



Certified Authorization
Professional

Certification **Exam Outline**

Effective Date: September 2013





About CAP

The Certified Authorization Professional (CAP) is an information security practitioner who champions system security commensurate with an organization's mission and risk tolerance, while meeting legal and regulatory requirements. CAP confirms an individual's knowledge, skill, and experience required for authorizing and maintaining information systems within the Risk Management Framework as outlined in NIST SP 800-37 Rev 1.

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:

- Risk Management Framework (RMF)
- Categorization of Information Systems
- Selection of Security Controls
- Security Control Implementation
- Security Control Assessment
- Information System Authorization
- Monitoring of Security Controls

Experience Requirements

Candidates must have a minimum of 2 years cumulative paid full-time 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.

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 questions	125
Question 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. Risk Management Framework (RMF)	20%
2. Categorization of Information Systems	8%
3. Selection of Security Controls	13%
4. Security Control Implementation	10%
5. Security Control Assessment	19%
6. Information System Authorization	13%
7. Monitoring of Security Controls	17%
Total:	100%



Domain 1: Risk Management Framework (RMF)

1.1 Describe the Risk Management Framework (RMF)

- » Distinguish between applying risk management principles and satisfying compliance requirements
- » Identify and maintain information systems inventory
- » Explain the importance of securing information
- » Understand organizational mission and operations

1.2 Describe and Distinguish Between the RMF Steps

- » Categorize information system
- » Select security controls
- » Implement security controls
- » Assess security controls
- » Authorize information system
- » Monitor security controls

1.3 Identify Roles and Define Responsibilities

- » Head of agency (Chief Executive Officer)
- » Risk executive (Function)
- » Chief information officer
- » Information owner/steward
- » Senior information security officer
- » Authorizing official
- » Authorizing official designated representative
- » Common control provider
- » Information system owner
- » Information system security officer
- » Information security architect
- » Information system security engineer
- » Security control assessor

1.4 Understand and Describe How the RMF Process Relates to:

- » Organization-wide risk management
- » Enterprise and information security architecture
- » Information System boundaries
- » Authorization decisions
- » Security control assessor independence
- » Security controls in external environments (e.g., third-party, cloud)
- » Security control allocation (e.g., resources, common controls, component level)



1.5 Understand the Relationship between the RMF and System Development Life Cycle (SDLC)

- » Promote security integration within SDLC (e.g., policy, procedures, standards)
- » Collaborate with stakeholders (e.g., integrated project teams, architects, developers, management)

1.6 Understand Legal, Regulatory, and Other Security Requirements

- » Federal information security and privacy legislation
- » Office of Management and Budget (OMB)
- » Committee on National Security Systems (CNSS)
- » National Institute of Standards and Technology (NIST) publications



Domain 2: Categorization of Information Systems

2.1 Categorize the System

- » Identify the information types
- » Determine confidentiality, integrity, and availability values
- » Determine potential impact on organizations and individuals
- » Categorize information types
- » Categorize information system
- » Document categorization in the Security Plan (SP)
- » Perform Privacy Threshold Analysis and Privacy Impact Assessment

2.2 Describe the Information System (Including the Security Authorization Boundaries)

2.3 Register the System



Domain 3: Selection of Security Controls

- 3.1 Identify and Document Common (Inheritable) Controls
- 3.2 Select, Tailor, and Document Security Controls
- 3.3 Develop Security Control Monitoring Strategy
- 3.4 Review and Approve SP



Domain 4: Security Control Implementation

- 4.1 Implement Selected Security Controls
- 4.2 Document Security Control Implementation



Domain 5: Security Control Assessment

5.1 Prepare for Security Control Assessment

- » Establish objectives and scope
- » Establish points of contact, provide notifications and timelines
- » Select security control assessor (e.g., independence, competency)
- » Collect and review artifacts (e.g., previous assessments, system documentation, policies)

5.2 Develop Security Control Assessment Plan

- » Determine security assessment methods and level of effort
- » Obtain necessary approvals (e.g., security assessment plan, rules of engagement, resources)

5.3 Assess Security Control Effectiveness

- » Apply standard assessment methods (e.g., examine, interview, test)
- » Collect and inventory assessment evidence

5.4 Develop Initial Security Assessment Report (SAR)

- » Analyze assessment results
- » Determine root causes of identified weaknesses
- » Propose remediation actions

5.5 Review Interim SAR and Perform Initial Remediation Actions

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

5.6 Develop Final SAR and Optional Addendum



Domain 6: Information System Authorization

- 6.1 Develop Plan of Action and Milestones (POAM) (e.g., Resources, Schedule, Requirements)
- 6.2 Assemble Security Authorization Package
- 6.3 Determine Risk
- 6.4 Determine the Acceptability of Risk
- 6.5 Obtain Security Authorization Decision



Domain 7: Monitoring Security Controls

- 7.1 Determine Security Impact of Changes to System and Environment
- 7.2 Perform Ongoing Security Control Assessments (e.g., continuous monitoring, internal and external assessments)
- 7.3 Conduct Ongoing Remediation Actions (resulting from incidents, vulnerability scans, audits, vendor updates, etc)
- 7.4 Update Key Documentation (e.g., SP, SAR, POAM)
- 7.5 Perform Periodic Security Status Reporting
- 7.6 Perform Ongoing Risk Determination and Acceptance
- 7.7 Decommission and Remove System



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/cap-cbk-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/exam-policies-procedures.

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