CAP®

Certified Authorization Professional

An (ISC)² Certification

Certification **Exam Outline**

Effective Date: October 15, 2018

(ISC)² INSPIRING A SAFE AND SECURE CYBER WORLD.

About CAP

The Certified Authorization Professional (CAP) is an information security practitioner who advocates for security risk management in pursuit of information system authorization to support an organization's mission and operations in accordance with legal and regulatory requirements.

The broad spectrum of topics included in the CAP Common Body of Knowledge (CBK) ensure its relevancy across all disciplines in the field of information security. Successful candidates are competent in the following 7 domains:

- Information Security Risk Management Program
- Categorization of Information Systems (IS)
- Selection of Security Controls
- Implementation of Security Controls
- Assessment of Security Controls
- Authorization of Information Systems (IS)
- Continuous Monitoring

Experience Requirements

Candidates must have a minimum of 2 years cumulative work experience in 1 or more of the 7 domains of the CAP CBK.

A candidate that doesn't have the required experience to become a CAP may become an Associate of (ISC)² by successfully passing the CAP examination. The Associate of (ISC)² will then have 3 years to earn the 2 year required experience. You can learn more about CAP experience requirements and how to account for part-time work and internships at www.isc2.org/Certifications/CAP/experience-requirements.

Accreditation

CAP is in compliance with the stringent requirements of ANSI/ISO/IEC Standard 17024.

Job Task Analysis (JTA)

(ISC)² has an obligation to its membership to maintain the relevancy of the CAP. Conducted at regular intervals, the Job Task Analysis (JTA) is a methodical and critical process of determining the tasks that are performed by security professionals who are engaged in the profession defined by the CAP. The results of the JTA are used to update the examination. This process ensures that candidates are tested on the topic areas relevant to the roles and responsibilities of today's practicing information security professionals.

CAP Examination Information

Length of exam	3 hours
Number of items	125
Item format	Multiple choice
Passing grade	700 out of 1000 points
Exam availability	English
Testing center	Pearson VUE Testing Center

CAP Examination Weights

Domains	Weight
1. Information Security Risk Management Program	15%
2. Categorization of Information Systems (IS)	13%
3. Selection of Security Controls	13%
4. Implementation of Security Controls	15%
5. Assessment of Security Controls	14%
6. Authorization of Information Systems (IS)	14%
7. Continuous Monitoring	16%
Total:	**100%**

Domain 1: Information Security Risk Management Program

1.1 Understand the Foundation of an Organization-Wide Information Security Risk Management Program

- Principles of information security
- National Institute of Standards and Technology (NIST) Risk Management Framework (RMF)
- RMF and System Development Life Cycle (SDLC) integration
- Information System (IS) boundary requirements
- Approaches to security control allocation
- Roles and responsibilities in the authorization process

1.2 Understand Risk Management Program Processes

- Enterprise program management controls
- Privacy requirements
- Third-party hosted Information Systems (IS)

1.3 Understand Regulatory and Legal Requirements

- Federal information security requirements
- Relevant privacy legislation
- Other applicable security-related mandates

Domain 2: Categorization of Information Systems (IS)

2.1 Define the Information System (IS)

» Identify the boundary of the Information System (IS)
» Describe the architecture
» Describe Information System (IS) purpose and functionality

2.2 Determine Categorization of the Information System (IS)

» Identify the information types processed, stored, or transmitted by the Information System (IS)
» Determine the impact level on confidentiality, integrity, and availability for each information type
» Determine Information System (IS) categorization and document results

Domain 3:
Selection of Security Controls

3.1 Identify and Document Baseline and Inherited Controls

3.2 Select and Tailor Security Controls

- Determine applicability of recommended baseline
- Determine appropriate use of overlays
- Document applicability of security controls

3.3 Develop Security Control Monitoring Strategy

3.4 Review and Approve Security Plan (SP)

Domain 4: Implementation of Security Controls

4.1 Implement Selected Security Controls

- Confirm that security controls are consistent with enterprise architecture
- Coordinate inherited controls implementation with common control providers
- Determine mandatory configuration settings and verify implementation (e.g., United States Government Configuration Baseline (USGCB), National Institute of Standards and Technology (NIST) checklists, Defense Information Systems Agency (DISA), Security Technical Implementation Guides (STIGs), Center for Internet Security (CIS) benchmarks)
- Determine compensating security controls

4.2 Document Security Control Implementation

- Capture planned inputs, expected behavior, and expected outputs of security controls
- Verify documented details are in line with the purpose, scope, and impact of the Information System (IS)
- Obtain implementation information from appropriate organization entities (e.g., physical security, personnel security)

Domain 5: Assessment of Security Controls

5.1 Prepare for Security Control Assessment (SCA)

- Determine Security Control Assessor (SCA) requirements
- Establish objectives and scope
- Determine methods and level of effort
- Determine necessary resources and logistics
- Collect and review artifacts (e.g., previous assessments, system documentation, policies)
- Finalize Security Control Assessment (SCA) plan

5.2 Conduct Security Control Assessment (SCA)

- Assess security control using standard assessment methods
- Collect and inventory assessment evidence

5.3 Prepare Initial Security Assessment Report (SAR)

- Analyze assessment results and identify weaknesses
- Propose remediation actions

5.4 Review Interim Security Assessment Report (SAR) and Perform Initial Remediation Actions

- Determine initial risk responses
- Apply initial remediations
- Reassess and validate the remediated controls

5.5 Develop Final Security Assessment Report (SAR) and Optional Addendum

Domain 6: Authorization of Information Systems (IS)

6.1 Develop Plan of Action and Milestones (POAM)

- Analyze identified weaknesses or deficiencies
- Prioritize responses based on risk level
- Formulate remediation plans
- Identify resources required to remediate deficiencies
- Develop schedule for remediation activities

6.2 Assemble Security Authorization Package

- Compile required security documentation for Authorizing Official (AO)

6.3 Determine Information System (IS) Risk

- Evaluate Information System (IS) risk
- Determine risk response options (i.e., accept, avoid, transfer, mitigate, share)

6.4 Make Security Authorization Decision

- Determine terms of authorization

Domain 7: Continuous Monitoring

7.1 Determine Security Impact of Changes to Information Systems (IS) and Environment

» Understand configuration management processes
» Analyze risk due to proposed changes
» Validate that changes have been correctly implemented

7.2 Perform Ongoing Security Control Assessments (SCA)

» Determine specific monitoring tasks and frequency based on the agency's strategy
» Perform security control assessments based on monitoring strategy
» Evaluate security status of common and hybrid controls and interconnections

7.3 Conduct Ongoing Remediation Actions (e.g., resulting from incidents, vulnerability scans, audits, vendor updates)

» Assess risk(s)
» Formulate remediation plan(s)
» Conduct remediation tasks

7.4 Update Documentation

» Determine which documents require updates based on results of the continuous monitoring process

7.5 Perform Periodic Security Status Reporting

» Determine reporting requirements

7.6 Perform Ongoing Information System (IS) Risk Acceptance

» Determine ongoing Information System (IS)

7.7 Decommission Information System (IS)

» Determine Information System (IS) decommissioning requirements
» Communicate decommissioning of Information System (IS)

Additional Examination Information

Supplementary References

Candidates are encouraged to supplement their education and experience by reviewing relevant resources that pertain to the CBK and identifying areas of study that may need additional attention.

View the full list of supplementary references at www.isc2.org/certifications/References.

Examination Policies and Procedures

(ISC)² recommends that CAP candidates review exam policies and procedures prior to registering for the examination. Read the comprehensive breakdown of this important information at www.isc2.org/Register-for-Exam.

Legal Info

For any questions related to (ISC)²'s legal policies, please contact the (ISC)² Legal Department at legal@isc2.org.

Any Questions?

(ISC)² Candidate Services
311 Park Place Blvd, Suite 400
Clearwater, FL 33759

(ISC)² Americas
Tel: +1.727.785.0189
Email: info@isc2.org

(ISC)² Asia Pacific
Tel: +(852) 28506951
Email: isc2asia@isc2.org

(ISC)² EMEA
Tel: +44 (0)203 300 1625
Email: info-emea@isc2.org