CISSP®

Certified Information Systems Security Professional

The Next Generation of Security Leaders

Certified Information Systems Security Professional (CISSP®) is the most globally recognized certification in the information security market. Required by some of the world's most security-conscious organizations, the CISSP is considered the gold standard credential that assures information security leaders possess the breadth of knowledge, skills and experience required to credibly build and manage the security posture of an organization.

Backed by (ISC)²®, the global leader in information security certifications, CISSPs have earned their place as trusted advisors. Their expertise plays a critical role in helping organizations integrate stronger security protocols and protect against threats in an increasingly complex cyber security landscape.

CISSP was the first credential in the field of information to meet the stringent requirements of ISO/IEC Standard 17024. Not only is the CISSP an objective measure of excellence, but also a globally recognized standard of achievement.

WHY BECOME A CISSP

The CISSP Helps You:

- Demonstrate your ability to effectively define the architecture, design, management and controls that assure the security of business environments.
- Validate your experience, skills and commitment as an information security professional.
- Advance your career with the most globally recognized information security certification in the industry.
- Affirm your commitment to continued competence in the most current information security practices through (ISC)²'s Continuing Professional Education (CPE) requirement.
- Fulfill government and organization requirements for information security certification mandates.

The CISSP Helps Employers:

- Increase credibility of the organization when working with vendors and contractors.
- Position candidates on a level playing field as the CISSP is internationally recognized.
- Ensure their employees use a universal language, circumventing ambiguity with industry-accepted terms and practices.
- Increase confidence that job candidates and employees possess the knowledge and experience to do the job right.
- Increase confidence that information security personnel are current and capable through CISSP's CPE credits requirement.
- Confirm their employee's commitment and years of experience gained in the industry.

CISSP in the News

"Today's Most In-Demand Certifications"
- Certification Magazine

"The top five in-demand IT certifications for 2013"
- TechRepublic

"The Most In-Demand Certifications in IT for 2013"
- IT Strategy News

CISSP INSIGHTS

"The CISSP certification I got after attending the official (ISC)² [review] seminar greatly added to my competitive edge and, as a result, I won my current position. I am now making the (ISC)² certification a requirement for the members of my team, confident in the knowledge that their skills are genuine and current."

Daniel, CISSP
The Netherlands

"Obtaining the CISSP certification opened up doors I thought inviolable. My career - both professional and academic - grew dramatically!"

Claudi, CISSP, CIA, CISA, CISM
Italy

(ISC)²®

WHO SHOULD BECOME A CISSP

CISSP® credential holders often hold job functions including:

o Security Consultant	o Security Analyst
o Security Manager	o Security Systems Engineer
o IT Director/Manager	o Chief Information Security Officer
o Security Auditor	o Director of Security
o Security Architect	o Network Architect

CISSP candidates must have a minimum of five years of cumulative paid full-time professional security work experience in two or more of the ten domains of the (ISC)²® CISSP CBK®, or four years of cumulative paid full-time professional security work experience in two or more of the ten domains of the CISSP CBK with a college degree. Alternatively, there is a one-year waiver of the professional experience requirement for holding an additional credential on the (ISC)² approved list.

ENGAGE WHILE OBTAINING EXPERIENCE

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 lacking the work experience. As a candidate, you may successfully pass the CISSP examination and subscribe to the (ISC)² Code of Ethics, however to earn the CISSP 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 six years from your exam pass date to acquire the necessary five years of professional experience. An Annual Maintenance Fee (AMF) of US$35 applies and 20 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**.

ADVANCE BEYOND THE CISSP

CISSP Concentrations

After the original conception of the CISSP, and the continuous evolution of information security, (ISC)² discovered a need to develop credentials which address the specific needs of our members. With this in mind, we produced our CISSP Concentrations to provide a career path that would open up new opportunities for our CISSP credential holders. Specifically, these credentials allow for more demanding roles in larger enterprises and recognize the specialized talents of CISSPs.

- Information Systems Security Architecture Professional (CISSP-ISSAP®)
- Information Systems Security Engineering Professional (CISSP-ISSEP®)
- Information Systems Security Management Professional (CISSP-ISSMP®)

To qualify for the CISSP-ISSAP, CISSP-ISSEP or the CISSP-ISSMP, a CISSP must maintain their credential in good standing and pass the appropriate concentration examination. Each of the three concentrations has its own CBK Domains.

For more information, visit **www.isc2.org/concentrations**.

THE CISSP CBK

The CISSP® domains are drawn from various information security topics within the (ISC)²® CBK®. Updated annually, the domains reflect the most up-to-date best practices worldwide, while establishing a common framework of terms and principles to discuss, debate and resolve matters pertaining to the profession.

The CISSP CBK consists of the following ten domains:

- **Access Control** – a collection of mechanisms that work together to create a security architecture to protect the assets of the information system.
  - Concepts/methodologies/techniques
  - Attacks
  - Effectiveness
- **Telecommunications and Network Security** – discusses network structures, transmission methods, transport formats and security measures used to provide availability, integrity and confidentiality.
  - Network architecture and design
  - Network components
  - Communication channels
  - Network attacks
- **Information Security Governance and Risk Management** – the identification of an organization's information assets and the development, documentation and implementation of policies, standards, procedures and guidelines.
  - Security governance and policy
  - Risk management concepts
  - Information classification/ownership
  - Personnel security
  - Contractual agreements and procurement processes
  - Security education, training and awareness
  - Certification and accreditation
- **Software Development Security** – refers to the controls that are included within systems and applications software and the steps used in their development.
  - Systems development life cycle (SDLC)
  - Effectiveness of application security
  - Application environment and security controls
- **Cryptography** – the principles, means and methods of disguising information to ensure its integrity, confidentiality and authenticity.
  - Encryption concepts
  - Public Key Infrastructure (PKI)
  - Digital signatures
  - Information hiding alternatives
  - Cryptanalytic attacks
- **Security Architecture and Design** – contains the concepts, principles, structures and standards used to design, implement, monitor, and secure, operating systems, equipment, networks, applications, and those controls used to enforce various levels of confidentiality, integrity and availability.
  - Fundamental concepts of security models
  - Countermeasure principles
  - Capabilities of information systems (e.g. memory protection, virtualization)
  - Vulnerabilities and threats (e.g. cloud computing, aggregation, data flow control)
- **Operations Security** – used to identify the controls over hardware, media and the operators with access privileges to any of these resources.
  - Resource protection
  - Attack prevention and response
  - Incident response
  - Patch and vulnerability management
- **Business Continuity and Disaster Recovery Planning** – addresses the preservation of the business in the face of major disruptions to normal business operations.
  - Business impact analysis
  - Disaster recovery process
  - Recovery strategy
  - Provide training
- **Legal, Regulations, Investigations and Compliance** – addresses computer crime laws and regulations; the investigative measures and techniques which can be used to determine if a crime has been committed and methods to gather evidence.
  - Legal issues
  - Forensic procedures
  - Investigations
  - Compliance requirements/procedures
- **Physical (Environmental) Security** – addresses the threats, vulnerabilities and countermeasures that can be utilized to physically protect an enterprise's resources and sensitive information.
  - Site/facility design considerations
  - Internal security
  - Perimeter security
  - Facilities security

Download a copy of the CISSP Exam Outline at **www.isc2.org/exam-outline**.

CISSP®

EDUCATION DELIVERED YOUR WAY

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

This official training seminar is the most comprehensive, complete review of information systems security concepts and industry best practices, and the only training course endorsed by (ISC)². As your exclusive way to review and refresh your knowledge of the domains and sub-domains of the CISSP CBK, the seminar will help you identify areas you need to study and includes:

- 100% up-to-date material
- An overview of the information security field
- Contributions from CISSPs, (ISC)² Authorized Instructors and subject matter experts
- Post-Seminar Self-Assessment

"Our training and trainer was excellent. All ten domains were covered with exact knowledge and experience that conveyed understanding. Dennis' use of difficult questions to prepare us for the test made it possible for me to pass."

Joe, CISSP
Virginia, USA

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

- **Classroom** Delivered in a multi-day, classroom setting. Course material focuses on covering the ten CISSP 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/cissprevsem** for more information or to register.

"I have been CISSP certified since 2005 and hope to attain CISSP-ISSAP certification this year. The benefits of the formalisation of my domain knowledge have always been clear, CISSP is recognised the world over, and when colleagues and customers alike see those letters on your business card, it visibly gives them a sense that they are talking to a domain expert, and more importantly a person that they can trust. The (ISC)² training that I have attended has always been run by knowledgeable and personable trainers with a wealth of real world experience to share."

Rik, CISSP
United Kingdom

OFFICIAL TRAINING PROVIDERS

(ISC)² OFFICIAL TRAINING PROVIDER

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.

2014 SC Magazine Award Winner – Best Professional Certification Program, CISSP

2013 SC Magazine Award Winner – Best Professional Training Program, (ISC)² Education

SC MAGAZINE AWARDS 2014 WINNER Honored in the U.S.

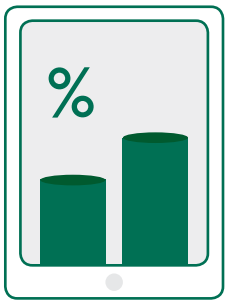
STUDY TOOLS

Exam Outline - Free

Your primary resource in your study efforts to become a CISSP®. 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

Official (ISC)²® Guide to the CISSP CBK®

The textbook is an authoritative information security textbook based on the CISSP CBK, a global compendium of security best practices. The textbook is available in hardcover or as an ebook and contains mandatory information written and compiled by world-class CISSP certified experts - an absolute essential for those seeking CISSP certification.
www.isc2.org/store



studISCope Self Assessment

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

CBK Domain Previews – Free Webcast Channel

View a series of short webcasts that provide a detailed overview of each domain of the CISSP, the value of certification and how to study for the exam.
www.isc2.org/previews

eLearning

These self-paced dynamic eLearning lectures and exercises are based on the proven CBK Training Seminars. Offered in 60 or 120-days access in an Internet-friendly format, these lectures and exercises are broken into individual domain review modules for focused study. Each eLearning package features end-of domain and end-of-course review questions modeled after the certification exam. eLearning also qualifies as Continuing Professional Education credits (CPEs) for (ISC)² members.
www.isc2.org/self-paced

CHECKLIST FOR CERTIFICATION

Obtain the Required Experience - For the CISSP® certification, candidates must have five years of cumulative paid full-time professional security work experience in two or more of the ten domains of the (ISC)²® CISSP CBK®, or four years of cumulative paid full-time professional security work experience in two or more of the ten domains of the CISSP CBK with a college degree. If you do not have the required experience, you may still sit for the exam and become an Associate of (ISC)² until you have gained the required experience.

Study for the Exam - Utilize these optional educational tools to learn the CISSP CBK.

- Exam Outline
- CBK Domain Preview Webcasts
- Official Textbook
- studISCope Self Assessment
- Self-paced eLearning
- Official Training Seminar

Register for the Exam

- Visit **www.isc2.org/certification-register-now** to schedule an exam date
- Submit the examination fee

Pass the Exam - Pass the CISSP examination with a scaled score of 700 points or greater. Read the Exam Scoring FAQs at **www.isc2.org/exam-scoring-faqs**.

Complete the Endorsement Process - Once you are notified that you have successfully passed the examination, you will have nine months from the date you sat for the exam to complete the following endorsement process:

- Complete an Application Endorsement Form
- Subscribe to the (ISC)² code of ethics
- Have your form endorsed by an (ISC)² member

The credential can be awarded once the steps above have been completed and your form has been submitted.* Get the guidelines and form at **www.isc2.org/endorsement**.

Maintain the Certification - Recertification is required every three years, with ongoing requirements to maintain your credentials in good standing. This is primarily accomplished through earning 120 Continuing Professional Education (CPE) credits every three years, with a minimum of 20 CPEs earned each year after certification. If the CPE requirements are not met, CISSPs must retake the exam to maintain certification. CISSPs must also pay an Annual Maintenance Fee (AMF) of US$85.

MEMBER BENEFITS

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

For more information on the CISSP, visit **www.isc2.org/cissp**.

**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.*

*Formed in 1989 and celebrating its 25th anniversary, (ISC)²® is the largest not-for-profit membership body of certified information and software security professionals worldwide, with nearly 100,000 members in more than 135 countries. Globally recognized as the Gold Standard, (ISC)² issues the Certified Information Systems Security Professional (CISSP®) and related concentrations, as well as the Certified Secure Software Lifecycle Professional (CSSLP®), the Certified Cyber Forensics Professional (CCFP℠), Certified Authorization Professional (CAP®), HealthCare Information Security and Privacy Practitioner (HCISPP℠), and Systems Security Certified Practitioner (SSCP®) credentials to qualifying candidates. (ISC)²'s certifications are among the first information technology credentials to meet the stringent requirements of ISO/IEC Standard 17024, a global benchmark for assessing and certifying personnel. (ISC)² also offers education programs and services based on its CBK®, a compendium of information and software security topics. More information is available at **www.isc2.org**.*

(ISC)²®

CIS.0
(01/14)