For the Next Generation of Information System Authorization Professionals

The Certified Authorization Professional (CAP) credential from (ISC)² is an objective measure of the knowledge, skills and abilities required for personnel involved in the process of authorizing and maintaining information systems. Specifically, this credential applies to those responsible for formalizing processes used to assess risk and establish security requirements and documentation. Their decisions will ensure that information systems possess security commensurate with the level of exposure to potential risk, as well as damage to assets or individuals.

Security authorization includes a tiered risk management approach to evaluate both strategic and tactical risk across the enterprise. The authorization process incorporates the application of a Risk Management Framework (RMF), a review of the organizational structure, and the business process/mission as the foundation for the implementation and assessment of specified security controls. This authorization management process identifies vulnerabilities and security controls and determines residual risks. The residual risks are evaluated and deemed either acceptable or unacceptable. More controls must be implemented to reduce unacceptable risk. The system may be deployed only when the residual risks are acceptable to the enterprise and a satisfactory security plan is complete.

Today’s utilization of technology will not assure the safety of information assets for tomorrow and must be vigilantly monitored and constantly validated against changing security requirements triggered by emerging threats.

**WHY BECOME A CAP**

The CAP Helps You:

- Validate your competence, skills and commitment to the profession.
- Differentiate and enhance your credibility and marketability.
- Advance your career and increase earnings – (ISC)² members report nearly 30% average higher salary than non-members.*
- Affirm your commitment to continued competence in the most current best practices through (ISC)²’s Continuing Professional Education (CPE) requirement.
- Face the DoD 8570 compliance in IAM Level I and IAM Level II.

The CAP Helps Employers:

- Positions candidates on a level playing field as (ISC)² certifications are recognized internationally.
- Increase credibility of the organization when working with vendors and contractors.
- Ensure employees use a universal language, circumventing ambiguity with industry-accepted terms and practices.
- Confirm employee’s commitment and years of experience gained in the industry.
- Increase confidence that job candidates and employees continue their education through Continuing Professional Education (CPE) credits and keep their skills current.
- Satisfy DoD certification requirements for service providers or subcontractors.

*Source: 2013 (ISC)² Global Information Security Workforce Study

**CAP INSIGHT**


“The NIST guidance outlines the integral role that continuous monitoring plays in the risk framework but also stresses that monitoring security controls is only one piece of a larger, integrated process. A CAP credential holder fully understands the entirety of the systems security authorization lifecycle.”

W. Hord Tipton
CISSP-ISSEP, CAP, CISA
Executive Director,
The ideal candidate should have experience, knowledge and skills in the following areas:

- System authorization processes
- Information risk management
- Systems development experience
- IT security/information assurance
- Information security policy
- Thorough understanding of NIST and OMB requirements
- Security control testing and continuous monitoring
- Technical or auditing experience within government, the U.S. Department of Defense, the financial or healthcare industries, and/or auditing firms

**Associate of (ISC)²®**

You don’t have to spend years in the field to demonstrate your competence in information security. Become an Associate of (ISC)², and you’re already part of a reputable and credible organization, earning recognition from employers and peers for the industry knowledge you’ve already gained.

**Participation Requirements**

Associate of (ISC)² status is available to those knowledgeable in key areas of industry concepts but are lacking the required work experience. As a candidate, you take the CAP examination and subscribe to the (ISC)² Code of Ethics, however to earn the CAP credential you will have to acquire the necessary years of professional experience required, provide proof and be endorsed by a member of (ISC)² in good standing. If you are working towards this credential, you will have a maximum of three years from your exam pass date to acquire the necessary two years of professional experience. An Annual Maintenance Fee (AMF) of US$35 applies and 10 Continuing Professional Education (CPE) credits must be earned each year to remain in good standing.

For more information on how you can become an Associate of (ISC)², visit [www.isc2.org/associate](http://www.isc2.org/associate).

**Face the DoD Mandate Requirements Head-On with the CAP**

Cyberspace is the new battlefield, where commercial and DoD assets have become virtual targets for our adversaries. The DoD 8570 Information Assurance Training, Certification and Workforce Management program addresses this threat by proactively educating and certifying commercial contractors and military and civilian personnel to perform their critical duties as Information Assurance professionals.

Under the 8570 Mandate, all personnel with “privileged access” to DoD systems must obtain an ANSI-approved commercial certification for IAM, IAT, CND and IASAE positions. (ISC)² was the first organization to receive ANSI accreditation under ISO/IEC Standard 17024 for its CISSP® certification and shortly thereafter received accreditation for the CAP and each of its security credentials.

**Matching Classifications with the Certifications**

In order to determine which certification is relevant, a classification grid has been constructed to pinpoint what duties you fulfill and what certification is appropriate for your specific job function. The grid provides guidance for assessing the proper certification commensurate with your job responsibilities. The CAP credential from (ISC)² satisfies DoD 8570 compliance in IAM Level I and IAM Level II.
The comprehensive (ISC)² CAP CBK Training Seminar covers the following domains:

• **Risk Management Framework (RMF)** – Security authorization includes a tiered risk management approach to evaluate both strategic and tactical risk across the enterprise. The authorization process incorporates the application of a Risk Management Framework (RMF), a review of the organizational structure, and the business process/mission as the foundation for the implementation and assessment of specified security controls. This authorization management process identifies vulnerabilities and security controls and determines residual risks. The residual risks are evaluated and deemed either acceptable or unacceptable. More controls must be implemented to reduce unacceptable risk. The system may be deployed only when the residual risks are acceptable to the enterprise and a satisfactory security plan is complete.

• **Categorization of Information Systems** – Categorization of the information system is based on an impact analysis. It is performed to determine the types of information included within the security authorization boundary, the security requirements for the information types, and the potential impact on the organization resulting from a security compromise. The result of the categorization is used as the basis for developing the security plan, selecting security controls, and determining the risk inherent in operating the system.

• **Selection of Security Controls** – The security control baseline is established by determining specific controls required to protect the system based on the security categorization of the system. The baseline is tailored and supplemented in accordance with an organizational assessment of risk and local parameters. The security control baseline, as well as the plan for monitoring it, is documented in the security plan.

• **Security Control Implementation** – The security controls specified in the security plan are implemented by taking into account the minimum organizational assurance requirements. The security plan describes how the controls are employed within the information system and its operational environment. The security assessment plan documents the methods for testing these controls and the expected results throughout the system’s life-cycle.

• **Security Control Assessment** – The security control assessment follows the approved plan, including defined procedures, to determine the effectiveness of the controls in meeting security requirements of the information system. The results are documented in the Security Assessment Report.

• **Information System Authorization** – The residual risks identified during the security control assessment are evaluated and the decision is made to authorize the system to operate, deny its operation, or remediate the deficiencies. Associated documentation is prepared and/or updated depending on the authorization decision.

• **Monitoring of Security Controls** – After an Authorization to Operate (ATO) is granted, ongoing continuous monitoring is performed on all identified security controls as well as the political, legal, and physical environment in which the system operates. Changes to the system or its operational environment are documented and analyzed. The security state of the system is reported to designated responsible officials. Significant changes will cause the system to reenter the security authorization process. Otherwise, the system will continue to be monitored on an ongoing basis in accordance with the organization’s monitoring strategy.

Official (ISC)²® CAP® CBK® Training Seminar

At the Official Training Seminar you will benefit from a rich learning environment providing a complete information systems security authorization experience. Through a series of structured training modules, class discussions, case examples and end-of-domain review questions, the CAP candidate will fully understand the requirements for security authorization, the overall process and all the supporting procedures to ensure compliance with current requirements. The seminar includes:

- (ISC)² Authorized Instructor, who is a Subject Matter Expert (SME)
- Courseware that is 100% up-to-date
- Exam Outline with guidance on CAP requirements
- End-of-domain review questions
- CD-ROM containing testable references identified in the Exam Outline

The Official CAP CBK Training Seminar is offered in the following formats:

- **Classroom** Delivered in a multi-day, classroom setting. Course material focuses on covering the seven CAP domains. Available throughout the world at (ISC)² facilities and (ISC)² Official Training Providers.

- **Private On-site** Host your own Training Seminar on- or off-site. Available for larger groups, this option often saves employee travel time and expense. Group pricing is also available to organizations with 15 or more employees planning to sit for the exam.

- **Live OnLine** Educate yourself from the convenience of your computer. Live OnLine brings you the same award winning course content as the classroom based or private on-site seminars and the benefit of an (ISC)² Authorized Instructor.

Visit [www.isc2.org/caprevsem](http://www.isc2.org/caprevsem) for more information or to register.

---

**OFFICIAL TRAINING PROVIDERS**

Official (ISC)² CBK Training Seminars are available throughout the world at (ISC)² facilities and through (ISC)² Official Training Providers. Official (ISC)² CBK Training Seminars are conducted only by (ISC)² Authorized Instructors who are experts in their field and have demonstrated their mastery of the covered domains.

Be wary of training providers that are not authorized by (ISC)². Be certain that your educator carries the (ISC)² Official Training Provider logo to ensure that you are experiencing the best and most current programs available.

2013 SC Magazine Award Winner – Best Professional Training Program, (ISC)² Education
Exam Outline - Free
Your primary resource in your study efforts to become a CAP. The Exam Outline contains an exam blueprint that outlines major topics and subtopics within the domains, a suggested reference list for further study, exam information and registration/administration policies and instructions. www.isc2.org/exam-outline

CBK Domain Previews - Free Webcast Channel
View a free series of short webcasts that provide a detailed overview of each domain of the CAP, the value of certification and how to study for the exam. www.isc2.org/previews

studISCope Self Assessment
Experience the CAP certification exam as closely as possible before you take it. The 100 question studISCope provides the look and feel of the real exam while identifying key domains to study. You’ll even receive a personalized study plan. www.isc2.org/studiscope

Social Media
Join the “Certified Authorization Professionals (CAP)” groups on Linkedin and (ISC)²’s own networking site, InterSeC. As a member of these professional communities you can converse with CAP subject matter experts, show your understanding of the CAP material by educating others and also search out assistance when you need it. www.linkedin.com and www.isc2intersec.com

For a detailed plan on how to study for the CAP exam, visit www.isc2.org/how-to-study-CAP.
For more information on the CAP visit www.isc2.org/cap.

*a Audit Notice - Passing candidates will be randomly selected and audited by (ISC)² prior to issuance of any certificate. Multiple certifications may result in a candidate being audited more than once.

FREE: (ISC)² One-Day SecureEvents Industry Initiatives Certification Verification Chapter Program (ISC)² Receptions/Networking Opportunities (ISC)² Global Awards Program Online Forum (ISC)² e-Symposium Webinars ThinkTANK Global Information Security Workforce Study InfoSecurity Professional Magazine Safe and Secure Online Volunteer Opportunities InterSeC

DISCOUNTED: (ISC)² Security Congress (ISC)² Local Two-Day Secure Events Industry Conferences The (ISC)² Journal

Maintain the certification with required CPEs and AMF