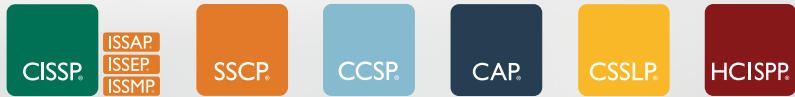


# CERTIFICATION ROADMAP





## OVERVIEW

The Certified Information Systems Security Professional (CISSP) is the most globally recognized certification in the information security market. CISSP validates an information security professional's deep technical and managerial knowledge and experience to effectively design, engineer, and manage the overall security posture of an organization.

## TARGET AUDIENCE

The CISSP is ideal for information security professionals with 5+ years in the information security field.

## TARGET JOB TITLES

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

## REQUIRED EXPERIENCE

Candidates must have a minimum of 5 years cumulative work experience in 2 or more of the 8 domains of the CISSP CBK. Earning a 4-year college degree or regional equivalent or an additional credential from the (ISC)<sup>2</sup> approved list will satisfy 1 year of the required experience. Education credit will only satisfy 1 year of experience. A candidate that doesn't have the required experience to become a CISSP may become an Associate of (ISC)<sup>2</sup> by successfully passing the

CISSP examination. The Associate of (ISC)<sup>2</sup> will then have 6 years to earn the 5 years required experience.

## DOMAINS COVERED

1. Security and Risk Management
2. Asset Security
3. Security Architecture and Engineering
4. Communication and Network Security
5. Identity and Access Management (IAM)
6. Security Assessment and Testing
7. Security Operations
8. Software Development Security

## STEPS TO CERTIFICATION

1. Obtain the required experience
2. Take and pass the exam
  - Find a local Pearson VUE Test Center and register for the exam at [www.pearsonvue.com/isc2](http://www.pearsonvue.com/isc2)
3. Complete the endorsement process
  - Get work experience endorsed by an (ISC)<sup>2</sup> member within 9 months of exam date
4. Maintain membership
  - Earn and submit a min. of 120 CPE credits by the end of the 3-year cycle
  - Pay the annual maintenance fee of U.S. \$125

## ABOUT THE EXAM

**Delivery Method:** Computer Adaptive Testing (CAT)

**Exam Language:** English

**Length of Exam:** Up to 3 hours

**Format:** 100-150 multiple choice and advanced innovative items

**Passing grade:** 700 out of 1000 points

**Testing center:** Pearson VUE Testing Center [pearsonvue.com/isc2](https://pearsonvue.com/isc2)

**Exam pricing:** U.S. \$749

**Delivery Method:** Computer Based Testing (CBT)

**Language:** Chinese, Japanese, French, German, Korean, Spanish - Modern, Brazilian Portuguese

**Length of Exam:** Up to 6 hours

**Format:** 250 multiple choice and advanced innovative items

**Passing grade:** 700 out of 1000 points

**Testing center:** Pearson VUE Testing Center [pearsonvue.com/isc2](https://pearsonvue.com/isc2)

**Exam pricing:** U.S. \$749

## ACE CREDIT

College Credit Eligible | Recognized by the American Council on Education's College Credit Recommendation. Service (ACE CREDIT) to receive 3 college credit hours for completing an Official CISSP Training Seminar.

## BENEFITS TO ORGANIZATION

- **Secure the organization's critical data:** Strengthen the security posture with qualified professionals who have proven expertise to competently design, build, and maintain a secure business environment.
- **Increase overall cybersecurity IQ:** Implement the latest security best practices.
- **Improve information security coherence across the organization:** Professionals that speak the same language across disciplines and have cross-department perspective.

- **Instant credibility:** Increases organizational integrity in the eyes of clients and other stakeholders.
- **Satisfy requirements:** Meet certification mandate requirements for service providers and subcontractors.
- **Stay current:** Ensures professionals stay current on emerging and changing technologies, and security issues related to these technologies through the continuing professional education requirements.
- **Ensure compliance:** Comply with government or industry regulations (DoD 8140.01/8570.01 approved).



## OVERVIEW

The Information Systems Security Architecture Professional (ISSAP) is a CISSP who specializes in designing security solutions and providing management with risk-based guidance to meet organizational goals. ISSAPs facilitate the alignment of security solutions within the organizational context (e.g., vision, mission, strategy, policies, requirements, change and external factors).

## TARGET AUDIENCE

The CISSP-ISSAP is an appropriate credential if you're a chief security architect or analyst. Responsibilities fall between the C-suite and upper managerial level and the implementation of security programs.

## TARGET JOB TITLES

- System Architect
- Chief Technology Officer
- System and Network Designer
- Business Analyst
- Chief Security Officer

## REQUIRED EXPERIENCE

Candidates must be a CISSP in good standing and have 2 years cumulative work experience in 1 or more of the 6 domains of the CISSP-ISSAP CBK.

## DOMAINS COVERED

1. Architect for Governance, Compliance and Risk Management
2. Security Architecture Modeling
3. Infrastructure Security Architecture
4. Identity and Access Management (IAM) Architecture

5. Architect for Application Security
6. Security Operations Architecture

## STEPS TO CERTIFICATION

1. Obtain the required experience
2. Take and pass the exam
  - Find a local Pearson VUE test center and register for the exam at [www.pearsonvue.com/isc2](http://www.pearsonvue.com/isc2).
3. Maintain membership
  - Earn 20 CPE credits each year. You may apply these 20 credits toward your CISSP CPE requirement as long as these credits are specific to security architecture.
  - There is no additional AMF for earning and maintaining CISSP concentrations.

## ABOUT THE EXAM

Length of Exam: Up to 3 hours

Questions: 125

Question Format: Multiple choice items

Passing grade: 700 out of 1000 points

Testing center: Pearson VUE Testing Center [pearsonvue.com/isc2](http://pearsonvue.com/isc2)

Exam availability: English

Exam pricing: U.S. \$599

## BENEFITS TO ORGANIZATION

- **Secure the organization's critical data:** Strengthen the security posture with qualified professionals who have proven expertise to competently design, build, and maintain a secure business environment.
- **Increase overall cybersecurity IQ:** Implement the latest security best practices.
- **Improve information security coherence across the organization:** Professionals that speak the same language across disciplines and have cross-department perspective.
- **Instant credibility:** Increases organizational integrity in the eyes of clients and other stakeholders.
- **Satisfy requirements:** Meet certification mandate requirements for service providers and subcontractors.
- **Stay current:** Ensures professionals stay current on emerging and changing technologies, and security issues related to these technologies through the continuing professional education requirements.
- **Ensure compliance:** Comply with government or industry regulations (DoD 8140.01/8570.01 approved).



## OVERVIEW

The Information Systems Security Engineering Professional (ISSEP) is a CISSP who specializes in the practical application of systems engineering principles and processes to develop secure systems. An ISSEP analyzes organizational needs, defines security requirements, designs security architectures, develops secure designs, implements system security, and supports system security assessment and authorization for government and industry.

## TARGET AUDIENCE

The CISSP-ISSEP is an ideal credential for proving you know how to incorporate security into all facets of business operations. This security engineering certification recognizes your keen ability to practically apply systems engineering principles and processes to develop secure systems. You have the knowledge and skills to incorporate security into projects, applications, business processes and all information systems.

The CISSP-ISSEP was developed in conjunction with the U.S. National Security Agency (NSA). It offers an invaluable tool for any systems security engineering professional.

## TARGET JOB TITLES

- Senior Systems Engineer
- Information Assurance Systems Engineer
- Information Assurance Officer
- Information Assurance Analyst
- Senior Security Analyst

## REQUIRED EXPERIENCE

Candidates must be a CISSP in good standing and have 2 years cumulative work experience in 1 or more of the 5 domains of the CISSP-ISSEP CBK.

## DOMAINS COVERED

1. Systems Security Engineering Foundations
2. Risk Management
3. Security Planning and Design
4. Systems Implementation, Verification and Validation
5. Secure Operations, Change Management and Disposal

## STEPS TO CERTIFICATION

1. Obtain the Required Experience
2. Take and Pass the Exam
  - Find a local Pearson VUE Test Center and register for the exam at [www.pearsonvue.com/isc2](http://www.pearsonvue.com/isc2).
3. Maintain membership
  - Earn 20 CPE credits each year. You may apply these 20 credits toward your CISSP CPE requirement as long as these credits are specific to security engineering.
  - There is no additional AMF for earning and maintaining CISSP concentrations.

## ABOUT THE EXAM

Length of Exam: Up to 3 hours

Questions: 125

Question Format: Multiple choice items

Passing grade: 700 out of 1000 points

Testing center: Pearson VUE Testing Center [www.pearsonvue.com/isc2](http://www.pearsonvue.com/isc2)

Exam availability: English

Exam pricing: U.S. \$599

## BENEFITS TO ORGANIZATION

- **Secure the organization's critical data:** Strengthen the security posture with qualified professionals who have proven expertise to competently design, build, and maintain a secure business environment.
- **Increase overall cybersecurity IQ:** Implement the latest security best practices.
- **Improve information security coherence across the organization:** Professionals that speak the same language across disciplines and have cross-department perspective.
- **Instant credibility:** Increases organizational integrity in the eyes of clients and other stakeholders.
- **Satisfy requirements:** Meet certification mandate requirements for service providers and subcontractors.
- **Stay current:** Ensures professionals stay current on emerging and changing technologies, and security issues related to these technologies through the continuing professional education requirements.
- **Ensure compliance:** Comply with government or industry regulations (DoD 8140.01/8570.01 approved).



## OVERVIEW

The Information Systems Security Management Professional (ISSMP) is a CISSP who specializes in establishing, presenting, and governing information security programs, and demonstrates management and leadership skills. ISSMPs direct the alignment of security programs with the organization's mission, goals and strategies in order to meet enterprise financial and operational requirements in support of its desired risk position.

## TARGET AUDIENCE

This cybersecurity management certification shows you excel at establishing, presenting and governing information security programs. You also demonstrate deep management and leadership skills whether you're leading incident handling and/or a breach mitigation team.

## TARGET JOB TITLES

- Chief Information Officer
- Chief Information Security Officer
- Chief Technology Officer
- Senior Security Executive

## REQUIRED EXPERIENCE

Candidates must be a CISSP in good standing and have 2 years cumulative work experience in 1 or more of the 6 domains of the CISSP-ISSMP CBK.

## DOMAINS COVERED

1. Leadership and Business Management
2. Systems Lifecycle Management
3. Risk Management
4. Threat Intelligence and Incident Management

5. Contingency Management
6. Law, Ethics, and Security Compliance Management

## STEPS TO CERTIFICATION

1. Obtain the Required Experience
2. Take and Pass the Exam
  - Find a local Pearson VUE Test Center and register for the exam at [www.pearsonvue.com/isc2](http://www.pearsonvue.com/isc2).
3. Maintain membership
  - Earn 20 CPE credits each year. You may apply these 20 credits toward your CISSP CPE requirement as long as these credits are specific to security management.
  - There is no additional AMF for earning and maintaining CISSP concentrations.

## ABOUT THE EXAM

Length of Exam: Up to 3 hours

Questions: 125

Question Format: Multiple choice items

Passing grade: 700 out of 1000 points

Testing center: Pearson VUE Testing Center [pearsonvue.com/isc2](http://pearsonvue.com/isc2)

Exam availability: English

Exam pricing: U.S. \$599



## BENEFITS TO ORGANIZATION

- **Secure the organization's critical data:** Strengthen the security posture with qualified professionals who have proven expertise to competently design, build, and maintain a secure business environment.
- **Increase overall cybersecurity IQ:** Implement the latest security best practices.
- **Improve information security coherence across the organization:** Professionals that speak the same language across disciplines and have cross-department perspective.
- **Instant credibility:** Increases organizational integrity in the eyes of clients and other stakeholders.
- **Satisfy requirements:** Meet certification mandate requirements for service providers and subcontractors.
- **Stay current:** Ensures professionals stay current on emerging and changing technologies, and security issues related to these technologies through the continuing professional education requirements.
- **Ensure compliance:** Comply with government or industry regulations (DoD 8140.01/8570.01 approved).



## OVERVIEW

The Systems Security Certified Practitioner (SSCP) is the ideal certification for those with proven technical skills and practical, hands-on security knowledge in operational IT roles. It provides confirmation of a practitioner's ability to implement, monitor and administer IT infrastructure in accordance with information security policies and procedures that ensure data confidentiality, integrity and availability.

## TARGET AUDIENCE

Cybersecurity and IT/ICT professionals who have hands-on responsibility for cyber, information, software and infrastructure security.

## TARGET JOB TITLES

- Network Security Engineer
- Systems/Network Administrator
- Security Analyst
- Systems Engineer
- Security Consultant/ Specialist
- Security Administrator
- Systems/Network Analyst
- Database Administrator

## REQUIRED EXPERIENCE

Candidates must have a minimum of 1 year cumulative work experience in 1 or more of the 7 domains of the SSCP CBK. A 1 year prerequisite pathway will be granted if the candidate has a degree in a cybersecurity program (bachelors or masters).

A candidate that doesn't have the required experience to become an SSCP may become an Associate of (ISC)<sup>2</sup> by successfully passing the SSCP examination. The Associate of (ISC)<sup>2</sup> will then have 2 years to earn the 1 year required experience.

## DOMAINS COVERED

1. Access Controls
2. Security Operations and Administration
3. Risk Identification, Monitoring and Analysis
4. Incident Response and Recovery
5. Cryptography
6. Network and Communications Security
7. Systems and Application Security

## STEPS TO CERTIFICATION

1. Obtain the Required Experience
2. Take and Pass the Exam
  - Find a local Pearson VUE Test Center and register for the exam at [pearsonvue.com/isc2](http://pearsonvue.com/isc2)
3. Complete the Endorsement Process
  - Get work experience endorsed by an (ISC)<sup>2</sup> member within 9 months of exam date
4. Maintain Membership
  - Earn and submit 60 CPE credits by the end of the 3-year cycle
  - Pay the annual maintenance fee of U.S. \$125

## ABOUT THE EXAM

Length of Exam: Up to 3 hours

Questions: 125

Question Format: Multiple choice

Passing grade: 700 out of 1000 points

Testing center: Pearson VUE Testing Center [pearsonvue.com/isc2](http://pearsonvue.com/isc2)

Exam Availability: English, Japanese and Portuguese-Brazilian

Exam pricing: U.S. \$249

## ACE CREDIT

**College Credit Eligible:** Recognized by the American Council on Education's College Credit Recommendation. Service (ACE CREDIT) to receive 3 college credit hours for completing an Official SSCP Training Seminar.

## BENEFITS TO ORGANIZATION

- **Secure the organization's critical data:** Strengthen the security posture with qualified practitioners who have proven hands-on technical ability to competently handle day-to-day operations.
- **Increase overall cybersecurity IQ:** Implement the latest security best practices.
- **Improve information security coherence across the organization:** Professionals that speak the same language across disciplines and have cross-department perspective.
- **Instant credibility:** Increases organizational integrity in the eyes of clients and other stakeholders.
- **Satisfy requirements:** Meet certification mandate requirements for service providers and subcontractors.
- **Stay current:** Ensures professionals stay current on emerging and changing technologies, and security issues related to these technologies through the continuing professional education requirements.
- **Ensure compliance:** Comply with government or industry regulations (DoD 8140.01/8570.01 approved).



## OVERVIEW

(ISC)<sup>2</sup> developed the Certified Cloud Security Professional (CCSP) credential to ensure that cloud security professionals have the required knowledge, skills, and abilities in cloud security design, implementation, architecture, operations, controls, and compliance with regulatory frameworks. A CCSP applies information security expertise to a cloud computing environment and demonstrates competence in cloud security architecture, design, operations, and service orchestration. This professional competence is measured against a globally recognized body of knowledge. The CCSP is a standalone credential that complements and builds upon existing credentials and educational programs.

## TARGET AUDIENCE

Experienced cybersecurity and IT/ICT professionals who are involved in transitioning to and maintaining cloud-based solutions and services.

## TARGET JOB TITLES

- Enterprise Architect
- Security Administrator
- Systems Engineer
- Security Architect
- Security Consultant
- Security Engineer
- Security Manager
- Systems Architect

## REQUIRED EXPERIENCE

Candidates must have a minimum of 5 years cumulative work experience in information technology, of which 3 years must be in information security and 1 year in 1 or more of the 6 domains of the CCSP CBK. Earning CSA's CCSK certificate can be substituted for 1

year of experience in 1 or more of the 6 domains of the CCSP CBK. Earning (ISC)<sup>2</sup>'s CISSP credential can be substituted for the entire CCSP experience requirement.

A candidate that doesn't have the required experience to become a CCSP may become an Associate of (ISC)<sup>2</sup> by successfully passing the CCSP examination. The Associate of (ISC)<sup>2</sup> will then have 6 years to earn the 5 years required experience.

## DOMAINS COVERED

1. Cloud Concepts, Architecture and Design
2. Cloud Data Security
3. Cloud Platform & Infrastructure Security
4. Cloud Application Security
5. Cloud Security Operations
6. Legal, Risk & Compliance

## STEPS TO CERTIFICATION

1. Obtain the Required Experience
2. Take and Pass the Exam
  - Find a local Pearson VUE Test Center and register for the exam at [www.pearsonvue.com/isc2](http://www.pearsonvue.com/isc2)
3. Complete the Endorsement Process
  - Get work experience endorsed by an (ISC)<sup>2</sup> member within 9 months of exam date
4. Maintain Membership
  - Earn and submit 90 CPE credits by the end of the 3-year cycle
  - Pay the annual maintenance fee of U.S. \$125

## ABOUT THE EXAM

Length of Exam: Up to 3 hours

Questions: 125

Question Format: Multiple choice

Passing grade: 700 out of 1000 points

Testing center: Pearson VUE Testing Center [pearsonvue.com/isc2](https://www.pearsonvue.com/isc2)

Exam availability: English and Japanese

Exam pricing: U.S. \$599

## ACE CREDIT

**College Credit Eligible:** Recognized by the American Council on Education's College Credit Recommendation. Service (ACE CREDIT) to receive 3 college credit hours for completing an Official CCSP Training Seminar.

## BENEFITS TO ORGANIZATION

- **Secure and optimize cloud infrastructure and services:** Strengthen the security posture with qualified and experienced cloud security professionals.
- **Ensure proper cloud security controls:** Reinforce risk and legal requirements through cloud contract and SLAs with cloud service providers.
- **Instant credibility:** Increases organizational integrity in the eyes of clients and other stakeholders.
- **Stay current:** Ensure work teams stay current on evolving cloud technologies, threats, and mitigation strategies by meeting (ISC)<sup>2</sup>'s continuing professional education requirements.





## OVERVIEW

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.

## TARGET AUDIENCE

The CAP is ideal for IT, information security and information assurance practitioners and contractors who use the RMF in federal government, military, civilian roles, local governments and private sector organizations.

## TARGET JOB TITLES

- ISSOs, ISSMs and other infosec/information assurance practitioners who are focused on security assessment and authorization (traditional C&A) and continuous monitoring issues.
- Executives who must "sign off" on Authority to Operate (ATO).
- Inspector generals (IGs) and auditors who perform independent reviews.
- Program managers who develop or maintain IT systems.
- IT professionals interested in improving cybersecurity and learning more about the importance of lifecycle cybersecurity risk management.

## REQUIRED EXPERIENCE

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)<sup>2</sup> by successfully passing the CAP examination. The Associate of (ISC)<sup>2</sup> will then have 3 years to earn the 2-year required experience.

## DOMAINS COVERED

1. Information Security Risk Management Program
2. Scope of the Information System
3. Selection and Approval of Security and Privacy Controls
4. Implementation of Security and Privacy Controls
5. Assessment/Audit of Security and Privacy Controls
6. Authorization/Approval of Information System
7. Continuous Monitoring

## STEPS TO CERTIFICATION

1. Obtain the Required Experience
2. Take and Pass the Exam
  - Find a local Pearson VUE Test Center and register for the exam at [www.pearsonvue.com/isc2](http://www.pearsonvue.com/isc2)
3. Complete the Endorsement Process
  - Get work experience endorsed by an (ISC)<sup>2</sup> member within 9 months of exam date
4. Maintain Membership
  - Earn and submit 60 CPE credits by the end of the 3-year cycle
  - Pay the annual maintenance fee of U.S. \$125

## ABOUT THE EXAM

**Length of Exam:** Up to 3 hours

**Questions:** 125

**Question Format:** Multiple choice

**Passing grade:** 700 out of 1000 points

**Testing center:** Pearson VUE Testing Center [pearsonvue.com/isc2](http://pearsonvue.com/isc2)

**Exam availability:** English

**Exam pricing:** U.S. \$599

## ACE CREDIT

**College Credit Eligible:** Recognized by the American Council on Education's College Credit Recommendation. Service (ACE CREDIT) to receive 3 college credit hours for completing an Official CAP Training Seminar.

## BENEFITS TO ORGANIZATION

- **Secure the organization's critical data:** Strengthen the security posture with qualified practitioners who have proven hands-on technical ability to competently handle day-to-day operations.
- **Increase overall cybersecurity IQ:** Implement the latest security best practices.
- **Improve information security coherence across the organization:** Professionals that speak the same language across disciplines and have cross-department perspective.
- **Instant credibility:** Increases organizational integrity in the eyes of clients and other stakeholders.
- **Satisfy requirements:** Meet certification mandate requirements for service providers and subcontractors.

- **Stay current:** Ensures professionals stay current on emerging and changing technologies, and security issues related to these technologies through the continuing professional education requirements.
- **Ensure compliance:** Comply with government or industry regulations (DoD 8140.01/8570.01 approved).



## OVERVIEW

The Certified Secure Software Lifecycle Professional (CSSLP) validates that software professionals have the expertise to incorporate security practices –authentication, authorization and auditing –into each phase of the software development lifecycle (SDLC), from software design and implementation to testing and deployment.

## TARGET AUDIENCE

The CSSLP is ideal for software development and security professionals responsible for applying best practices to each phase of the software development lifecycle (SDLC). It shows you have advanced knowledge and the technical skills to effectively design, develop and implement security practices within each phase of the software lifecycle.

## TARGET JOB TITLES

- Software Architect
- Software Engineer
- Software Developer
- Application Security Specialist
- Software Program Manager
- Quality Assurance Tester
- Penetration Tester
- Software Procurement Analyst
- Project Manager
- Security Manager
- IT Director/Manager

## REQUIRED EXPERIENCE

A candidate is required to have a minimum of 4 years cumulative paid full-time Software Development Lifecycle (SDLC) professional work experience in 1 or more of the 8 domains of the (ISC)<sup>2</sup> CSSLP CBK, or three years of cumulative paid full-time SDLC professional work

experience in one or more of the 8 domains of the CSSLP CBK with a 4-year degree leading to a Baccalaureate, or regional equivalent in Computer Science, Information Technology (IT) or related fields.

A candidate that doesn't have the required experience to become a CSSLP may become an Associate of (ISC)<sup>2</sup> by successfully passing the CSSLP examination. The Associate of (ISC)<sup>2</sup> will then have 5 years to earn the 4 years required experience.

## DOMAINS COVERED

1. Secure Software Concepts
2. Secure Software Requirements
3. Secure Software Architecture and Design
4. Secure Software Implementation
5. Secure Software Testing
6. Secure Software Lifecycle Management
7. Secure Software Deployment, Operations, Maintenance
8. Secure Software Supply Chain

## STEPS TO CERTIFICATION

1. Obtain the Required Experience
2. Take and Pass the Exam
  - Find a local Pearson VUE Test Center and register for the exam at [www.pearsonvue.com/isc2](http://www.pearsonvue.com/isc2)
3. Complete the Endorsement Process
  - Get work experience endorsed by an (ISC)<sup>2</sup> member within 9 months of exam date
4. Maintain Membership
  - Earn and submit 90 CPE credits by the end of the 3-year cycle
  - Pay the annual maintenance fee of U.S. \$125



## ABOUT THE EXAM

Length of Exam: Up to 3 hours

Questions: 125

Question Format: Multiple choice

Passing grade: 700 out of 1000 points

Testing center: Pearson VUE Testing Center [pearsonvue.com/isc2](https://pearsonvue.com/isc2)

Exam availability: English

Exam pricing: U.S. \$599

## ACE CREDIT

**College Credit Eligible:** Recognized by the American Council on Education's College Credit Recommendation Service (ACE CREDIT) to receive 3 college credit hours for completing an Official CSSLP Training Seminar.

## BENEFITS TO ORGANIZATION

- **Protect reputation:** Reduce loss of revenue and reputation due to a breach resulting from insecure software.
- **Improve processes:** Break the "penetrate and patch" test approach.
- **Save money:** Reduce production cost, vulnerabilities, and delivery delays.
- **Instant credibility:** Increases credibility of the organization and its development team.
- **Stay current:** Ensures professionals stay current on best practices, policies and procedures throughout the software development life cycle through the continuing professional education requirements.
- **Ensure compliance:** Comply with government or industry regulations (DoD 8140.01/8570.01 approved).





## OVERVIEW

Associate of (ISC)² designation is the best way to start your journey to a rewarding career in cybersecurity, when you don't yet have the necessary experience to earn a globally recognized cybersecurity certification.

Through the Associate of (ISC)² program, you can take any of our certification exams without the required work experience. When you pass, you become an Associate of (ISC)² as you work to gain the necessary experience to achieve full certification.

## TARGET AUDIENCE

Anyone who does not have the required work experience.

After successfully passing any (ISC)² exam, candidate can pay their first AMF of \$U.S. 50 to become an Associate of (ISC)². They will have access to all the benefits of membership, including PDI courses, webinars, member discounts and more.

## About (ISC)²

(ISC)²® is an international nonprofit membership association focused on inspiring a safe and secure cyber world. Best known for the acclaimed Certified Information Systems Security Professional (CISSP®) certification, (ISC)² offers a portfolio of credentials that are part of a holistic, programmatic approach to security. Our membership, more than 160,000 strong, is made up of certified cyber, information, software and infrastructure security professionals who are making a difference and helping to advance the industry. Our vision is supported by our commitment to educate and reach the general public through our charitable foundation – The Center for Cyber Safety and Education™.

### For more information on (ISC)²,

visit [www.isc2.org](http://www.isc2.org), follow us on [Twitter](#) or connect with us on [Facebook](#) and [LinkedIn](#).