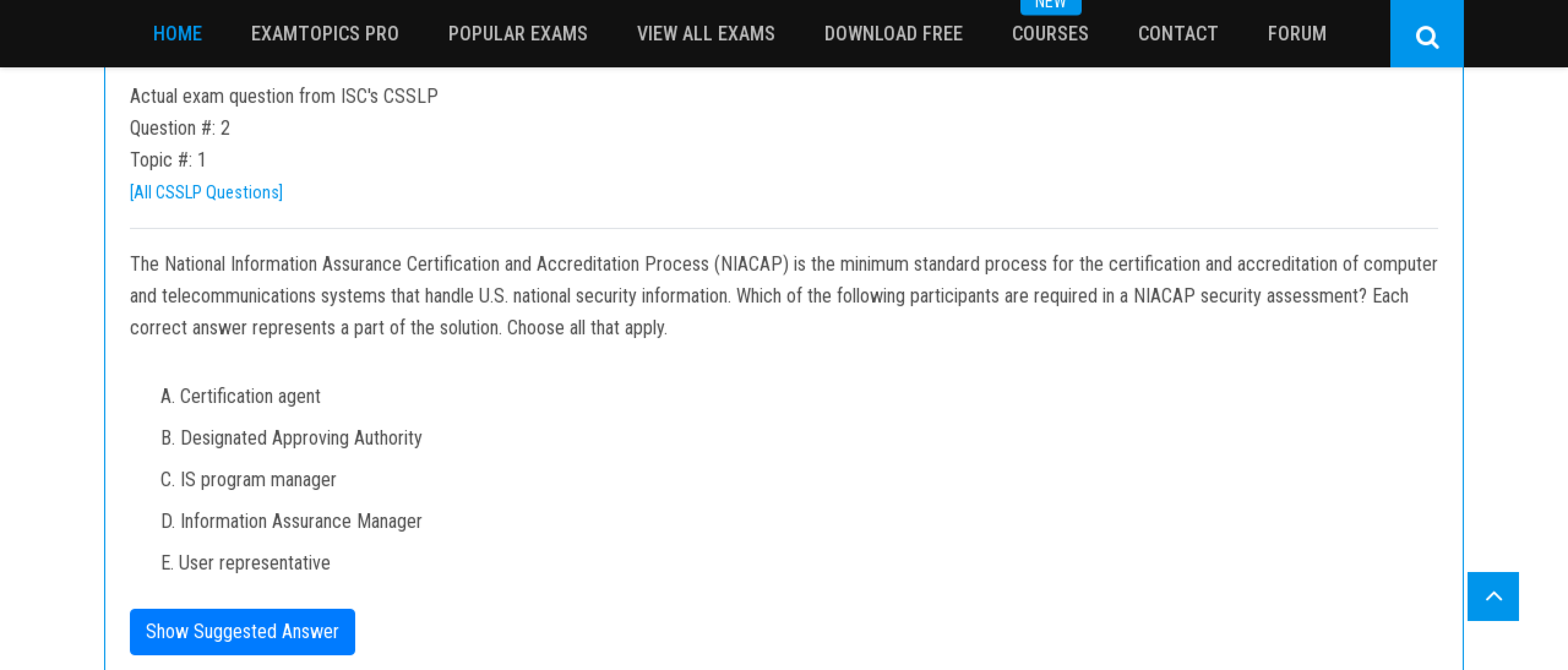
You work as a Network Auditor for Net Perfect Inc. The company has a Windows-based network. While auditing the company's network, you are facing problems in searching the faults and other entities that belong to it. Which of the following risks may occur due to the existence of these problems?

A. Residual risk

B. Secondary risk

C. Detection risk

D. Inherent risk



Actual exam question from ISC's CSSLP

Question #: 2

Topic #: 1

[All CSSLP Questions]

The National Information Assurance Certification and Accreditation Process (NIACAP) is the minimum standard process for the certification and accreditation of computer and telecommunications systems that handle U.S. national security information. Which of the following participants are required in a NIACAP security assessment? Each correct answer represents a part of the solution. Choose all that apply.

A. Certification agent

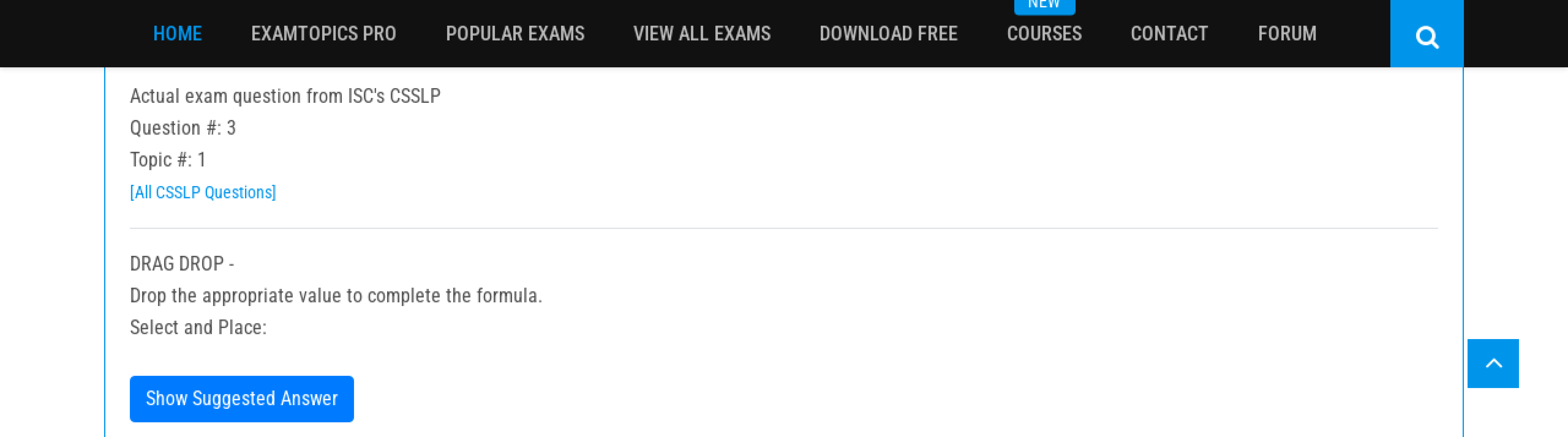
B. Designated Approving Authority

C. IS program manager

D. Information Assurance Manager

E. User representative

Show Suggested Answer



Actual exam question from ISC's CSSLP

Question #: 3

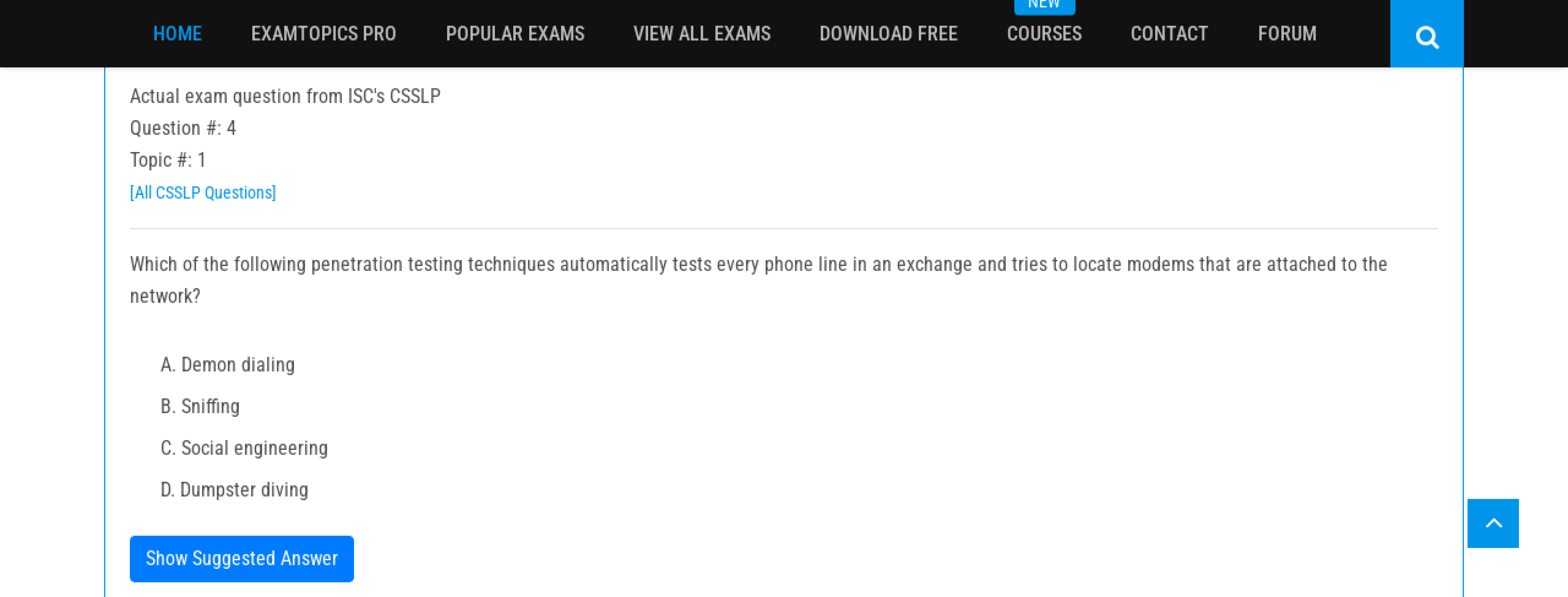
Topic #: 1

[All CSSLP Questions]

DRAG DROP -

Drop the appropriate value to complete the formula.

Select and Place:



Actual exam question from ISC's CSSLP

Question #: 4

Topic #: 1

[All CSSLP Questions]

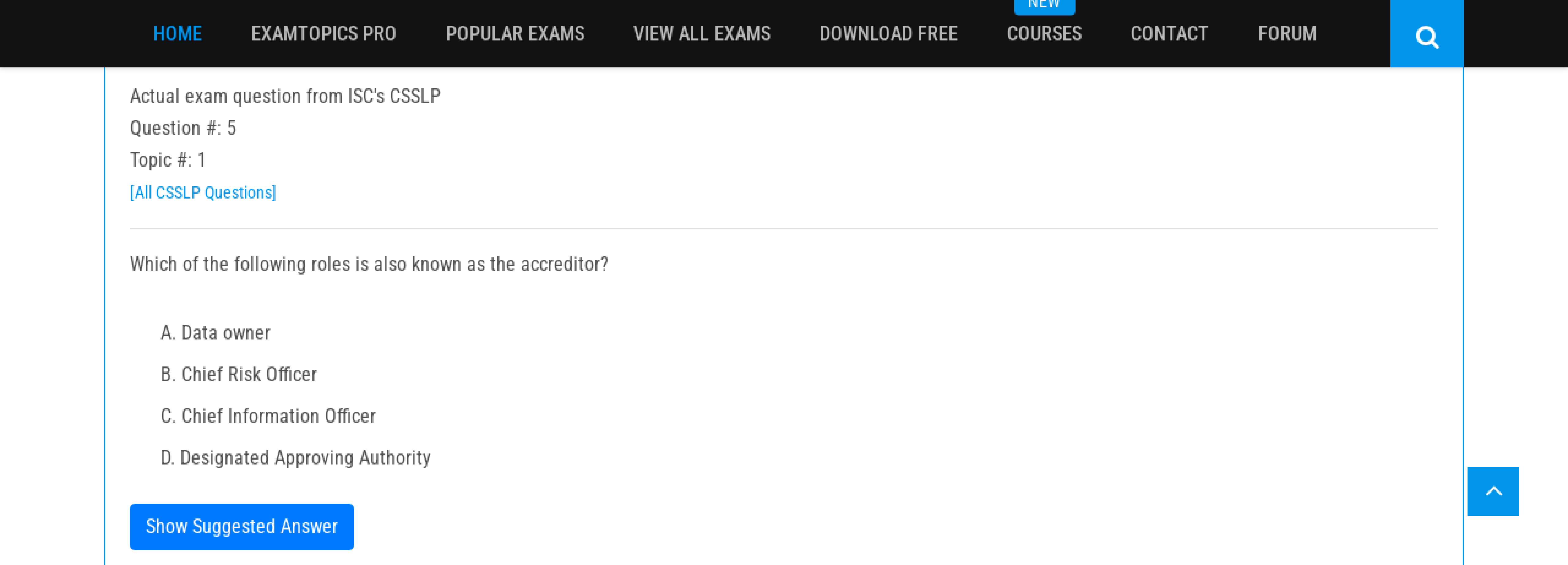
Which of the following penetration testing techniques automatically tests every phone line in an exchange and tries to locate modems that are attached to the network?

A. Demon dialing

B. Sniffing

C. Social engineering

D. Dumpster diving



Actual exam question from ISC's CSSLP

Question #: 5

Topic #: 1

[All CSSLP Questions]

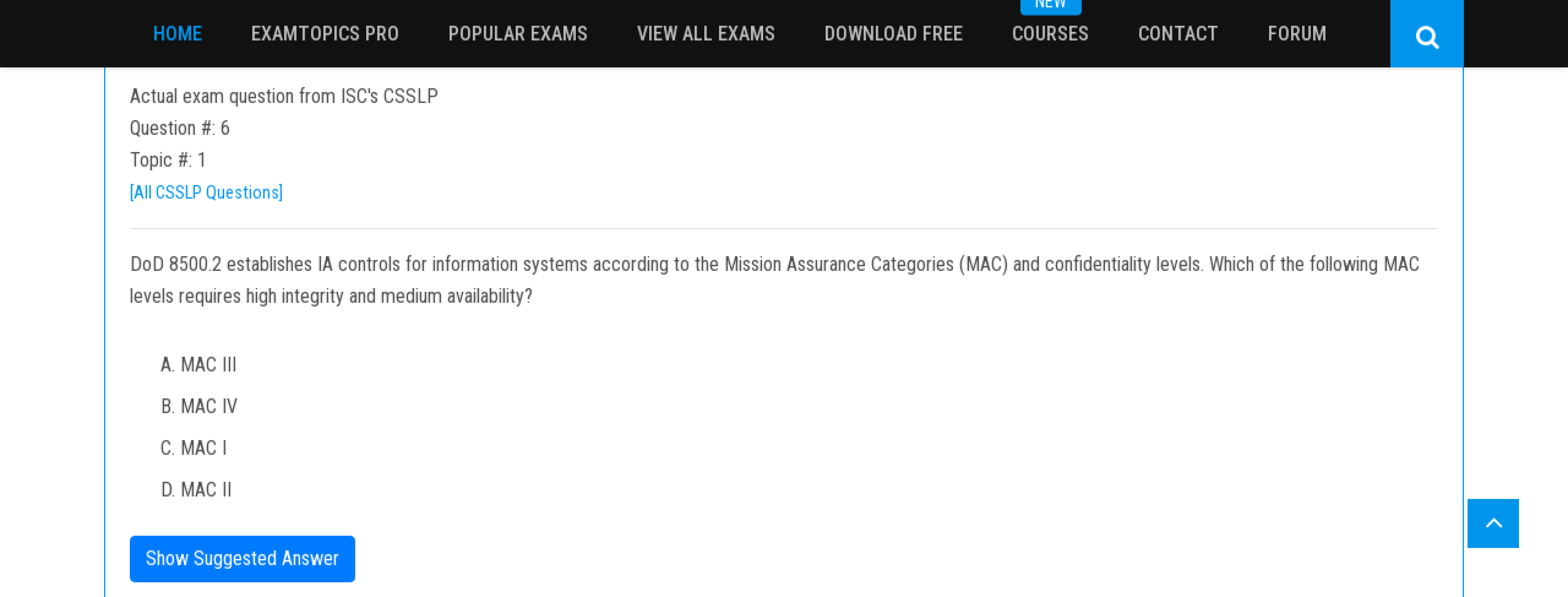
Which of the following roles is also known as the accreditor?

A. Data owner

B. Chief Risk Officer

C. Chief Information Officer

D. Designated Approving Authority



Actual exam question from ISC's CSSLP

Question #: 6

Topic #: 1

[All CSSLP Questions]

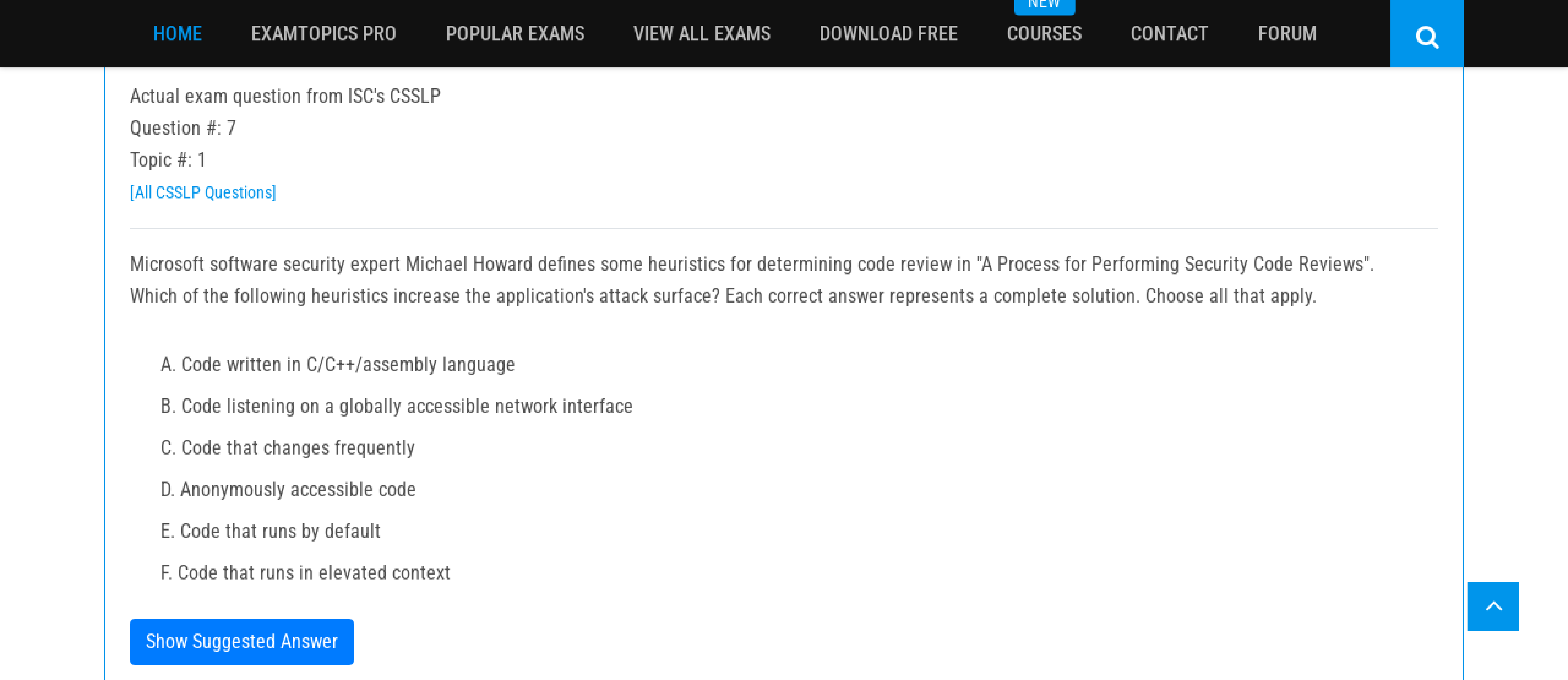
DoD 8500.2 establishes IA controls for information systems according to the Mission Assurance Categories (MAC) and confidentiality levels. Which of the following MAC levels requires high integrity and medium availability?

A. MAC III

B. MAC IV

C. MAC I

D. MAC II



Actual exam question from ISC's CSSLP

Question #: 7

Topic #: 1

[All CSSLP Questions]

Microsoft software security expert Michael Howard defines some heuristics for determining code review in "A Process for Performing Security Code Reviews". Which of the following heuristics increase the application's attack surface? Each correct answer represents a complete solution. Choose all that apply.

A. Code written in C/C++/assembly language

B. Code listening on a globally accessible network interface

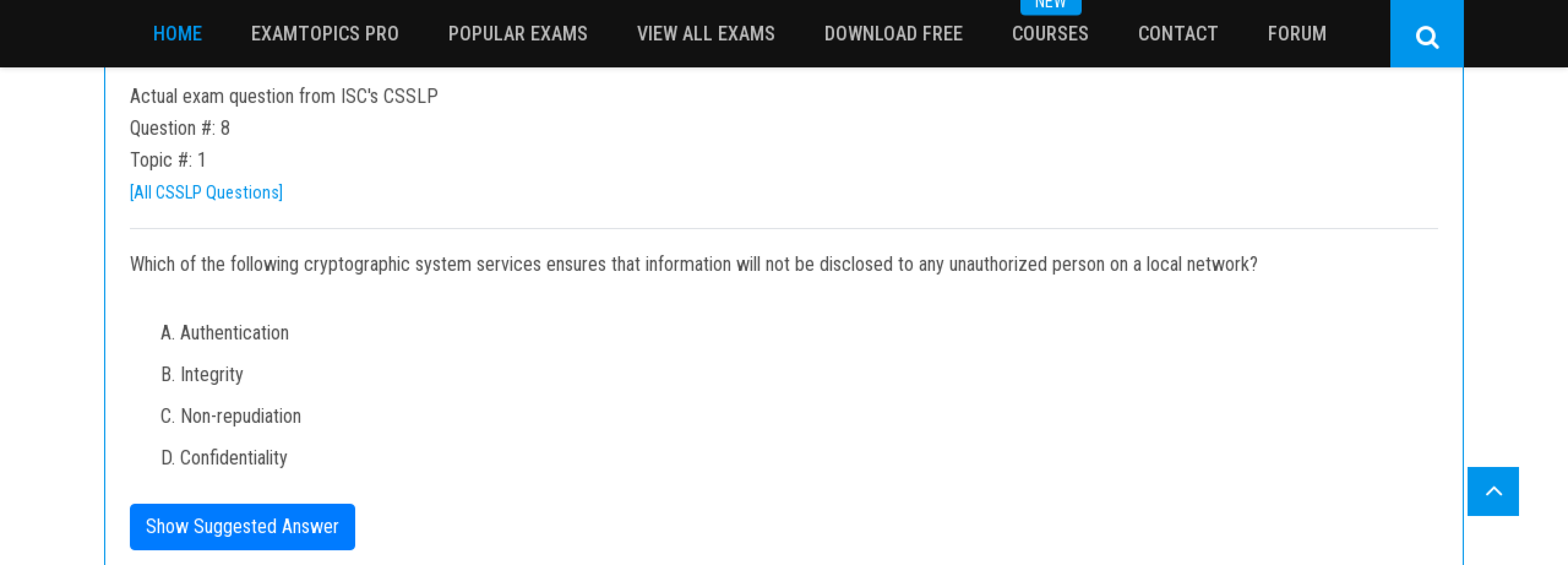
C. Code that changes frequently

D. Anonymously accessible code

E. Code that runs by default

F. Code that runs in elevated context

Show Suggested Answer



Actual exam question from ISC's CSSLP

Question #: 8

Topic #: 1

[All CSSLP Questions]

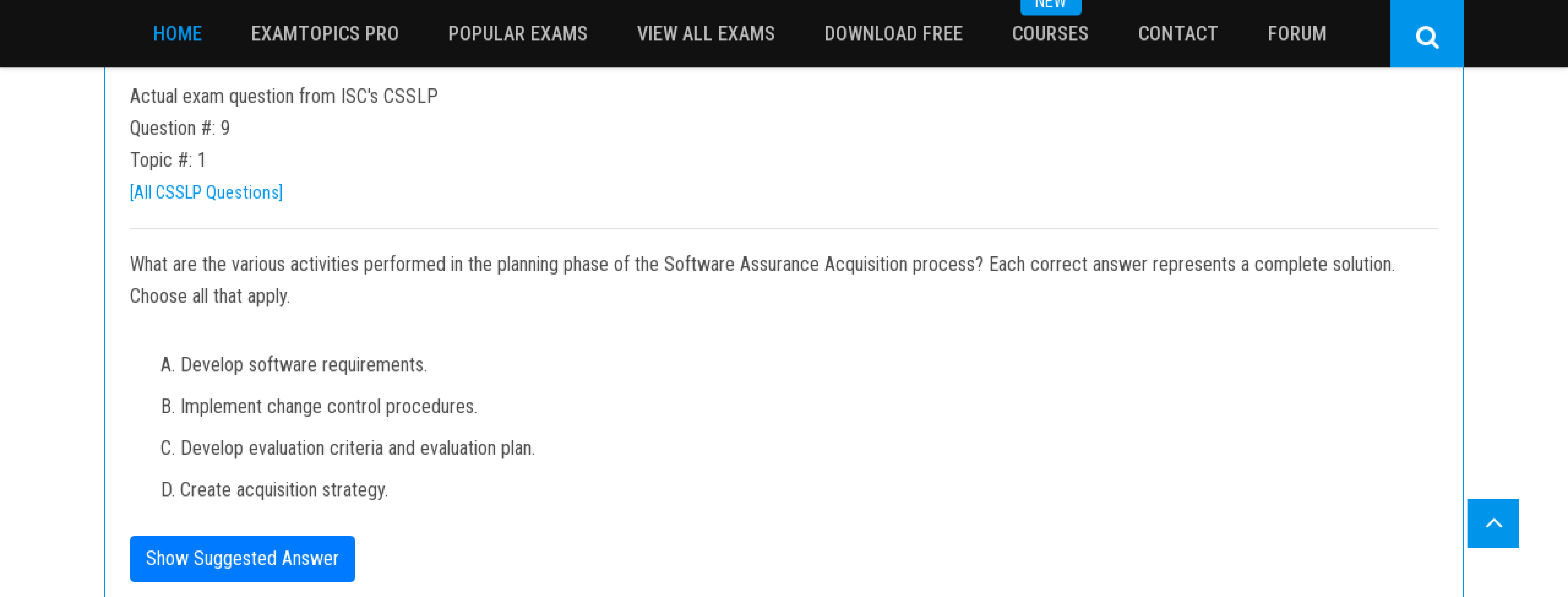
Which of the following cryptographic system services ensures that information will not be disclosed to any unauthorized person on a local network?

A. Authentication

B. Integrity

C. Non-repudiation

D. Confidentiality



Actual exam question from ISC's CSSLP
Question #: 9
Topic #: 1
[All CSSLP Questions]

What are the various activities performed in the planning phase of the Software Assurance Acquisition process? Each correct answer represents a complete solution. Choose all that apply.

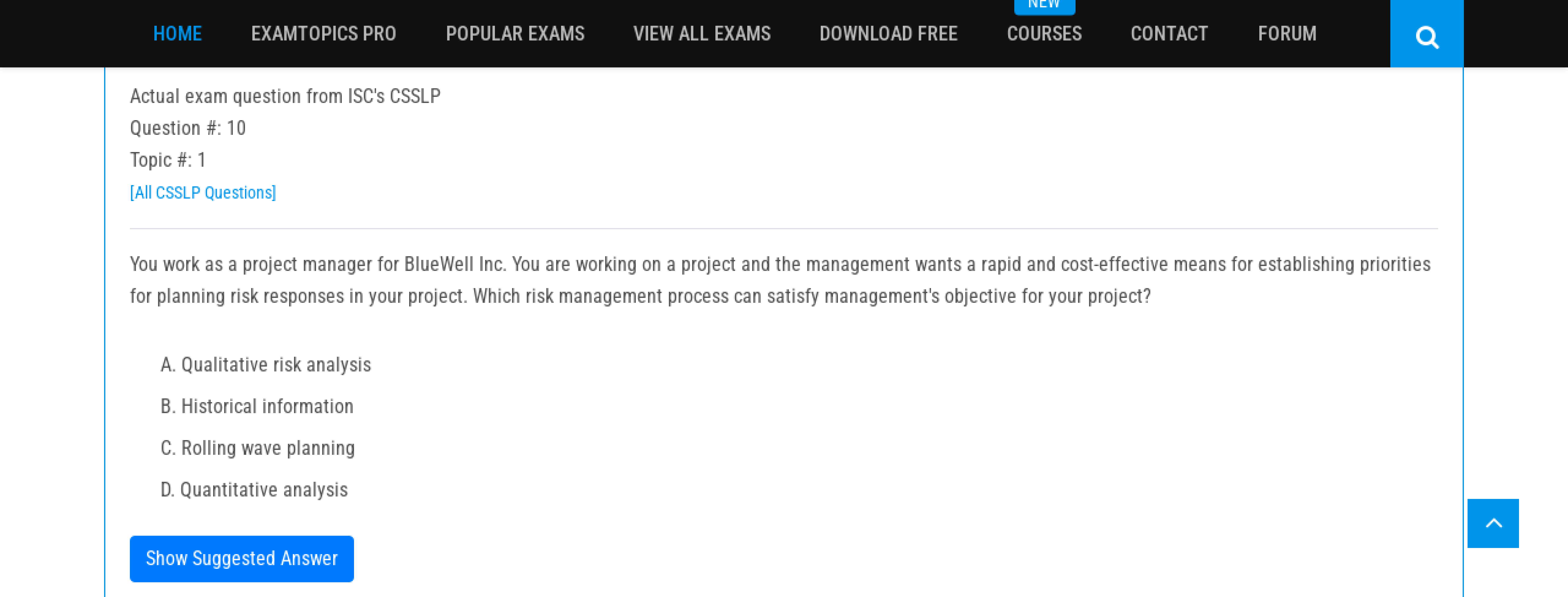
A. Develop software requirements.

B. Implement change control procedures.

C. Develop evaluation criteria and evaluation plan.

D. Create acquisition strategy.

Show Suggested Answer



Actual exam question from ISC's CSSLP

Question #: 10

Topic #: 1

[All CSSLP Questions]

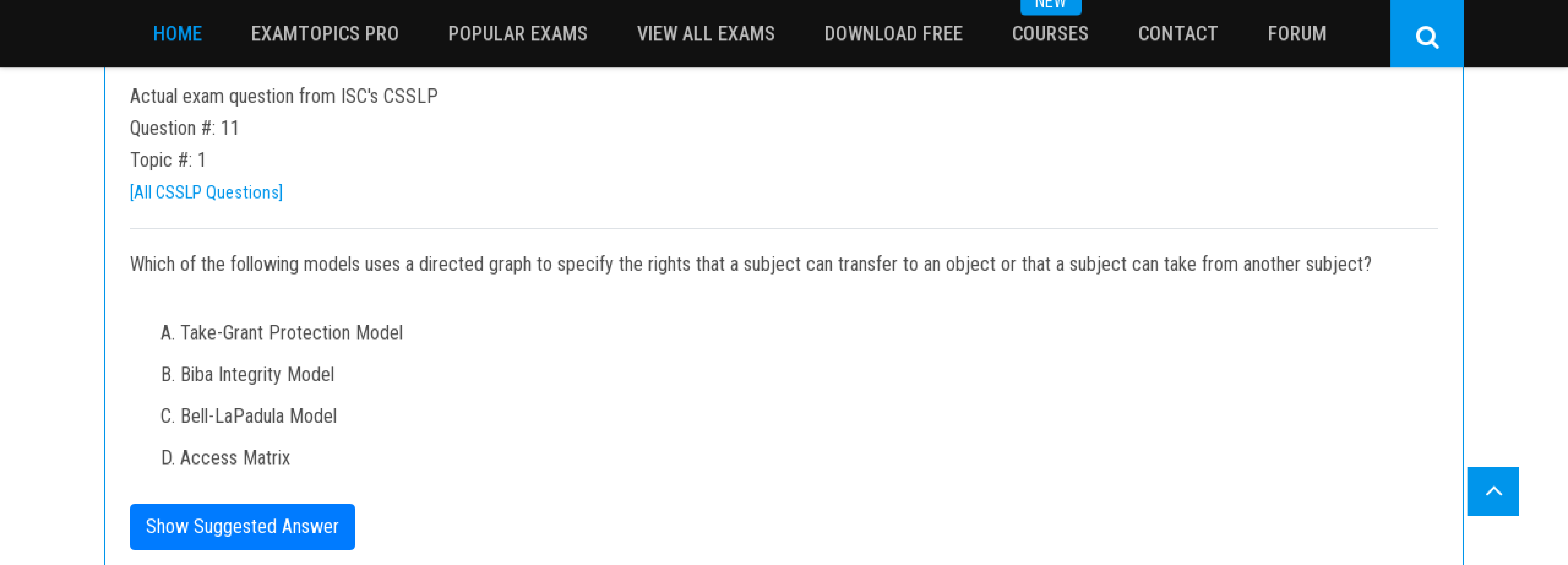
You work as a project manager for BlueWell Inc. You are working on a project and the management wants a rapid and cost-effective means for establishing priorities for planning risk responses in your project. Which risk management process can satisfy management's objective for your project?

A. Qualitative risk analysis

B. Historical information

C. Rolling wave planning

D. Quantitative analysis



Actual exam question from ISC's CSSLP

Question #: 11

Topic #: 1

[All CSSLP Questions]

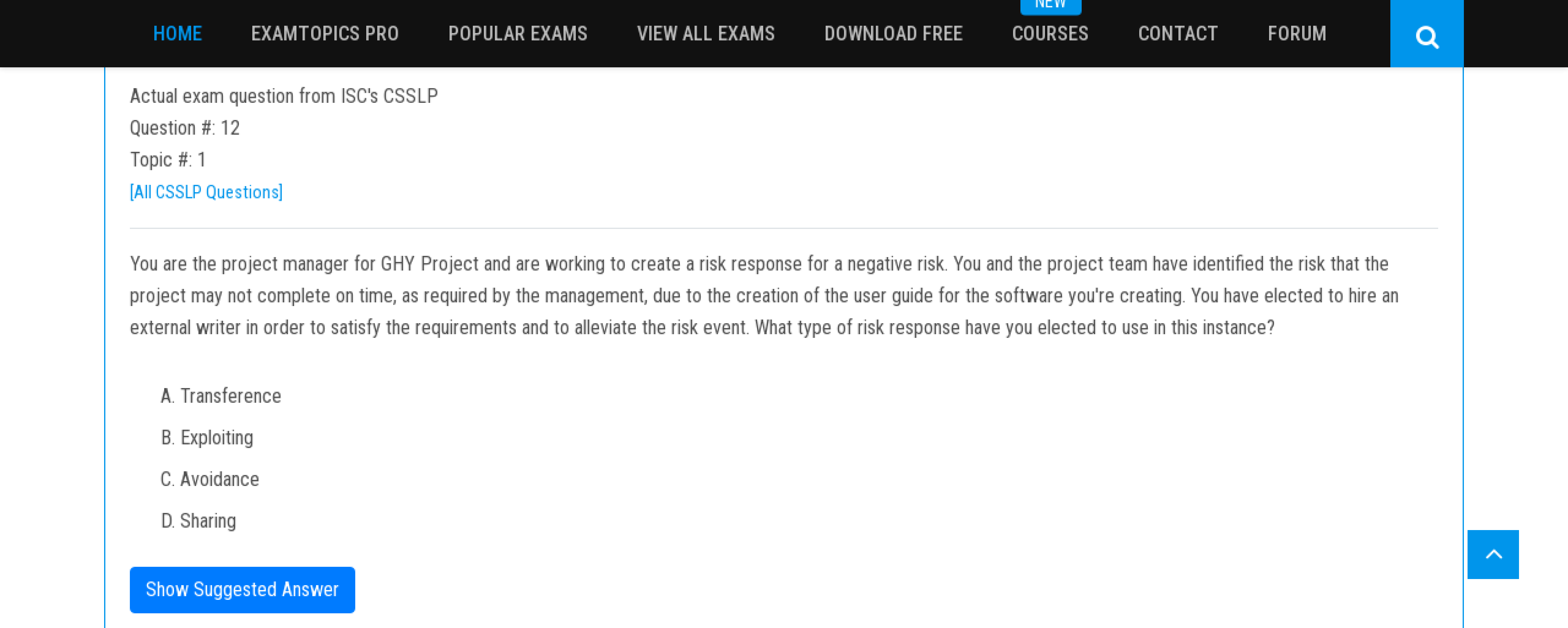
Which of the following models uses a directed graph to specify the rights that a subject can transfer to an object or that a subject can take from another subject?

A. Take-Grant Protection Model

B. Biba Integrity Model

C. Bell-LaPadula Model

D. Access Matrix



Actual exam question from ISC's CSSLP

Question #: 12

Topic #: 1

[All CSSLP Questions]

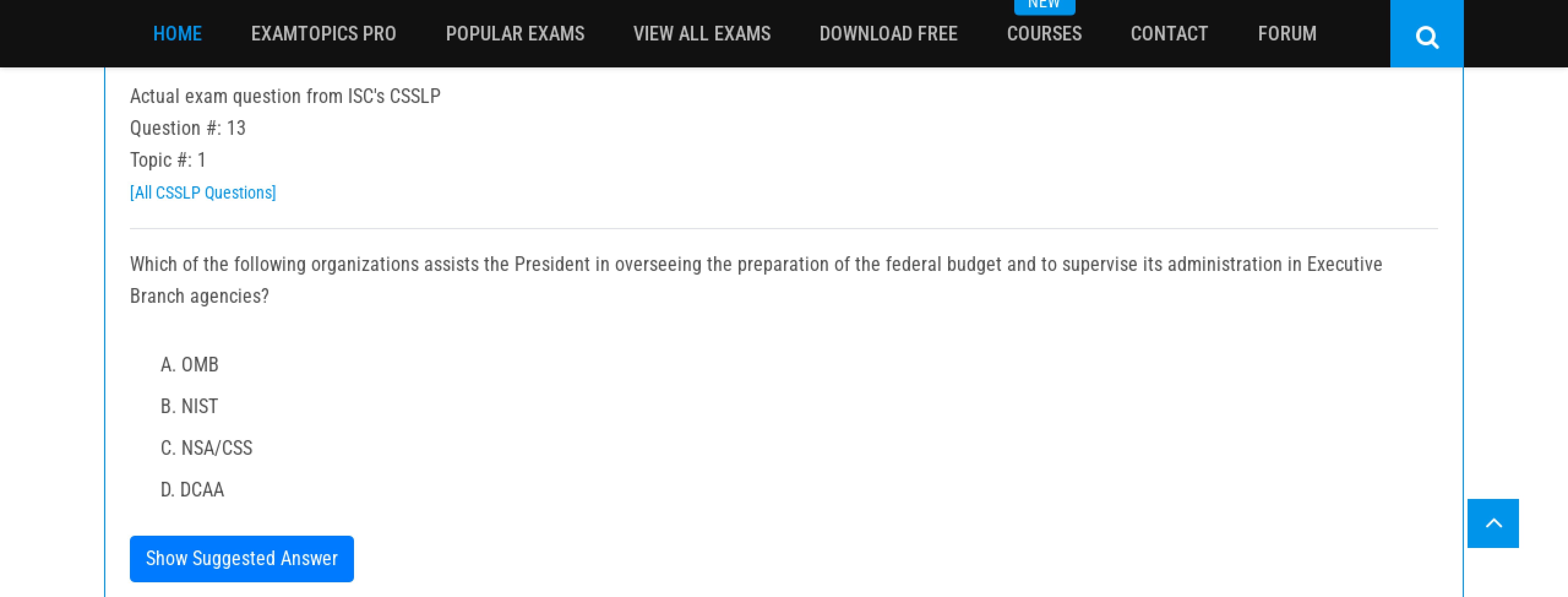
You are the project manager for GHY Project and are working to create a risk response for a negative risk. You and the project team have identified the risk that the project may not complete on time, as required by the management, due to the creation of the user guide for the software you're creating. You have elected to hire an external writer in order to satisfy the requirements and to alleviate the risk event. What type of risk response have you elected to use in this instance?

A. Transference

B. Exploiting

C. Avoidance

D. Sharing



Actual exam question from ISC's CSSLP

Question #: 13

Topic #: 1

[All CSSLP Questions]

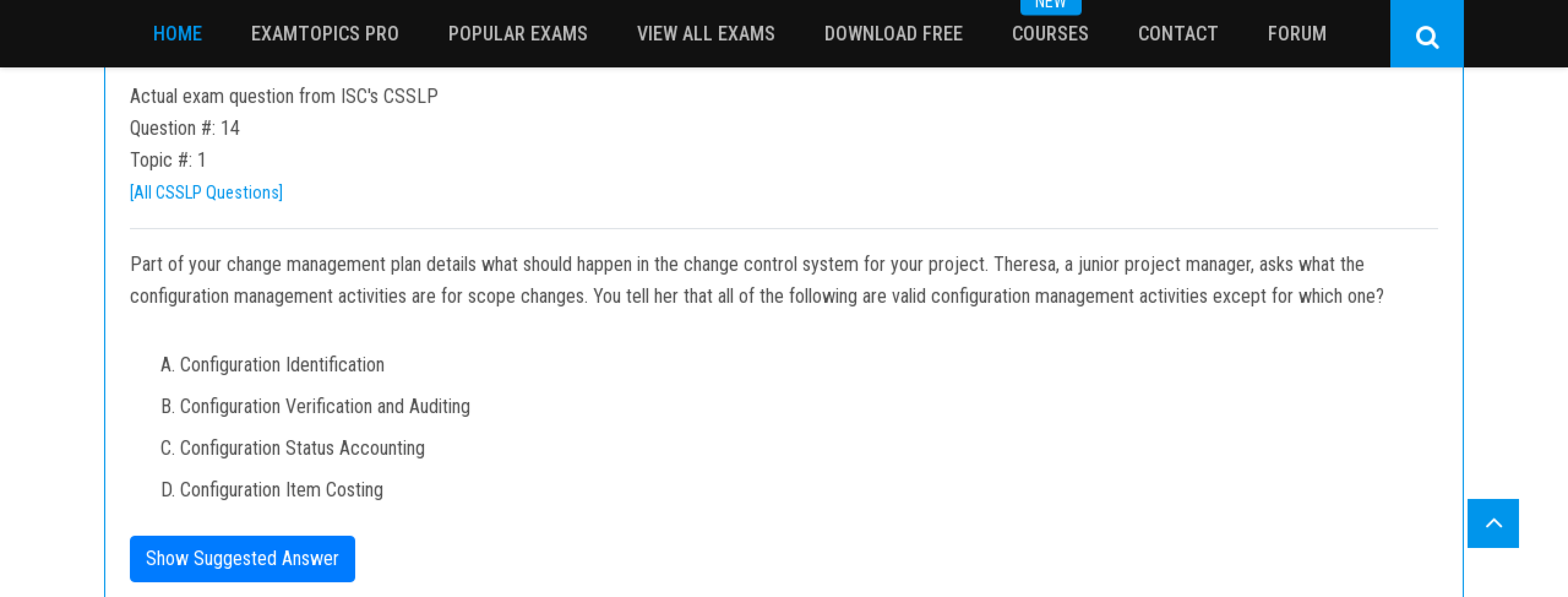
Which of the following organizations assists the President in overseeing the preparation of the federal budget and to supervise its administration in Executive Branch agencies?

A. OMB

B. NIST

C. NSA/CSS

D. DCAA



Actual exam question from ISC's CSSLP

Question #: 14

Topic #: 1

[All CSSLP Questions]

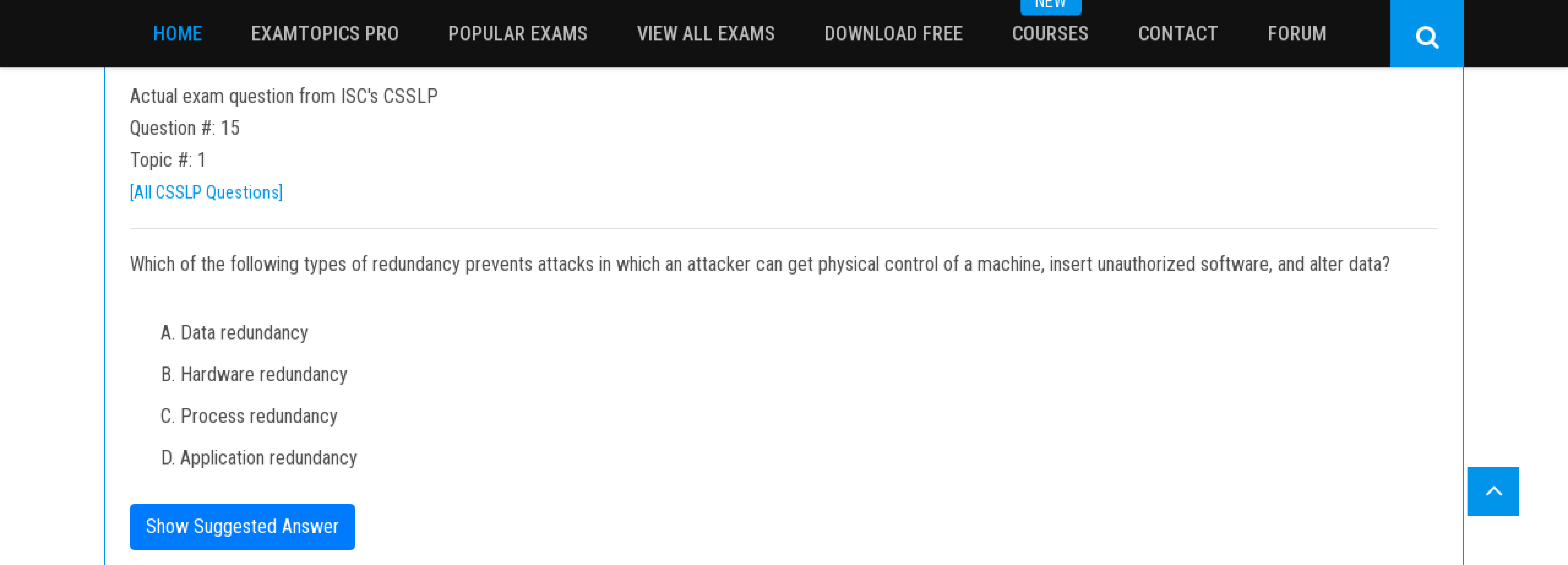
Part of your change management plan details what should happen in the change control system for your project. Theresa, a junior project manager, asks what the configuration management activities are for scope changes. You tell her that all of the following are valid configuration management activities except for which one?

A. Configuration Identification

B. Configuration Verification and Auditing

C. Configuration Status Accounting

D. Configuration Item Costing



Actual exam question from ISC's CSSLP

Question #: 15

Topic #: 1

[All CSSLP Questions]

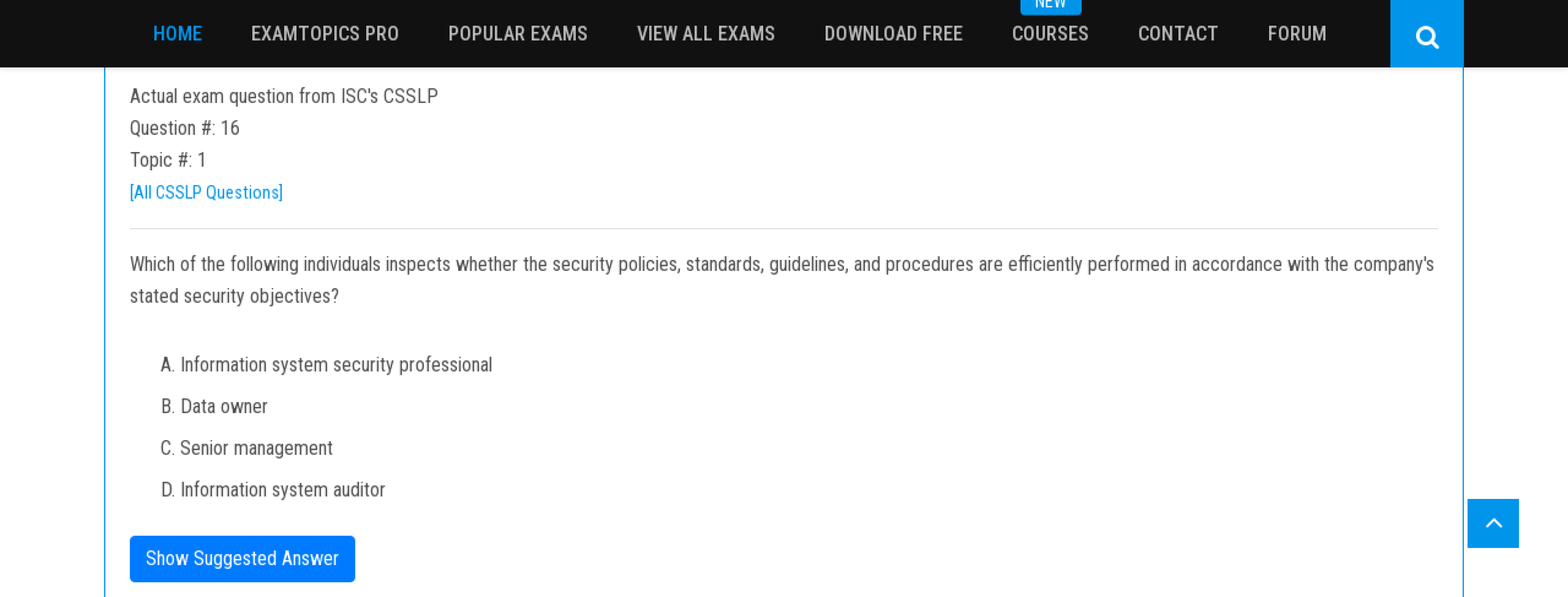
Which of the following types of redundancy prevents attacks in which an attacker can get physical control of a machine, insert unauthorized software, and alter data?

A. Data redundancy

B. Hardware redundancy

C. Process redundancy

D. Application redundancy



Actual exam question from ISC's CSSLP
Question #: 16
Topic #: 1
[All CSSLP Questions]

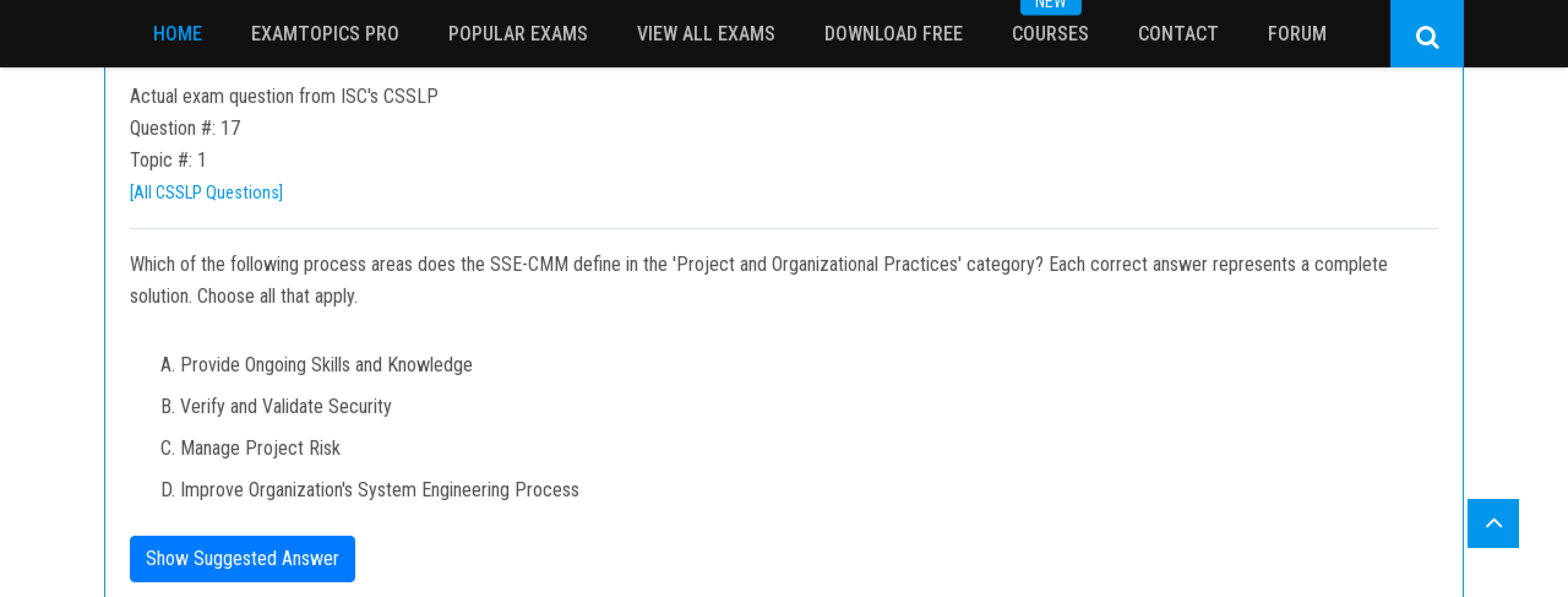
Which of the following individuals inspects whether the security policies, standards, guidelines, and procedures are efficiently performed in accordance with the company's stated security objectives?

A. Information system security professional

B. Data owner

C. Senior management

D. Information system auditor



Actual exam question from ISC's CSSLP
Question #: 17
Topic #: 1
[All CSSLP Questions]

Which of the following process areas does the SSE-CMM define in the 'Project and Organizational Practices' category? Each correct answer represents a complete solution. Choose all that apply.

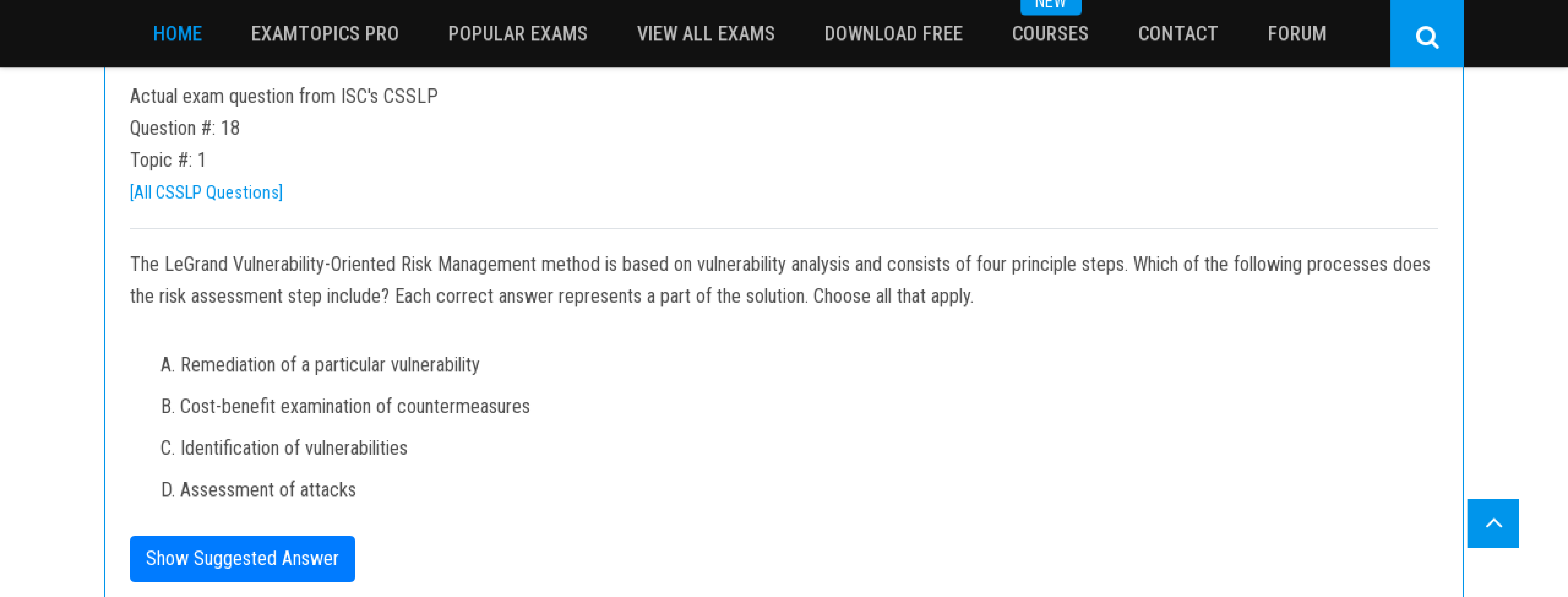
A. Provide Ongoing Skills and Knowledge

B. Verify and Validate Security

C. Manage Project Risk

D. Improve Organization's System Engineering Process

Show Suggested Answer



Actual exam question from ISC's CSSLP
Question #: 18
Topic #: 1
[All CSSLP Questions]

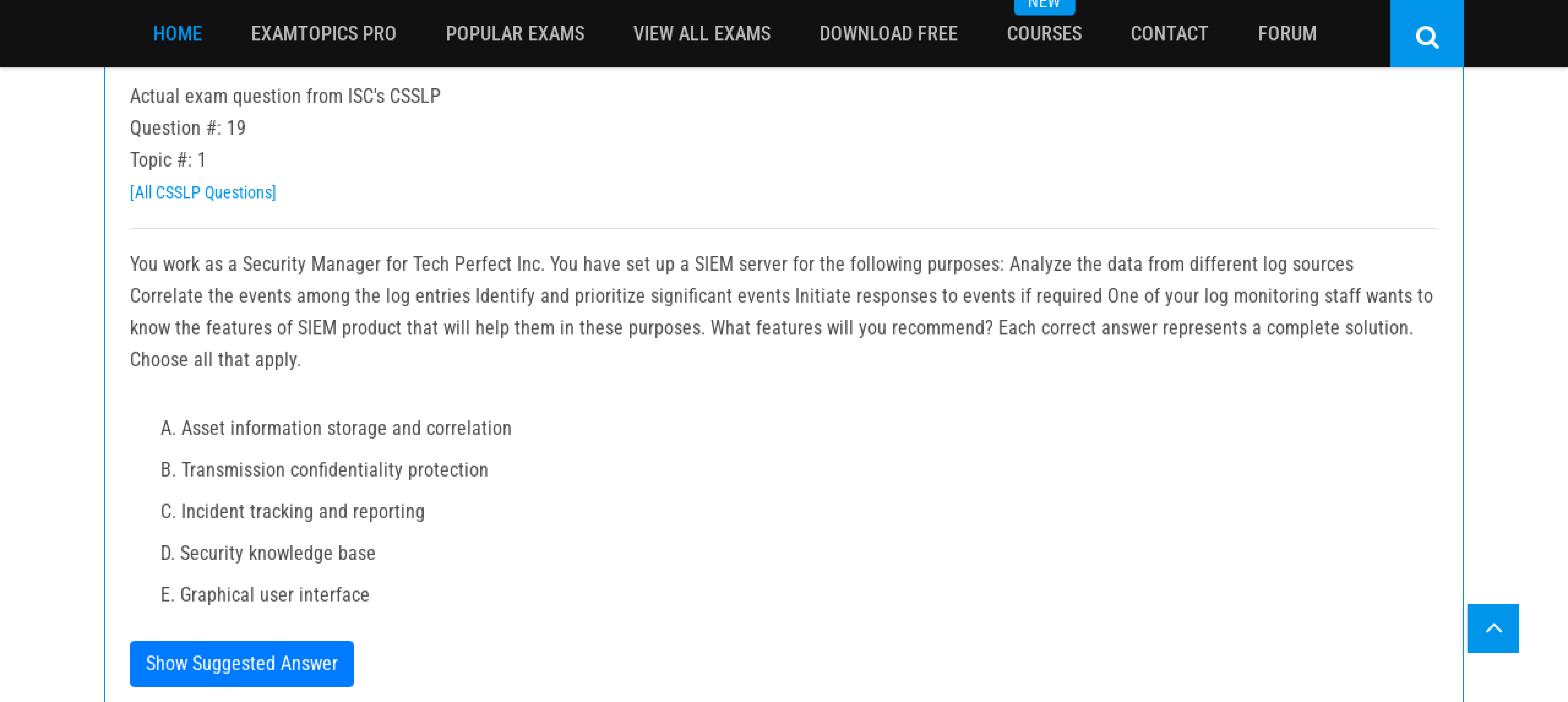
The LeGrand Vulnerability-Oriented Risk Management method is based on vulnerability analysis and consists of four principle steps. Which of the following processes does the risk assessment step include? Each correct answer represents a part of the solution. Choose all that apply.

A. Remediation of a particular vulnerability

B. Cost-benefit examination of countermeasures

C. Identification of vulnerabilities

D. Assessment of attacks



Actual exam question from ISC's CSSLP

Question #: 19

Topic #: 1

[All CSSLP Questions]

You work as a Security Manager for Tech Perfect Inc. You have set up a SIEM server for the following purposes: Analyze the data from different log sources Correlate the events among the log entries Identify and prioritize significant events Initiate responses to events if required One of your log monitoring staff wants to know the features of SIEM product that will help them in these purposes. What features will you recommend? Each correct answer represents a complete solution. Choose all that apply.

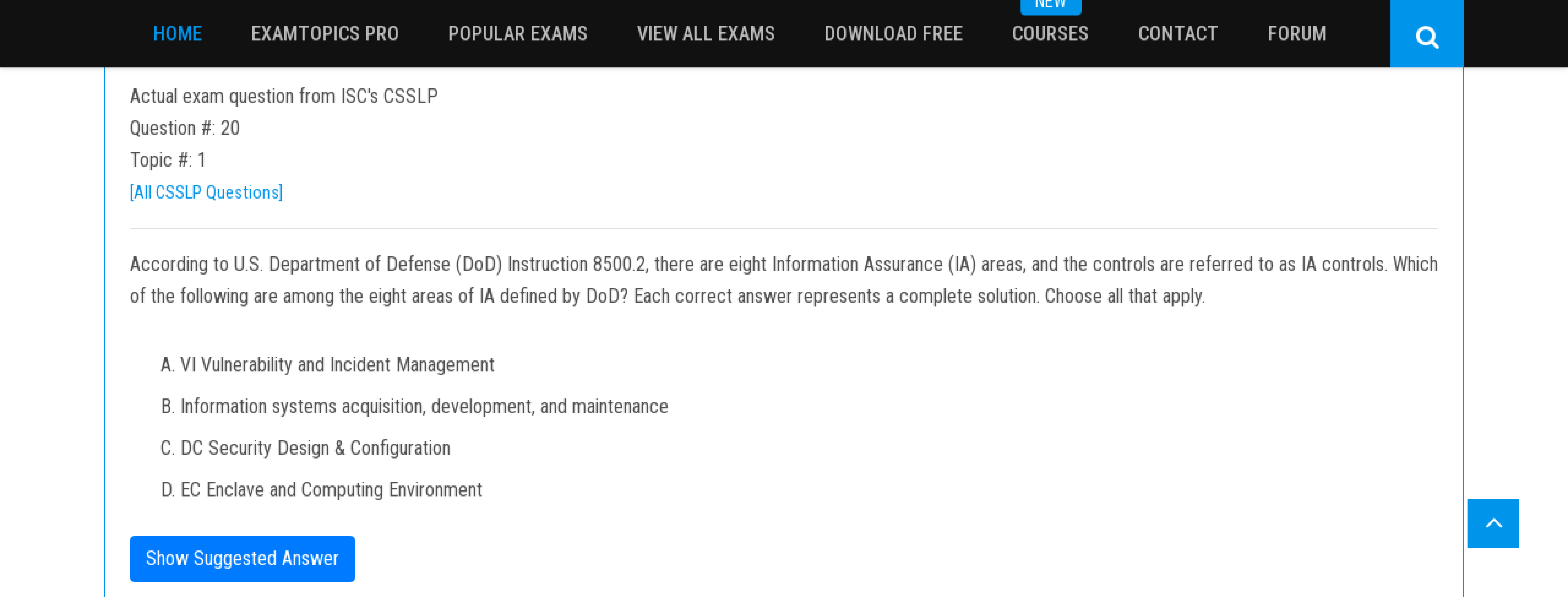
A. Asset information storage and correlation

B. Transmission confidentiality protection

C. Incident tracking and reporting

D. Security knowledge base

E. Graphical user interface



Actual exam question from ISC's CSSLP
Question #: 20
Topic #: 1
[All CSSLP Questions]

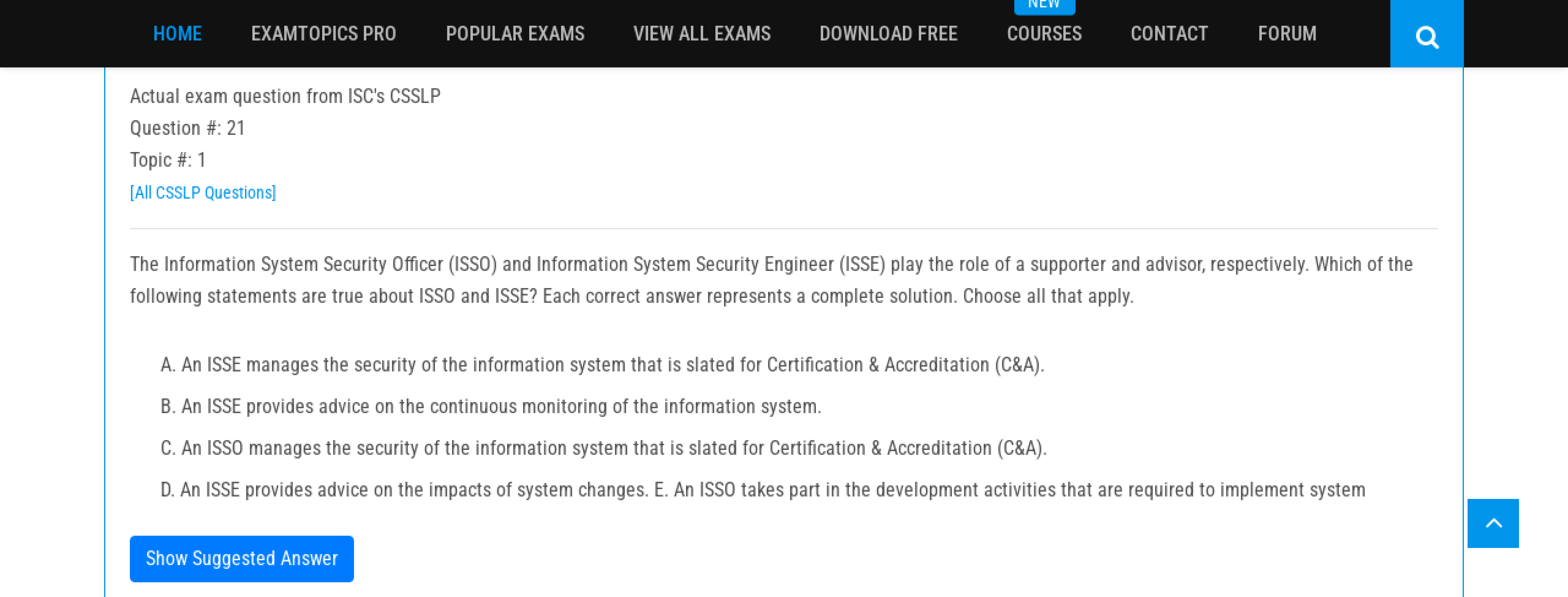
According to U.S. Department of Defense (DoD) Instruction 8500.2, there are eight Information Assurance (IA) areas, and the controls are referred to as IA controls. Which of the following are among the eight areas of IA defined by DoD? Each correct answer represents a complete solution. Choose all that apply.

A. VI Vulnerability and Incident Management

B. Information systems acquisition, development, and maintenance

C. DC Security Design & Configuration

D. EC Enclave and Computing Environment



Actual exam question from ISC's CSSLP

Question #: 21

Topic #: 1

[All CSSLP Questions]

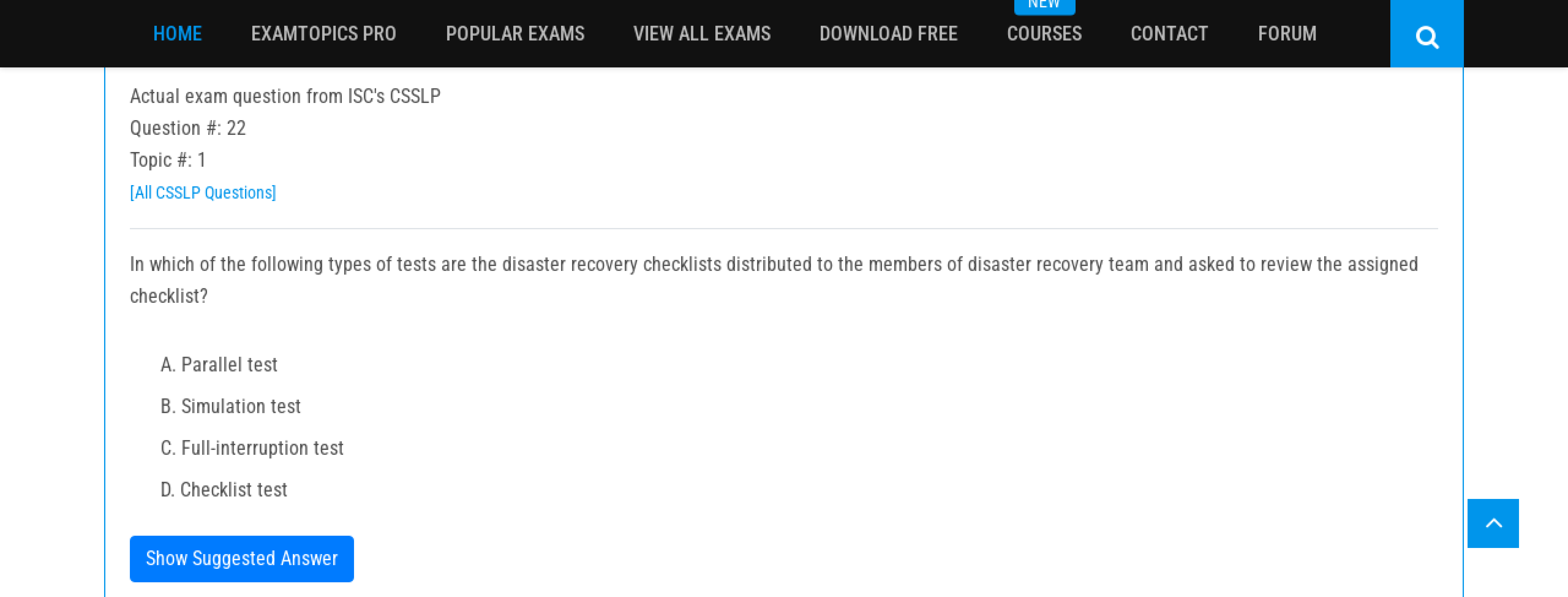
The Information System Security Officer (ISSO) and Information System Security Engineer (ISSE) play the role of a supporter and advisor, respectively. Which of the following statements are true about ISSO and ISSE? Each correct answer represents a complete solution. Choose all that apply.

A. An ISSE manages the security of the information system that is slated for Certification & Accreditation (C&A).

B. An ISSE provides advice on the continuous monitoring of the information system.

C. An ISSO manages the security of the information system that is slated for Certification & Accreditation (C&A).

D. An ISSE provides advice on the impacts of system changes. E. An ISSO takes part in the development activities that are required to implement system



Actual exam question from ISC's CSSLP

Question #: 22

Topic #: 1

[All CSSLP Questions]

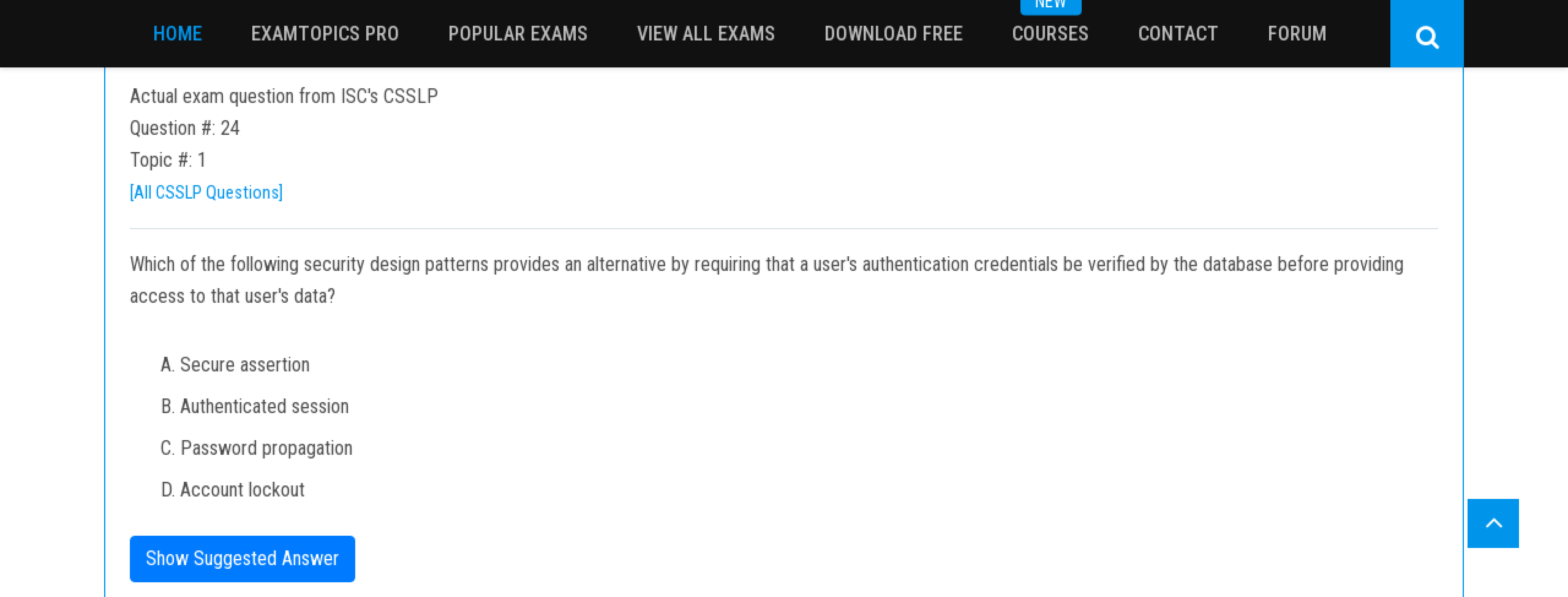
In which of the following types of tests are the disaster recovery checklists distributed to the members of disaster recovery team and asked to review the assigned checklist?

A. Parallel test

B. Simulation test

C. Full-interruption test

D. Checklist test



Actual exam question from ISC's CSSLP

Question #: 24

Topic #: 1

[All CSSLP Questions]

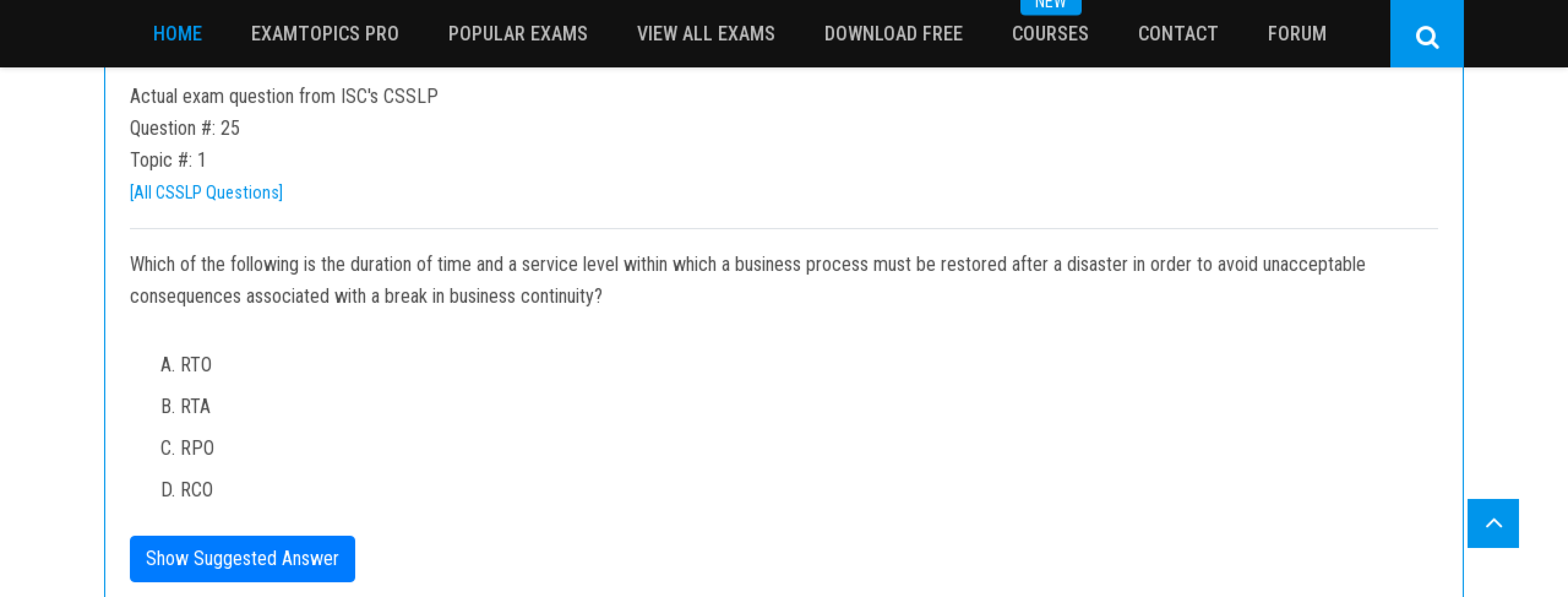
Which of the following security design patterns provides an alternative by requiring that a user's authentication credentials be verified by the database before providing access to that user's data?

A. Secure assertion

B. Authenticated session

C. Password propagation

D. Account lockout



Actual exam question from ISC's CSSLP

Question #: 25

Topic #: 1

[All CSSLP Questions]

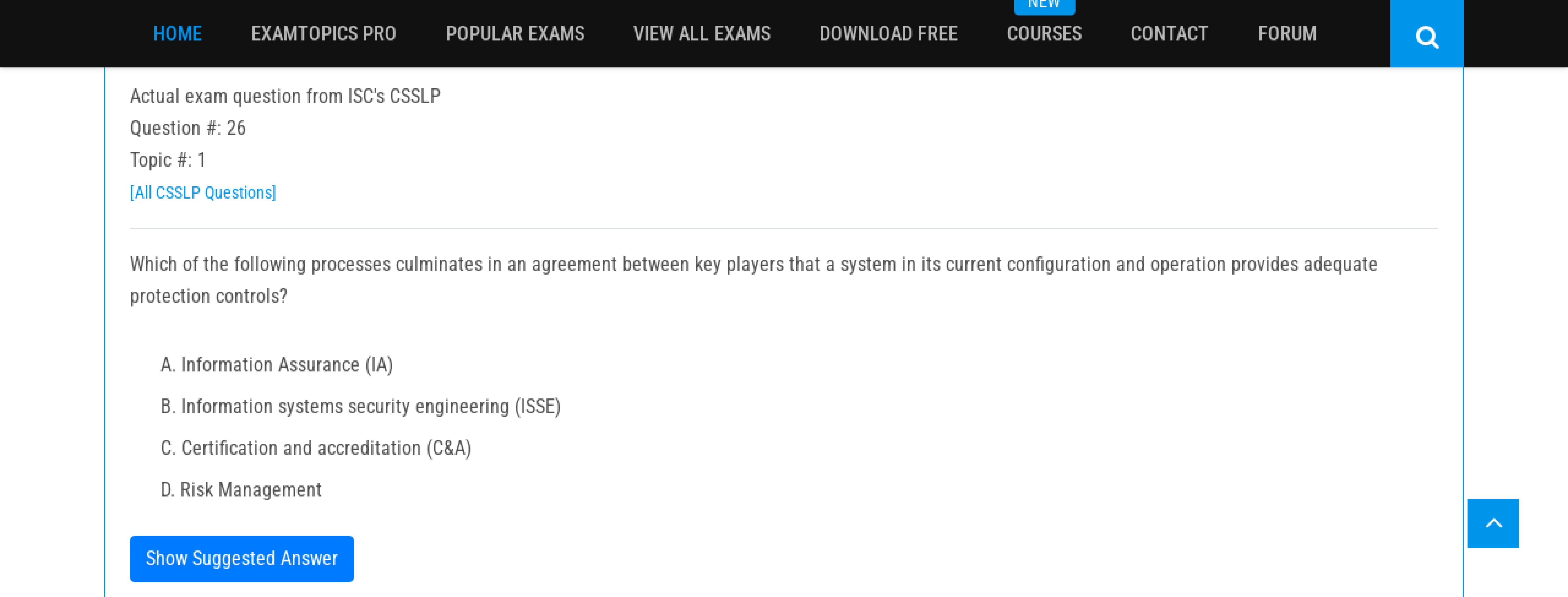
Which of the following is the duration of time and a service level within which a business process must be restored after a disaster in order to avoid unacceptable consequences associated with a break in business continuity?

A. RTO

B. RTA

C. RPO

D. RCO



Actual exam question from ISC's CSSLP

Question #: 26

Topic #: 1

[All CSSLP Questions]

Which of the following processes culminates in an agreement between key players that a system in its current configuration and operation provides adequate protection controls?

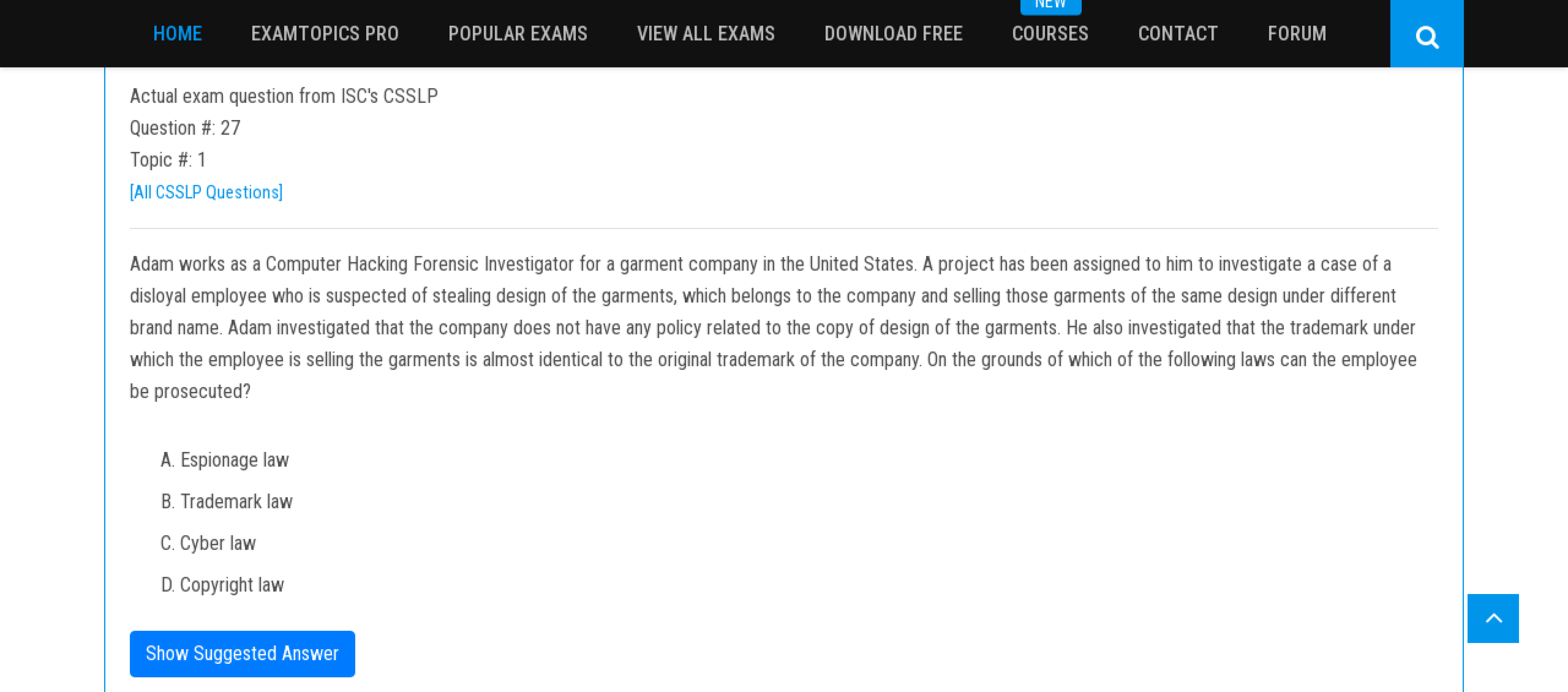
A. Information Assurance (IA)

B. Information systems security engineering (ISSE)

C. Certification and accreditation (C&A)

D. Risk Management

Show Suggested Answer



Actual exam question from ISC's CSSLP

Question #: 27

Topic #: 1

[All CSSLP Questions]

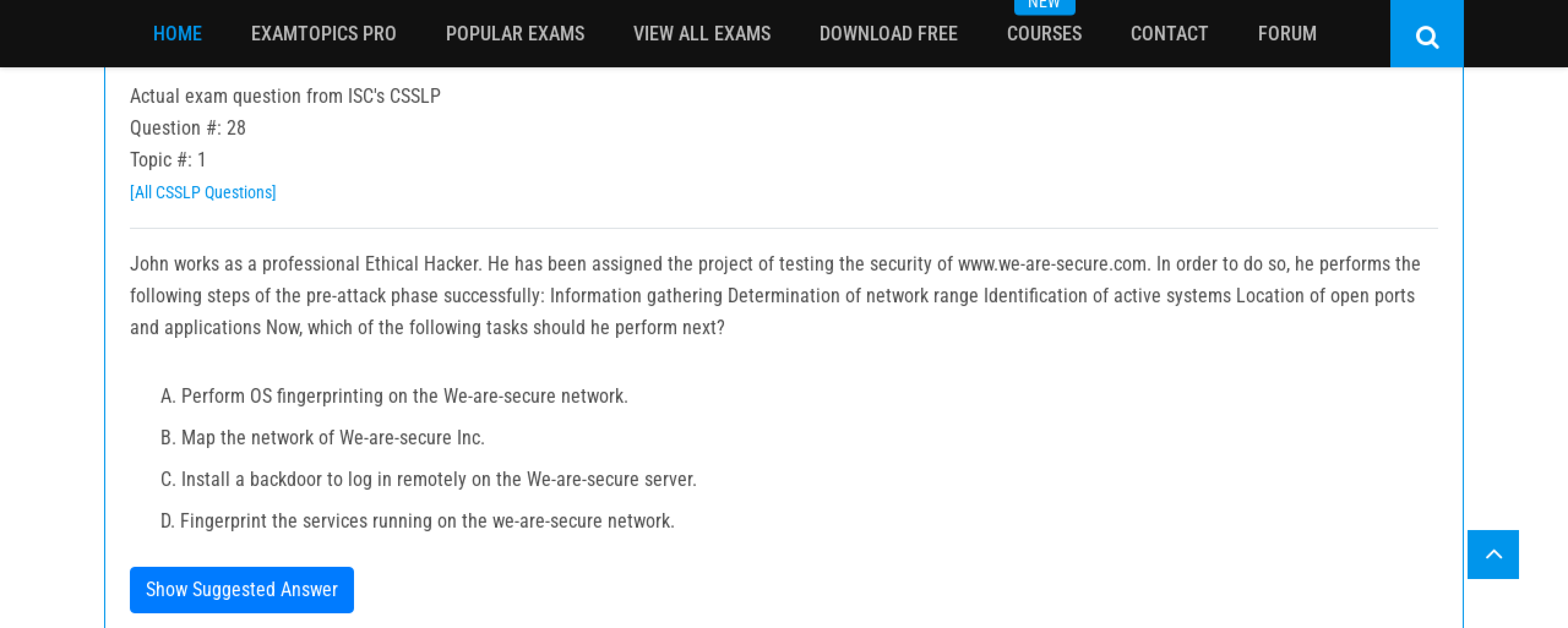
Adam works as a Computer Hacking Forensic Investigator for a garment company in the United States. A project has been assigned to him to investigate a case of a disloyal employee who is suspected of stealing design of the garments, which belongs to the company and selling those garments of the same design under different brand name. Adam investigated that the company does not have any policy related to the copy of design of the garments. He also investigated that the trademark under which the employee is selling the garments is almost identical to the original trademark of the company. On the grounds of which of the following laws can the employee be prosecuted?

A. Espionage law

B. Trademark law

C. Cyber law

D. Copyright law



Actual exam question from ISC's CSSLP

Question #: 28

Topic #: 1

[All CSSLP Questions]

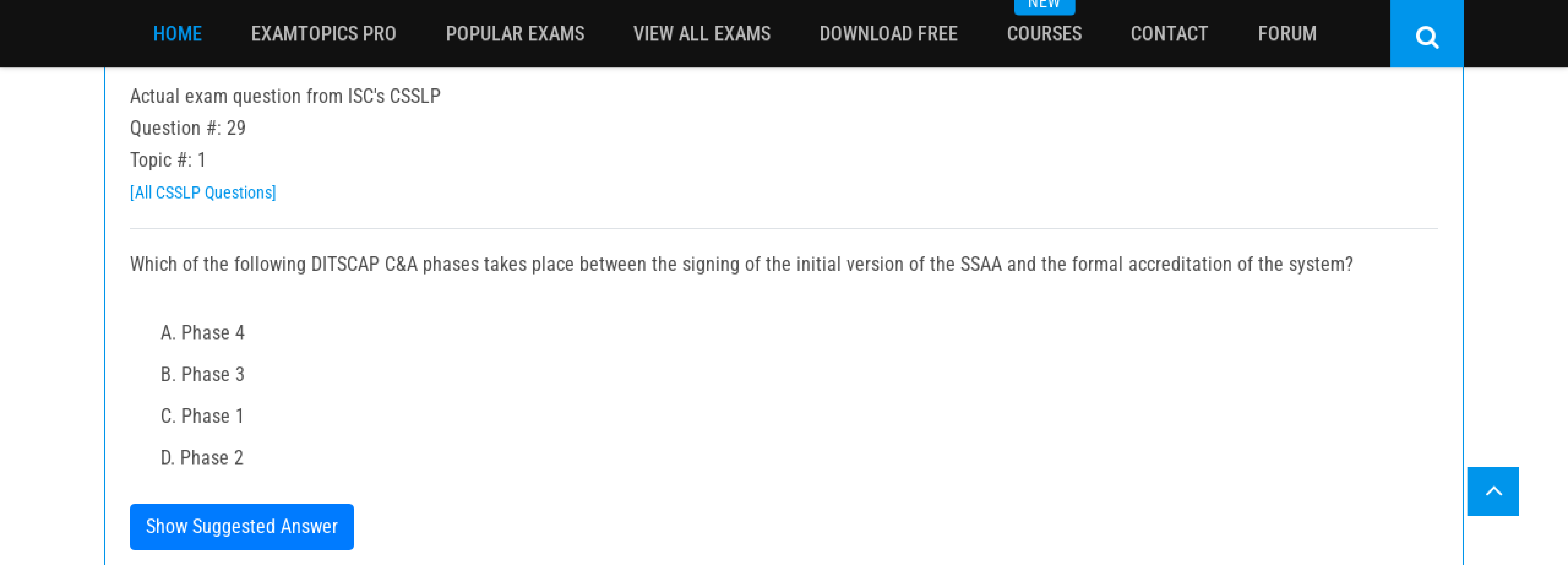
John works as a professional Ethical Hacker. He has been assigned the project of testing the security of www.we-are-secure.com. In order to do so, he performs the following steps of the pre-attack phase successfully: Information gathering Determination of network range Identification of active systems Location of open ports and applications Now, which of the following tasks should he perform next?

A. Perform OS fingerprinting on the We-are-secure network.

B. Map the network of We-are-secure Inc.

C. Install a backdoor to log in remotely on the We-are-secure server.

D. Fingerprint the services running on the we-are-secure network.



Actual exam question from ISC's CSSLP

Question #: 29

Topic #: 1

[All CSSLP Questions]

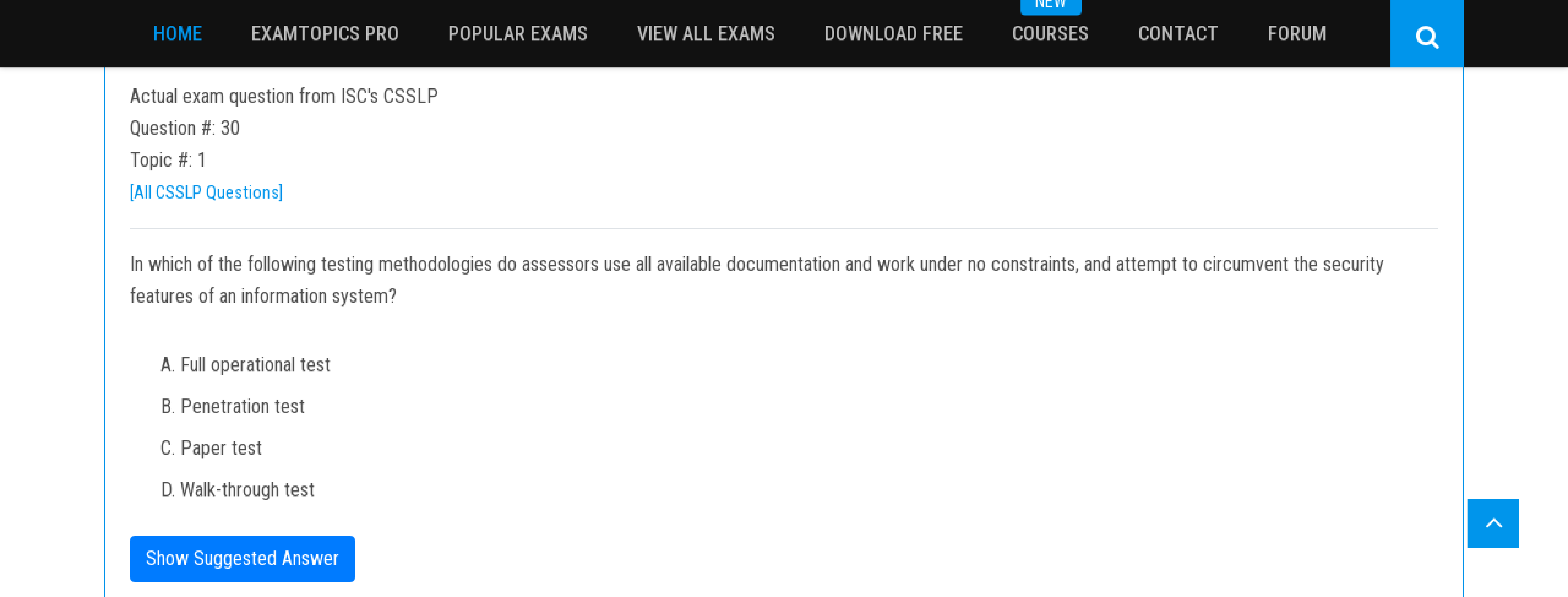
Which of the following DITSCAP C&A phases takes place between the signing of the initial version of the SSAA and the formal accreditation of the system?

A. Phase 4

B. Phase 3

C. Phase 1

D. Phase 2



Actual exam question from ISC's CSSLP

Question #: 30

Topic #: 1

[All CSSLP Questions]

In which of the following testing methodologies do assessors use all available documentation and work under no constraints, and attempt to circumvent the security features of an information system?

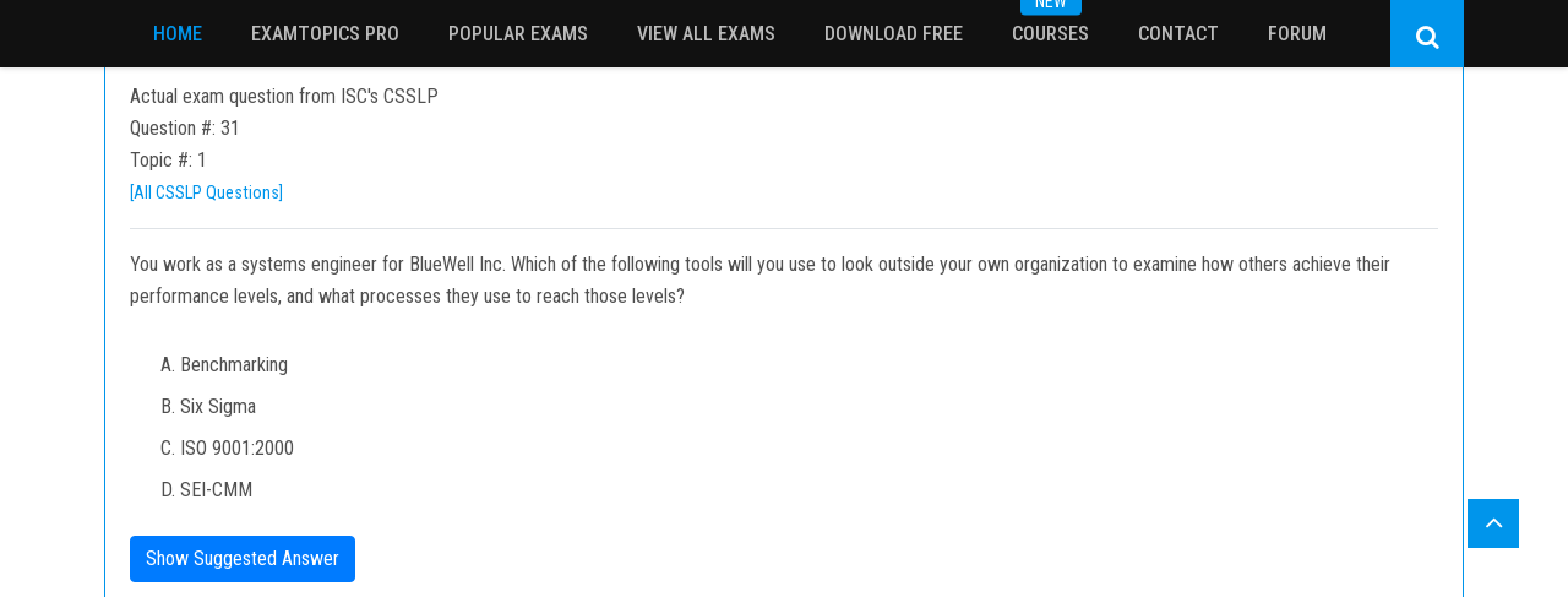
A. Full operational test

B. Penetration test

C. Paper test

D. Walk-through test

Show Suggested Answer



Actual exam question from ISC's CSSLP

Question #: 31

Topic #: 1

[All CSSLP Questions]

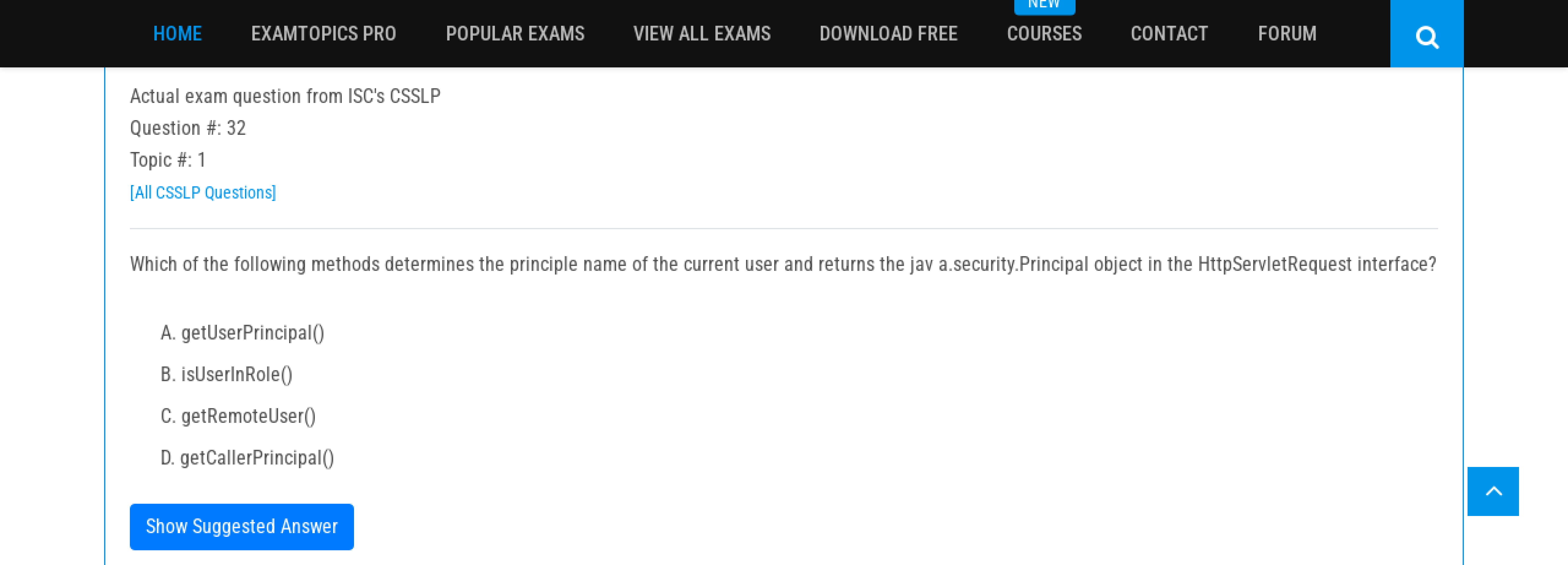
You work as a systems engineer for BlueWell Inc. Which of the following tools will you use to look outside your own organization to examine how others achieve their performance levels, and what processes they use to reach those levels?

A. Benchmarking

B. Six Sigma

C. ISO 9001:2000

D. SEI-CMM



Actual exam question from ISC's CSSLP

Question #: 32

Topic #: 1

[All CSSLP Questions]

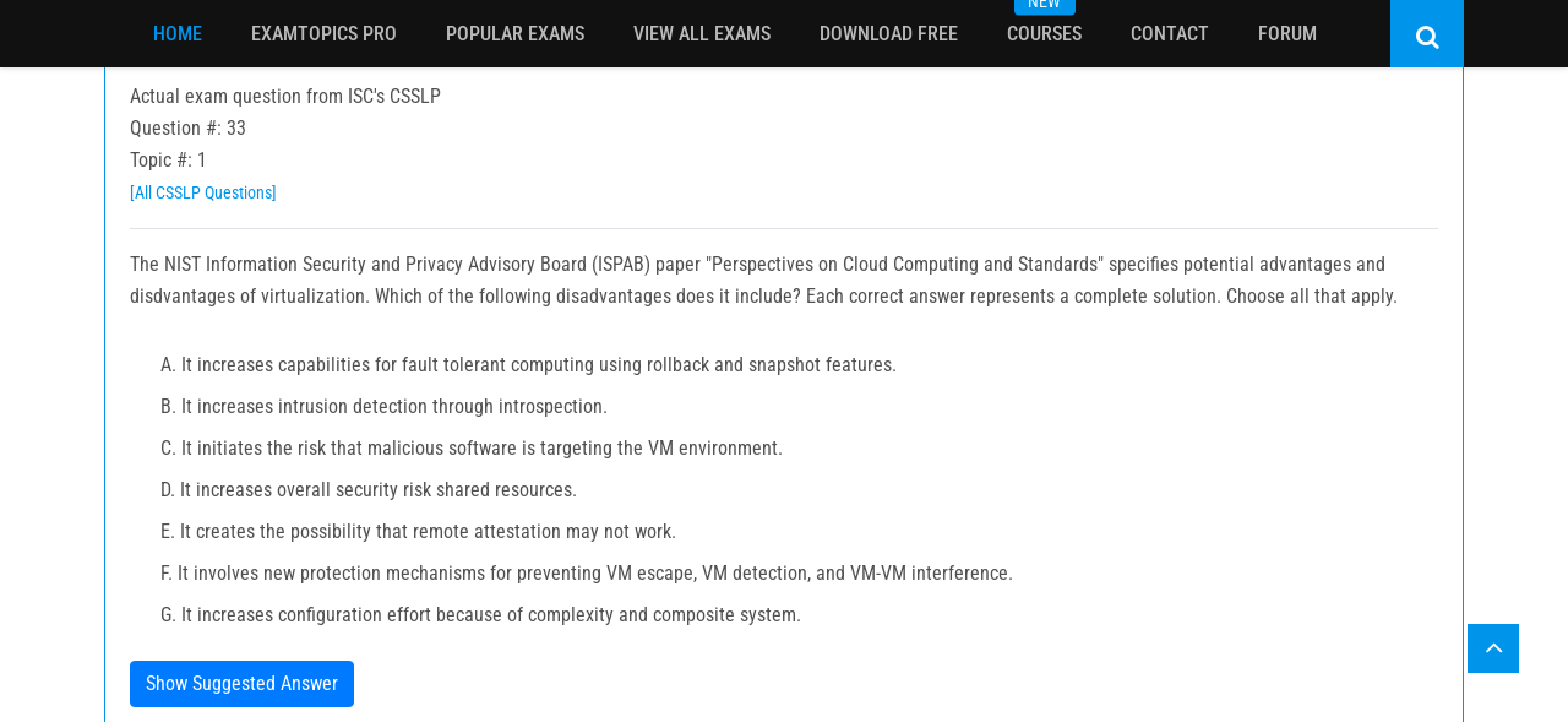
Which of the following methods determines the principle name of the current user and returns the jav a.security.Principal object in the HttpServletRequest interface?

A. getUserPrincipal()

B. isUserInRole()

C. getRemoteUser()

D. getCallerPrincipal()



Actual exam question from ISC's CSSLP

Question #: 33

Topic #: 1

[All CSSLP Questions]

The NIST Information Security and Privacy Advisory Board (ISPAB) paper "Perspectives on Cloud Computing and Standards" specifies potential advantages and disdvantages of virtualization. Which of the following disadvantages does it include? Each correct answer represents a complete solution. Choose all that apply.

A. It increases capabilities for fault tolerant computing using rollback and snapshot features.

B. It increases intrusion detection through introspection.

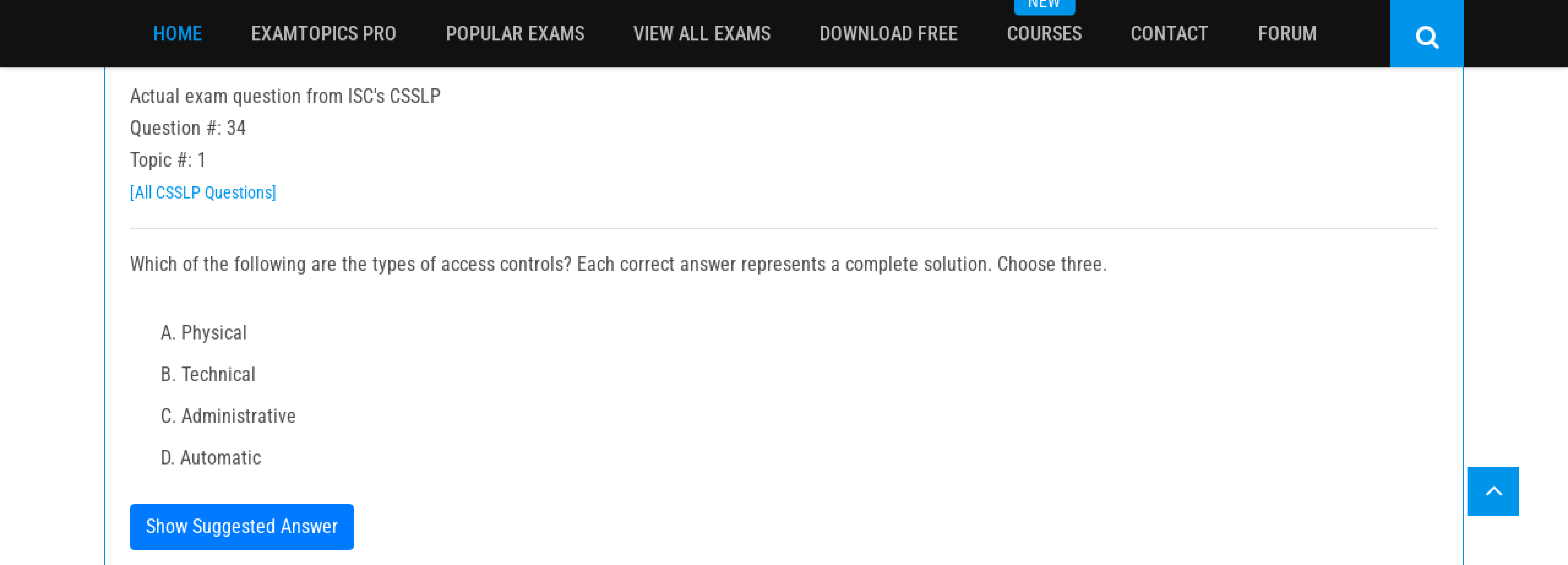
C. It initiates the risk that malicious software is targeting the VM environment.

D. It increases overall security risk shared resources.

E. It creates the possibility that remote attestation may not work.

F. It involves new protection mechanisms for preventing VM escape, VM detection, and VM-VM interference.

G. It increases configuration effort because of complexity and composite system.



Actual exam question from ISC's CSSLP

Question #: 34

Topic #: 1

[All CSSLP Questions]

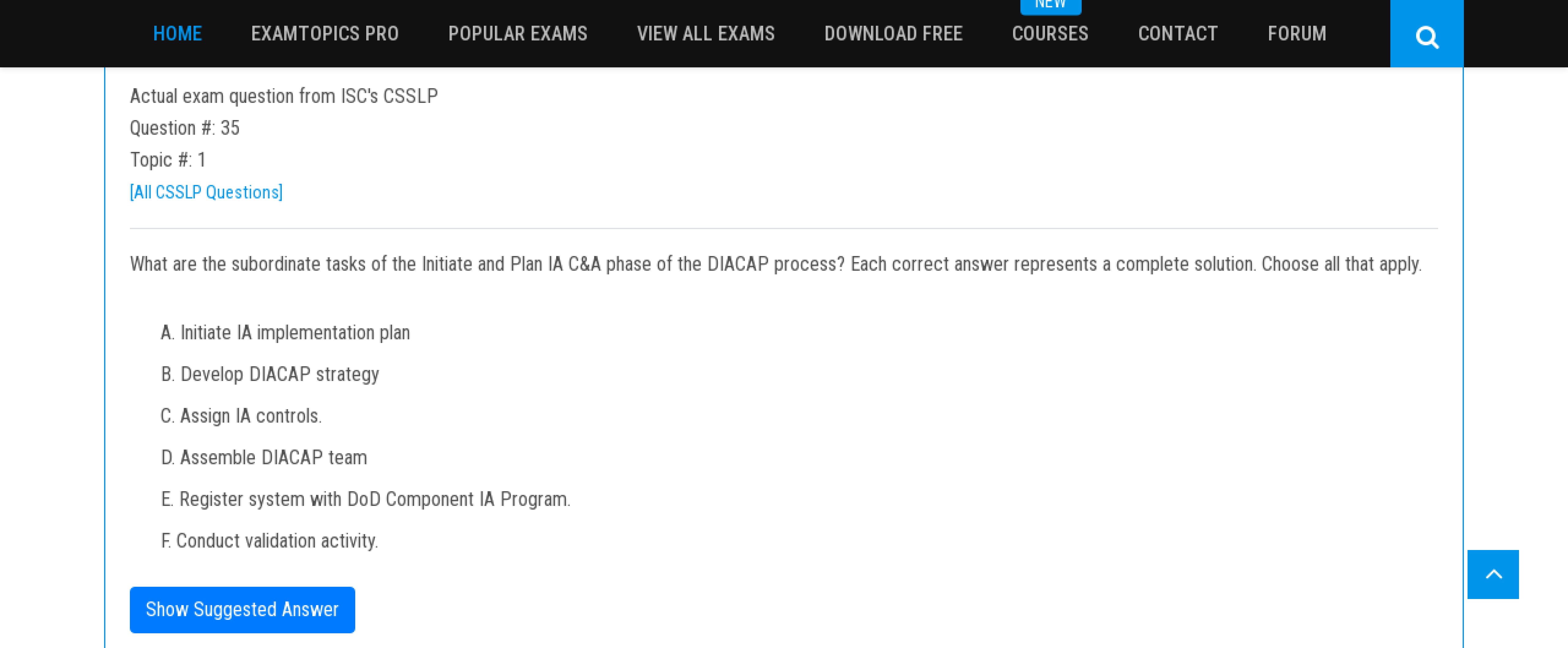
Which of the following are the types of access controls? Each correct answer represents a complete solution. Choose three.

A. Physical

B. Technical

C. Administrative

D. Automatic



Actual exam question from ISC's CSSLP

Question #: 35

Topic #: 1

[All CSSLP Questions]

What are the subordinate tasks of the Initiate and Plan IA C&A phase of the DIACAP process? Each correct answer represents a complete solution. Choose all that apply.

A. Initiate IA implementation plan

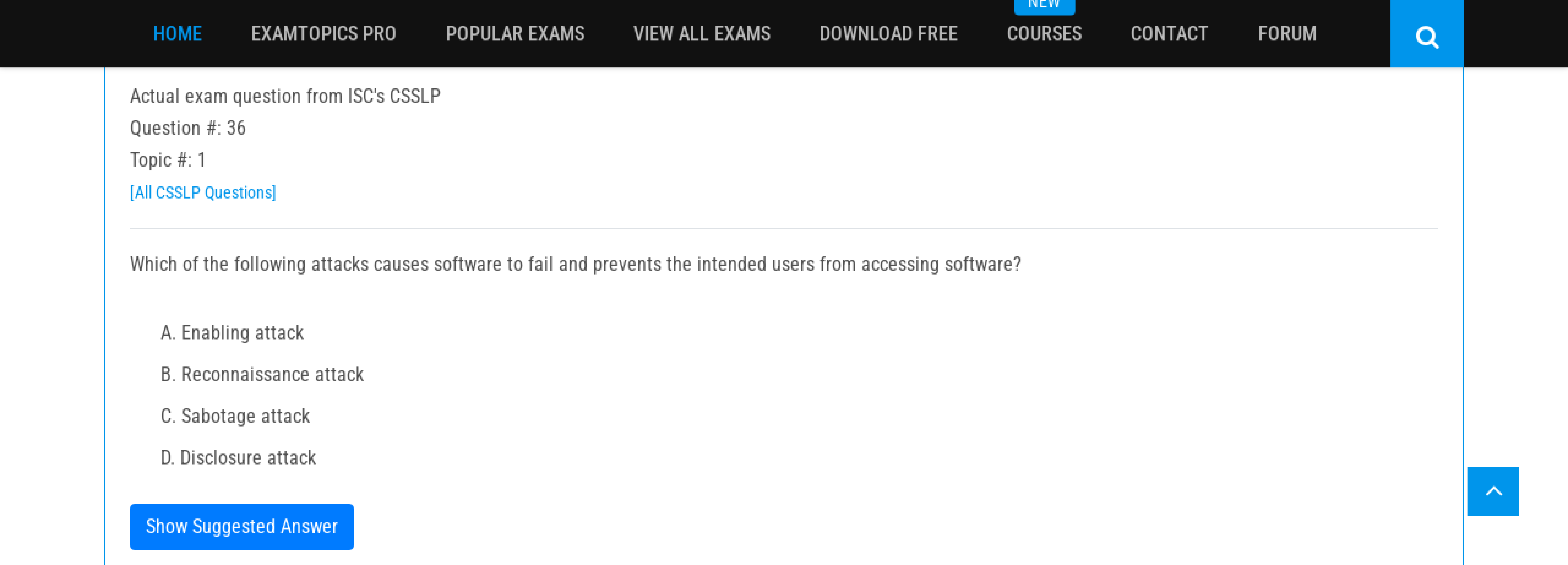
B. Develop DIACAP strategy

C. Assign IA controls.

D. Assemble DIACAP team

E. Register system with DoD Component IA Program.

F. Conduct validation activity.



Actual exam question from ISC's CSSLP

Question #: 36

Topic #: 1

[All CSSLP Questions]

Which of the following attacks causes software to fail and prevents the intended users from accessing software?

A. Enabling attack

B. Reconnaissance attack

C. Sabotage attack

D. Disclosure attack

Show Suggested Answer

Actual exam question from ISC's CSSLP
Question #: 37
Topic #: 1
[All CSSLP Questions]

FITSAF stands for Federal Information Technology Security Assessment Framework. It is a methodology for assessing the security of information systems. Which of the following FITSAF levels shows that the procedures and controls have been implemented?

A. Level 2

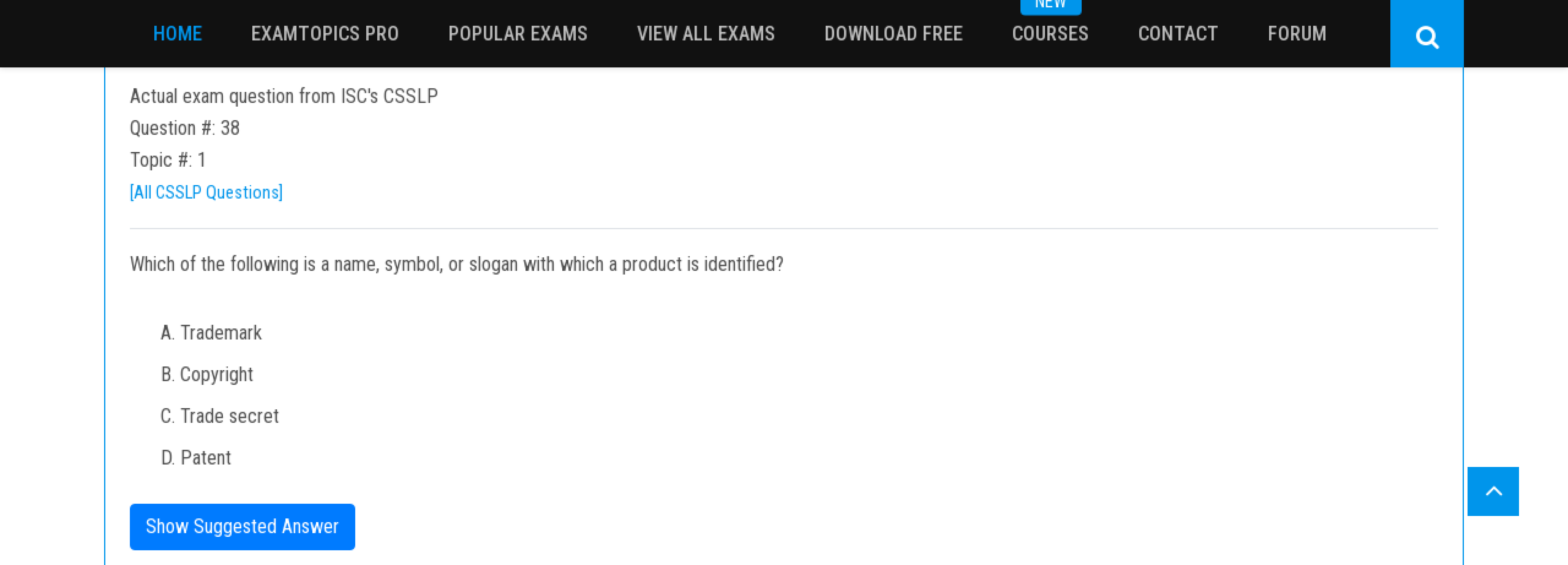
B. Level 3

C. Level 5

D. Level 1

E. Level 4

Show Suggested Answer



Actual exam question from ISC's CSSLP

Question #: 38

Topic #: 1

[All CSSLP Questions]

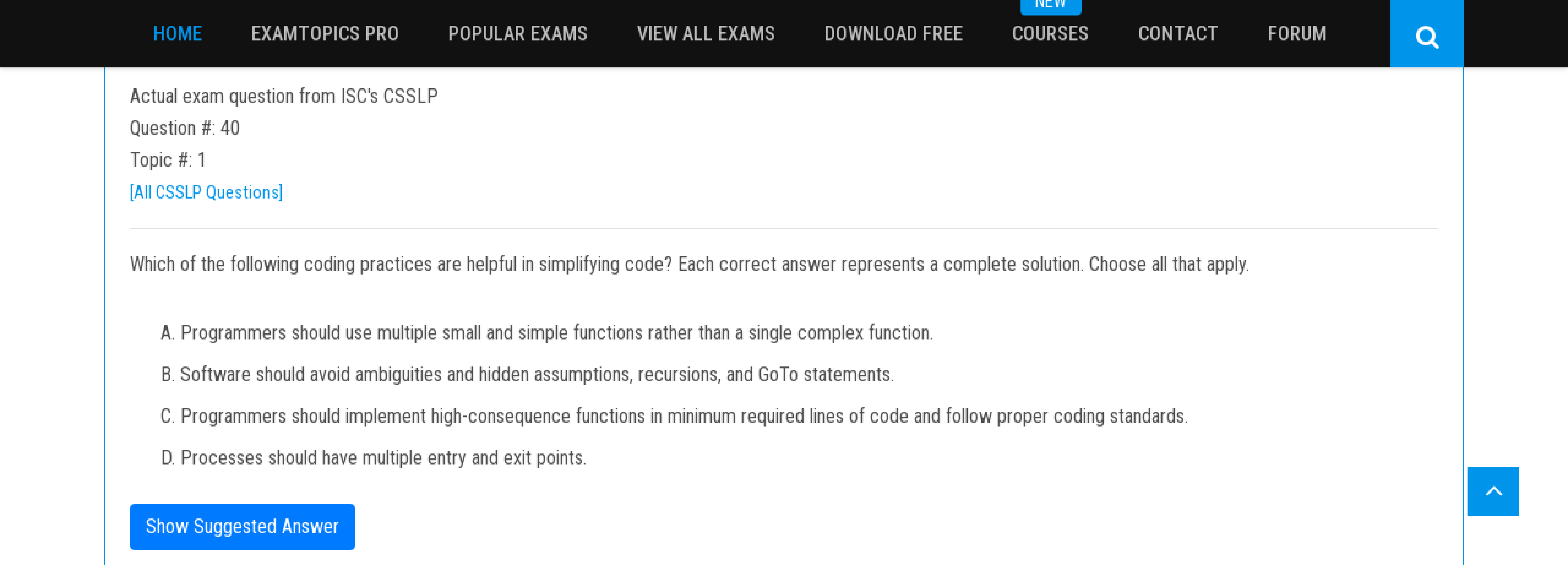
Which of the following is a name, symbol, or slogan with which a product is identified?

A. Trademark

B. Copyright

C. Trade secret

D. Patent



Actual exam question from ISC's CSSLP

Question #: 40

Topic #: 1

[All CSSLP Questions]

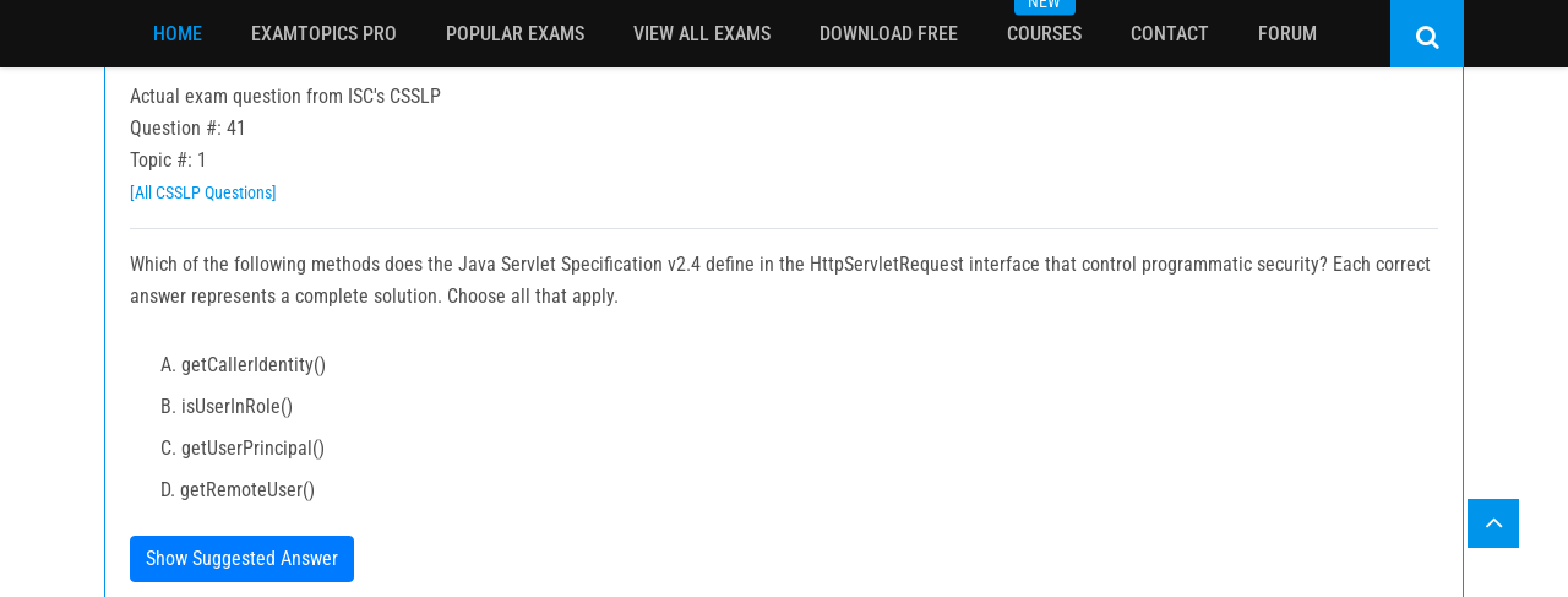
Which of the following coding practices are helpful in simplifying code? Each correct answer represents a complete solution. Choose all that apply.

A. Programmers should use multiple small and simple functions rather than a single complex function.

B. Software should avoid ambiguities and hidden assumptions, recursions, and GoTo statements.

C. Programmers should implement high-consequence functions in minimum required lines of code and follow proper coding standards.

D. Processes should have multiple entry and exit points.



Actual exam question from ISC's CSSLP

Question #: 41

Topic #: 1

[All CSSLP Questions]

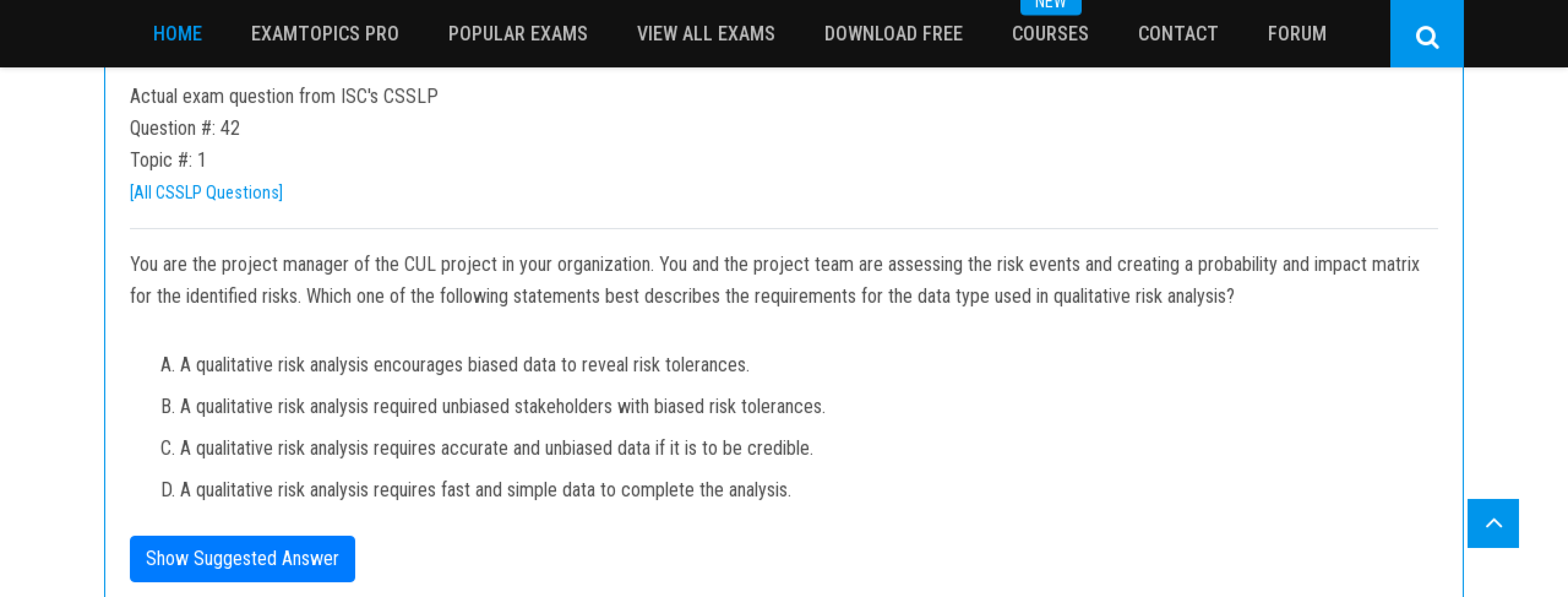
Which of the following methods does the Java Servlet Specification v2.4 define in the HttpServletRequest interface that control programmatic security? Each correct answer represents a complete solution. Choose all that apply.

A. getCallerIdentity()

B. isUserInRole()

C. getUserPrincipal()

D. getRemoteUser()



Actual exam question from ISC's CSSLP
Question #: 42
Topic #: 1
[All CSSLP Questions]

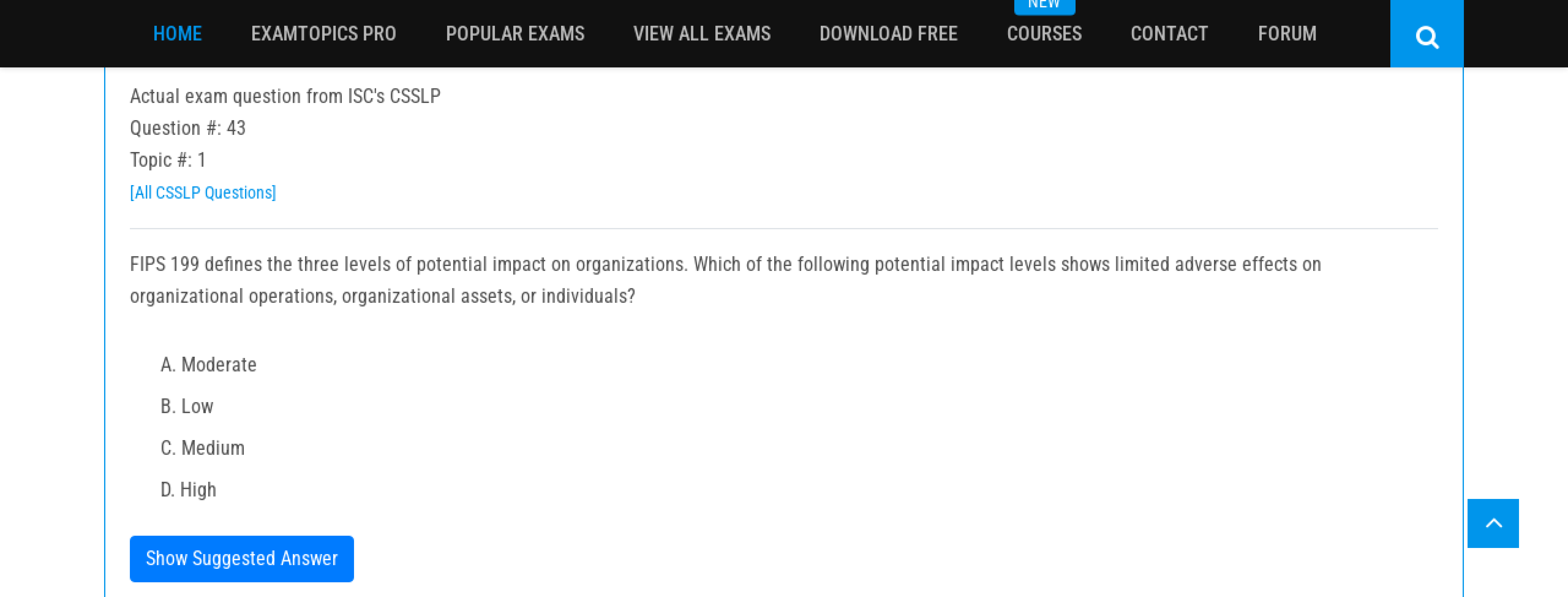
You are the project manager of the CUL project in your organization. You and the project team are assessing the risk events and creating a probability and impact matrix for the identified risks. Which one of the following statements best describes the requirements for the data type used in qualitative risk analysis?

A. A qualitative risk analysis encourages biased data to reveal risk tolerances.

B. A qualitative risk analysis required unbiased stakeholders with biased risk tolerances.

C. A qualitative risk analysis requires accurate and unbiased data if it is to be credible.

D. A qualitative risk analysis requires fast and simple data to complete the analysis.



Actual exam question from ISC's CSSLP

Question #: 43

Topic #: 1

[All CSSLP Questions]

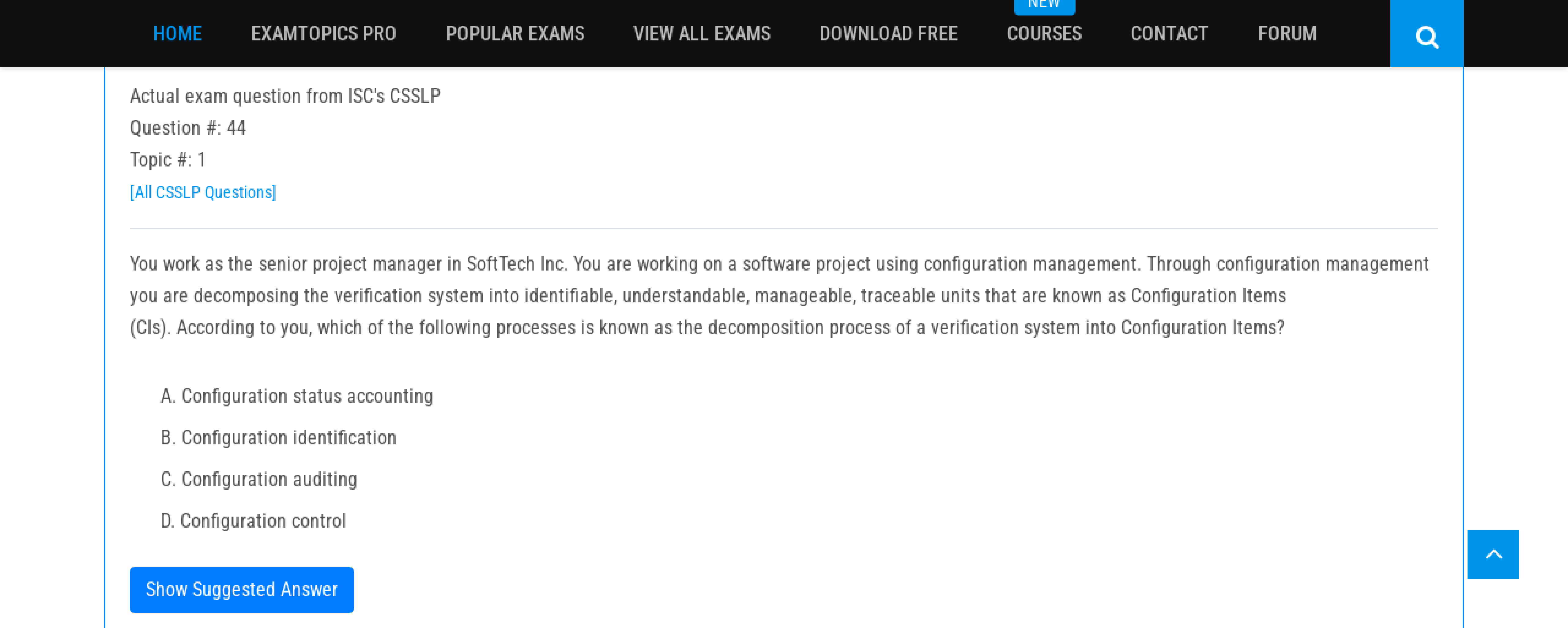
FIPS 199 defines the three levels of potential impact on organizations. Which of the following potential impact levels shows limited adverse effects on organizational operations, organizational assets, or individuals?

A. Moderate

B. Low

C. Medium

D. High



Actual exam question from ISC's CSSLP

Question #: 44

Topic #: 1

[All CSSLP Questions]

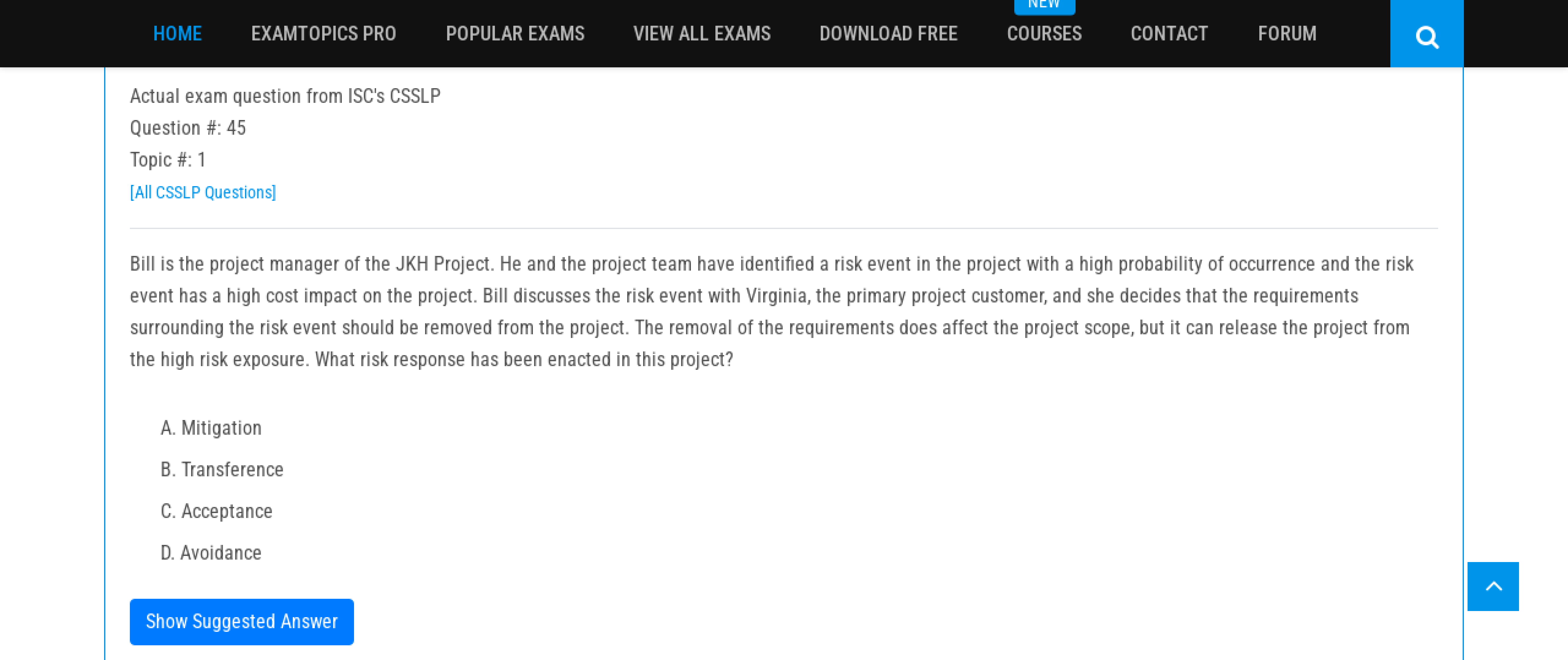
You work as the senior project manager in SoftTech Inc. You are working on a software project using configuration management. Through configuration management you are decomposing the verification system into identifiable, understandable, manageable, traceable units that are known as Configuration Items (CIs). According to you, which of the following processes is known as the decomposition process of a verification system into Configuration Items?

A. Configuration status accounting

B. Configuration identification

C. Configuration auditing

D. Configuration control



Actual exam question from ISC's CSSLP

Question #: 45

Topic #: 1

[All CSSLP Questions]

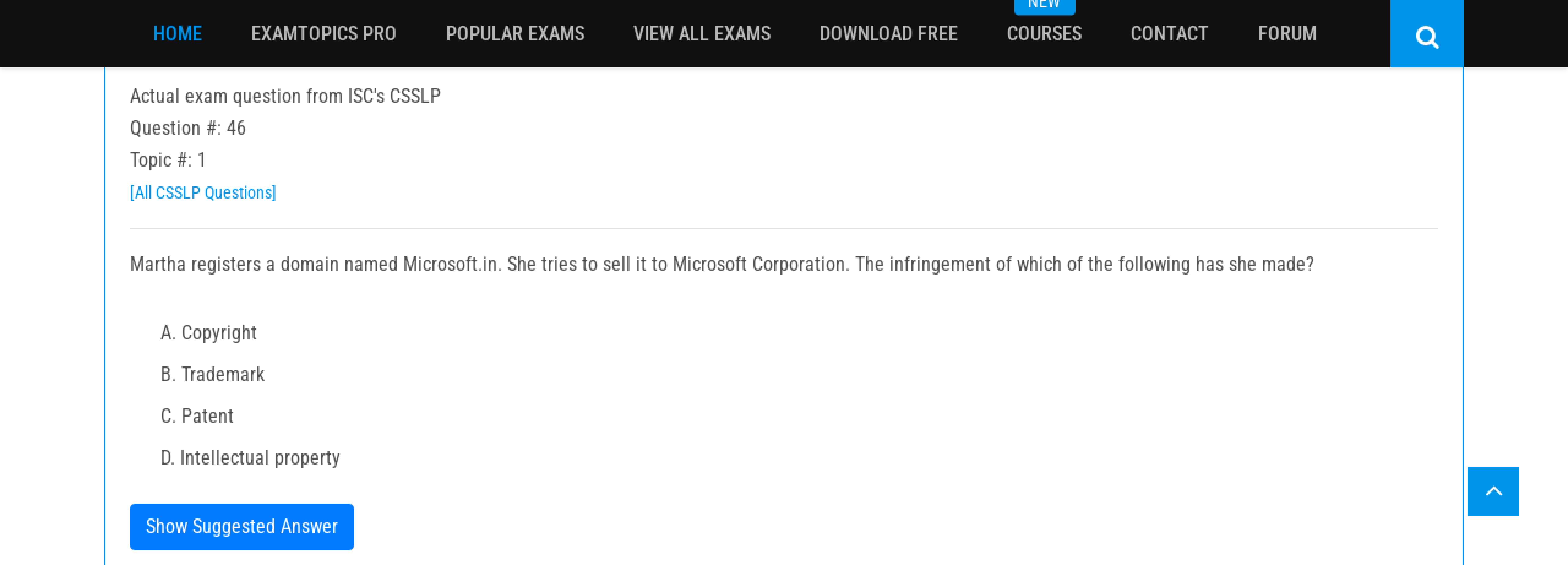
Bill is the project manager of the JKH Project. He and the project team have identified a risk event in the project with a high probability of occurrence and the risk event has a high cost impact on the project. Bill discusses the risk event with Virginia, the primary project customer, and she decides that the requirements surrounding the risk event should be removed from the project. The removal of the requirements does affect the project scope, but it can release the project from the high risk exposure. What risk response has been enacted in this project?

A. Mitigation

B. Transference

C. Acceptance

D. Avoidance



Actual exam question from ISC's CSSLP

Question #: 46

Topic #: 1

[All CSSLP Questions]

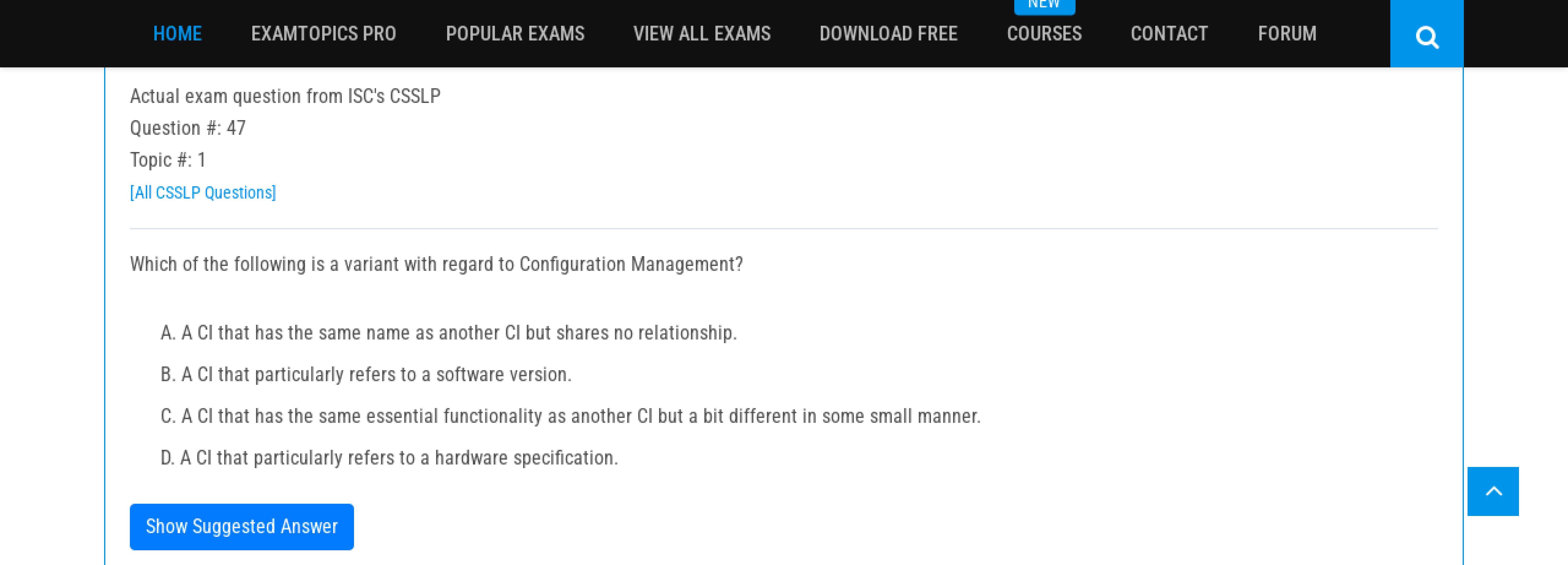
Martha registers a domain named Microsoft.in. She tries to sell it to Microsoft Corporation. The infringement of which of the following has she made?

A. Copyright

B. Trademark

C. Patent

D. Intellectual property



Actual exam question from ISC's CSSLP

Question #: 47

Topic #: 1

[All CSSLP Questions]

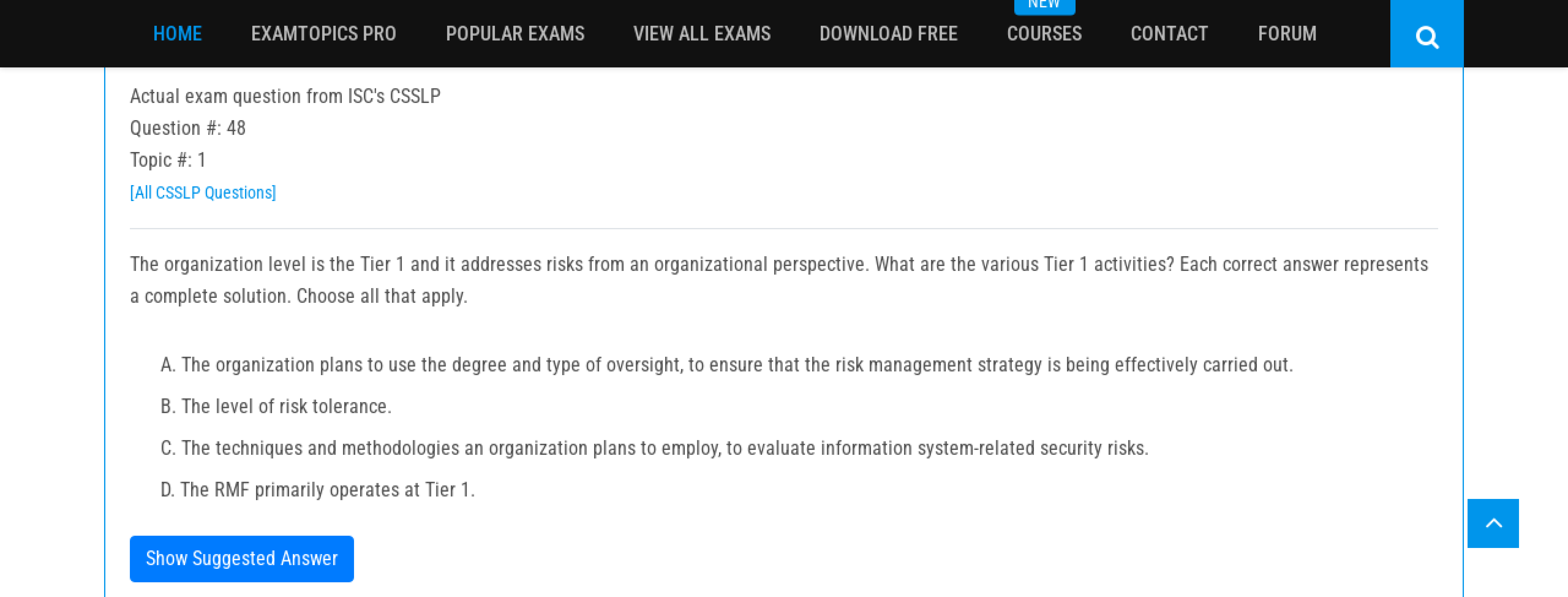
Which of the following is a variant with regard to Configuration Management?

A. A CI that has the same name as another CI but shares no relationship.

B. A CI that particularly refers to a software version.

C. A CI that has the same essential functionality as another CI but a bit different in some small manner.

D. A CI that particularly refers to a hardware specification.



Actual exam question from ISC's CSSLP

Question #: 48

Topic #: 1

[All CSSLP Questions]

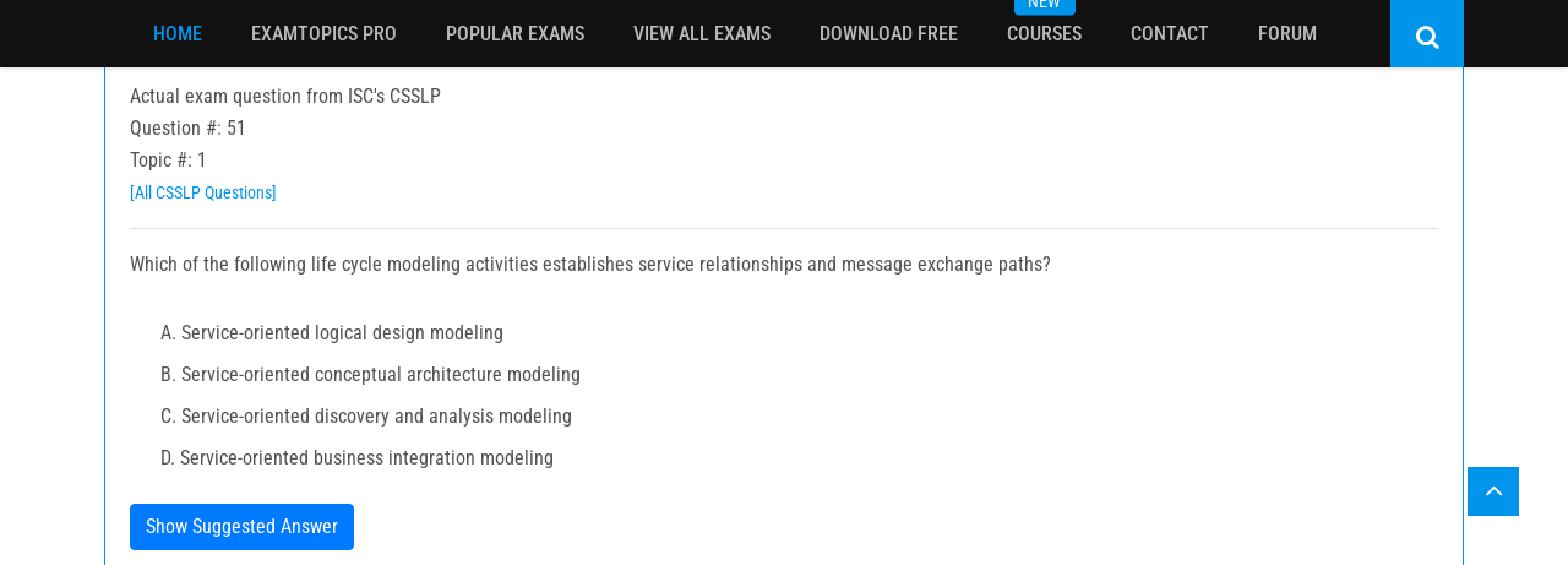
The organization level is the Tier 1 and it addresses risks from an organizational perspective. What are the various Tier 1 activities? Each correct answer represents a complete solution. Choose all that apply.

A. The organization plans to use the degree and type of oversight, to ensure that the risk management strategy is being effectively carried out.

B. The level of risk tolerance.

C. The techniques and methodologies an organization plans to employ, to evaluate information system-related security risks.

D. The RMF primarily operates at Tier 1.



Actual exam question from ISC's CSSLP

Question #: 51

Topic #: 1

[All CSSLP Questions]

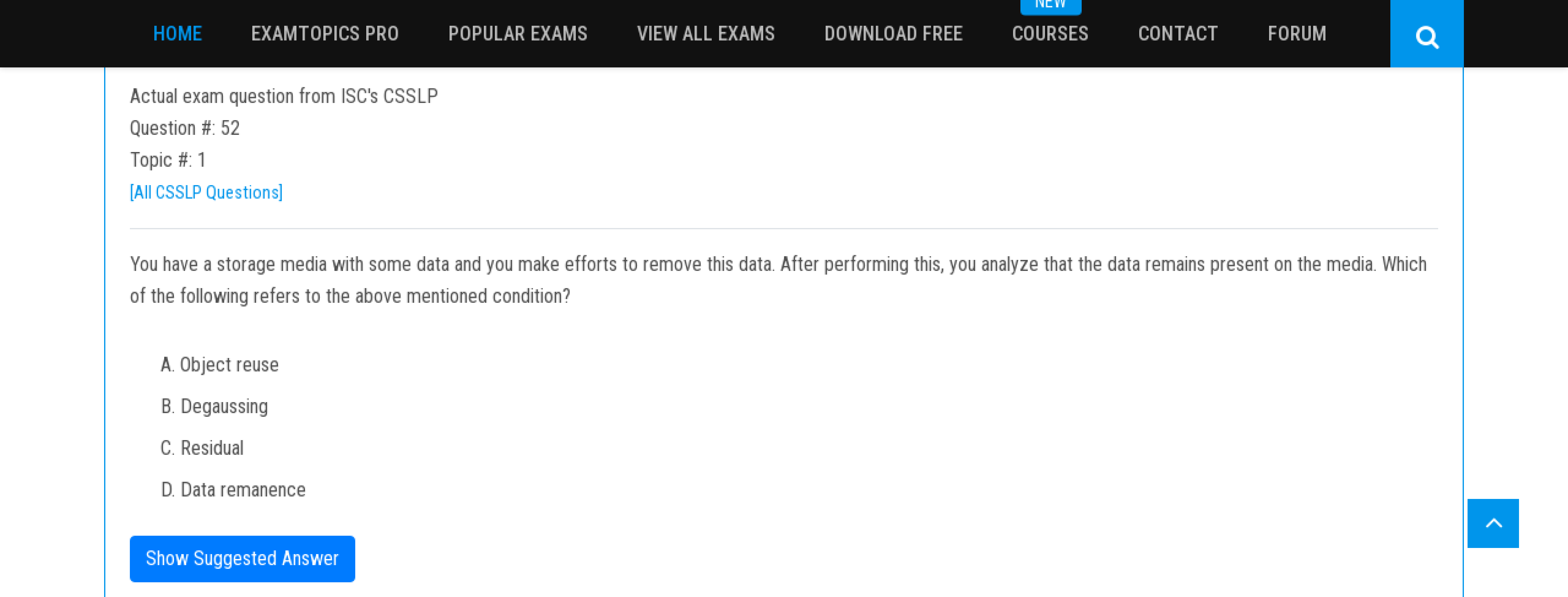
Which of the following life cycle modeling activities establishes service relationships and message exchange paths?

A. Service-oriented logical design modeling

B. Service-oriented conceptual architecture modeling

C. Service-oriented discovery and analysis modeling

D. Service-oriented business integration modeling



Actual exam question from ISC's CSSLP
Question #: 52
Topic #: 1
[All CSSLP Questions]

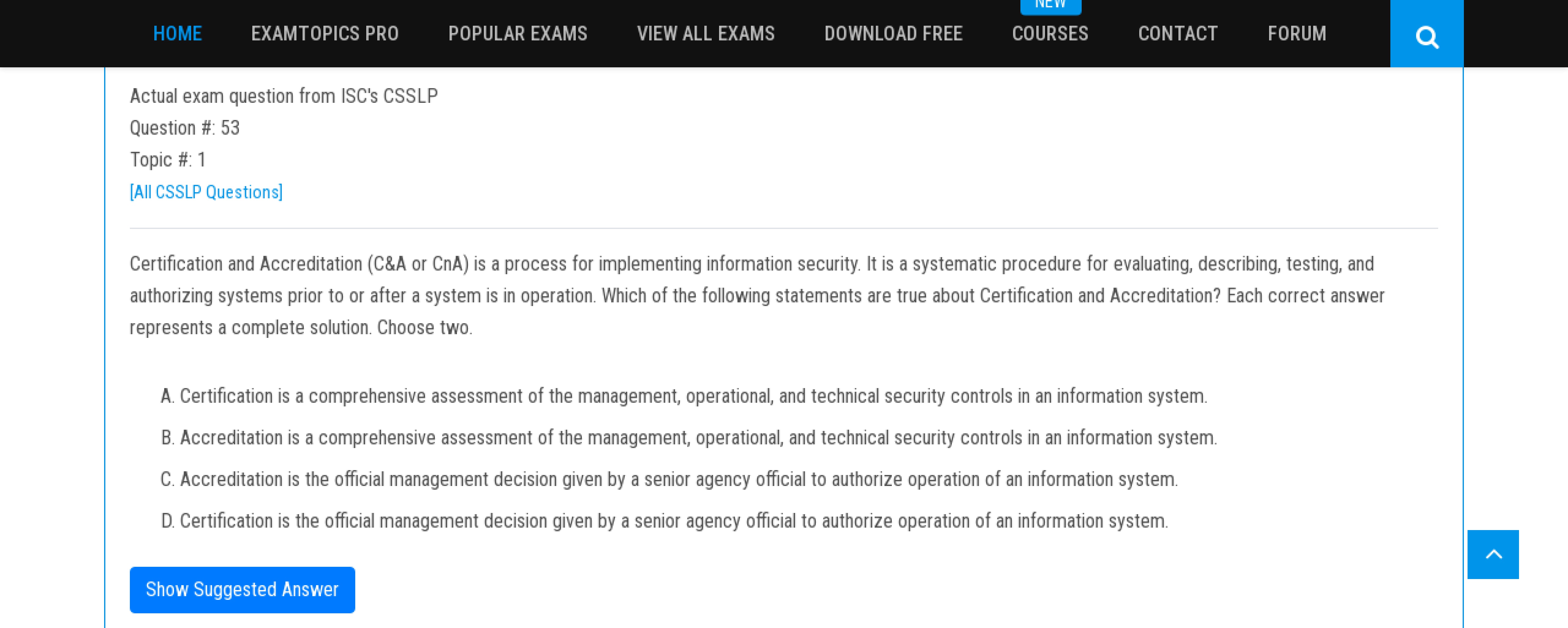
You have a storage media with some data and you make efforts to remove this data. After performing this, you analyze that the data remains present on the media. Which of the following refers to the above mentioned condition?

A. Object reuse

B. Degaussing

C. Residual

D. Data remanence



Actual exam question from ISC's CSSLP

Question #: 53

Topic #: 1

[All CSSLP Questions]

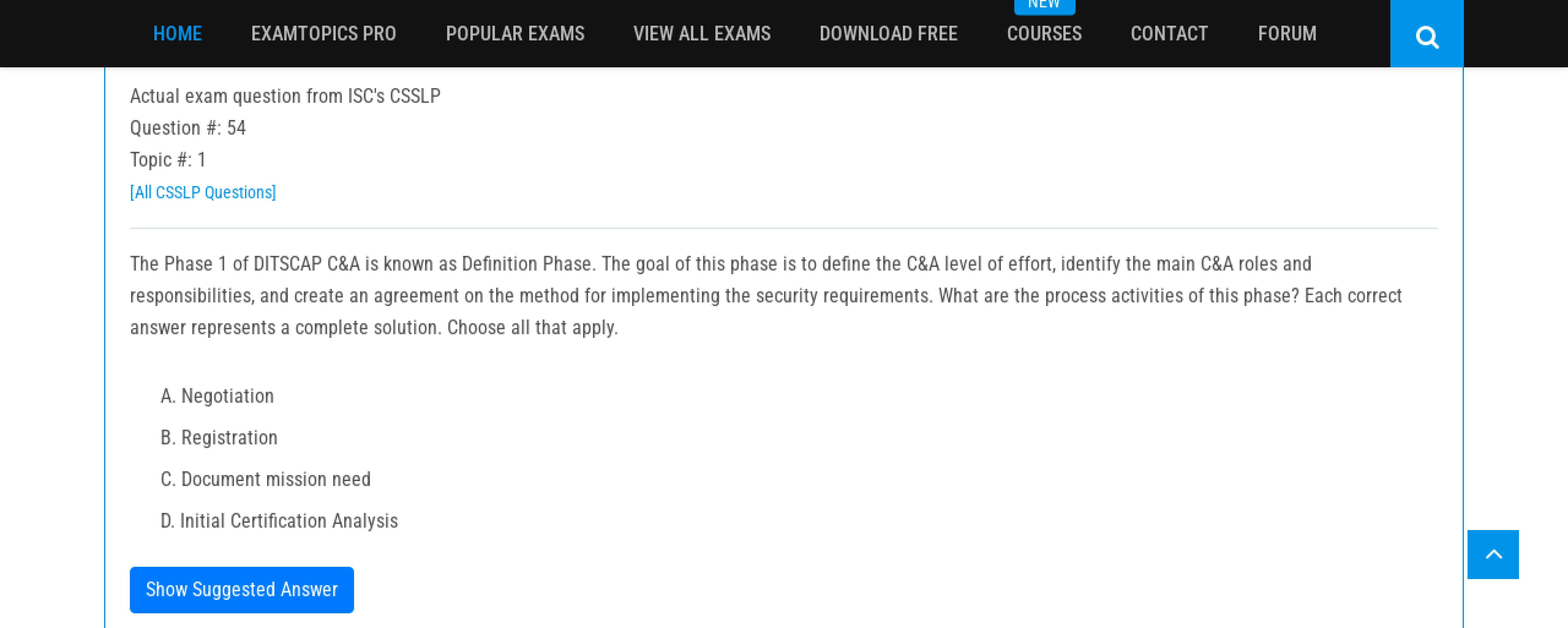
Certification and Accreditation (C&A or CnA) is a process for implementing information security. It is a systematic procedure for evaluating, describing, testing, and authorizing systems prior to or after a system is in operation. Which of the following statements are true about Certification and Accreditation? Each correct answer represents a complete solution. Choose two.

A. Certification is a comprehensive assessment of the management, operational, and technical security controls in an information system.

B. Accreditation is a comprehensive assessment of the management, operational, and technical security controls in an information system.

C. Accreditation is the official management decision given by a senior agency official to authorize operation of an information system.

D. Certification is the official management decision given by a senior agency official to authorize operation of an information system.



Actual exam question from ISC's CSSLP

Question #: 54

Topic #: 1

[All CSSLP Questions]

The Phase 1 of DITSCAP C&A is known as Definition Phase. The goal of this phase is to define the C&A level of effort, identify the main C&A roles and responsibilities, and create an agreement on the method for implementing the security requirements. What are the process activities of this phase? Each correct answer represents a complete solution. Choose all that apply.

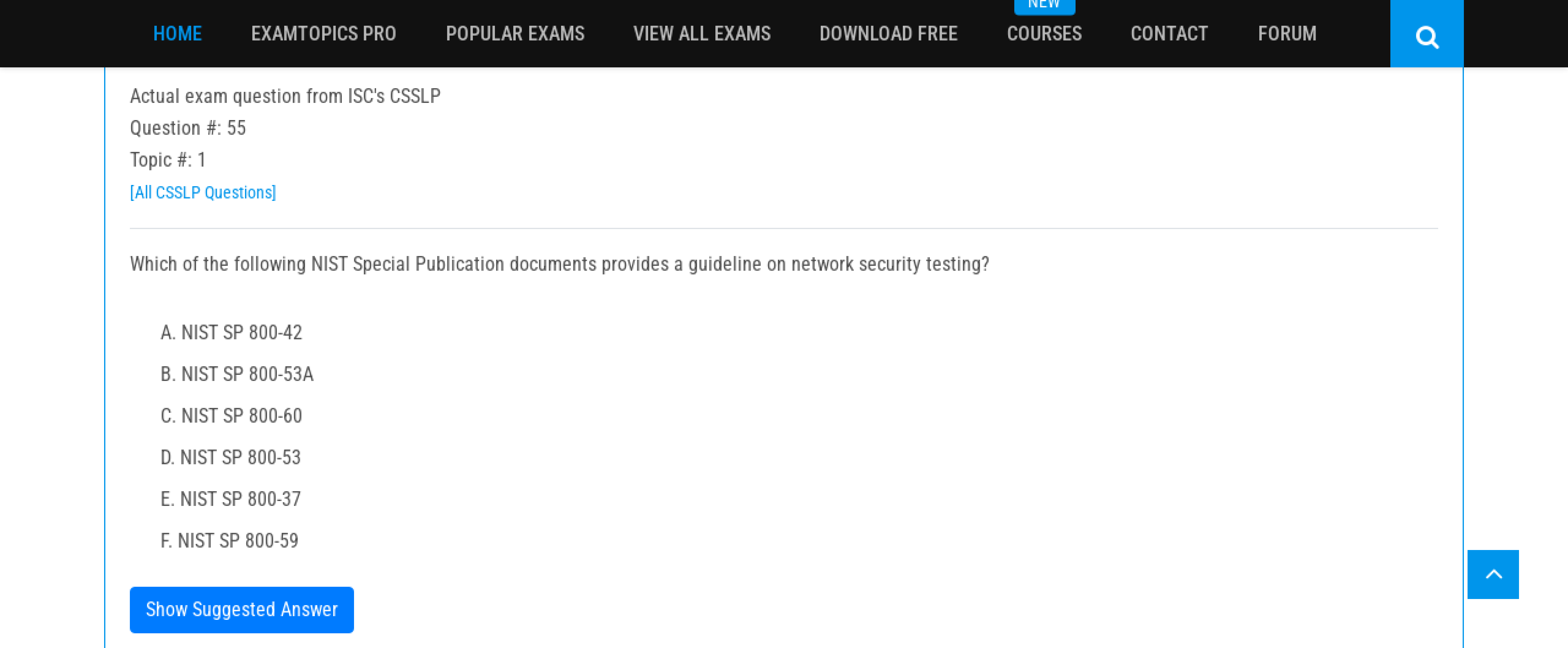
A. Negotiation

B. Registration

C. Document mission need

D. Initial Certification Analysis

Show Suggested Answer



Actual exam question from ISC's CSSLP

Question #: 55

Topic #: 1

[All CSSLP Questions]

Which of the following NIST Special Publication documents provides a guideline on network security testing?

A. NIST SP 800-42

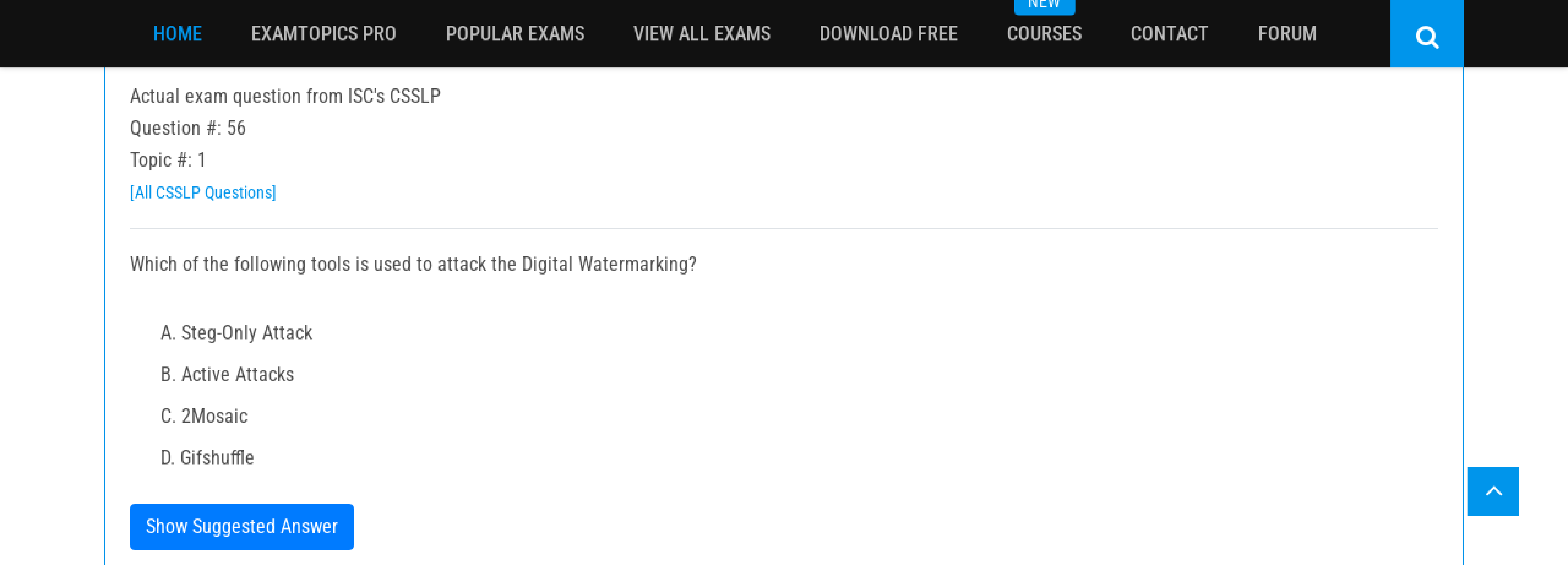
B. NIST SP 800-53A

C. NIST SP 800-60

D. NIST SP 800-53

E. NIST SP 800-37

F. NIST SP 800-59



Actual exam question from ISC's CSSLP

Question #: 56

Topic #: 1

[All CSSLP Questions]

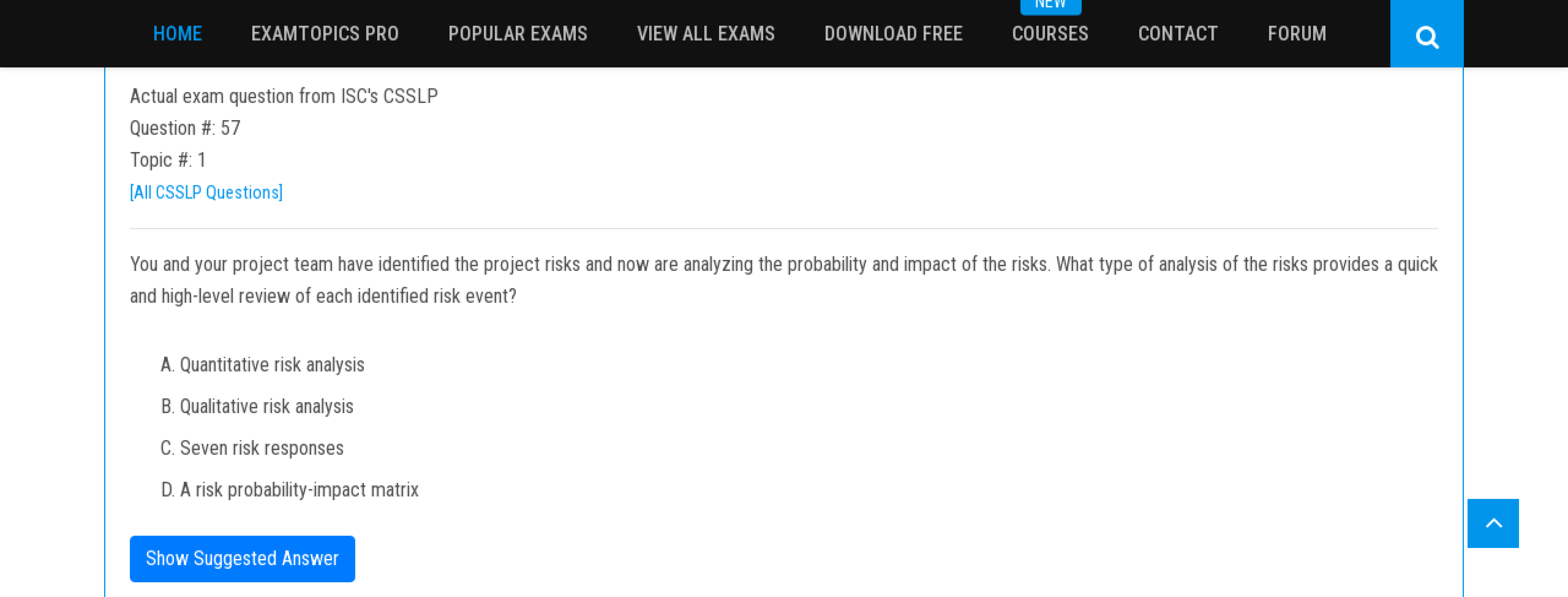
Which of the following tools is used to attack the Digital Watermarking?

A. Steg-Only Attack

B. Active Attacks

C. 2Mosaic

D. Gifshuffle



Actual exam question from ISC's CSSLP

Question #: 57

Topic #: 1

[All CSSLP Questions]

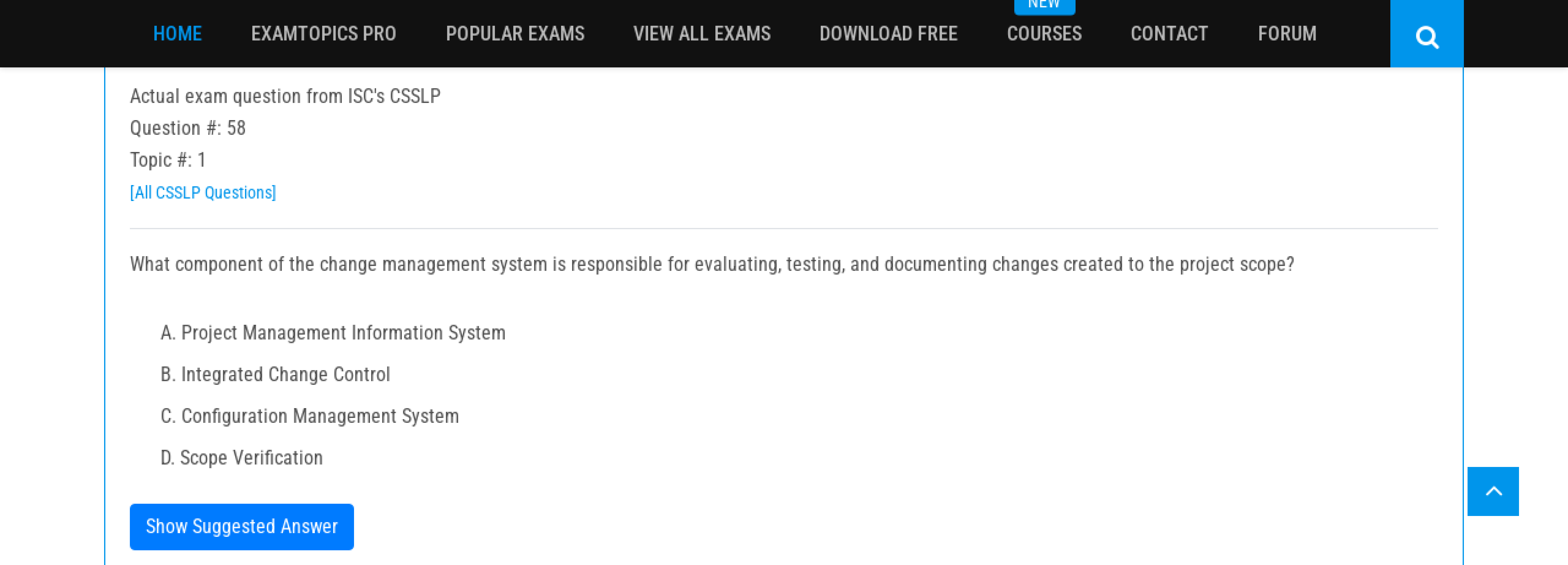
You and your project team have identified the project risks and now are analyzing the probability and impact of the risks. What type of analysis of the risks provides a quick and high-level review of each identified risk event?

A. Quantitative risk analysis

B. Qualitative risk analysis

C. Seven risk responses

D. A risk probability-impact matrix



Actual exam question from ISC's CSSLP

Question #: 58

Topic #: 1

[All CSSLP Questions]

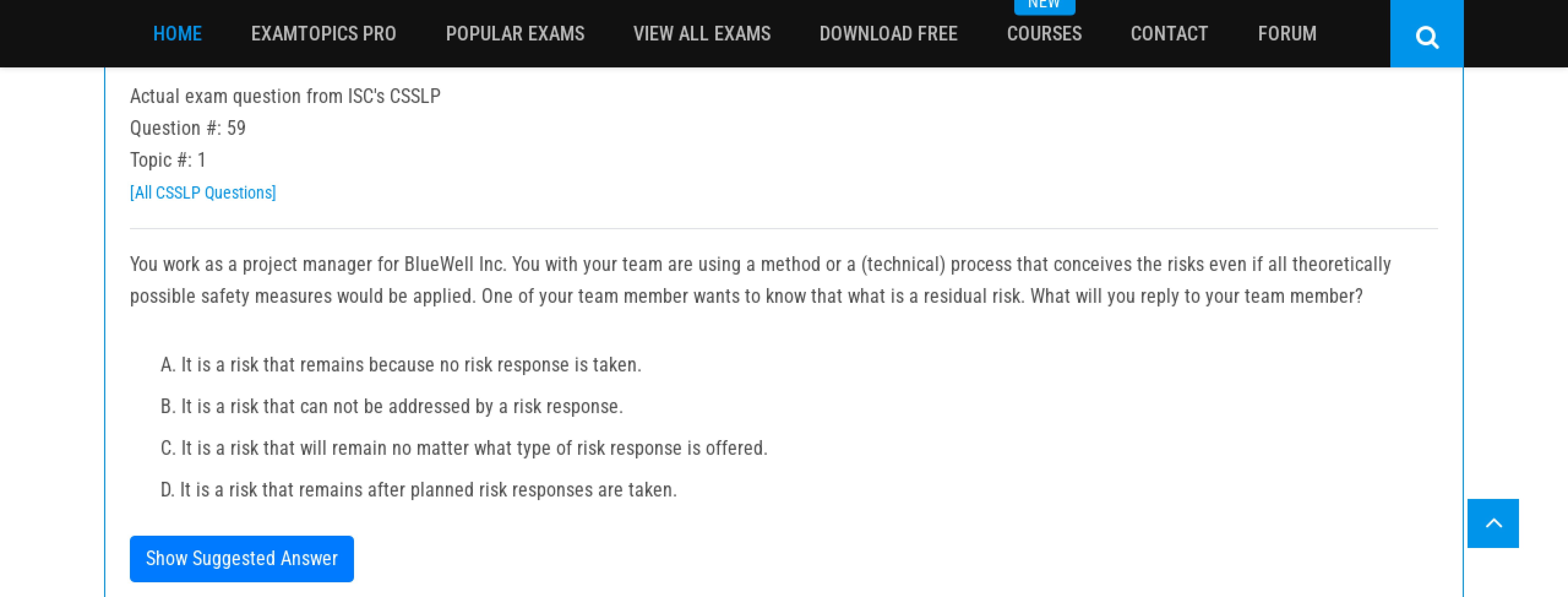
What component of the change management system is responsible for evaluating, testing, and documenting changes created to the project scope?

A. Project Management Information System

B. Integrated Change Control

C. Configuration Management System

D. Scope Verification



Actual exam question from ISC's CSSLP

Question #: 59

Topic #: 1

[All CSSLP Questions]

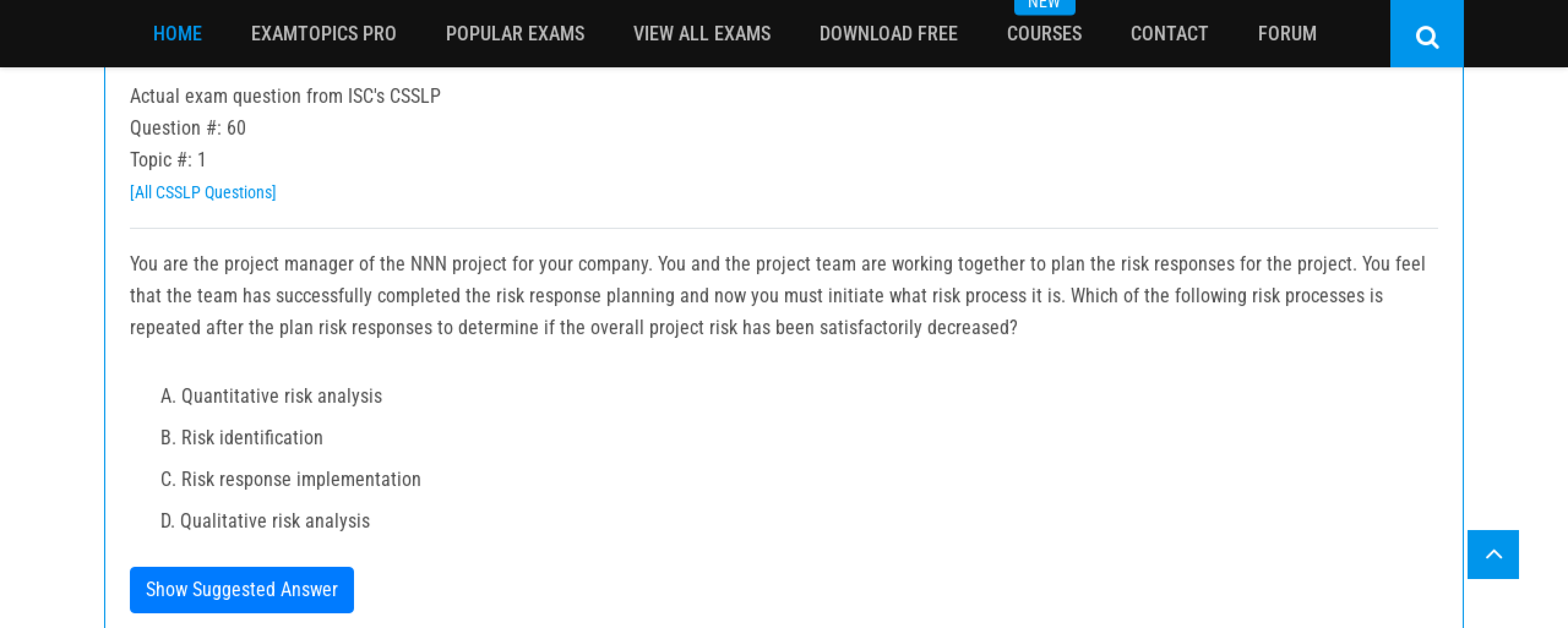
You work as a project manager for BlueWell Inc. You with your team are using a method or a (technical) process that conceives the risks even if all theoretically possible safety measures would be applied. One of your team member wants to know that what is a residual risk. What will you reply to your team member?

A. It is a risk that remains because no risk response is taken.

B. It is a risk that can not be addressed by a risk response.

C. It is a risk that will remain no matter what type of risk response is offered.

D. It is a risk that remains after planned risk responses are taken.



Actual exam question from ISC's CSSLP

Question #: 60

Topic #: 1

[All CSSLP Questions]

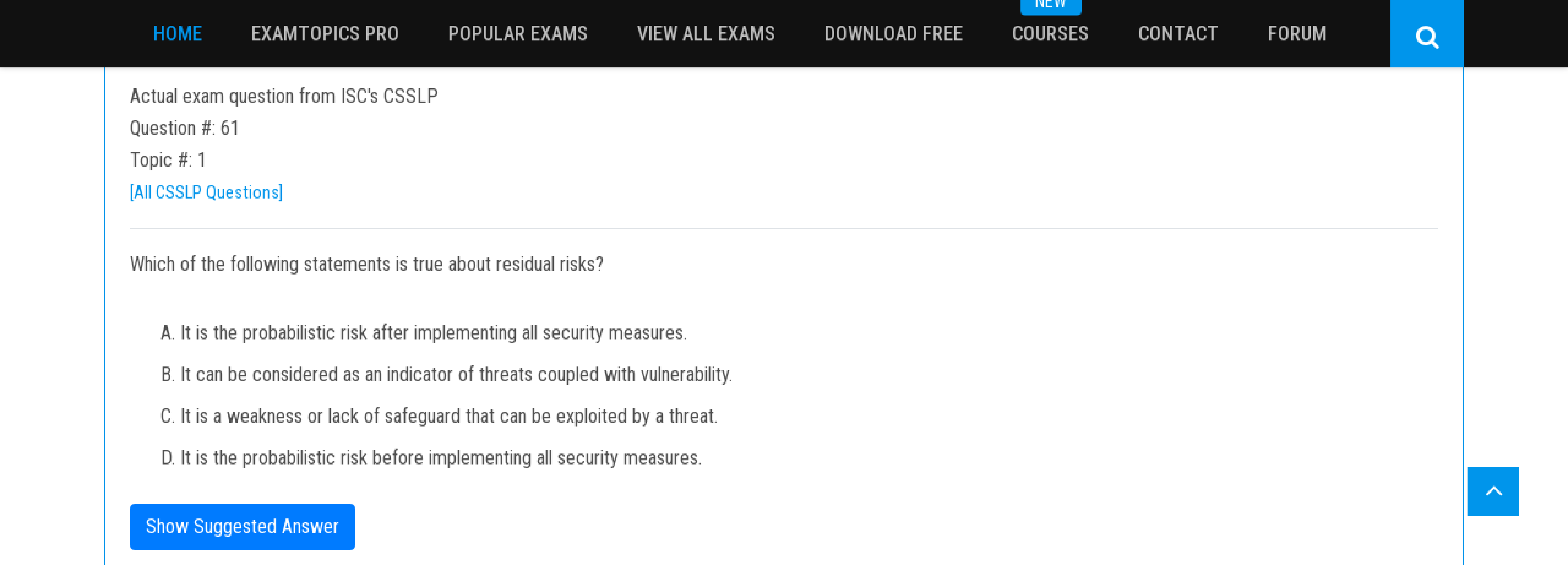
You are the project manager of the NNN project for your company. You and the project team are working together to plan the risk responses for the project. You feel that the team has successfully completed the risk response planning and now you must initiate what risk process it is. Which of the following risk processes is repeated after the plan risk responses to determine if the overall project risk has been satisfactorily decreased?

A. Quantitative risk analysis

B. Risk identification

C. Risk response implementation

D. Qualitative risk analysis



Actual exam question from ISC's CSSLP

Question #: 61

Topic #: 1

[All CSSLP Questions]

Which of the following statements is true about residual risks?

A. It is the probabilistic risk after implementing all security measures.

B. It can be considered as an indicator of threats coupled with vulnerability.

C. It is a weakness or lack of safeguard that can be exploited by a threat.

D. It is the probabilistic risk before implementing all security measures.

Actual exam question from ISC's CSSLP

Question #: 62

Topic #: 1

[All CSSLP Questions]

To help review or design security controls, they can be classified by several criteria . One of these criteria is based on their nature. According to this criterion, which of the following controls consists of incident response processes, management oversight, security awareness, and training?

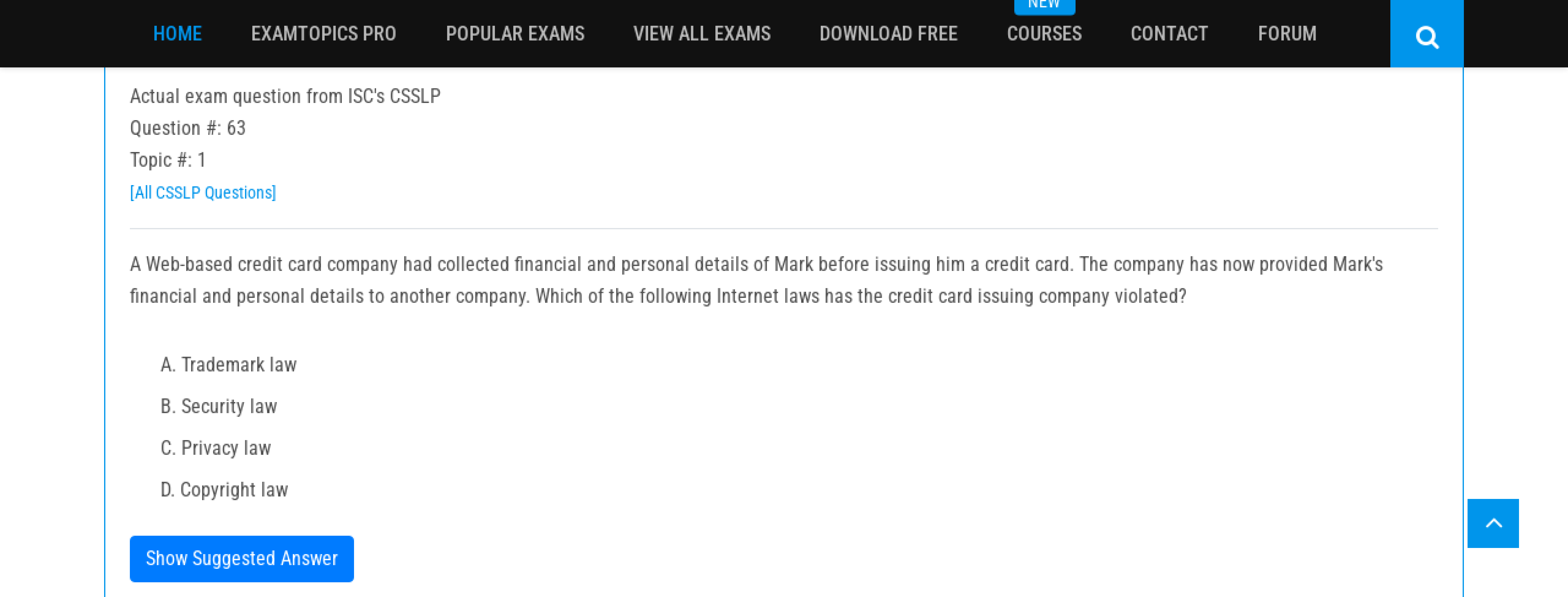
A. Compliance control

B. Physical control

C. Procedural control

D. Technical control

Show Suggested Answer



Actual exam question from ISC's CSSLP

Question #: 63

Topic #: 1

[All CSSLP Questions]

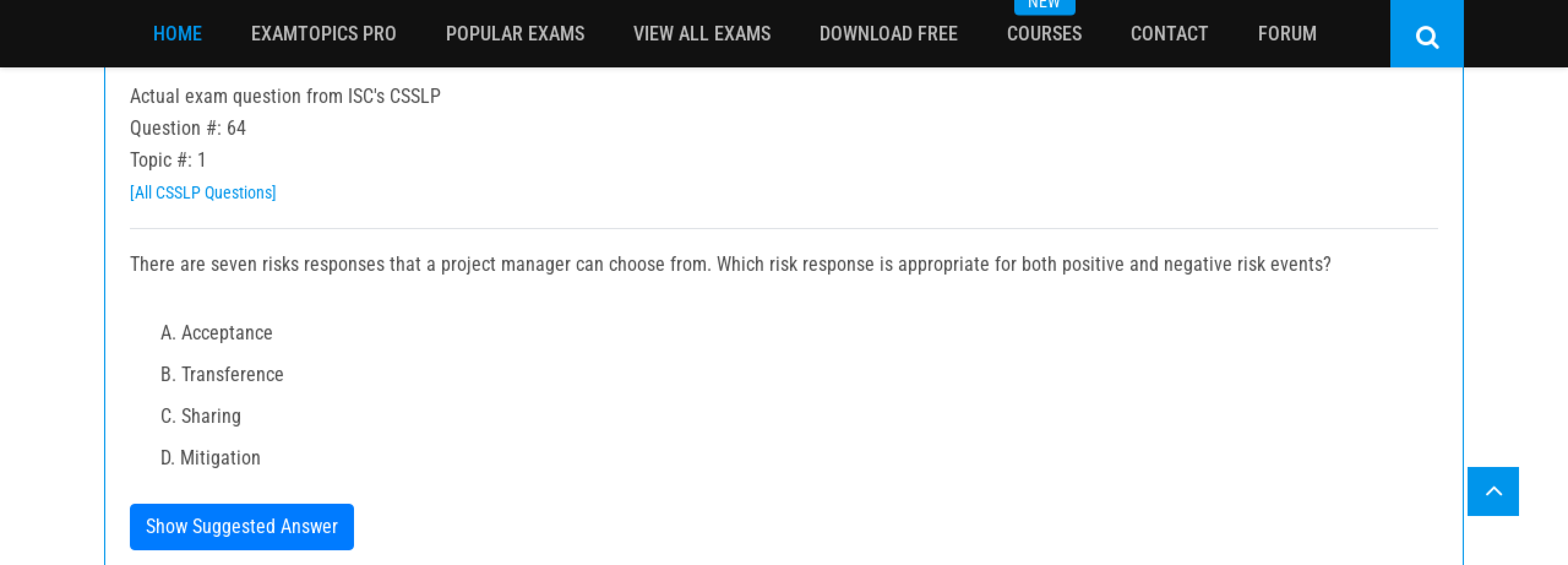
A Web-based credit card company had collected financial and personal details of Mark before issuing him a credit card. The company has now provided Mark's financial and personal details to another company. Which of the following Internet laws has the credit card issuing company violated?

A. Trademark law

B. Security law

C. Privacy law

D. Copyright law



Actual exam question from ISC's CSSLP

Question #: 64

Topic #: 1

[All CSSLP Questions]

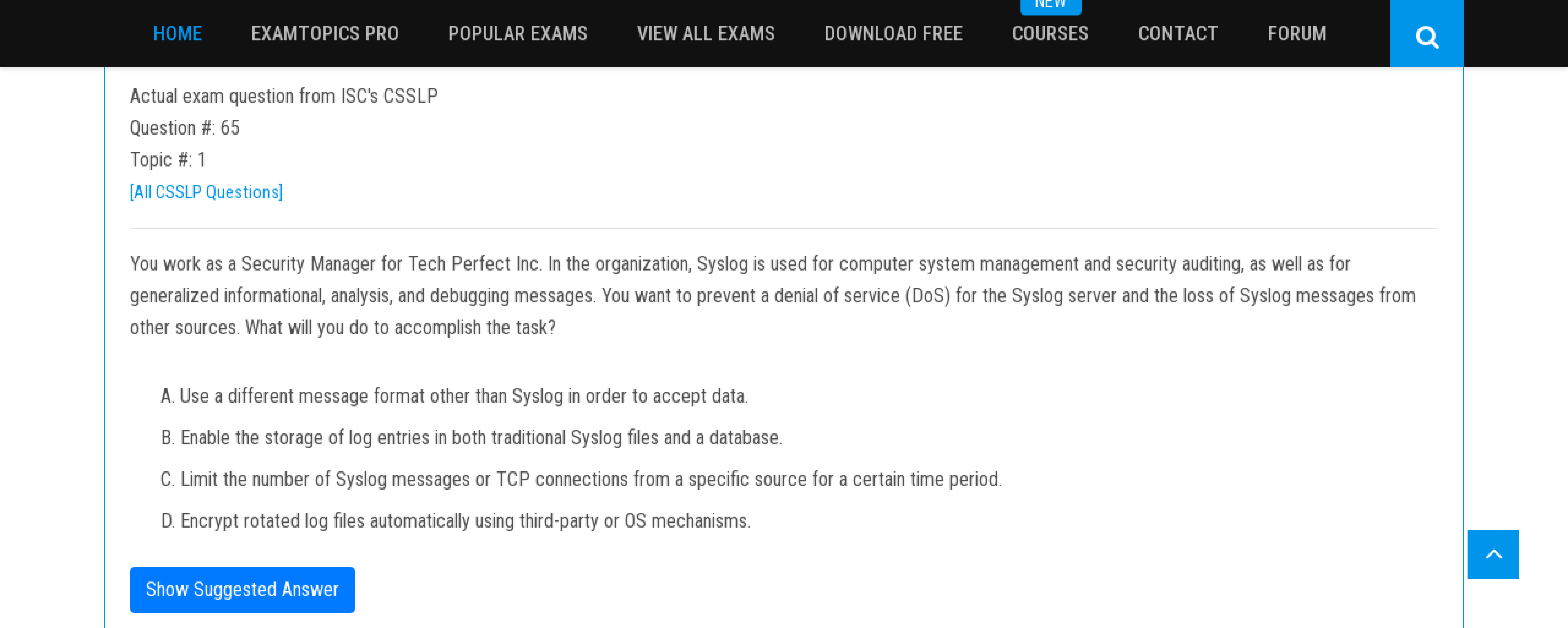
There are seven risks responses that a project manager can choose from. Which risk response is appropriate for both positive and negative risk events?

A. Acceptance

B. Transference

C. Sharing

D. Mitigation



Actual exam question from ISC's CSSLP

Question #: 65

Topic #: 1

[All CSSLP Questions]

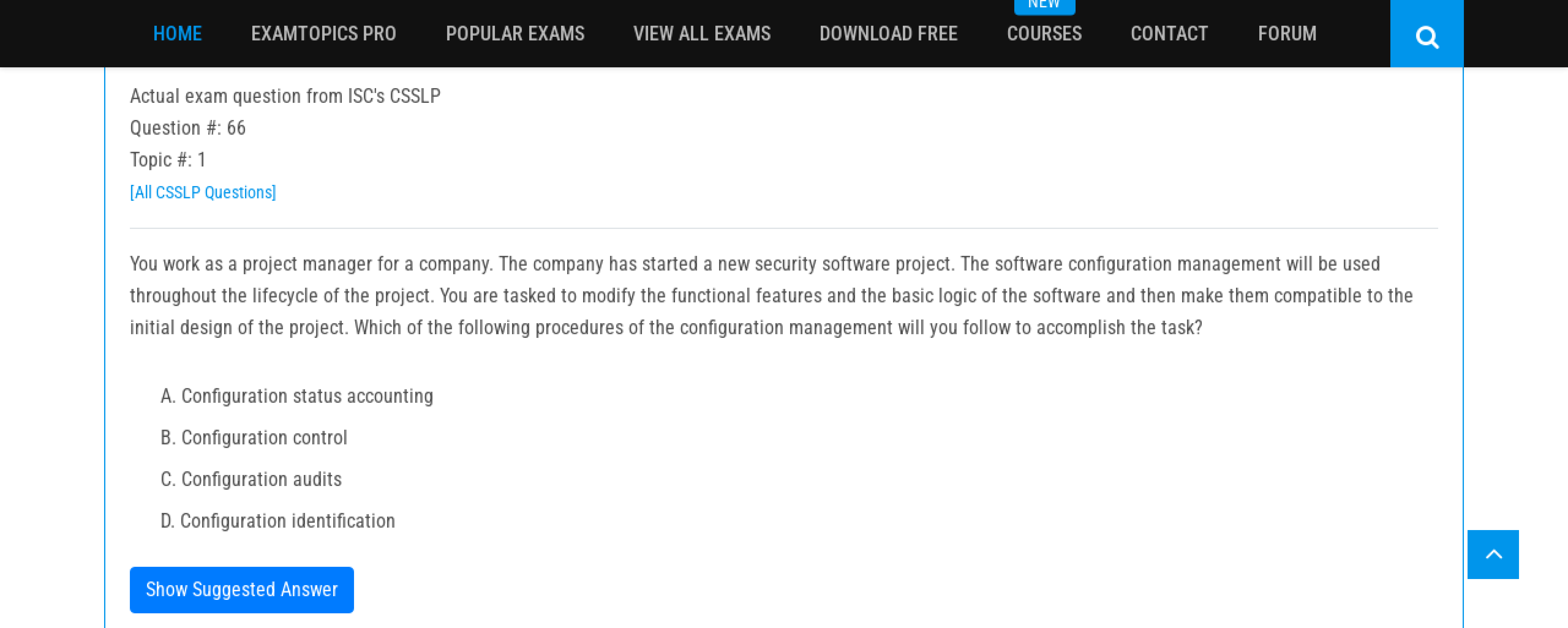
You work as a Security Manager for Tech Perfect Inc. In the organization, Syslog is used for computer system management and security auditing, as well as for generalized informational, analysis, and debugging messages. You want to prevent a denial of service (DoS) for the Syslog server and the loss of Syslog messages from other sources. What will you do to accomplish the task?

A. Use a different message format other than Syslog in order to accept data.

B. Enable the storage of log entries in both traditional Syslog files and a database.

C. Limit the number of Syslog messages or TCP connections from a specific source for a certain time period.

D. Encrypt rotated log files automatically using third-party or OS mechanisms.



Actual exam question from ISC's CSSLP

Question #: 66

Topic #: 1

[All CSSLP Questions]

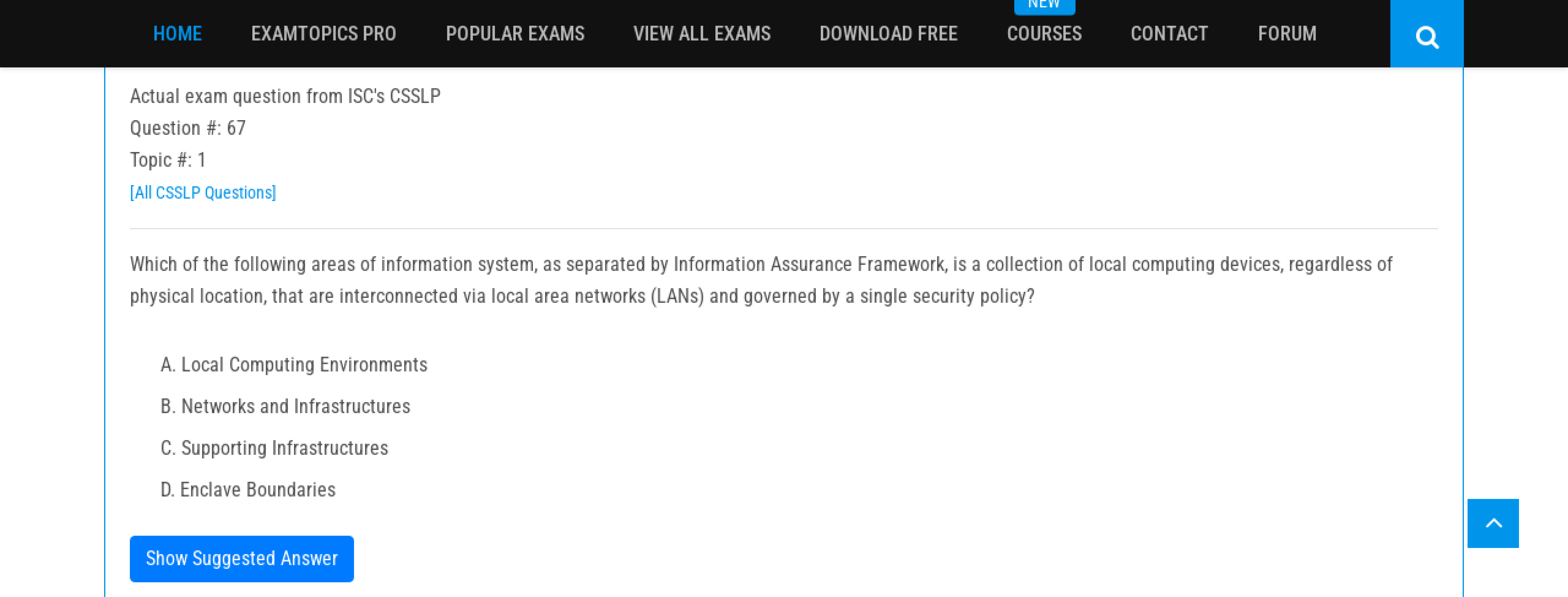
You work as a project manager for a company. The company has started a new security software project. The software configuration management will be used throughout the lifecycle of the project. You are tasked to modify the functional features and the basic logic of the software and then make them compatible to the initial design of the project. Which of the following procedures of the configuration management will you follow to accomplish the task?

A. Configuration status accounting

B. Configuration control

C. Configuration audits

D. Configuration identification



Actual exam question from ISC's CSSLP

Question #: 67

Topic #: 1

[All CSSLP Questions]

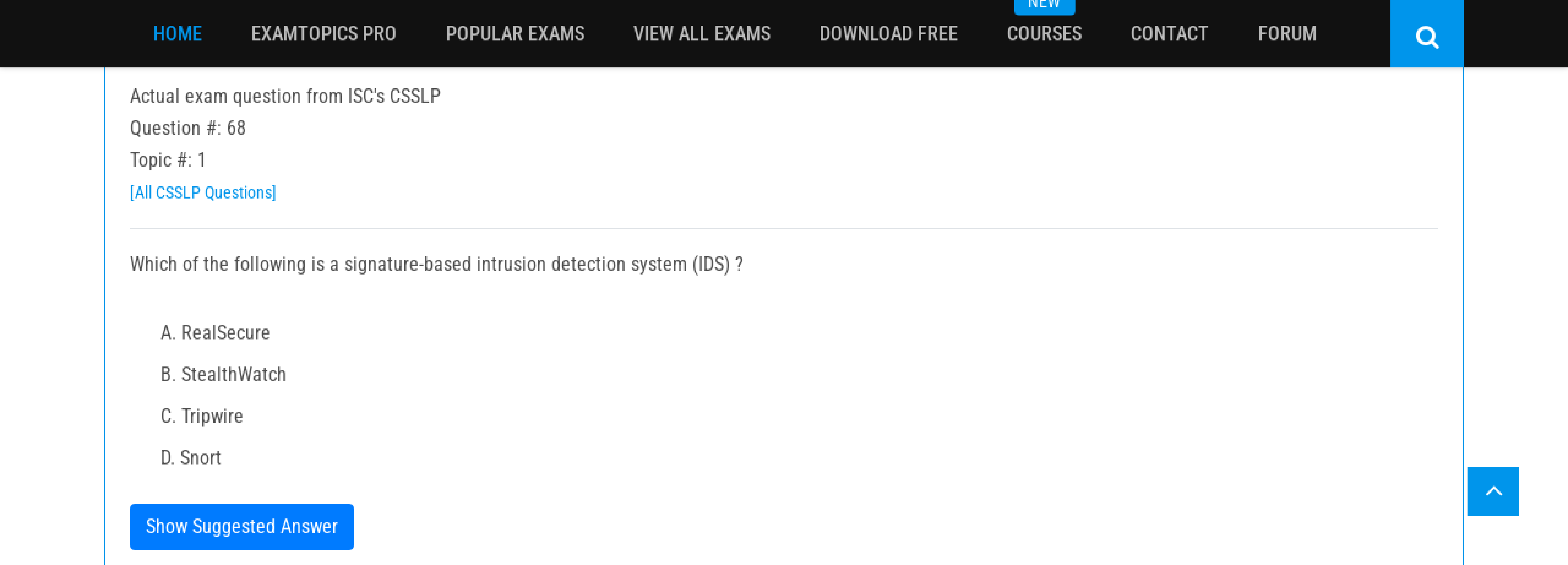
Which of the following areas of information system, as separated by Information Assurance Framework, is a collection of local computing devices, regardless of physical location, that are interconnected via local area networks (LANs) and governed by a single security policy?

A. Local Computing Environments

B. Networks and Infrastructures

C. Supporting Infrastructures

D. Enclave Boundaries



Actual exam question from ISC's CSSLP

Question #: 68

Topic #: 1

[All CSSLP Questions]

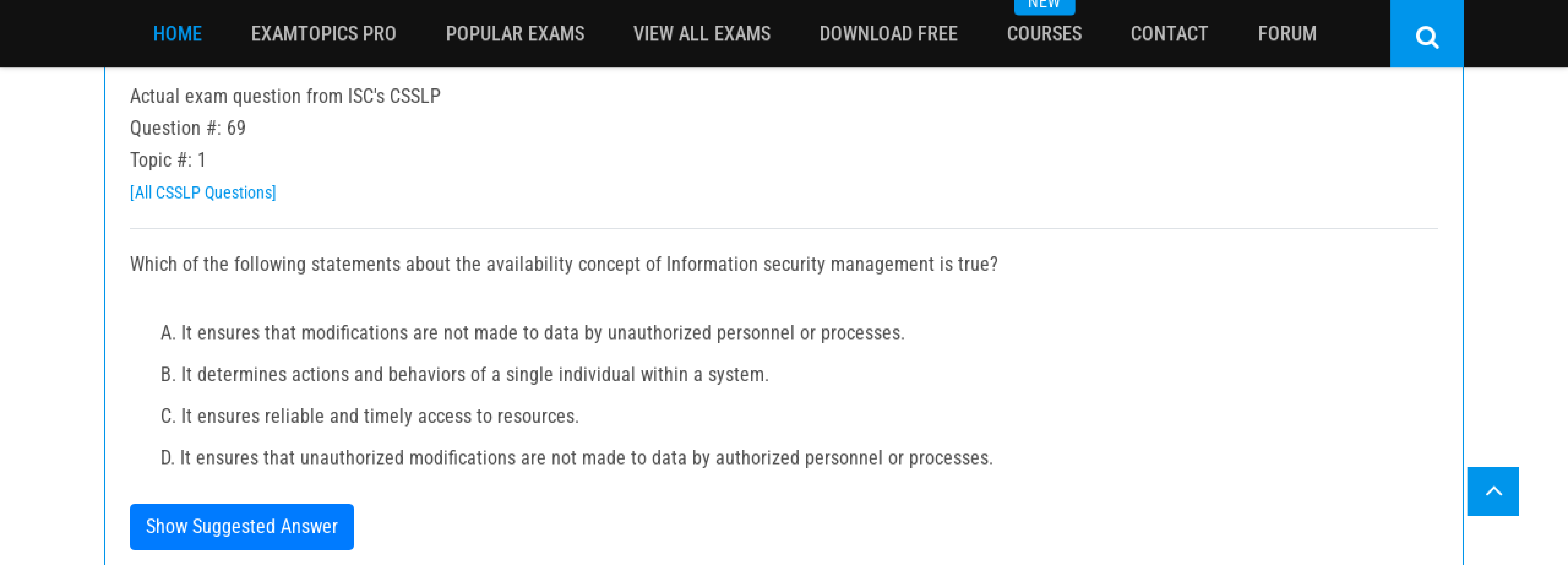
Which of the following is a signature-based intrusion detection system (IDS) ?

A. RealSecure

B. StealthWatch

C. Tripwire

D. Snort



Actual exam question from ISC's CSSLP

Question #: 69

Topic #: 1

[All CSSLP Questions]

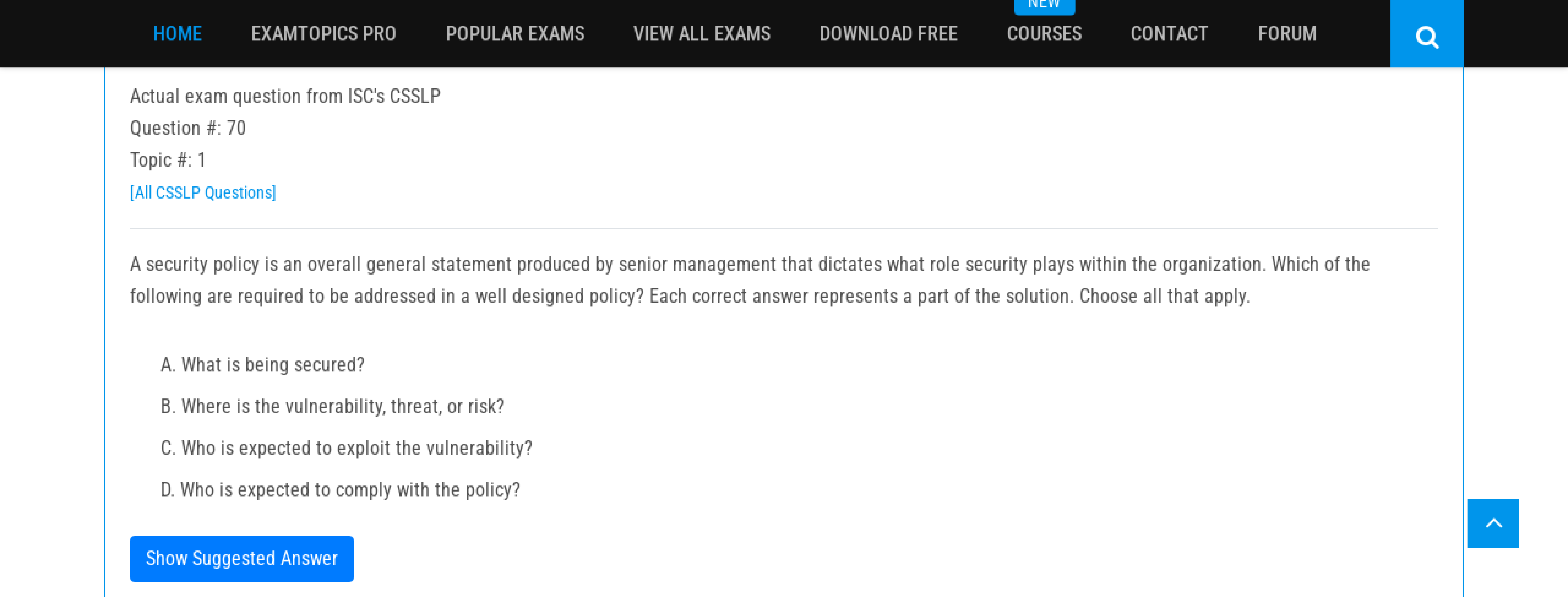
Which of the following statements about the availability concept of Information security management is true?

A. It ensures that modifications are not made to data by unauthorized personnel or processes.

B. It determines actions and behaviors of a single individual within a system.

C. It ensures reliable and timely access to resources.

D. It ensures that unauthorized modifications are not made to data by authorized personnel or processes.



Actual exam question from ISC's CSSLP

Question #: 70

Topic #: 1

[All CSSLP Questions]

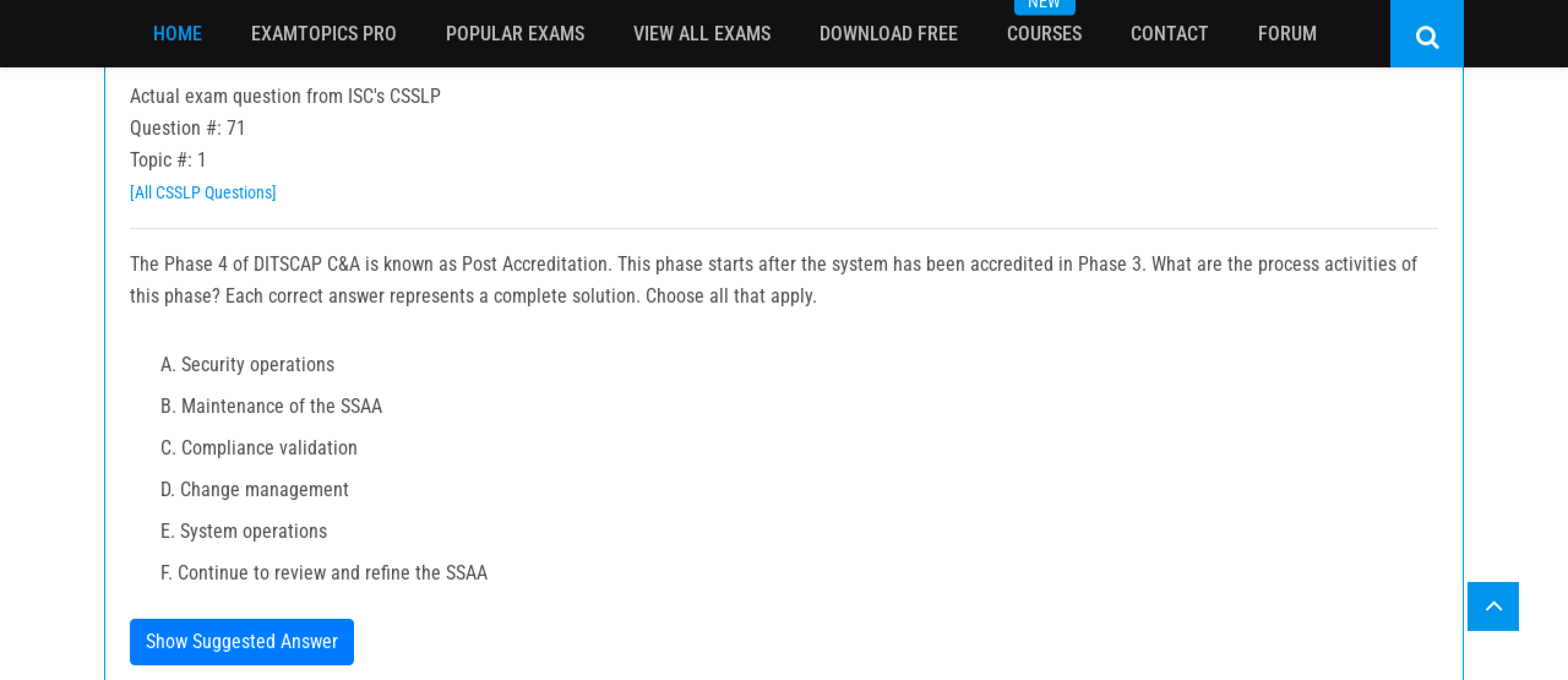
A security policy is an overall general statement produced by senior management that dictates what role security plays within the organization. Which of the following are required to be addressed in a well designed policy? Each correct answer represents a part of the solution. Choose all that apply.

A. What is being secured?

B. Where is the vulnerability, threat, or risk?

C. Who is expected to exploit the vulnerability?

D. Who is expected to comply with the policy?



Actual exam question from ISC's CSSLP

Question #: 71

Topic #: 1

[All CSSLP Questions]

The Phase 4 of DITSCAP C&A is known as Post Accreditation. This phase starts after the system has been accredited in Phase 3. What are the process activities of this phase? Each correct answer represents a complete solution. Choose all that apply.

A. Security operations

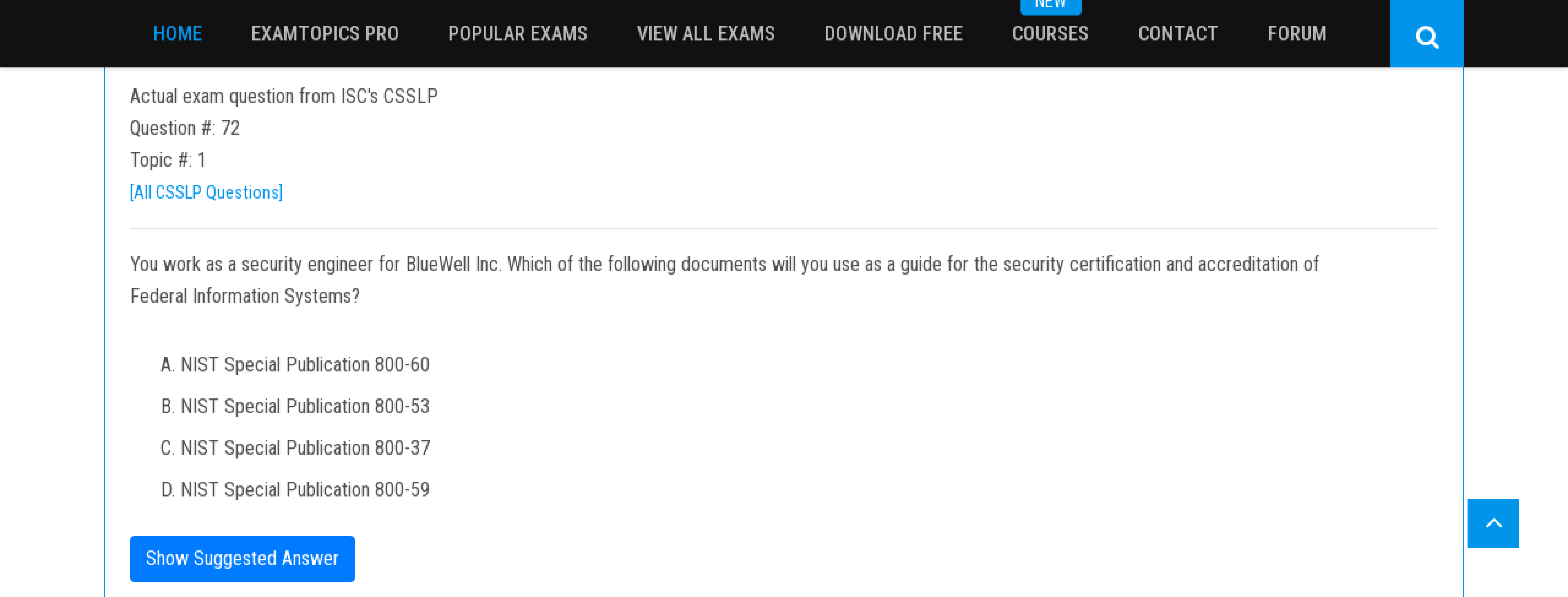
B. Maintenance of the SSAA

C. Compliance validation

D. Change management

E. System operations

F. Continue to review and refine the SSAA



Actual exam question from ISC's CSSLP
Question #: 72
Topic #: 1
[All CSSLP Questions]

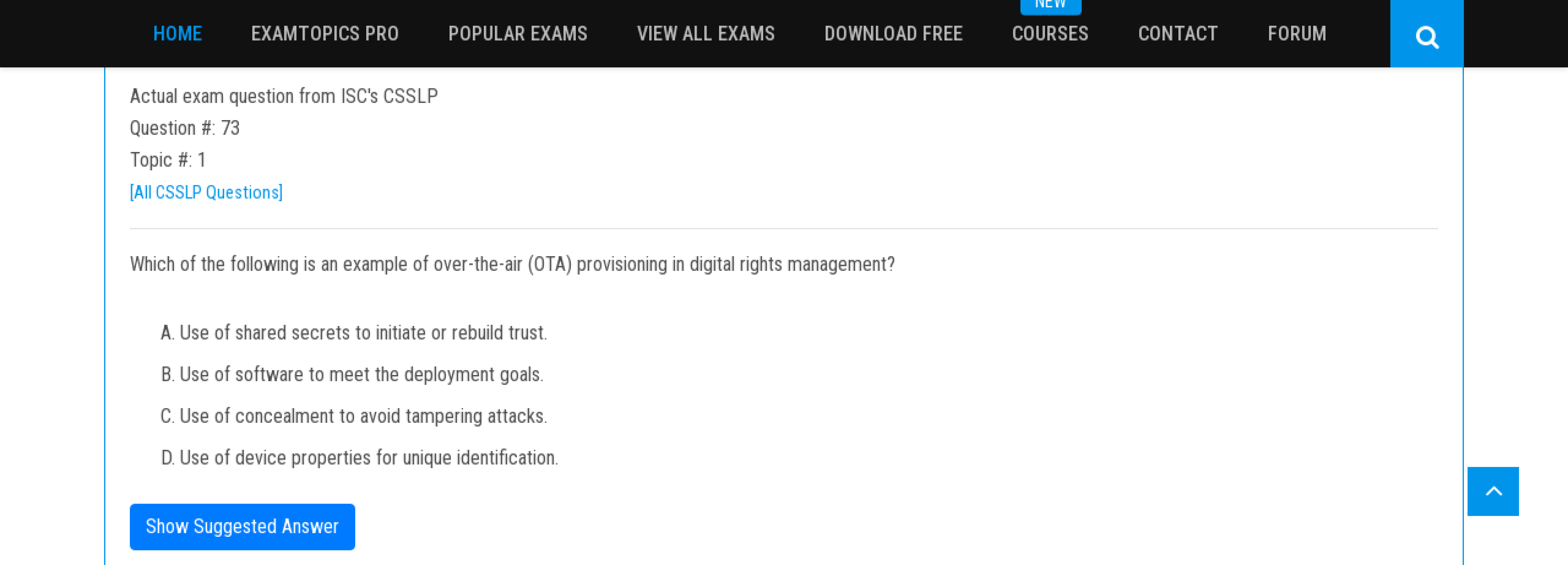
You work as a security engineer for BlueWell Inc. Which of the following documents will you use as a guide for the security certification and accreditation of Federal Information Systems?

A. NIST Special Publication 800-60

B. NIST Special Publication 800-53

C. NIST Special Publication 800-37

D. NIST Special Publication 800-59



Actual exam question from ISC's CSSLP

Question #: 73

Topic #: 1

[All CSSLP Questions]

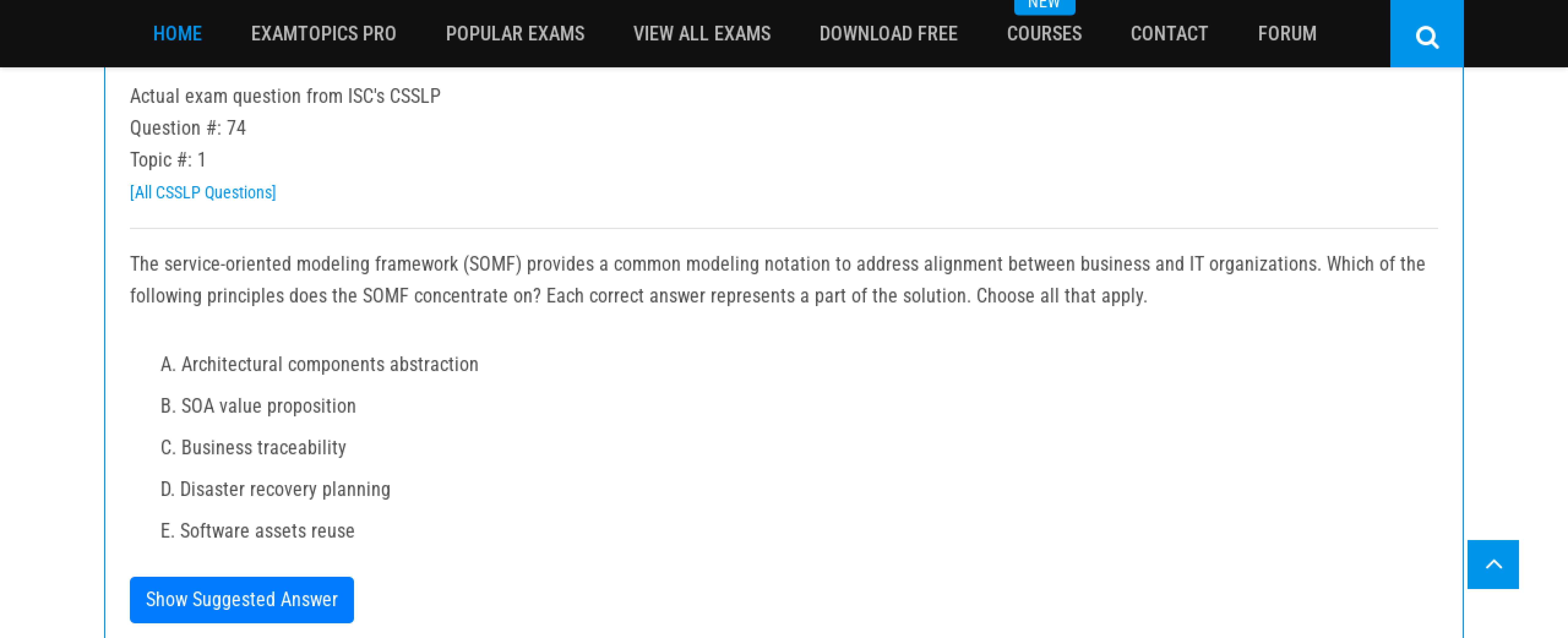
Which of the following is an example of over-the-air (OTA) provisioning in digital rights management?

A. Use of shared secrets to initiate or rebuild trust.

B. Use of software to meet the deployment goals.

C. Use of concealment to avoid tampering attacks.

D. Use of device properties for unique identification.



Actual exam question from ISC's CSSLP

Question #: 74

Topic #: 1

[All CSSLP Questions]

The service-oriented modeling framework (SOMF) provides a common modeling notation to address alignment between business and IT organizations. Which of the following principles does the SOMF concentrate on? Each correct answer represents a part of the solution. Choose all that apply.

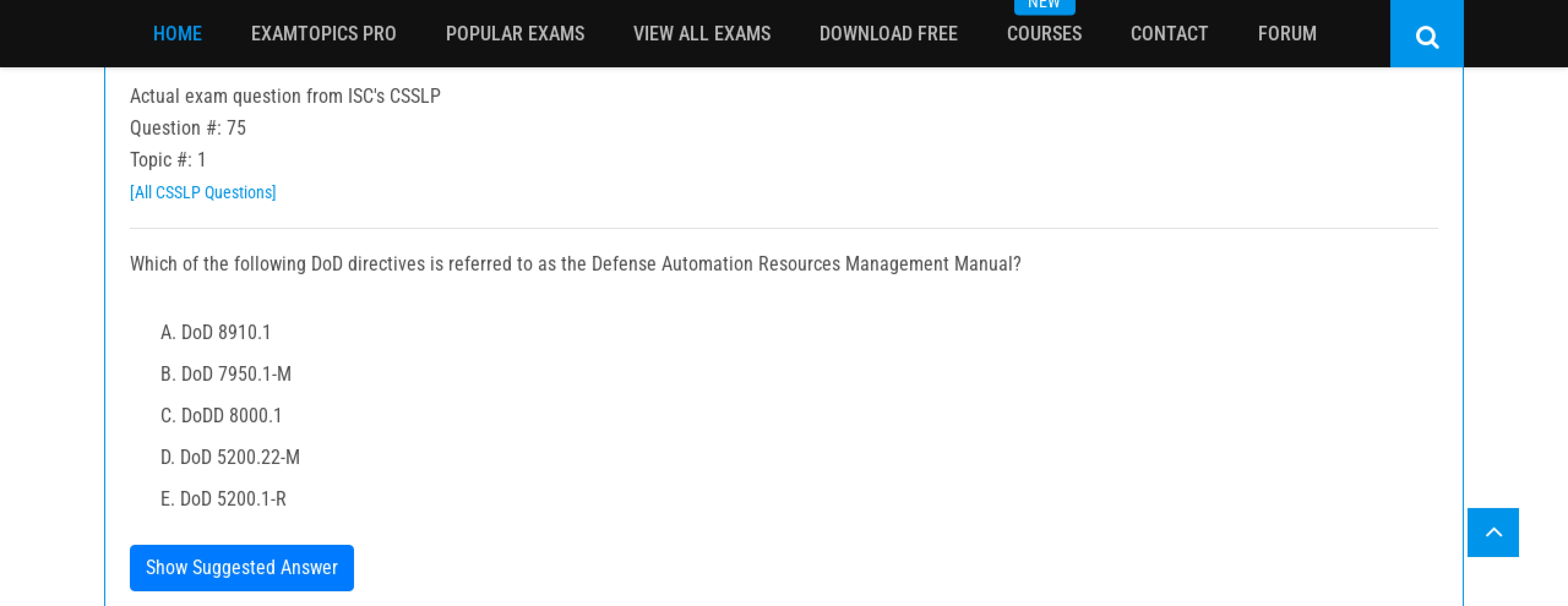
A. Architectural components abstraction

B. SOA value proposition

C. Business traceability

D. Disaster recovery planning

E. Software assets reuse



Actual exam question from ISC's CSSLP

Question #: 75

Topic #: 1

[All CSSLP Questions]

Which of the following DoD directives is referred to as the Defense Automation Resources Management Manual?

A. DoD 8910.1

B. DoD 7950.1-M

C. DoDD 8000.1

D. DoD 5200.22-M

E. DoD 5200.1-R

Actual exam question from ISC's CSSLP

Question #: 76

Topic #: 1

[All CSSLP Questions]

Which of the following access control models are used in the commercial sector? Each correct answer represents a complete solution. Choose two.

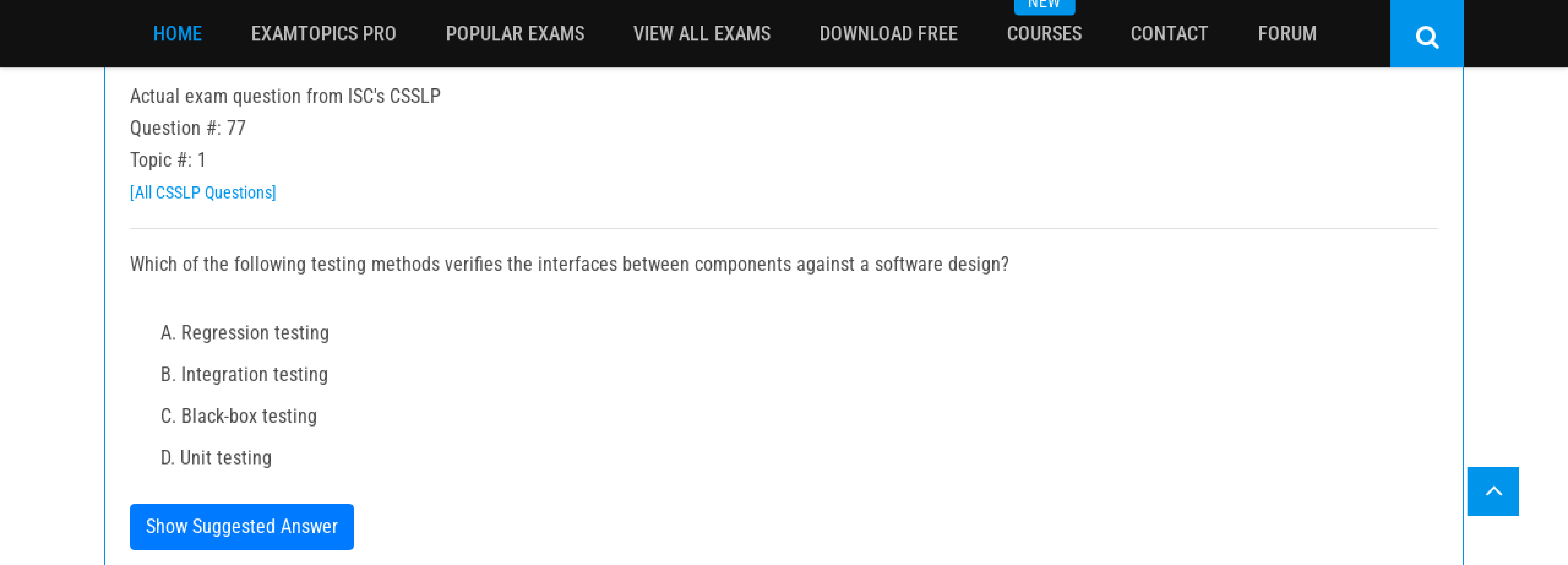
A. Biba model

B. Clark-Biba model

C. Clark-Wilson model

D. Bell-LaPadula model

Show Suggested Answer



Actual exam question from ISC's CSSLP

Question #: 77

Topic #: 1

[All CSSLP Questions]

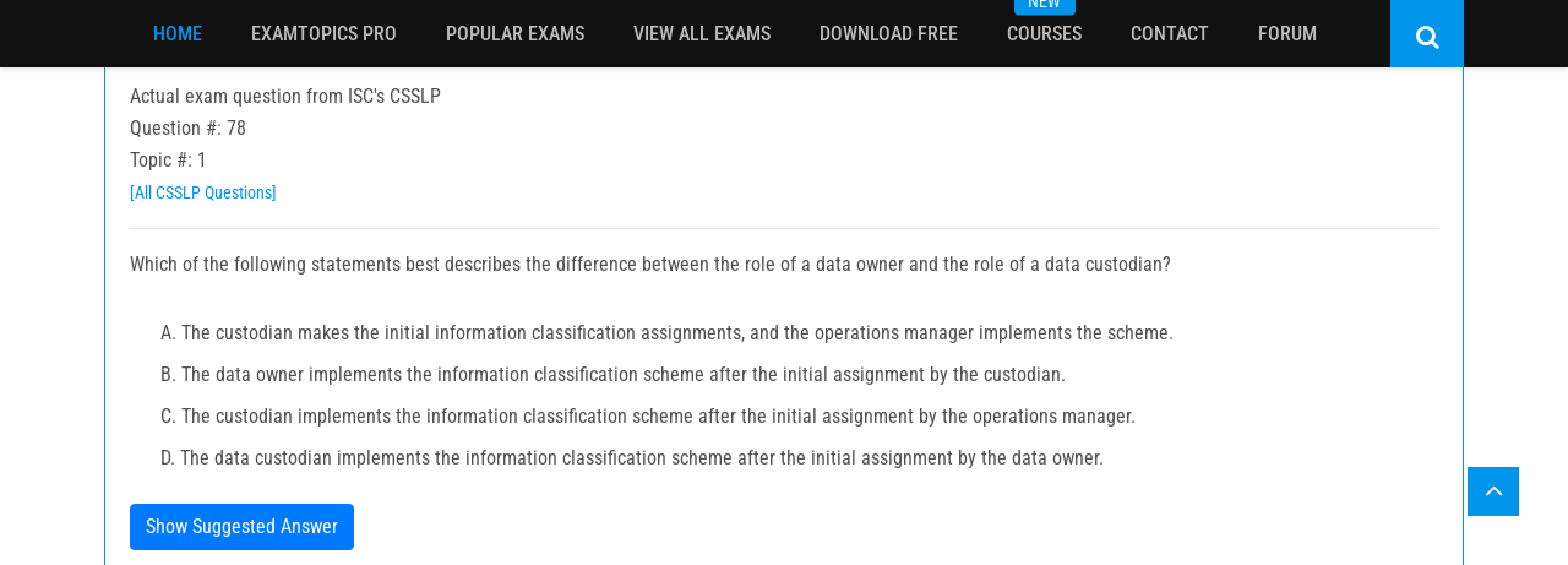
Which of the following testing methods verifies the interfaces between components against a software design?

A. Regression testing

B. Integration testing

C. Black-box testing

D. Unit testing



Actual exam question from ISC's CSSLP

Question #: 78

Topic #: 1

[All CSSLP Questions]

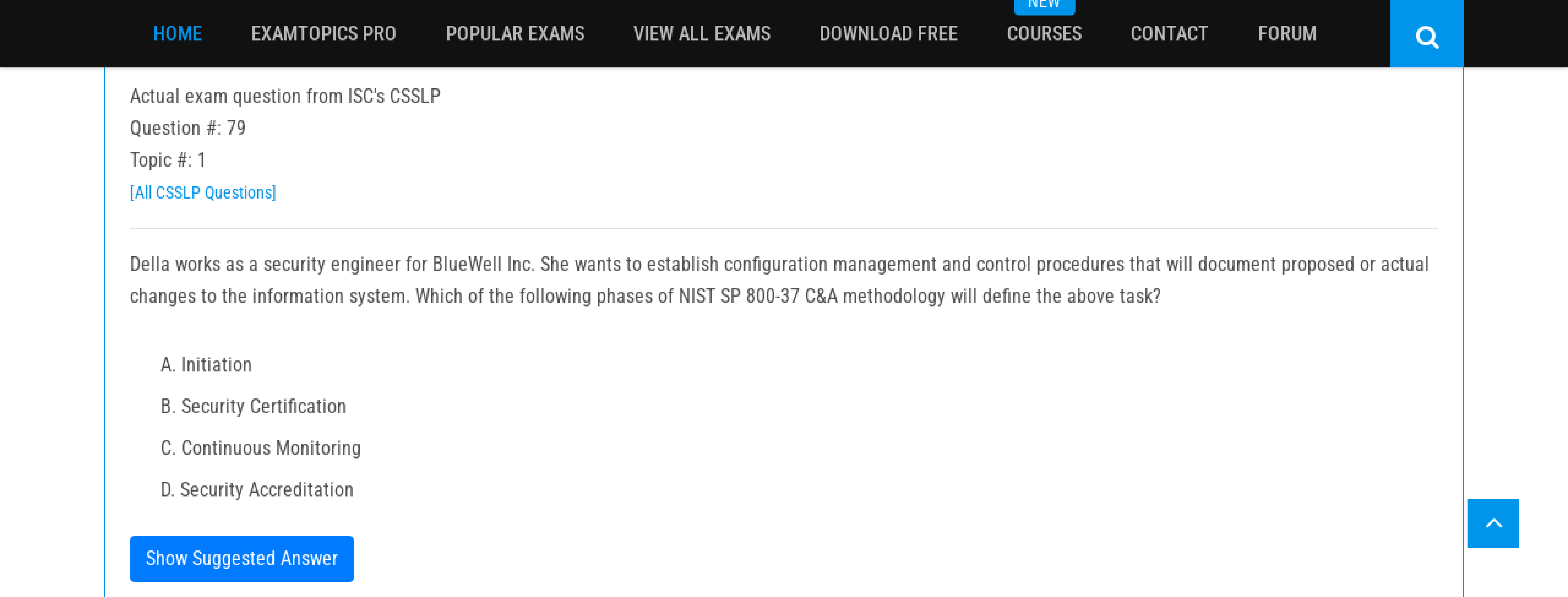
Which of the following statements best describes the difference between the role of a data owner and the role of a data custodian?

A. The custodian makes the initial information classification assignments, and the operations manager implements the scheme.

B. The data owner implements the information classification scheme after the initial assignment by the custodian.

C. The custodian implements the information classification scheme after the initial assignment by the operations manager.

D. The data custodian implements the information classification scheme after the initial assignment by the data owner.



Actual exam question from ISC's CSSLP

Question #: 79

Topic #: 1

[All CSSLP Questions]

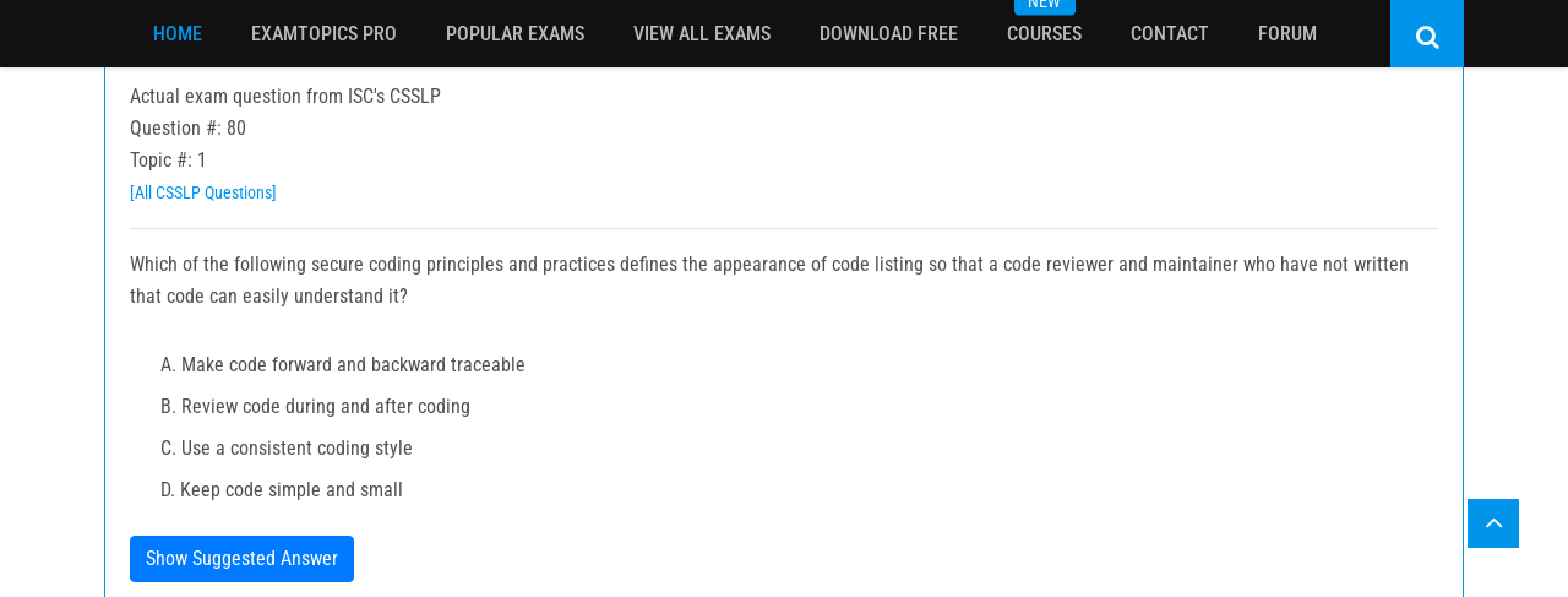
Della works as a security engineer for BlueWell Inc. She wants to establish configuration management and control procedures that will document proposed or actual changes to the information system. Which of the following phases of NIST SP 800-37 C&A methodology will define the above task?

A. Initiation

B. Security Certification

C. Continuous Monitoring

D. Security Accreditation



Actual exam question from ISC's CSSLP

Question #: 80

Topic #: 1

[All CSSLP Questions]

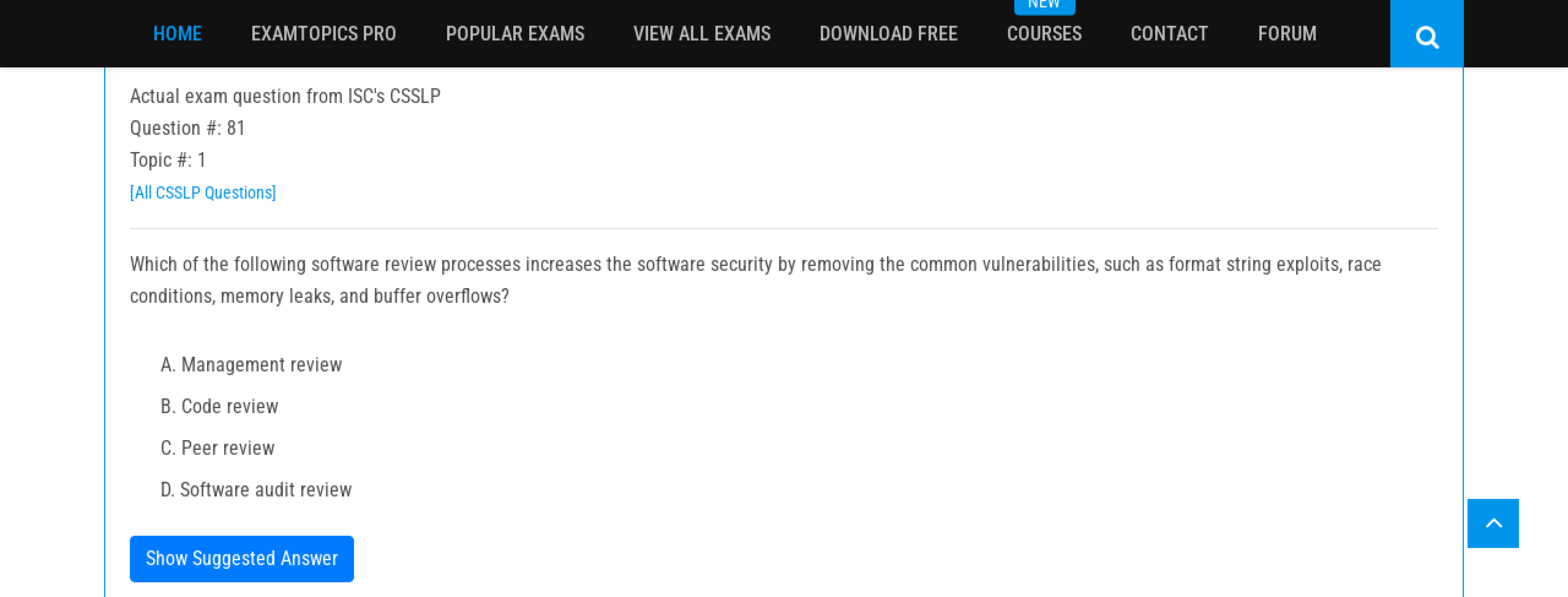
Which of the following secure coding principles and practices defines the appearance of code listing so that a code reviewer and maintainer who have not written that code can easily understand it?

A. Make code forward and backward traceable

B. Review code during and after coding

C. Use a consistent coding style

D. Keep code simple and small



Actual exam question from ISC's CSSLP

Question #: 81

Topic #: 1

[All CSSLP Questions]

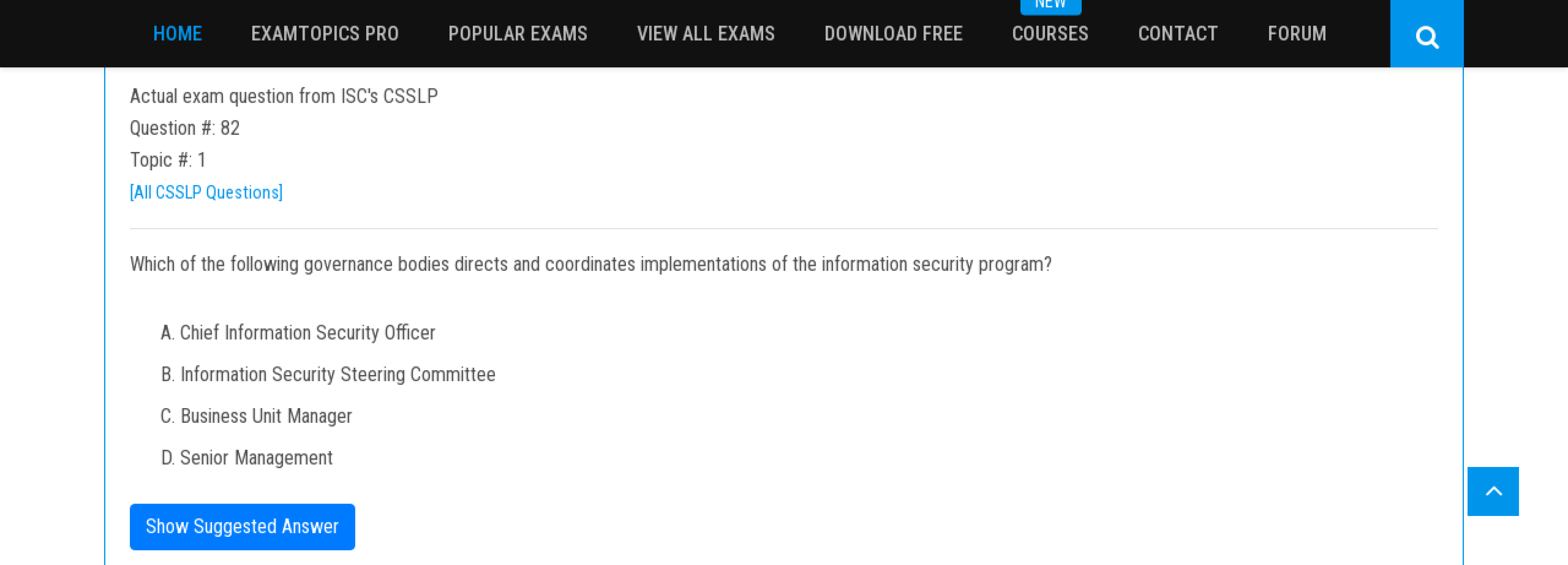
Which of the following software review processes increases the software security by removing the common vulnerabilities, such as format string exploits, race conditions, memory leaks, and buffer overflows?

A. Management review

B. Code review

C. Peer review

D. Software audit review



Actual exam question from ISC's CSSLP

Question #: 82

Topic #: 1

[All CSSLP Questions]

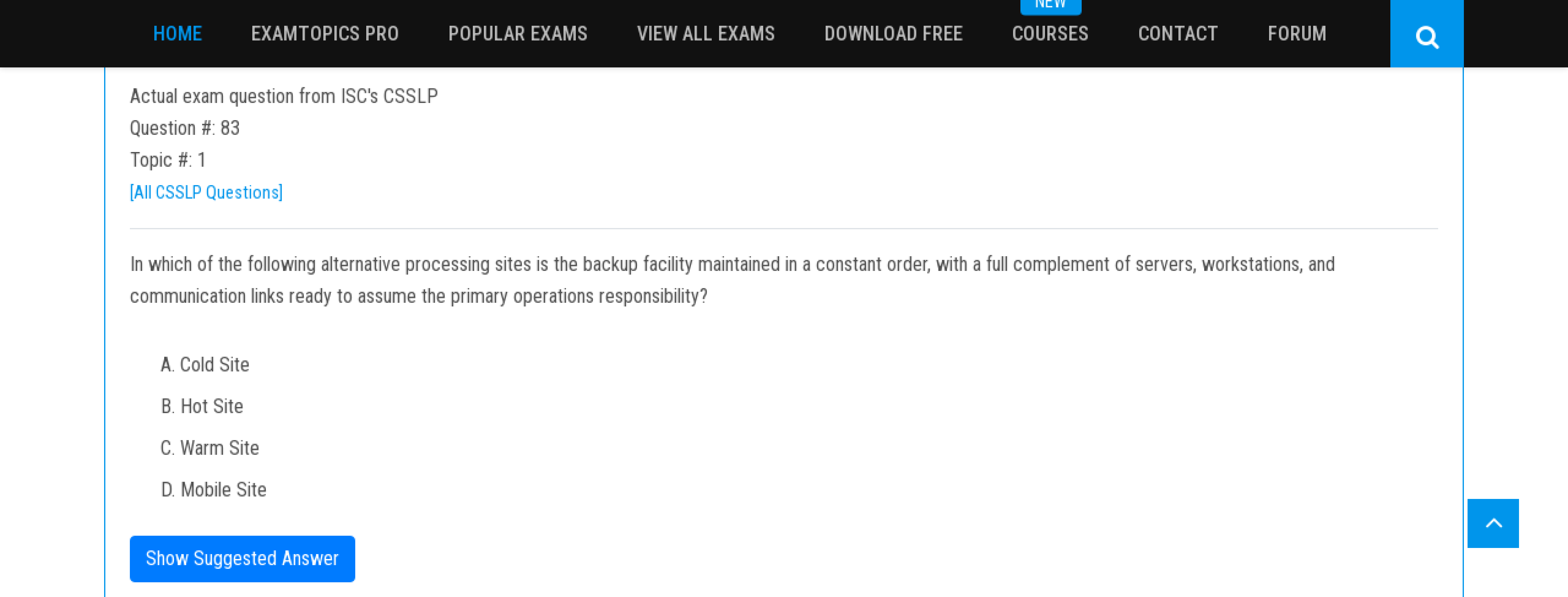
Which of the following governance bodies directs and coordinates implementations of the information security program?

A. Chief Information Security Officer

B. Information Security Steering Committee

C. Business Unit Manager

D. Senior Management



Actual exam question from ISC's CSSLP

Question #: 83

Topic #: 1

[All CSSLP Questions]

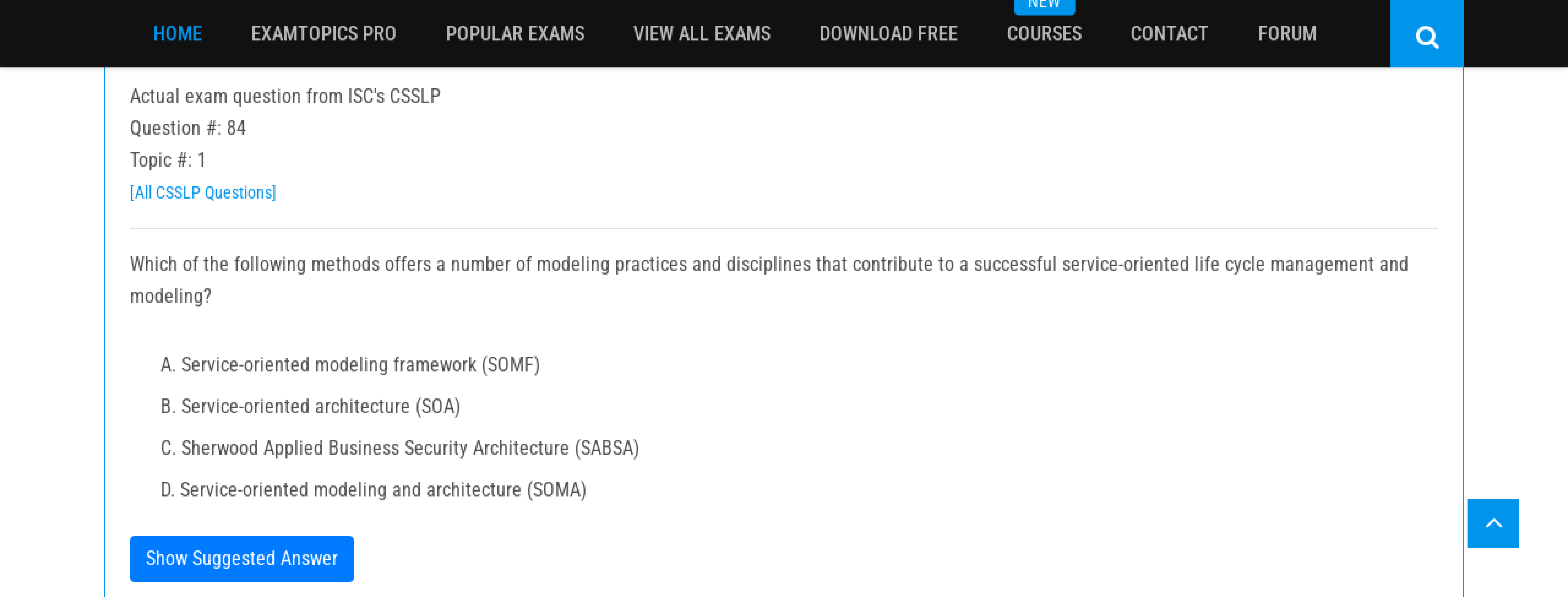
In which of the following alternative processing sites is the backup facility maintained in a constant order, with a full complement of servers, workstations, and communication links ready to assume the primary operations responsibility?

A. Cold Site

B. Hot Site

C. Warm Site

D. Mobile Site



Actual exam question from ISC's CSSLP

Question #: 84

Topic #: 1

[All CSSLP Questions]

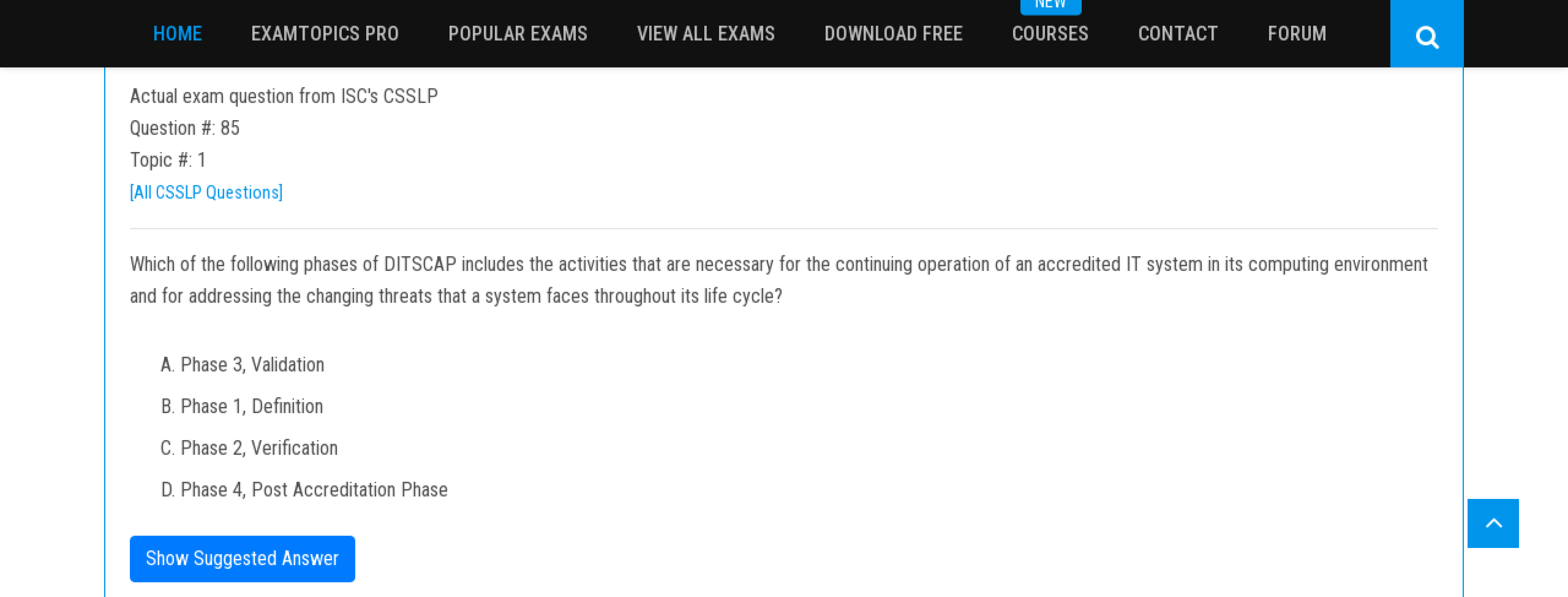
Which of the following methods offers a number of modeling practices and disciplines that contribute to a successful service-oriented life cycle management and modeling?

A. Service-oriented modeling framework (SOMF)

B. Service-oriented architecture (SOA)

C. Sherwood Applied Business Security Architecture (SABSA)

D. Service-oriented modeling and architecture (SOMA)



Actual exam question from ISC's CSSLP

Question #: 85

Topic #: 1

[All CSSLP Questions]

Which of the following phases of DITSCAP includes the activities that are necessary for the continuing operation of an accredited IT system in its computing environment and for addressing the changing threats that a system faces throughout its life cycle?

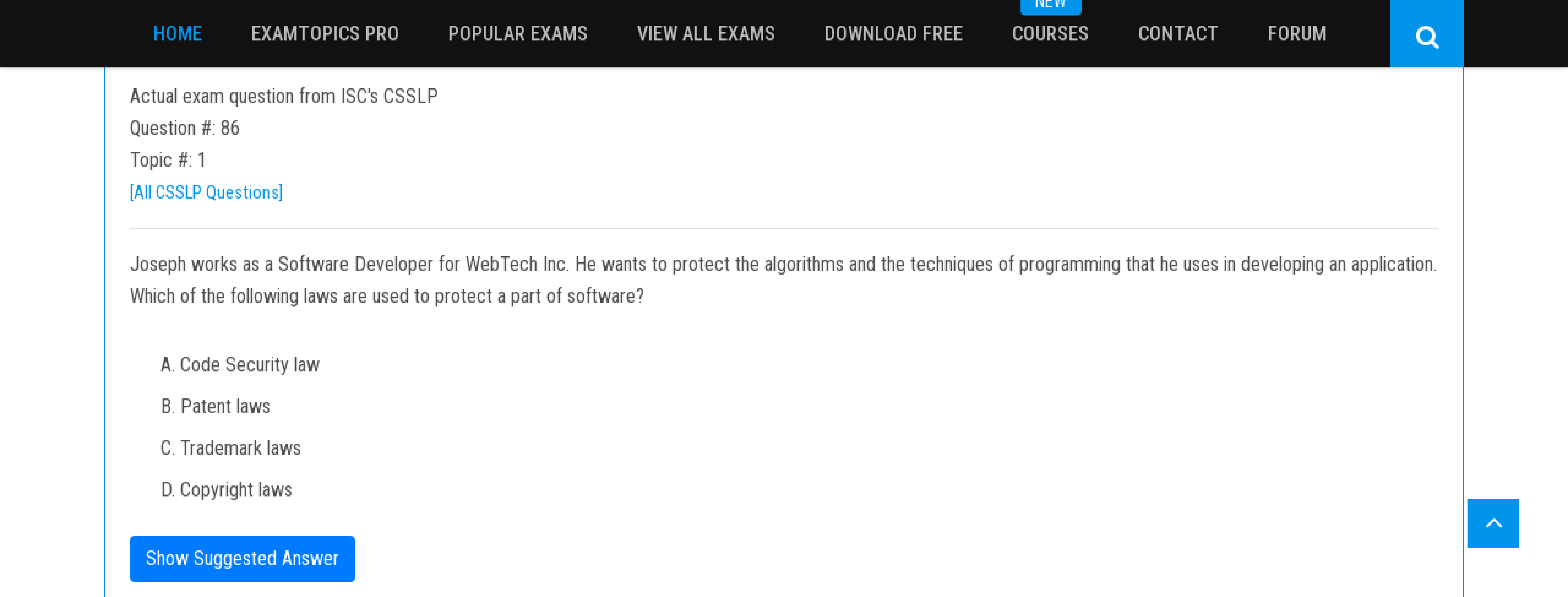
A. Phase 3, Validation

B. Phase 1, Definition

C. Phase 2, Verification

D. Phase 4, Post Accreditation Phase

Show Suggested Answer



Actual exam question from ISC's CSSLP

Question #: 86

Topic #: 1

[All CSSLP Questions]

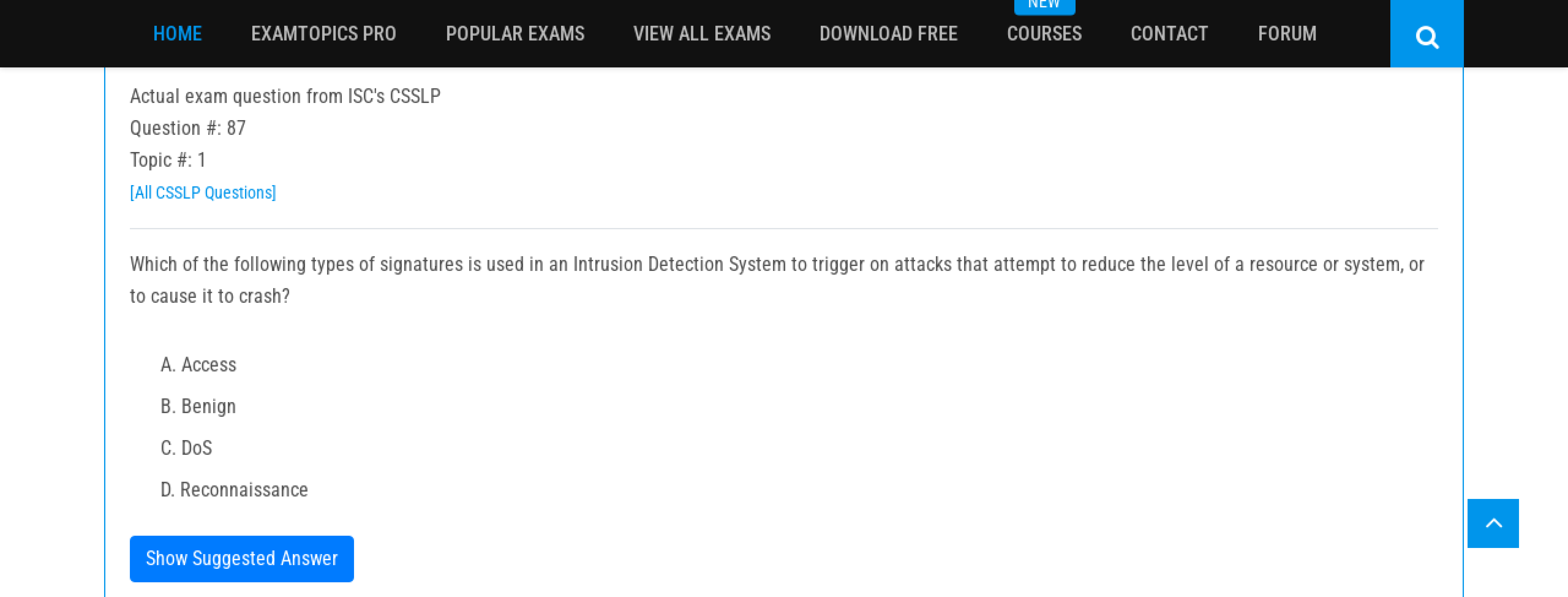
Joseph works as a Software Developer for WebTech Inc. He wants to protect the algorithms and the techniques of programming that he uses in developing an application. Which of the following laws are used to protect a part of software?

A. Code Security law

B. Patent laws

C. Trademark laws

D. Copyright laws



Actual exam question from ISC's CSSLP

Question #: 87

Topic #: 1

[All CSSLP Questions]

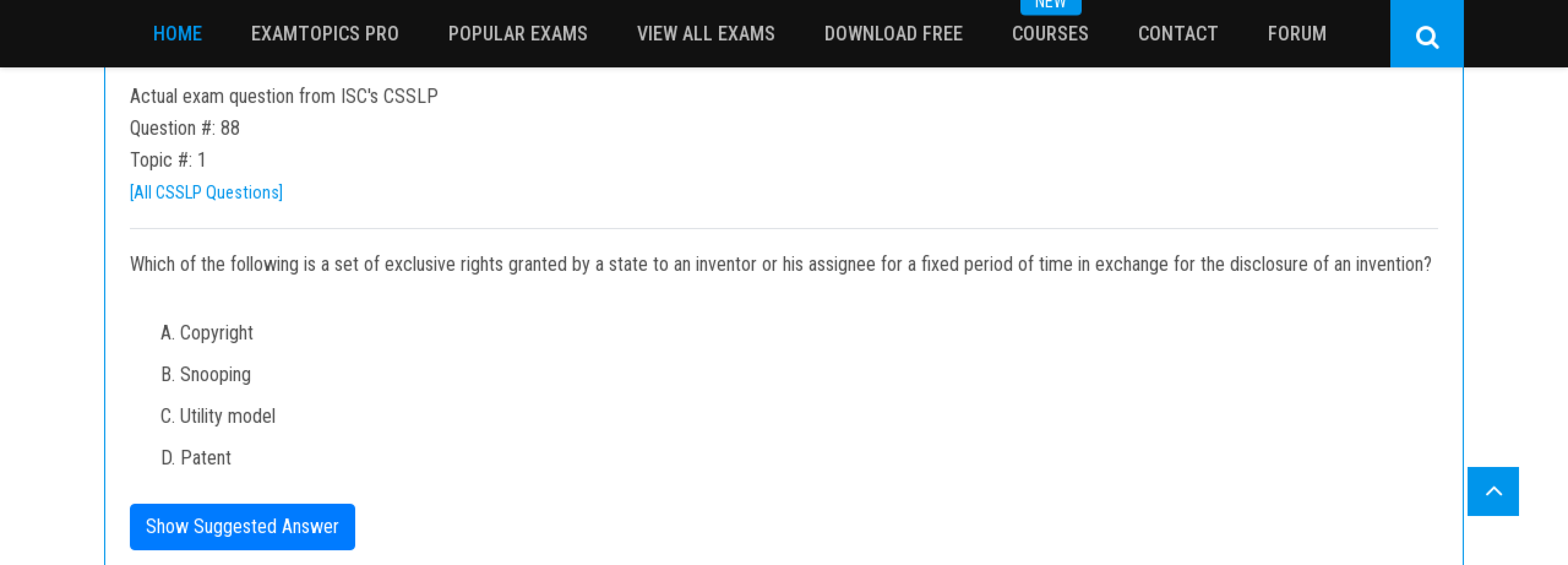
Which of the following types of signatures is used in an Intrusion Detection System to trigger on attacks that attempt to reduce the level of a resource or system, or to cause it to crash?

A. Access

B. Benign

C. DoS

D. Reconnaissance



Actual exam question from ISC's CSSLP

Question #: 88

Topic #: 1

[All CSSLP Questions]

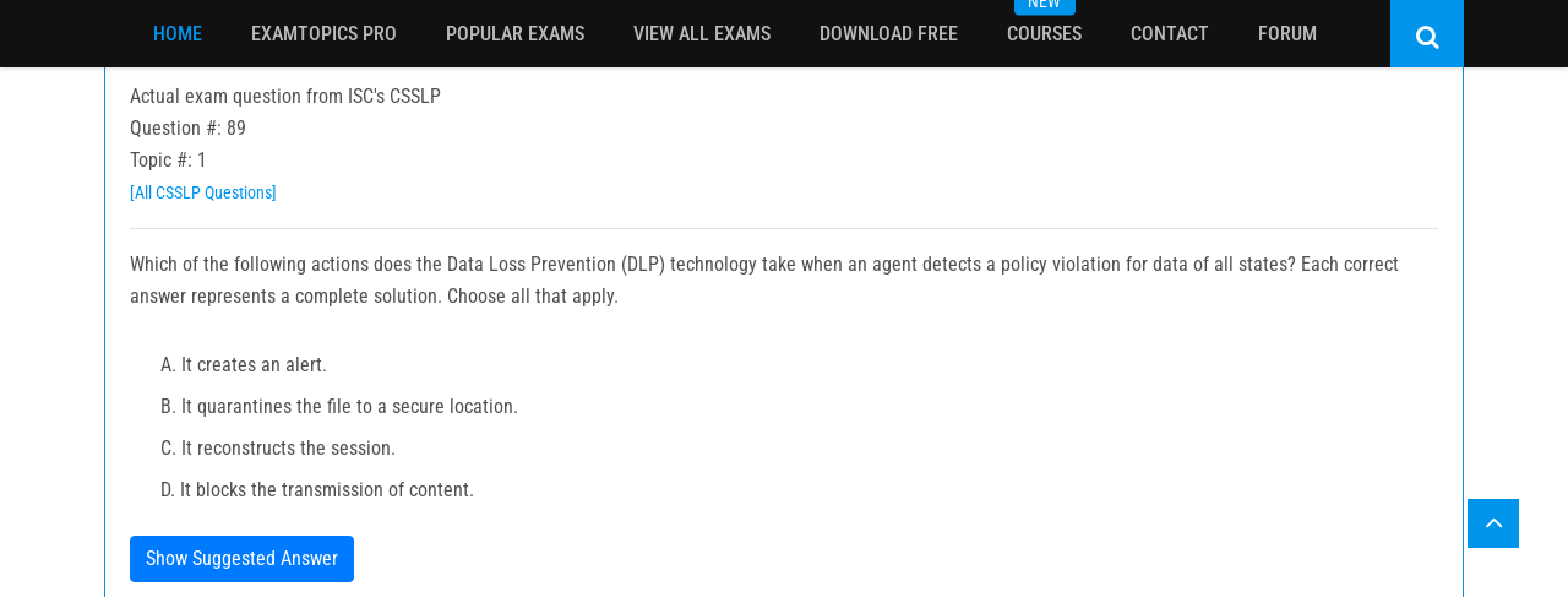
Which of the following is a set of exclusive rights granted by a state to an inventor or his assignee for a fixed period of time in exchange for the disclosure of an invention?

A. Copyright

B. Snooping

C. Utility model

D. Patent



Actual exam question from ISC's CSSLP

Question #: 89

Topic #: 1

[All CSSLP Questions]

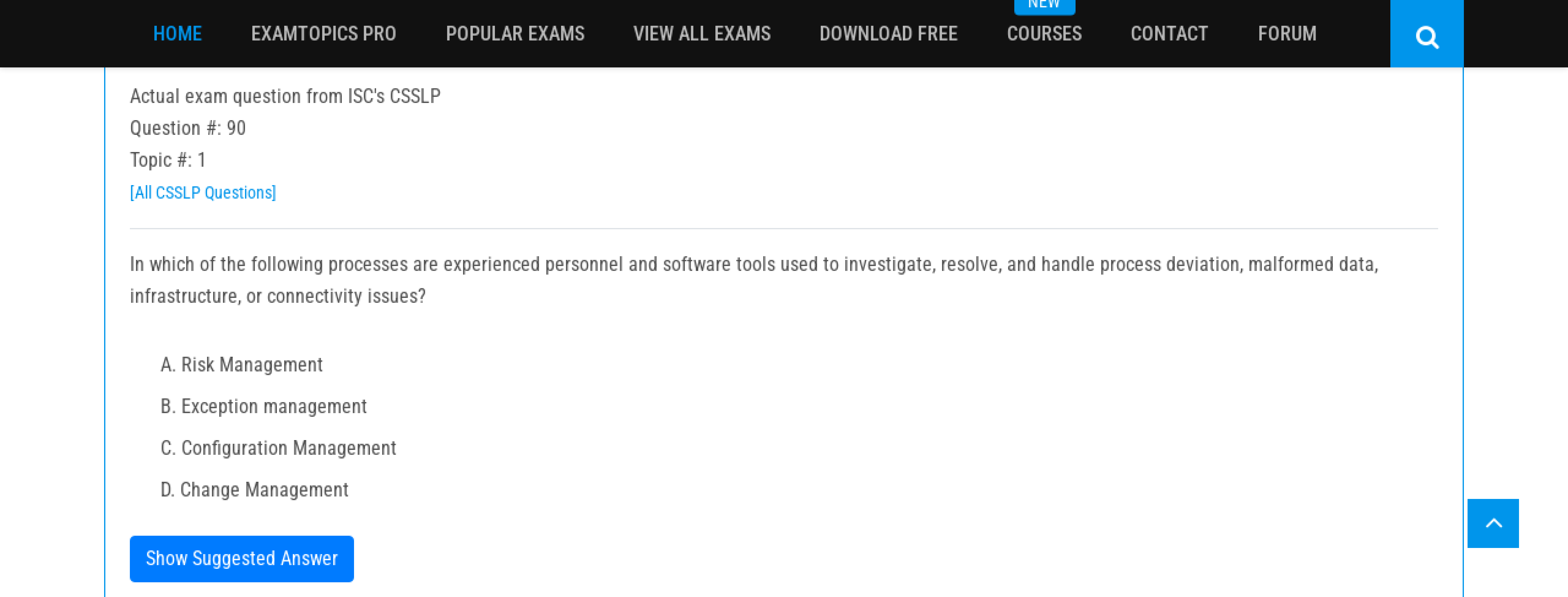
Which of the following actions does the Data Loss Prevention (DLP) technology take when an agent detects a policy violation for data of all states? Each correct answer represents a complete solution. Choose all that apply.

A. It creates an alert.

B. It quarantines the file to a secure location.

C. It reconstructs the session.

D. It blocks the transmission of content.



Actual exam question from ISC's CSSLP

Question #: 90

Topic #: 1

[All CSSLP Questions]

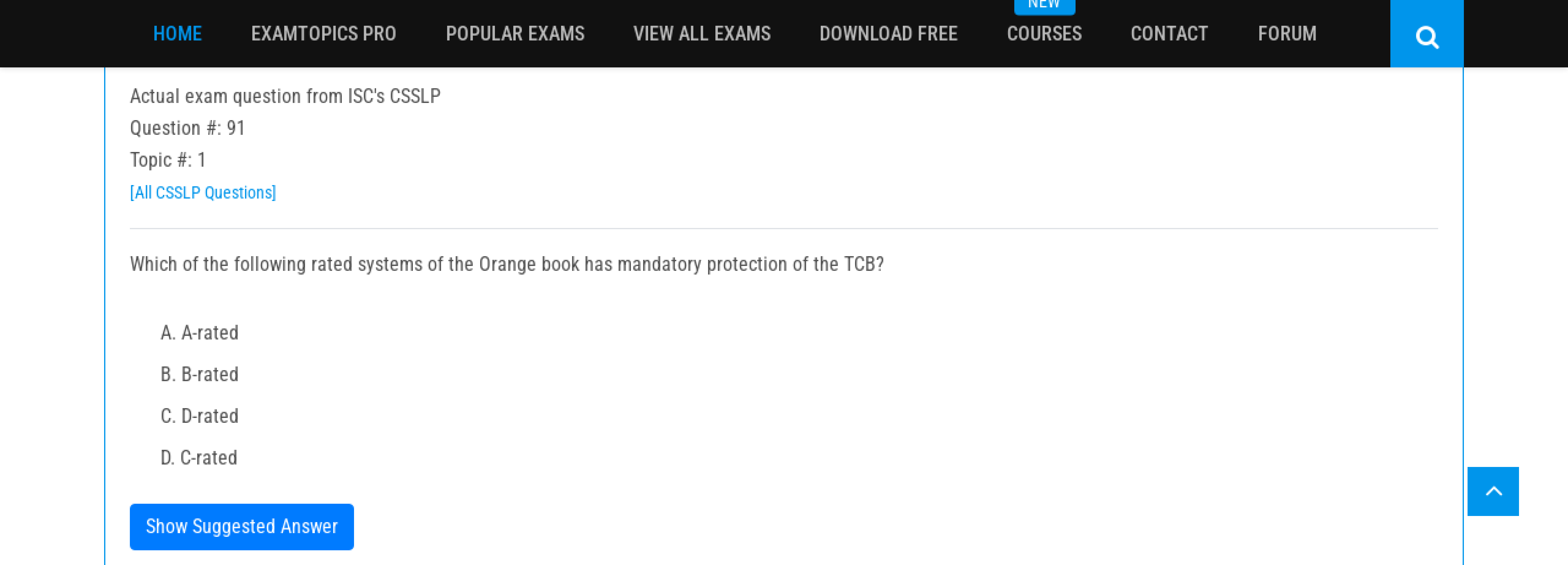
In which of the following processes are experienced personnel and software tools used to investigate, resolve, and handle process deviation, malformed data, infrastructure, or connectivity issues?

A. Risk Management

B. Exception management

C. Configuration Management

D. Change Management



Actual exam question from ISC's CSSLP

Question #: 91

Topic #: 1

[All CSSLP Questions]

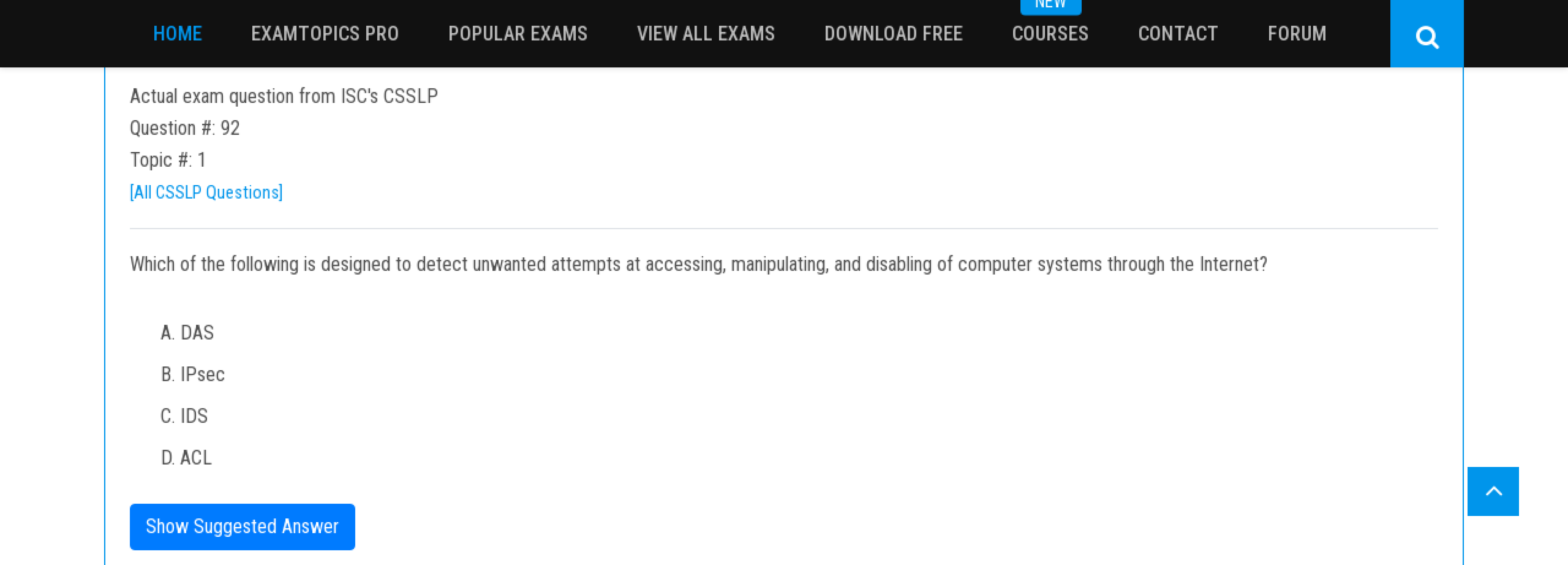
Which of the following rated systems of the Orange book has mandatory protection of the TCB?

A. A-rated

B. B-rated

C. D-rated

D. C-rated



Actual exam question from ISC's CSSLP

Question #: 92

Topic #: 1

[All CSSLP Questions]

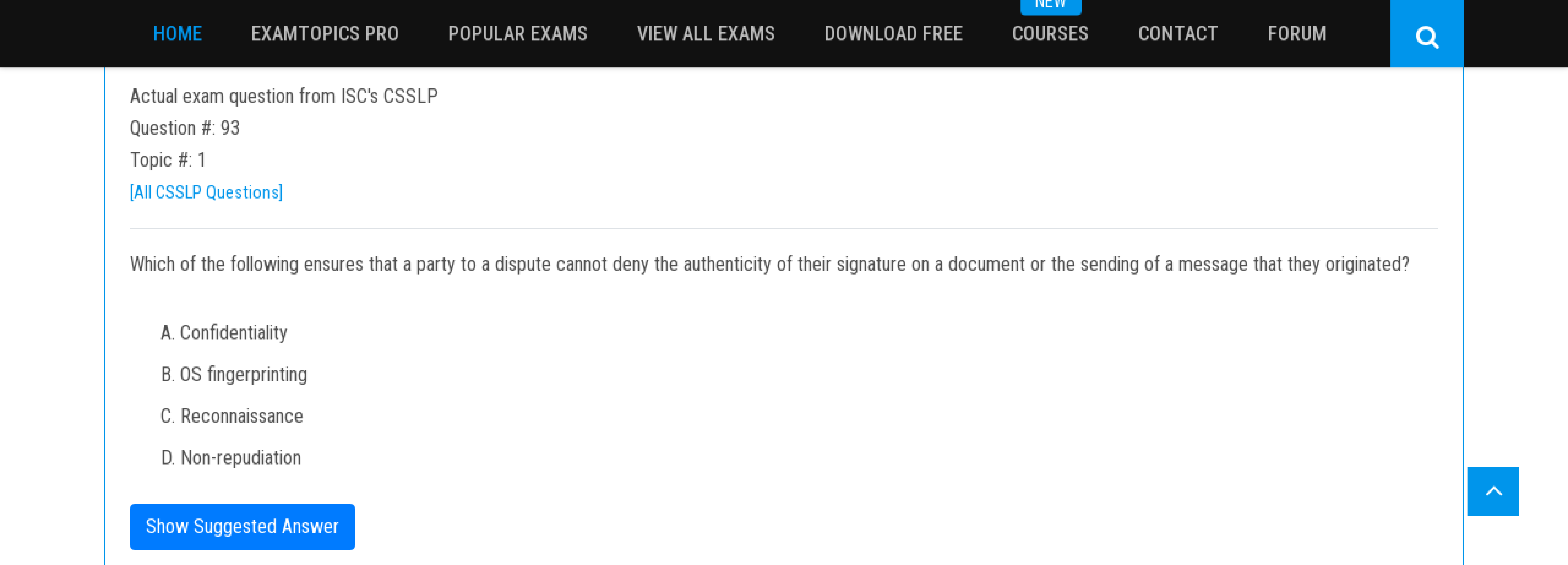
Which of the following is designed to detect unwanted attempts at accessing, manipulating, and disabling of computer systems through the Internet?

A. DAS

B. IPsec

C. IDS

D. ACL



Actual exam question from ISC's CSSLP

Question #: 93

Topic #: 1

[All CSSLP Questions]

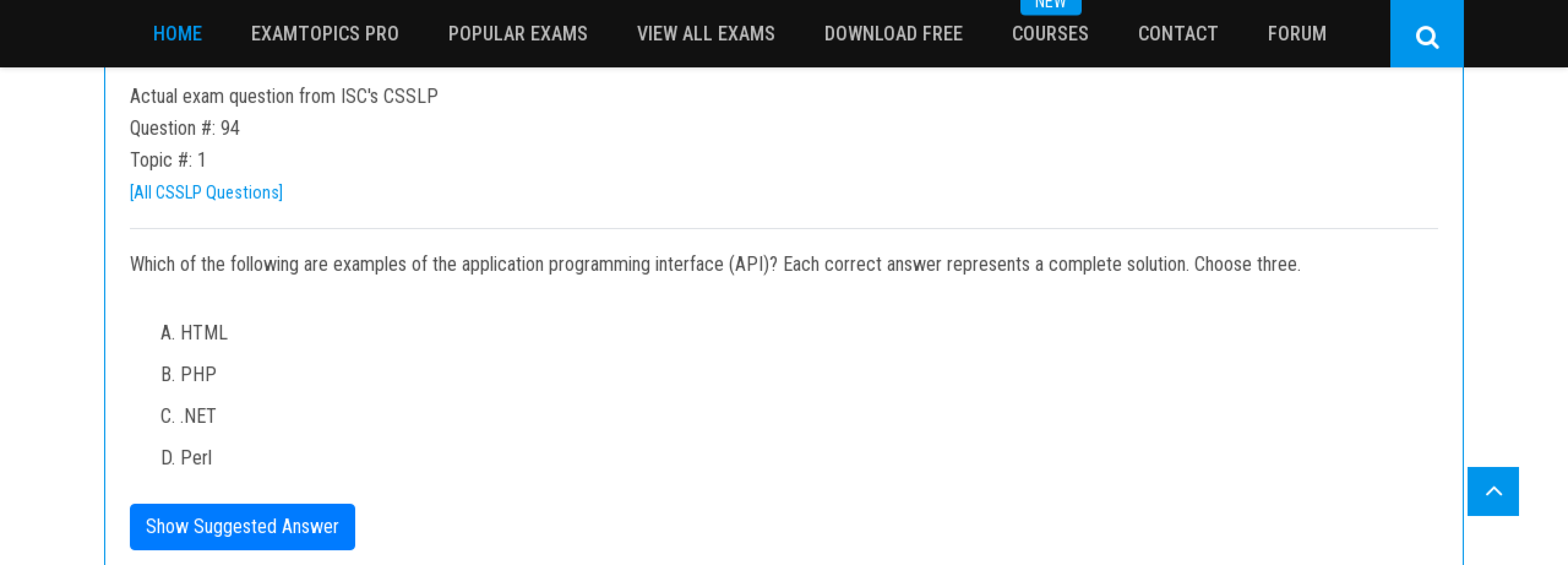
Which of the following ensures that a party to a dispute cannot deny the authenticity of their signature on a document or the sending of a message that they originated?

A. Confidentiality

B. OS fingerprinting

C. Reconnaissance

D. Non-repudiation



Actual exam question from ISC's CSSLP

Question #: 94

Topic #: 1

[All CSSLP Questions]

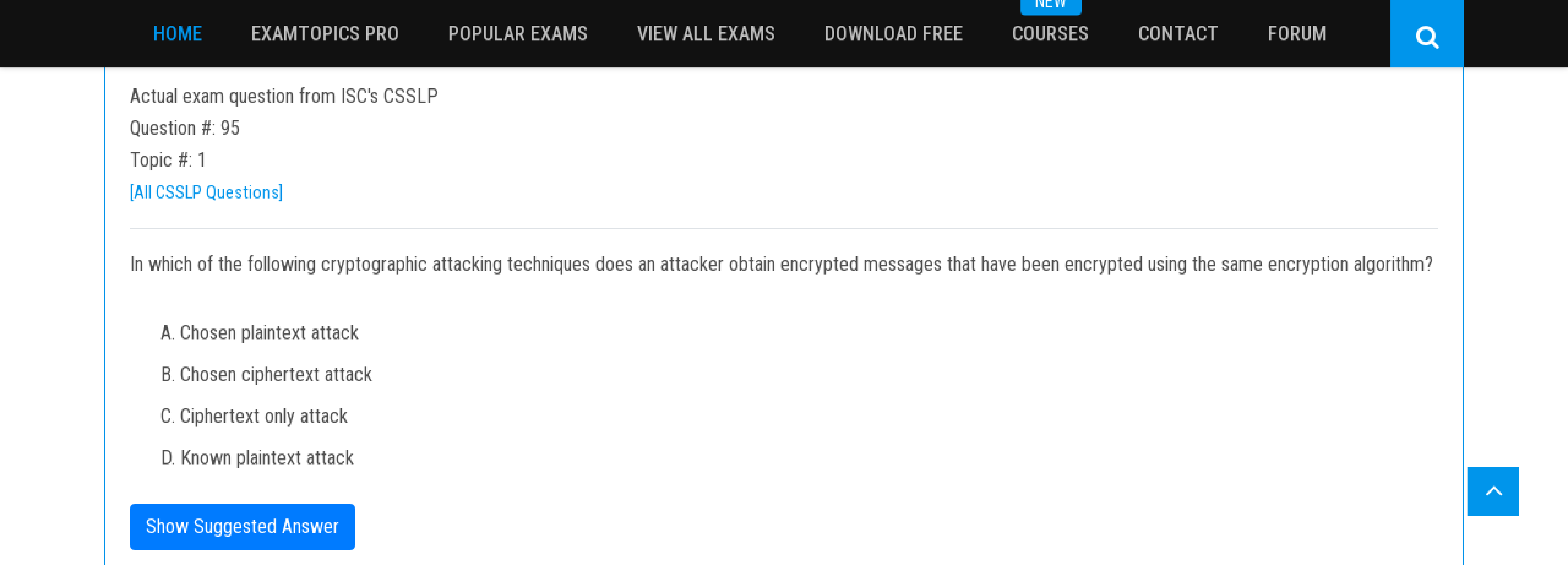
Which of the following are examples of the application programming interface (API)? Each correct answer represents a complete solution. Choose three.

A. HTML

B. PHP

C. .NET

D. Perl



Actual exam question from ISC's CSSLP

Question #: 95

Topic #: 1

[All CSSLP Questions]

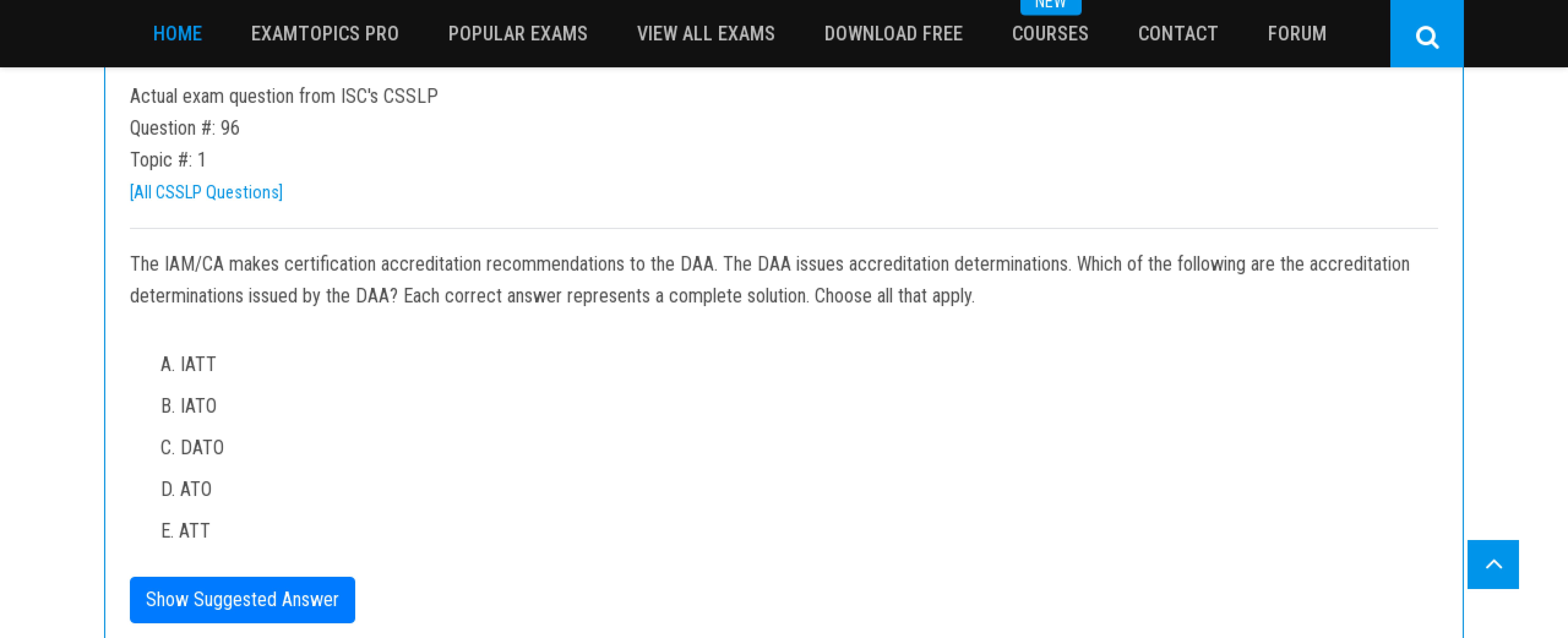
In which of the following cryptographic attacking techniques does an attacker obtain encrypted messages that have been encrypted using the same encryption algorithm?

A. Chosen plaintext attack

B. Chosen ciphertext attack

C. Ciphertext only attack

D. Known plaintext attack



Actual exam question from ISC's CSSLP

Question #: 96

Topic #: 1

[All CSSLP Questions]

The IAM/CA makes certification accreditation recommendations to the DAA. The DAA issues accreditation determinations. Which of the following are the accreditation determinations issued by the DAA? Each correct answer represents a complete solution. Choose all that apply.

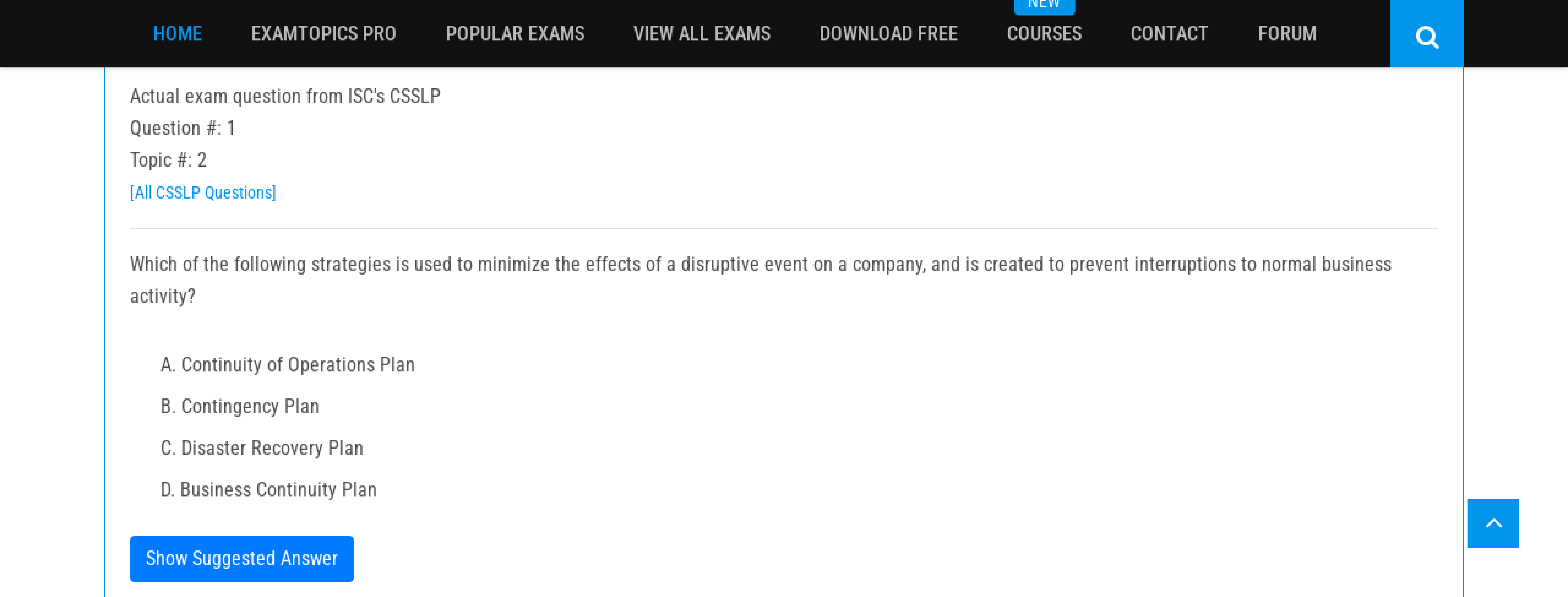
A. IATT

B. IATO

C. DATO

D. ATO

E. ATT



Actual exam question from ISC's CSSLP

Question #: 1

Topic #: 2

[All CSSLP Questions]

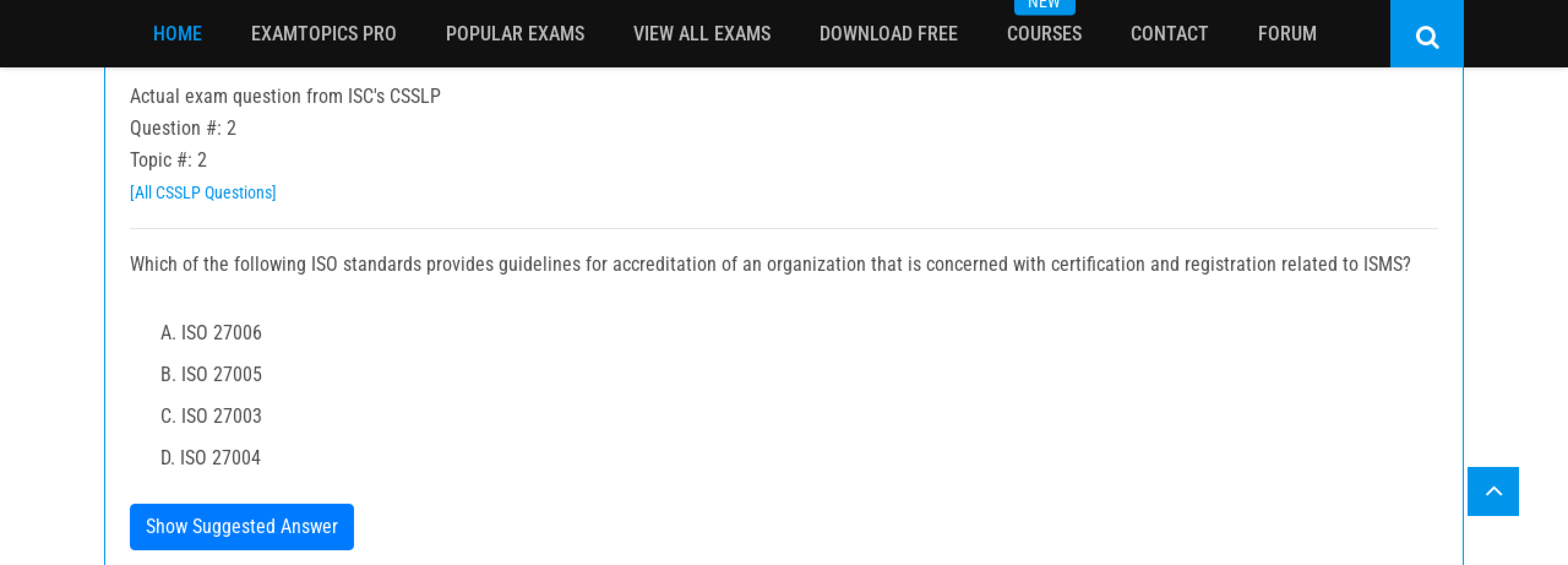
Which of the following strategies is used to minimize the effects of a disruptive event on a company, and is created to prevent interruptions to normal business activity?

A. Continuity of Operations Plan

B. Contingency Plan

C. Disaster Recovery Plan

D. Business Continuity Plan



Actual exam question from ISC's CSSLP

Question #: 2

Topic #: 2

[All CSSLP Questions]

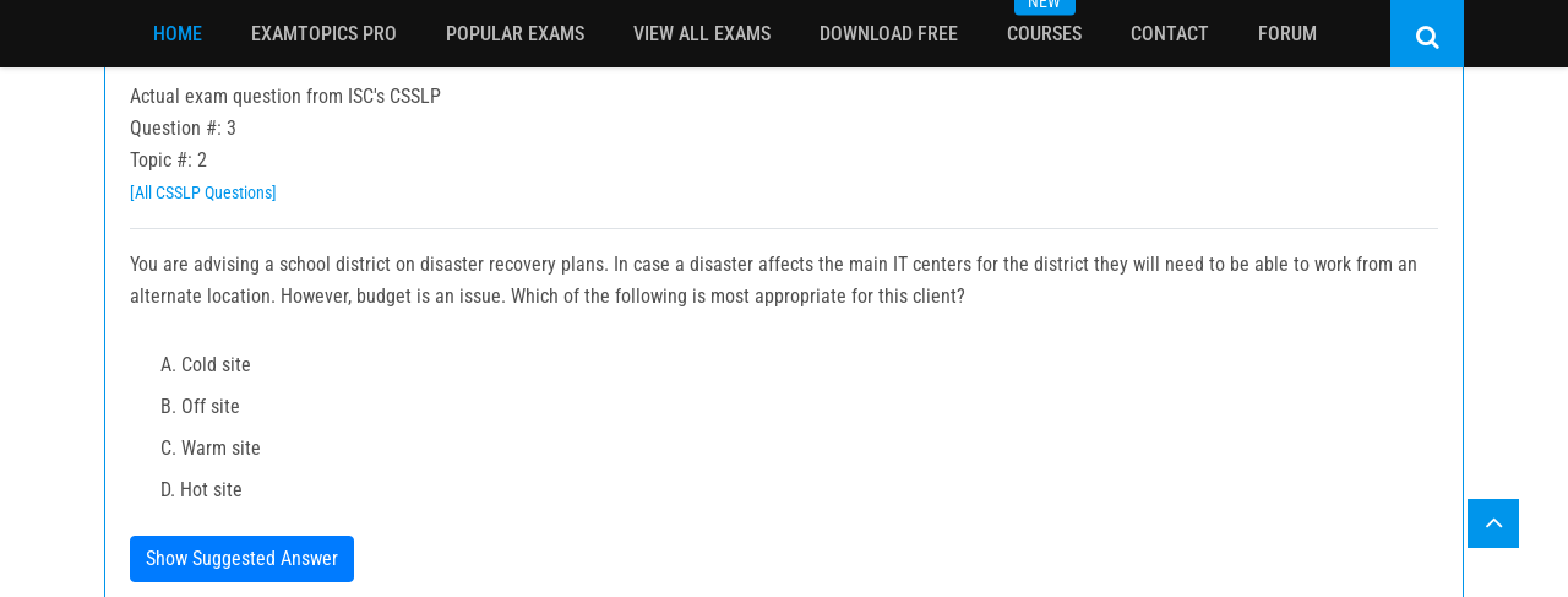
Which of the following ISO standards provides guidelines for accreditation of an organization that is concerned with certification and registration related to ISMS?

A. ISO 27006

B. ISO 27005

C. ISO 27003

D. ISO 27004



Actual exam question from ISC's CSSLP

Question #: 3

Topic #: 2

[All CSSLP Questions]

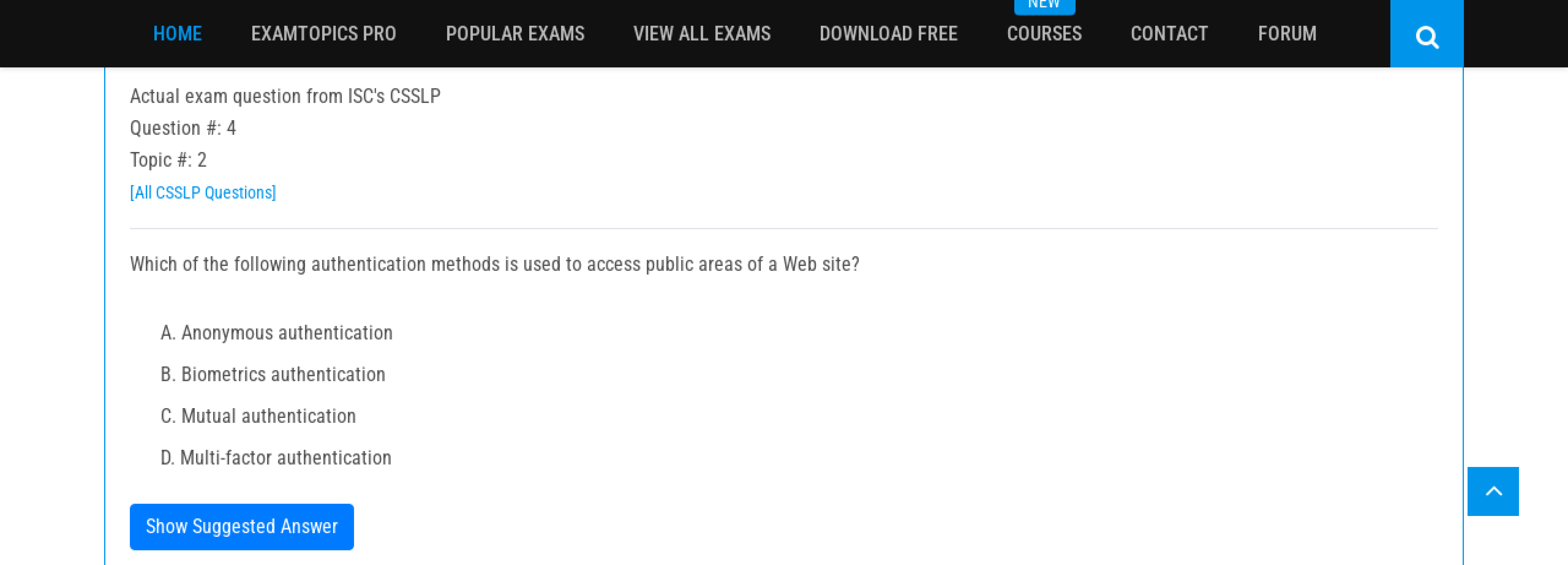
You are advising a school district on disaster recovery plans. In case a disaster affects the main IT centers for the district they will need to be able to work from an alternate location. However, budget is an issue. Which of the following is most appropriate for this client?

A. Cold site

B. Off site

C. Warm site

D. Hot site



Actual exam question from ISC's CSSLP

Question #: 4

Topic #: 2

[All CSSLP Questions]

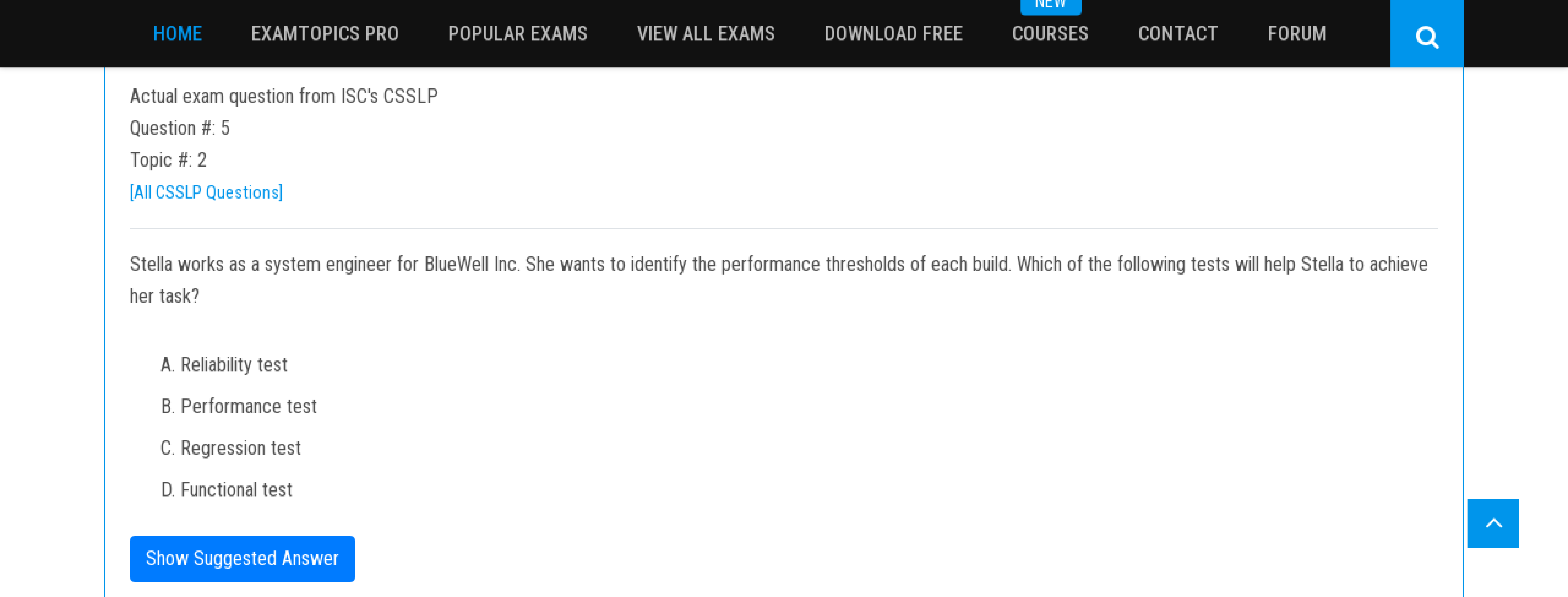
Which of the following authentication methods is used to access public areas of a Web site?

A. Anonymous authentication

B. Biometrics authentication

C. Mutual authentication

D. Multi-factor authentication



Actual exam question from ISC's CSSLP

Question #: 5

Topic #: 2

[All CSSLP Questions]

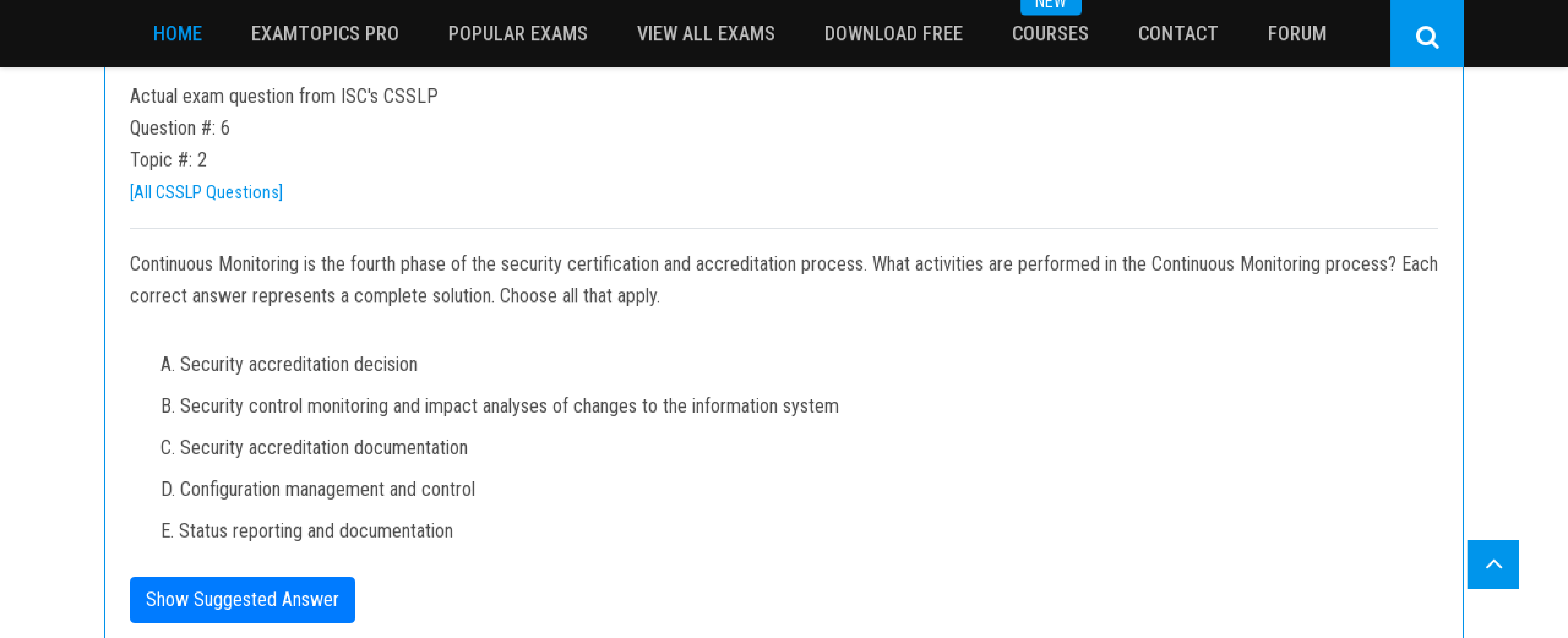
Stella works as a system engineer for BlueWell Inc. She wants to identify the performance thresholds of each build. Which of the following tests will help Stella to achieve her task?

A. Reliability test

B. Performance test

C. Regression test

D. Functional test



Actual exam question from ISC's CSSLP

Question #: 6

Topic #: 2

[All CSSLP Questions]

Continuous Monitoring is the fourth phase of the security certification and accreditation process. What activities are performed in the Continuous Monitoring process? Each correct answer represents a complete solution. Choose all that apply.

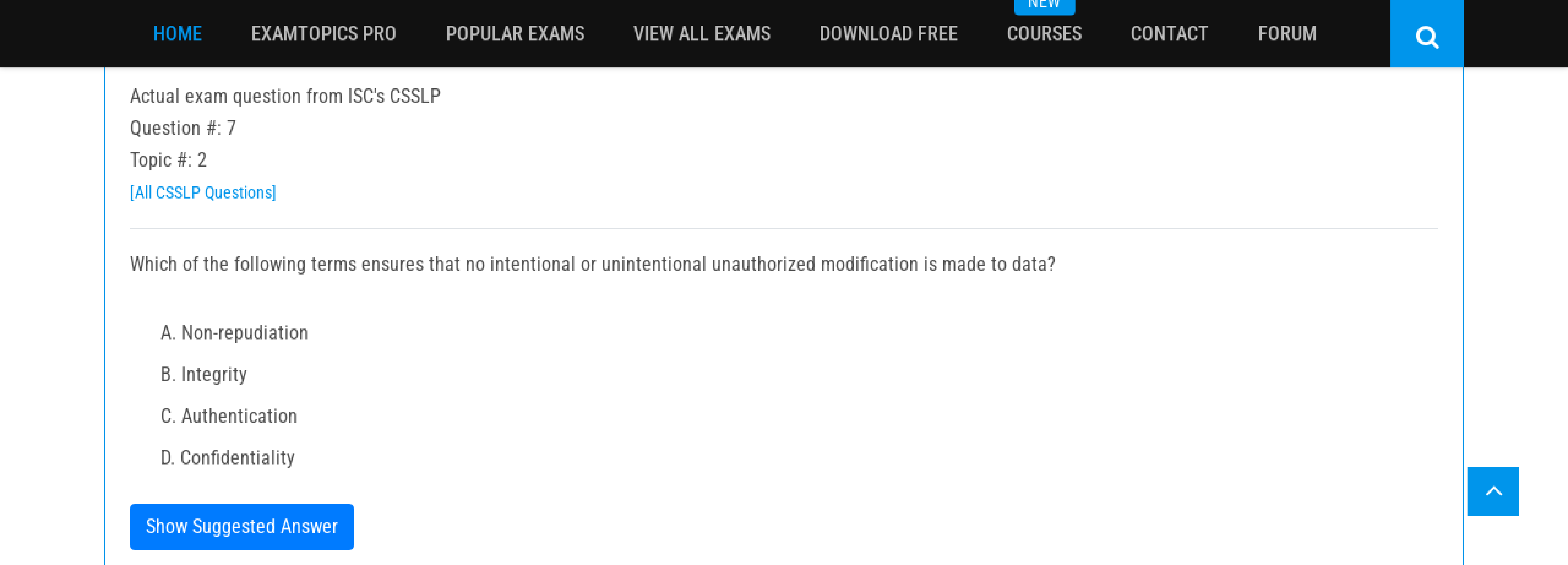
A. Security accreditation decision

B. Security control monitoring and impact analyses of changes to the information system

C. Security accreditation documentation

D. Configuration management and control

E. Status reporting and documentation



Actual exam question from ISC's CSSLP

Question #: 7

Topic #: 2

[All CSSLP Questions]

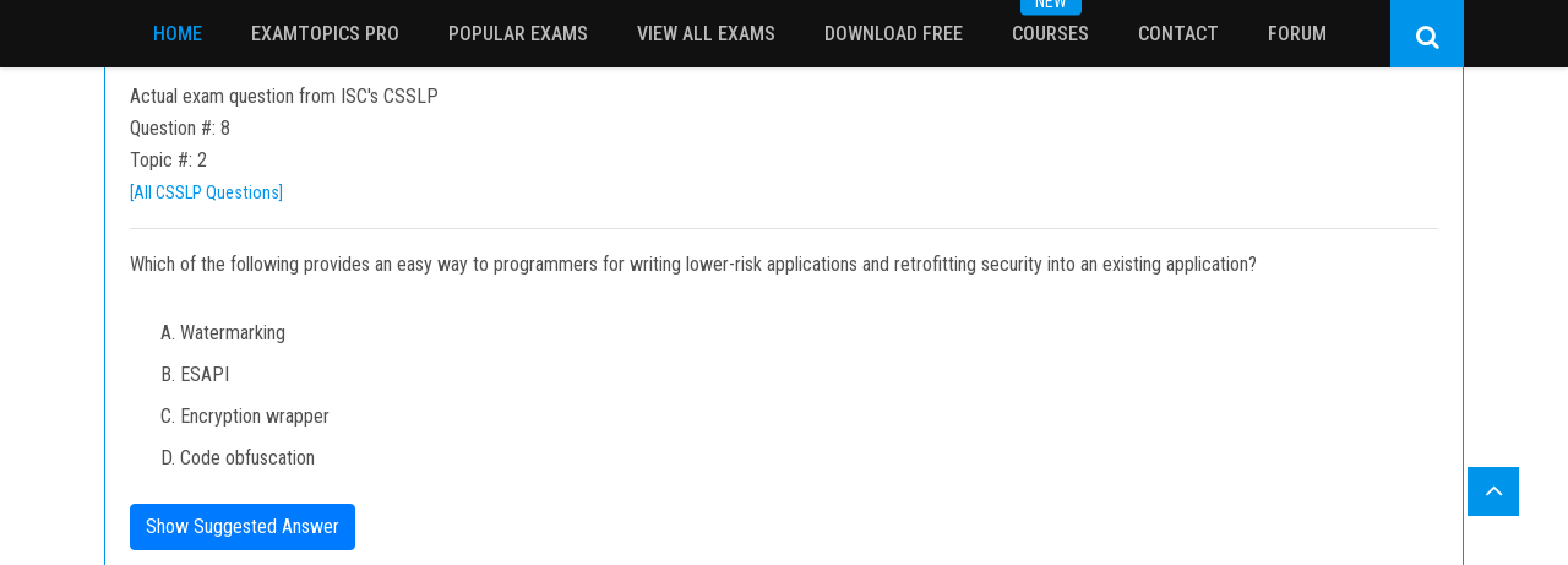
Which of the following terms ensures that no intentional or unintentional unauthorized modification is made to data?

A. Non-repudiation

B. Integrity

C. Authentication

D. Confidentiality



Actual exam question from ISC's CSSLP

Question #: 8

Topic #: 2

[All CSSLP Questions]

Which of the following provides an easy way to programmers for writing lower-risk applications and retrofitting security into an existing application?

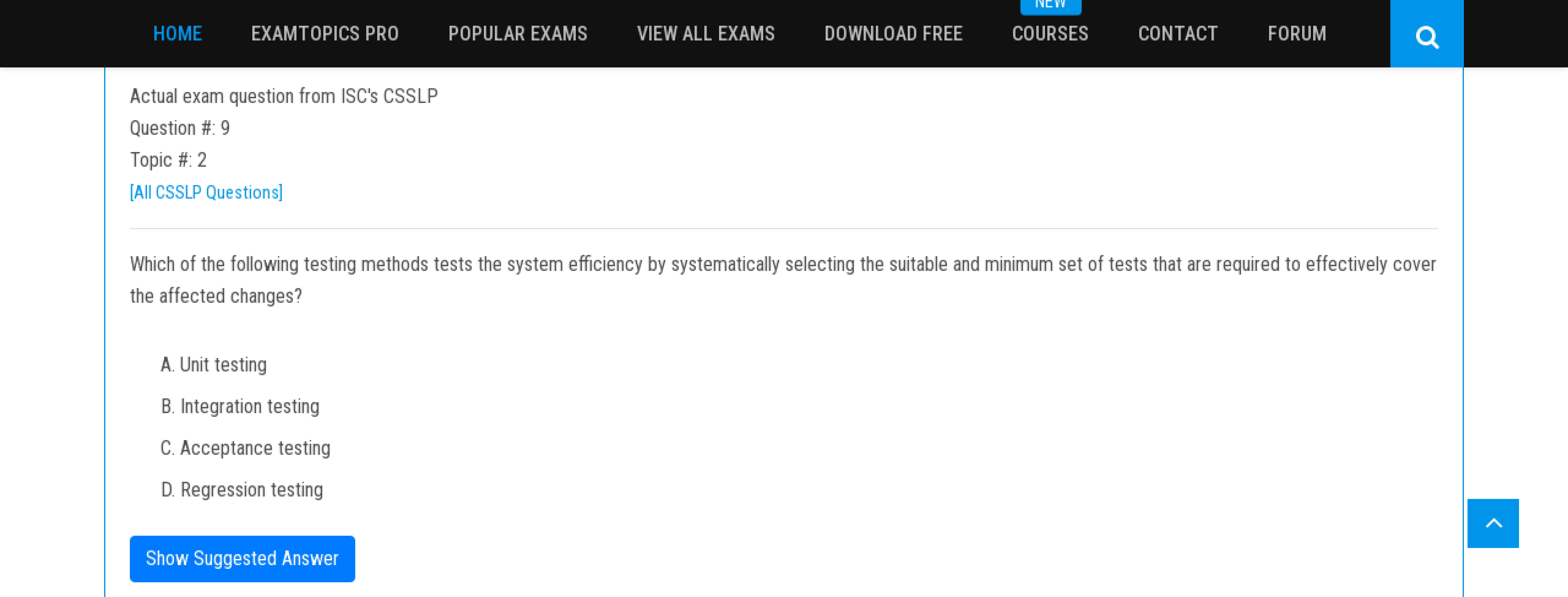
A. Watermarking

B. ESAPI

C. Encryption wrapper

D. Code obfuscation

Show Suggested Answer



Actual exam question from ISC's CSSLP

Question #: 9

Topic #: 2

[All CSSLP Questions]

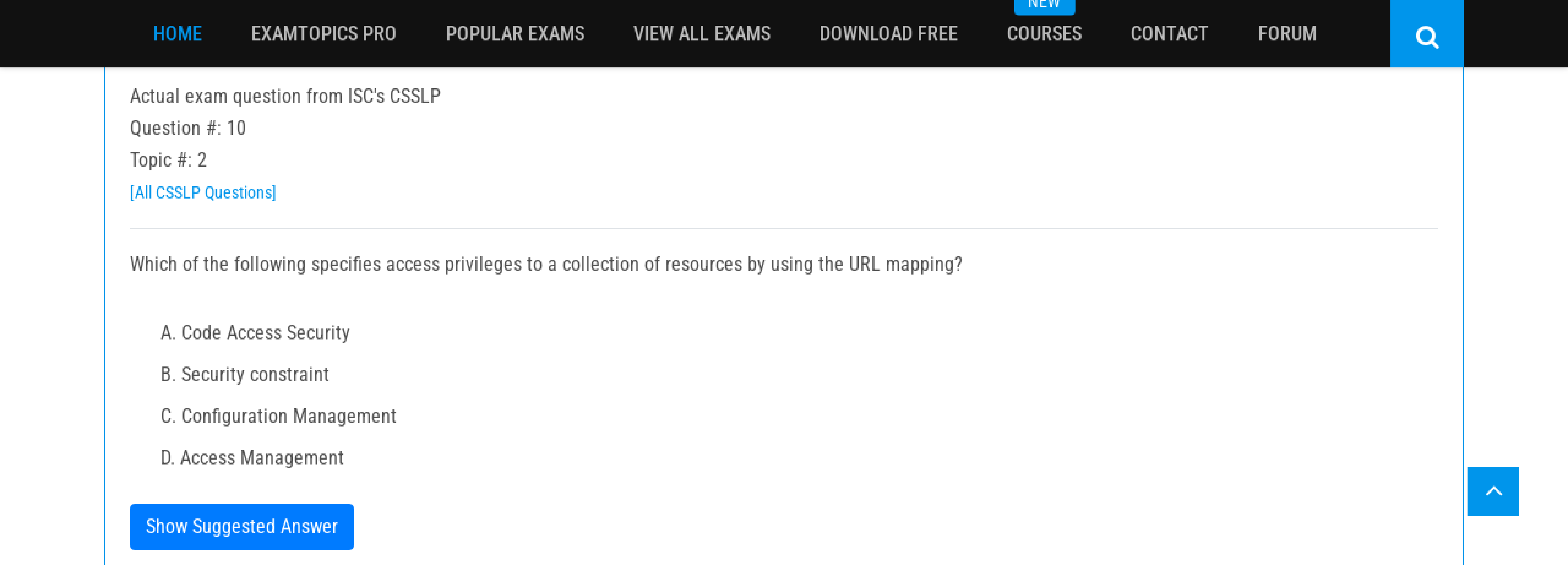
Which of the following testing methods tests the system efficiency by systematically selecting the suitable and minimum set of tests that are required to effectively cover the affected changes?

A. Unit testing

B. Integration testing

C. Acceptance testing

D. Regression testing



Actual exam question from ISC's CSSLP

Question #: 10

Topic #: 2

[All CSSLP Questions]

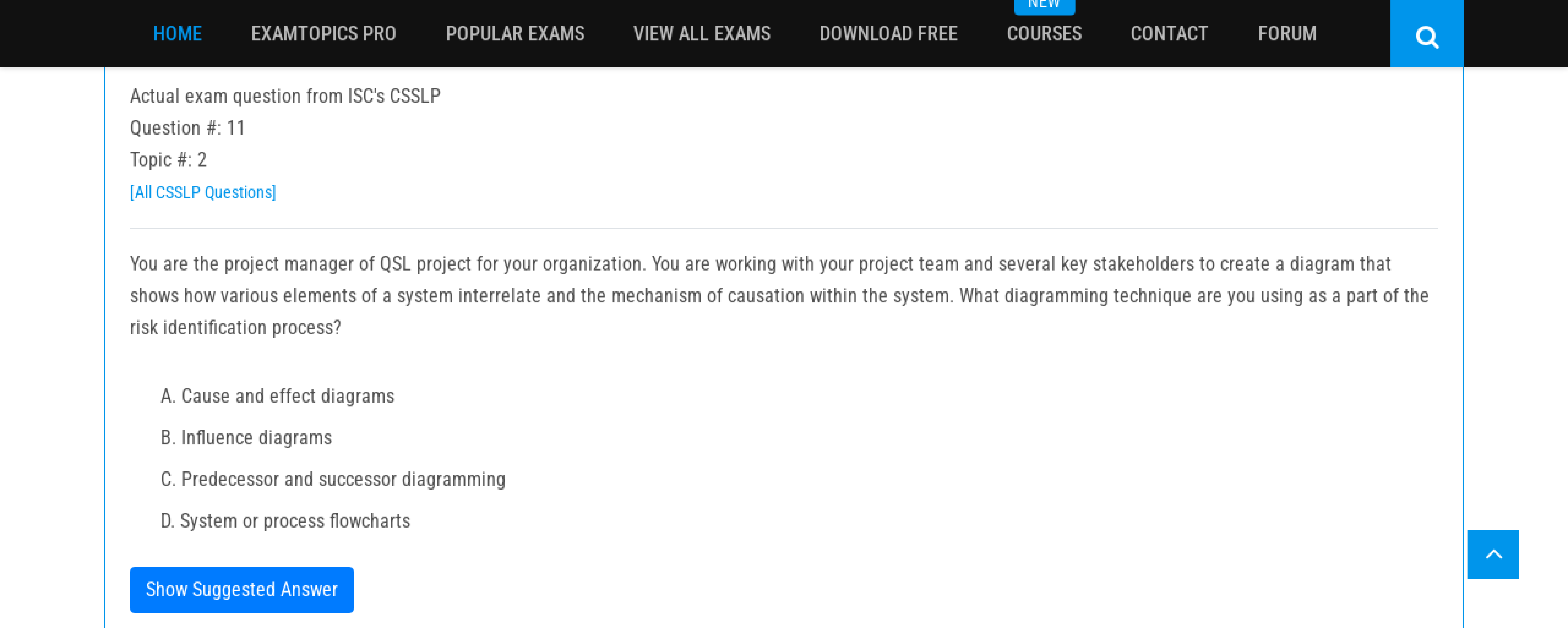
Which of the following specifies access privileges to a collection of resources by using the URL mapping?

A. Code Access Security

B. Security constraint

C. Configuration Management

D. Access Management



Actual exam question from ISC's CSSLP

Question #: 11

Topic #: 2

[All CSSLP Questions]

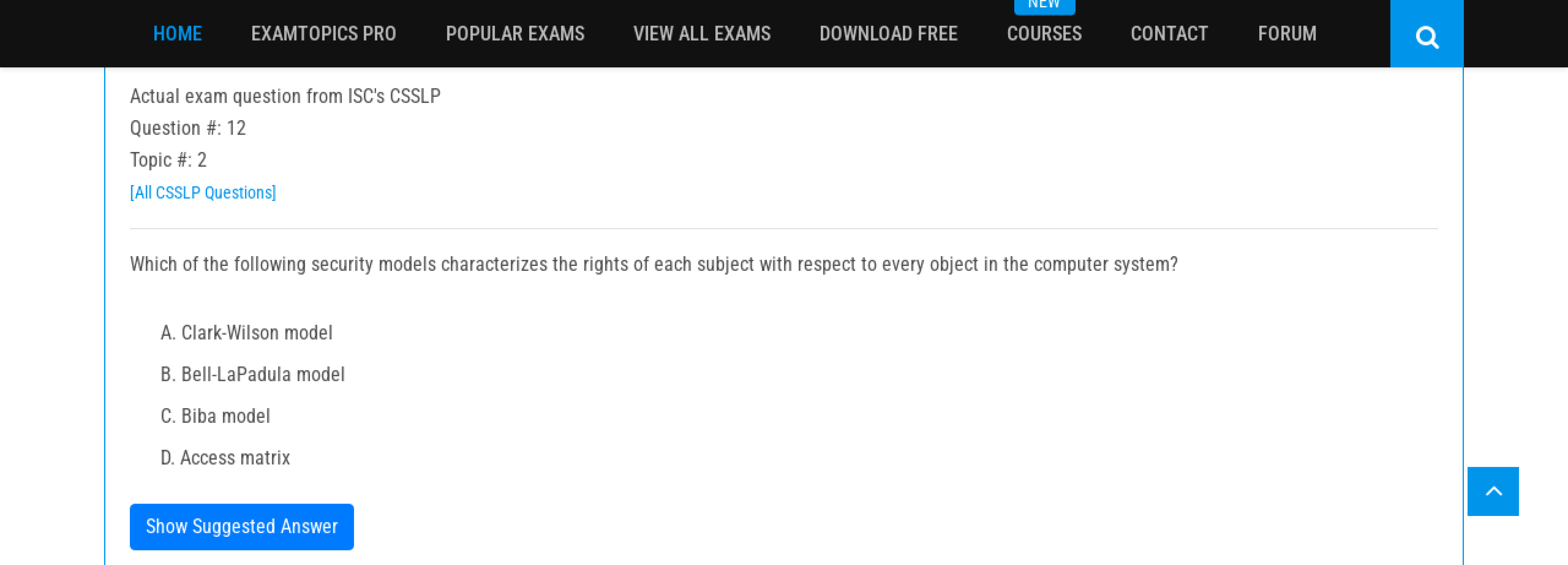
You are the project manager of QSL project for your organization. You are working with your project team and several key stakeholders to create a diagram that shows how various elements of a system interrelate and the mechanism of causation within the system. What diagramming technique are you using as a part of the risk identification process?

A. Cause and effect diagrams

B. Influence diagrams

C. Predecessor and successor diagramming

D. System or process flowcharts



Actual exam question from ISC's CSSLP

Question #: 12

Topic #: 2

[All CSSLP Questions]

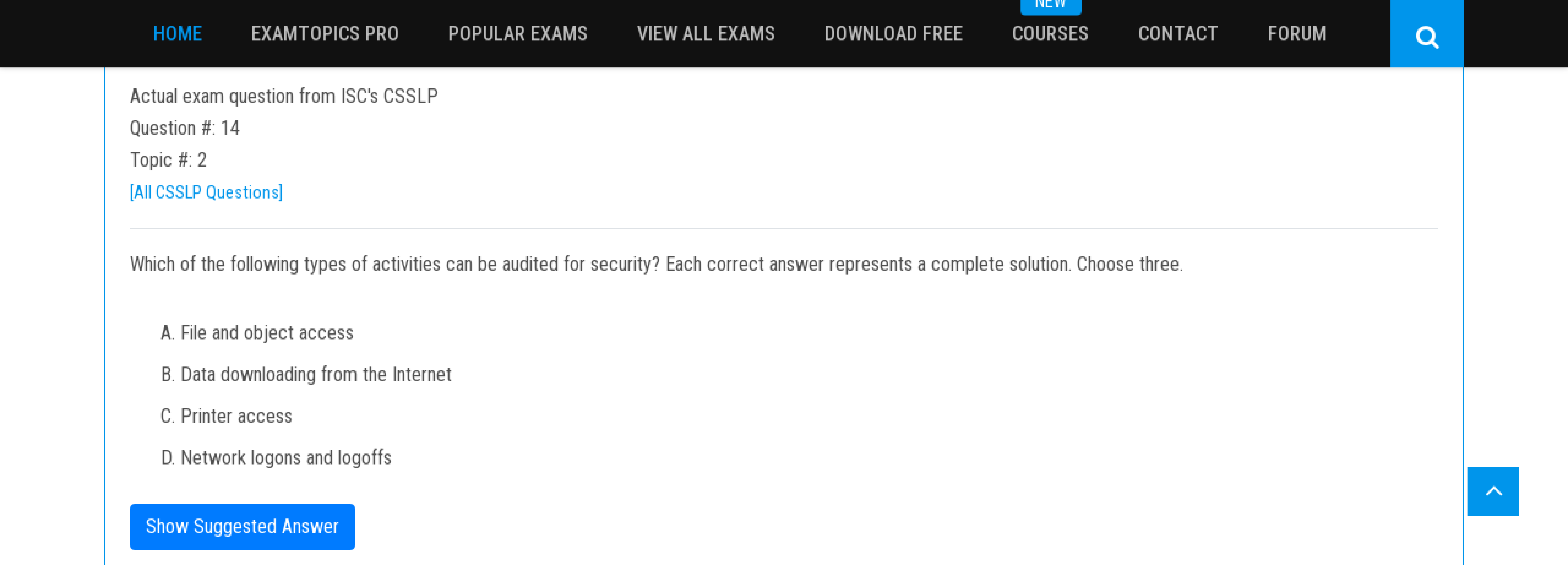
Which of the following security models characterizes the rights of each subject with respect to every object in the computer system?

A. Clark-Wilson model

B. Bell-LaPadula model

C. Biba model

D. Access matrix



Actual exam question from ISC's CSSLP

Question #: 14

Topic #: 2

[All CSSLP Questions]

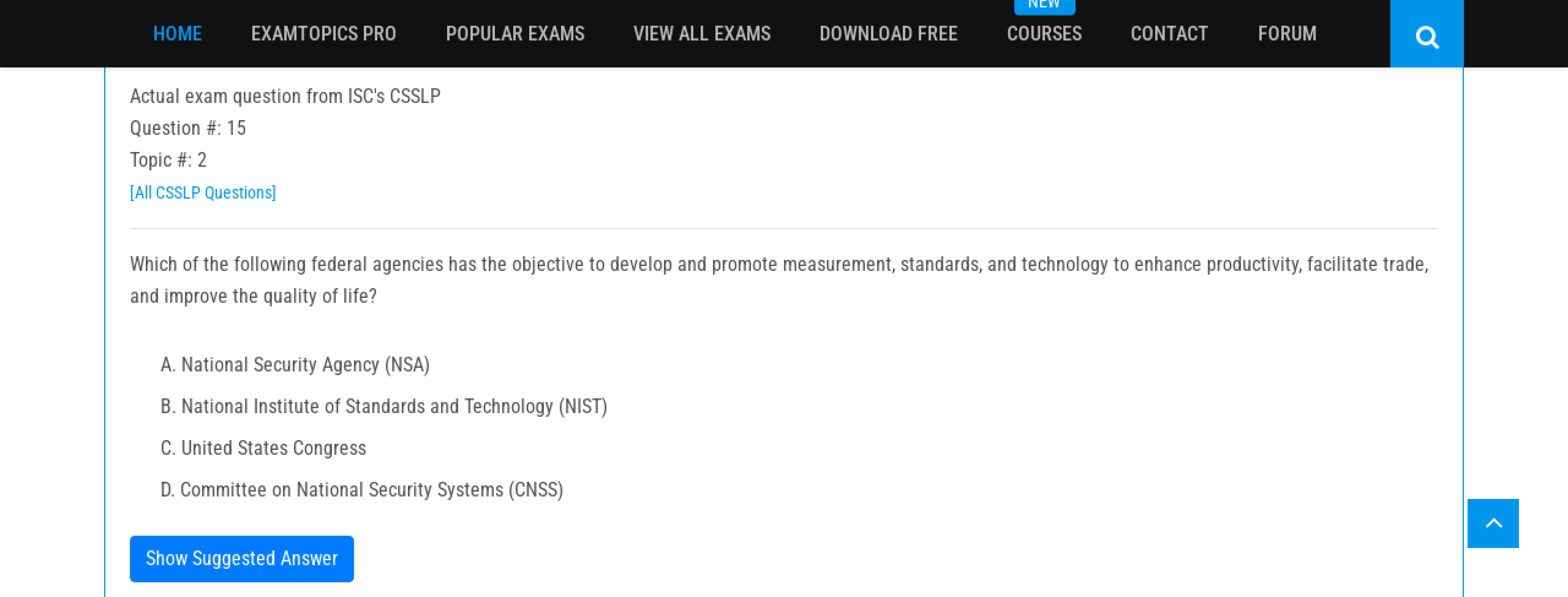
Which of the following types of activities can be audited for security? Each correct answer represents a complete solution. Choose three.

A. File and object access

B. Data downloading from the Internet

C. Printer access

D. Network logons and logoffs



Actual exam question from ISC's CSSLP

Question #: 15

Topic #: 2

[All CSSLP Questions]

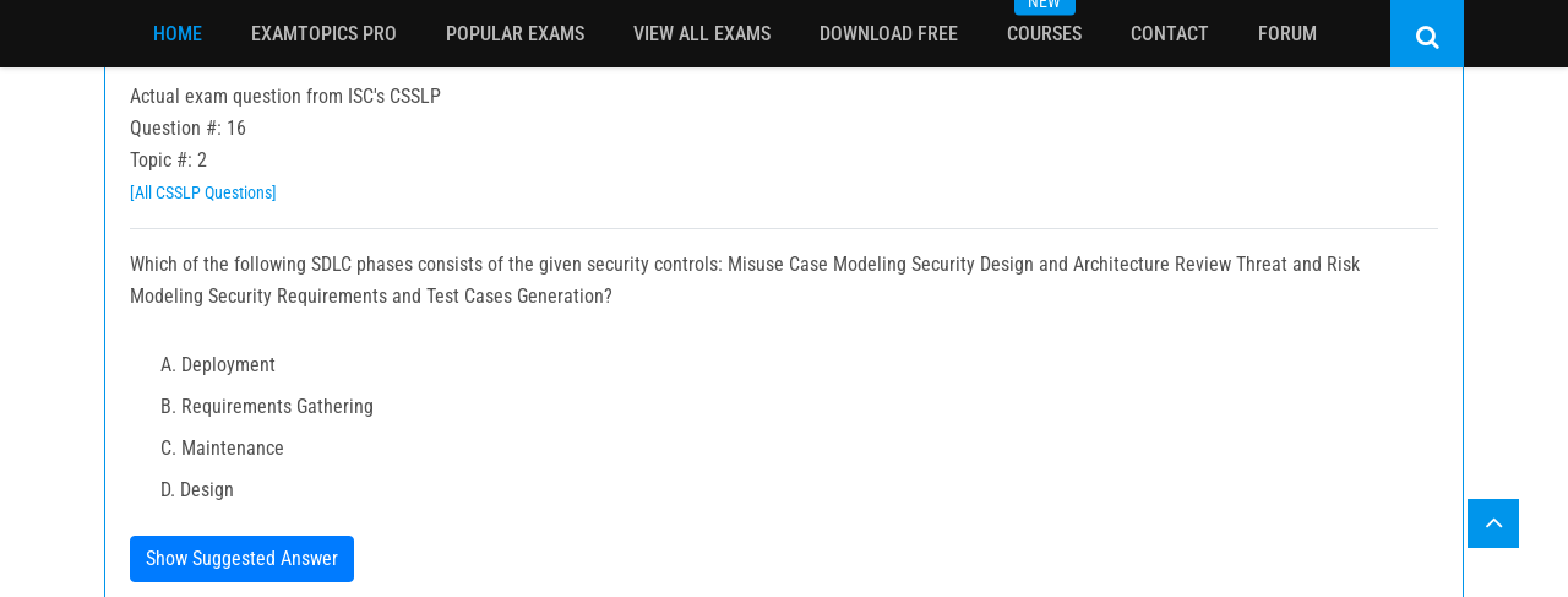
Which of the following federal agencies has the objective to develop and promote measurement, standards, and technology to enhance productivity, facilitate trade, and improve the quality of life?

A. National Security Agency (NSA)

B. National Institute of Standards and Technology (NIST)

C. United States Congress

D. Committee on National Security Systems (CNSS)



Actual exam question from ISC's CSSLP

Question #: 16

Topic #: 2

[All CSSLP Questions]

Which of the following SDLC phases consists of the given security controls: Misuse Case Modeling Security Design and Architecture Review Threat and Risk Modeling Security Requirements and Test Cases Generation?

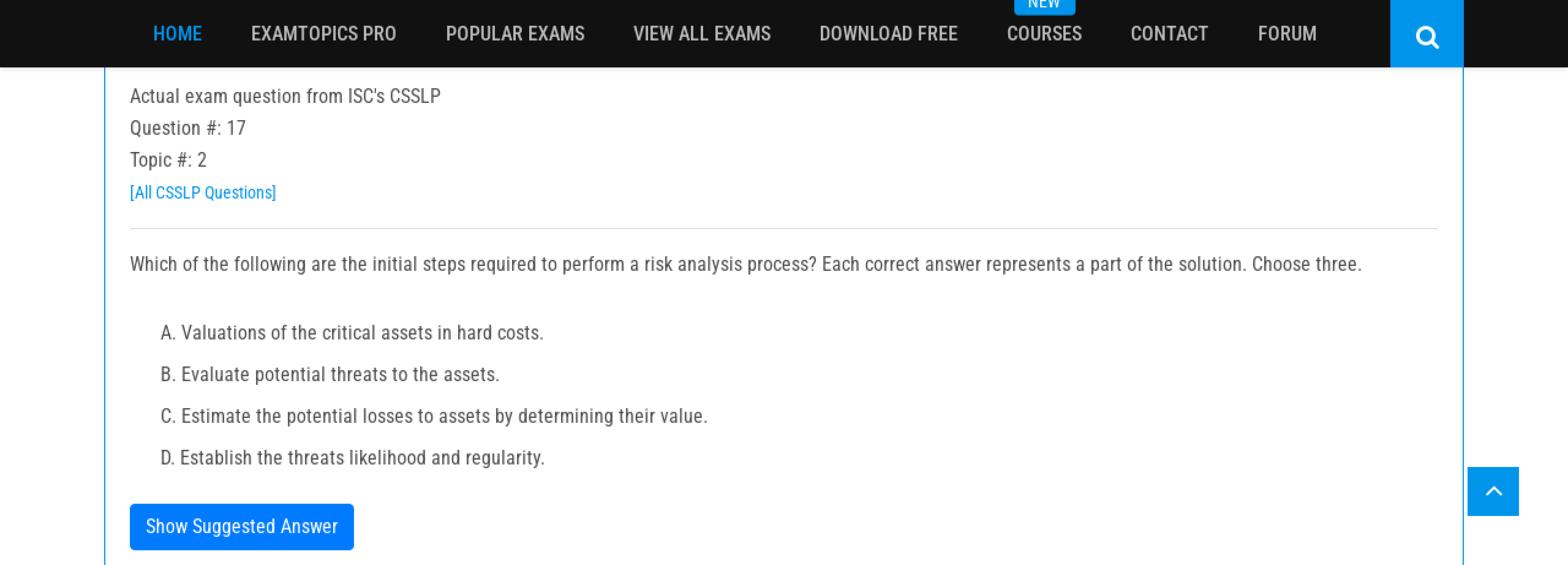
A. Deployment

B. Requirements Gathering

C. Maintenance

D. Design

Show Suggested Answer



Actual exam question from ISC's CSSLP

Question #: 17

Topic #: 2

[All CSSLP Questions]

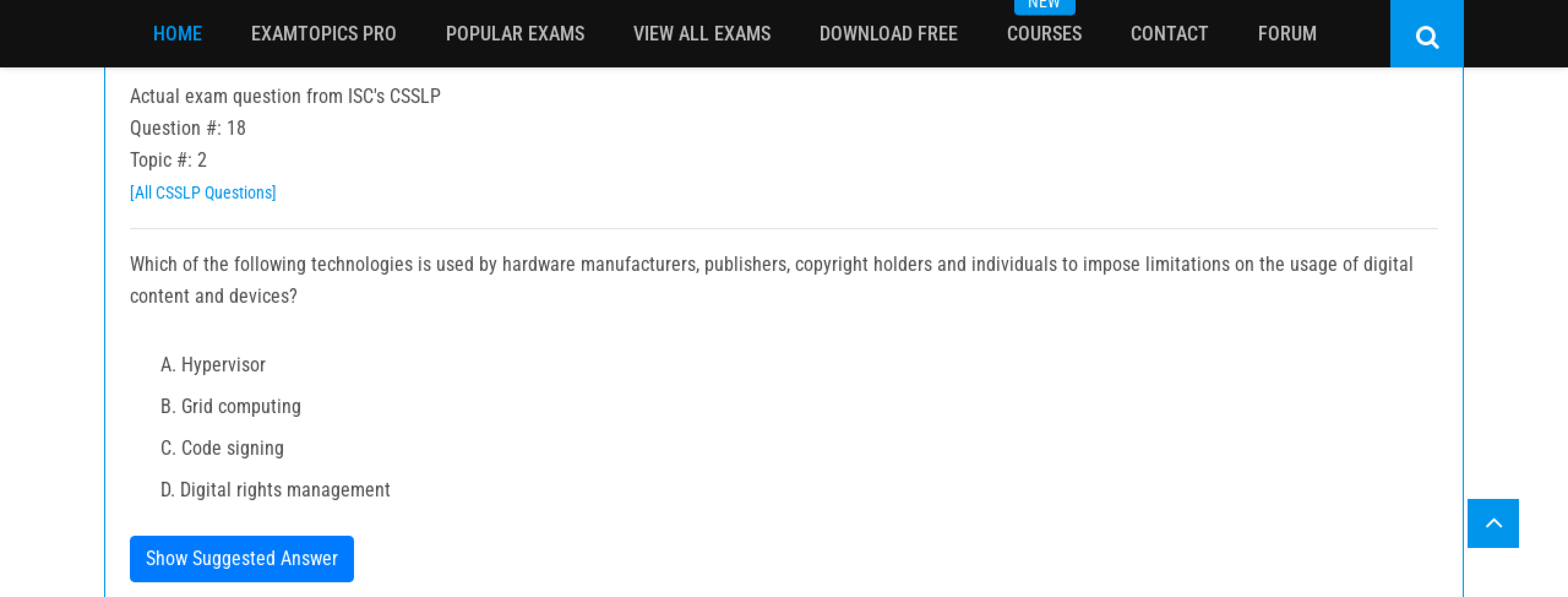
Which of the following are the initial steps required to perform a risk analysis process? Each correct answer represents a part of the solution. Choose three.

A. Valuations of the critical assets in hard costs.

B. Evaluate potential threats to the assets.

C. Estimate the potential losses to assets by determining their value.

D. Establish the threats likelihood and regularity.



Actual exam question from ISC's CSSLP

Question #: 18

Topic #: 2

[All CSSLP Questions]

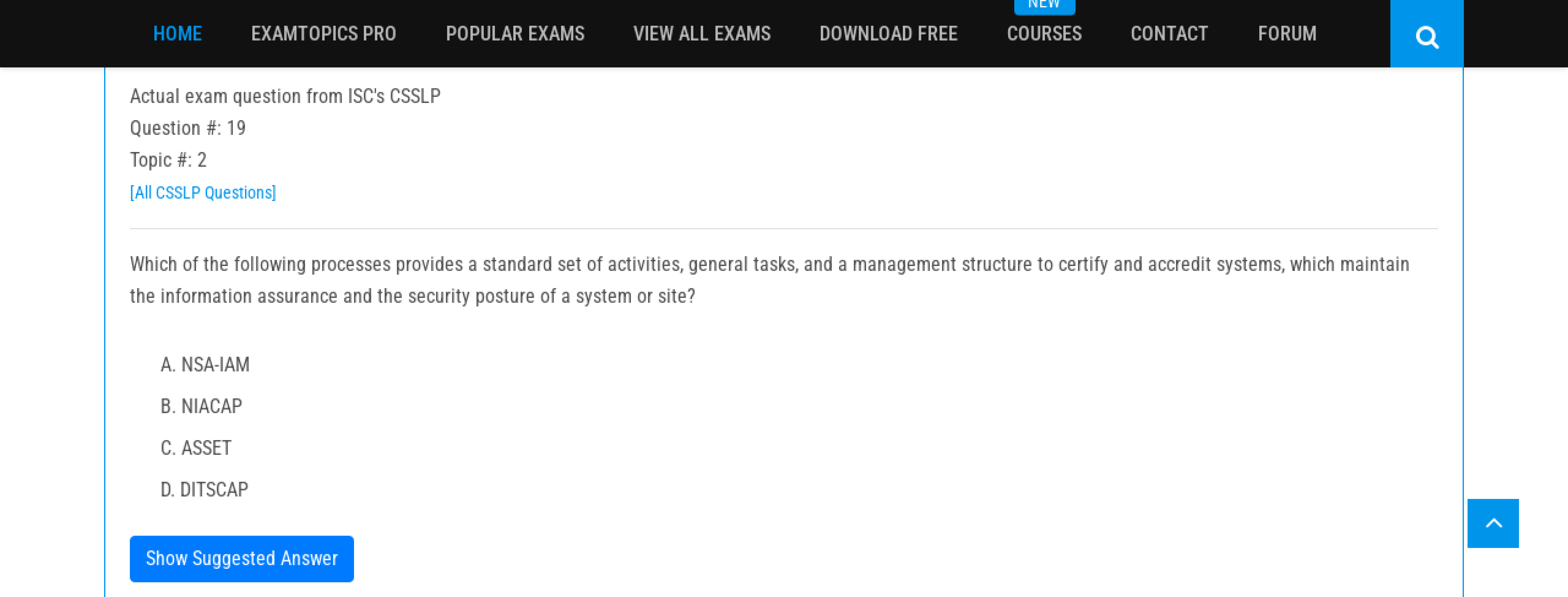
Which of the following technologies is used by hardware manufacturers, publishers, copyright holders and individuals to impose limitations on the usage of digital content and devices?

A. Hypervisor

B. Grid computing

C. Code signing

D. Digital rights management



Actual exam question from ISC's CSSLP
Question #: 19
Topic #: 2
[All CSSLP Questions]

Which of the following processes provides a standard set of activities, general tasks, and a management structure to certify and accredit systems, which maintain the information assurance and the security posture of a system or site?

A. NSA-IAM

B. NIACAP

C. ASSET

D. DITSCAP

Actual exam question from ISC's CSSLP

Question #: 20

Topic #: 2

[All CSSLP Questions]

Which of the following security issues does the Bell-La Padula model focus on?

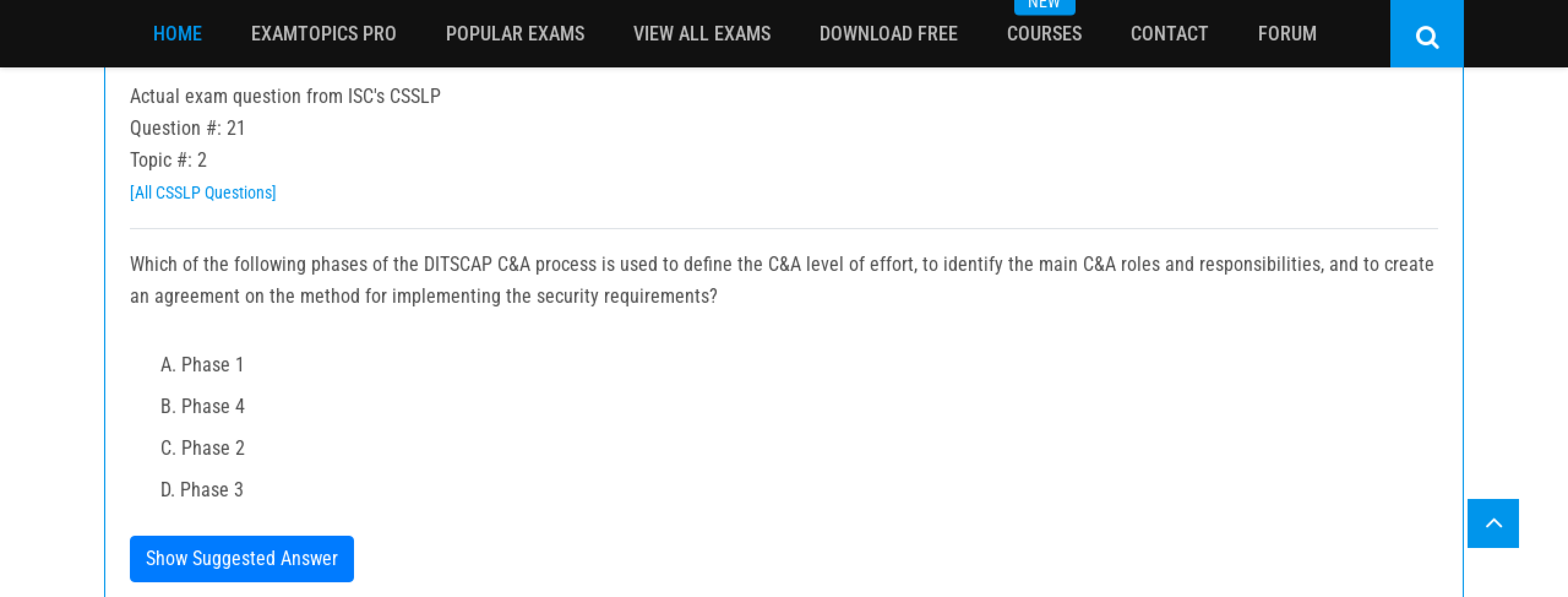
A. Authorization

B. Confidentiality

C. Integrity

D. Authentication

Show Suggested Answer



Actual exam question from ISC's CSSLP

Question #: 21

Topic #: 2

[All CSSLP Questions]

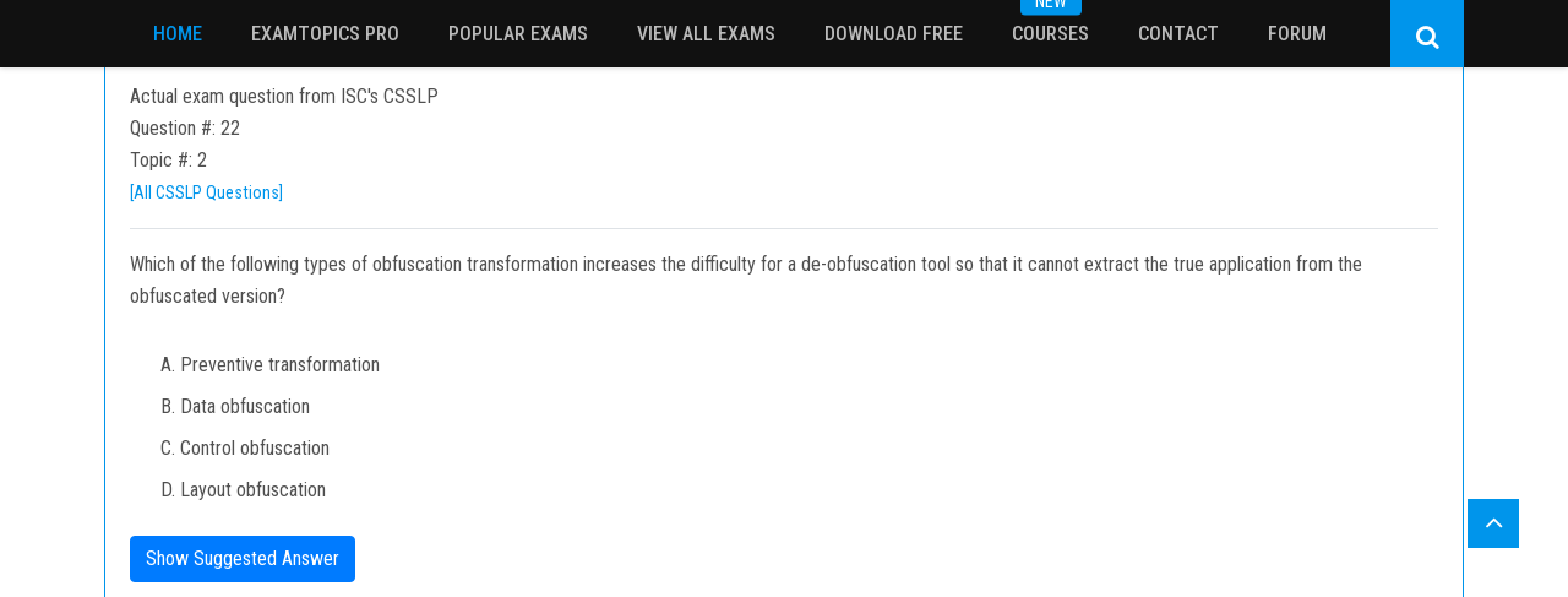
Which of the following phases of the DITSCAP C&A process is used to define the C&A level of effort, to identify the main C&A roles and responsibilities, and to create an agreement on the method for implementing the security requirements?

A. Phase 1

B. Phase 4

C. Phase 2

D. Phase 3



Actual exam question from ISC's CSSLP
Question #: 22
Topic #: 2
[All CSSLP Questions]

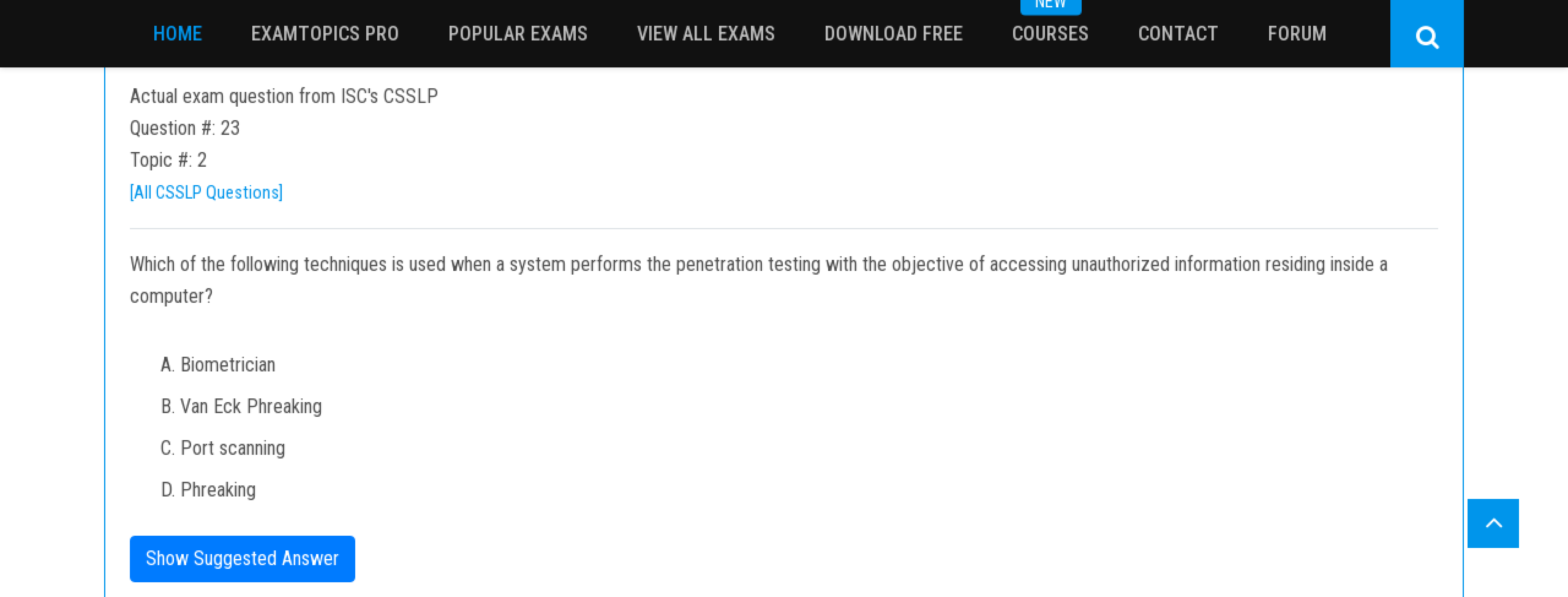
Which of the following types of obfuscation transformation increases the difficulty for a de-obfuscation tool so that it cannot extract the true application from the obfuscated version?

A. Preventive transformation

B. Data obfuscation

C. Control obfuscation

D. Layout obfuscation



Actual exam question from ISC's CSSLP

Question #: 23

Topic #: 2

[All CSSLP Questions]

Which of the following techniques is used when a system performs the penetration testing with the objective of accessing unauthorized information residing inside a computer?

A. Biometrician

B. Van Eck Phreaking

C. Port scanning

D. Phreaking