SECURE CODE
ALLIANCE

Sample CSCAP & CSCAA Exam Questions

Version 2023.1

EXECUTIVE SUMMARY

The following questions are examples of what you can expect on the Certified SCA Practitioner (**CSCAP**) and Certified SCA Architect (**CSCAA**) exams.

Software developers (practitioners) are expected to use Secure Development Lifecycle (**SDL**) processes for new systems, system upgrades, or systems that are being repurposed. These processes can be employed at any stage of the system lifecycle and can take advantage of any system or software development methodology, including agile, spiral, or waterfall. Therefore, CSCAPs are expected to:

- Understand and operationalize the organization's security architecture that must be followed for application development processes for development, testing, staging, and production environments.
- Incorporate the organization's risk management practices throughout application development processes across the entire Software/System Development Life Cycle (**SDLC**).
- Develop software applications in accordance with industry-recognized secure coding practices.
- Incorporate security and privacy measures throughout the SDLC.
- Control changes to applications, systems, and processes across the SDLC using formal change control procedures.
- Review custom code through a formal change management and approval process prior to release to production.
- Remove custom application accounts, user IDs and passwords before applications become active or are released to customers.
- Confidently review Software Bill of Materials (**SBOM**) documentation for security and privacy-related implications.
- Perform software conformity assessments.

Software architects (architects) are expected to employ cyber resiliency constructs (e.g., goals, objectives, techniques, approaches, and design principles), as well as the analytic and lifecycle processes, to tailor them to the technical, operational, and threat environments for which the architect's systems need to be engineered. Therefore, CSCAAs are expected to:

- Define the security architecture(s) the organization will follow for application development processes.
- Define application development considerations for the organization's risk management practices across the entire SDLC.
- Publish rules for the organization's application development processes for development, testing, staging, and production environments.
- Develop conformity assessment practices for the organization to follow in order to demonstrate alignment with stated Secure Software Development Practices.
- Ensure that information security and privacy principles are an integral part of Secure Software Development Practices (**SSDP**) across the entire SDLC.
- Ensure security & privacy-related measures are included in the requirements for new systems or enhancements to existing systems.
- Ensure application development practices (internal and external) adhere to industry-recognized secure coding practices.
- Develop SBOM documentation for application development projects.
- Oversee changes to Applications, Services and Processes (**ASP**) across the SDLC using formal change control procedures.
- Oversee application security testing practices.
- implement the SSDP concepts and techniques for all High-Value Assets (**HVA**):
  - New Systems;
  - Dedicated or Special-Purpose Systems;
  - System of Systems;
  - System Modifications;
  - System Evolution; and
  - System Retirement.

Example CSCAP & CSCAA Questions

Example Question #1

When working on a software project, it's imperative to conduct a quality control process to ensure the results provide error-free code? [1]

A. True
B. False

Example Question #2

Which of the following is not a core principle of password-based authentication? [2]

A. Password strength
B. Ensure uniqueness
C. Force complexity
D. Use passphrases
E. Enforce multi-factor authentication
F. Use a password manager

Example Question #3

The Digital Millennium Copyright Act (DMCA): [3]

A. Enables registered copyright owners to file an infringement lawsuit in federal court.
B. Encourages copyright owners to give greater access to their works in digital formats.
C. Reverse engineering for the purposes of making a program usable with a wider range of other programs to promote a competitive technological market
D. Only A & B
E. Only A & C

Example Question #4

Why should CAPTCHA (Completely Automated Public Turing test to tell Computers and Humans Apart) be used in a web application? [4]

A. Protects from bots that can read and solve complex problems
B. Protects the user from spam
C. Protects the user from password decryption
D. Protection from remote digital entry
E. None of the above

Example Question #5

Adopting a Secure Software Development Framework (SSDF) helps mitigate the risk of software vulnerabilities. Which of the following is a true statement for making verification information available to software consumers? [5]

A. It’s acceptable to post cryptographic hashes for release files on an unsecured website
B. Periodically review the code signing processes, including certificate renewal and protection
C. Do not store all release files in a repository
D. All of the above
E. None of the above

[1] *Correct answer = A | References NIST SP 800-160 vol 1 rev 1 Appendix I.8 and NIST SP 800-161 rev 1 Section 3.4.1 (Foundational Practices)*

[2] *Correct answer = C | References NIST SP 800-53 rev 5 control IA-5(1) and OWASP Top 10 A07*

[3] *Correct answer = D | Reference Copyright.gov*

[4] *Correct answer = E | Reference OWASP Top 10 A01 & A07*

[5] *Correct answer = B | References NIST SP 800-170 vol 2 rev 1 Appendices D & E and NIST SP 800-218 PS.2*

EXAMPLE QUESTION #6

System security engineering principles include which of the following? [6]

A. Establishing security and privacy policies, architecture, and controls as the foundation for design and development
B. Delineating physical and logical security boundaries
C. Tailoring controls to meet organizational needs
D. Determining compensating controls needed to mitigate risk
E. All the above
F. None of the above

EXAMPLE QUESTION #7

Dynamic code analyses provide: [7]

A. Tools that attempt to highlight possible vulnerabilities within non-running source code by using techniques such as Taint Analysis and Data Flow Analysis
B. Runtime verification of software programs using tools capable of monitoring programs for memory corruption
C. Peer review to expose flaws in coding
D. User privilege issues
E. Testing that introduces program failures by deliberately introducing malformed or random data into software programs
F. All the above
G. Only A & C
H. Only B, D & E

EXAMPLE QUESTION #8

A "criticality analysis" requires the developer of the system, system component, or system service to analyze organization-defined decision points in the system development life cycle. Developer input is especially important when organizations conduct supply chain criticality analyses. [8]

A. True
B. False

EXAMPLE QUESTION #9

Which of the following helps effectively reduce the level of privacy risk created by a system? [9]

A. Using de-identification or synthetic data in test environments
B. Using known PII for test purposes
C. Using production system data for test purposes
D. Limiting the use of PII during the development
E. All the above
F. Only B & C
G. Only A & D

EXAMPLE QUESTION #10

Providing a purchaser with a Software Bill of Materials (SBOM) for a product by publishing it on a public website is an applicable SSDP practice. [10]

A. True
B. False

[6] *Correct answer = E | Reference NIST SP 800-53 rev 5 control SA-8*
[7] *Correct answer = H | Reference NIST SP 800-53 rev 5 control SA-11(8)*
[8] *Correct answer = A | Reference NIST SP 800-53 rev 5 control SA-15(3)*
[9] *Correct answer = G | Reference NIST SP 800-160 vol 2 rev 1 Appendix E*
[10] *Correct answer = A | References NIST SP 800-161 rev 1 and NIST SP 800-53 rev 5 control SR-4*

Example Question #11

What are acceptable methods for attesting to conformity with secure software development practices? [11]

A. Define quality metrics at the beginning of the development process
B. Require the developer to provide evidence of meeting the quality metrics
C. Provide organization-defined program review milestones
D. Provide organization-defined frequency
E. All the above
F. Only A & B
G. Only C & D

Example Question #12

An input validation attack is which of the following? [12]

A. Data exposure directly from the database due to improper input validation
B. Data exposure or vulnerability exploitation by entering specially crafted inputs into the application
C. Application users can pass malformed inputs and overwrite the memory of the application server
D. None of the above

[11] *Correct answer = E | Reference FIPS 200 and NIST SP 800-53 rev 5 controls CA-1, SA-1 & SR-3*

[12] *Correct answer = B | Reference OWASP Top 10 A03*