CSSLP®

Certified Secure Software Lifecycle Professional

ISC2 Certification

The Art and Science of

SECURE SOFTWARE DEVELOPMENT

in the Age of AI and Automation

Software security requires a creative, disciplined and forward-thinking approach. It demands a clear vision to develop secure strategies and implement effective tactics, executing them seamlessly in a dynamic and evolving technological landscape. Drawing from successes and failures and leveraging cutting-edge tools and methodologies enable professionals to excel in this critical discipline.

In this eBook, practitioners share insights from their diverse experiences, showcasing how Certified Secure Software Lifecycle Professional (CSSLP) certification empowered them to navigate challenges, embrace innovation and succeed in building secure, resilient software systems.

To excel, you need to combine creativity and security-driven practices while mastering the essential pillars of secure software development. Mistakes at any stage and emerging risks like those posed by AI can introduce vulnerabilities, underscoring the need for immediate identification and resolution.

We spoke to industry professionals to uncover their lessons learned and demonstrate how CSSLP equips them to prevent predictable and costly errors while navigating the complexities of secure software development.

STRATEGY

Develop a forward-thinking plan that integrates security from the outset, addressing both traditional and emerging risks like those posed by AI and evolving threat landscapes.

First-thought Process

“In the pre-AI era, planning, building and testing infrastructure required significant effort added to the overall project schedule. With the help of AI, multiple tools are used in both the development cycle and the deployment/testing of infrastructure components.

However, AI-assisted applications pose completely new threats to the software development cycle by introducing direct or indirect vulnerabilities. The knowledge obtained from CSSLP not only helps in navigating some of the challenges associated with the AI-assisted development lifecycle but also addresses some of the key compliance-related aspects when introducing AI-assisted tooling.

CSSLP ensures that developers, architects and managers think through the entire journey of the secure software lifecycle, enforcing security as a first-thought process.

CSSLP certainly helps in bringing a more disciplined approach to the secure software development lifecycle. It is a comprehensive certification that addresses the entire spectrum of software lifecycle security.”

Santosh Kumar
Chief Security Architect/Director - CCBU, Cisco
London

Security by Design

"One significant software failure I worked with was the problem of hard coded, backdoor passwords. While working for a building controls company, the previously closed networks within a single building or several buildings were merged into larger and larger networks, and ultimately became accessible to the internet.

Although the use of backdoor passwords is never a good idea, they absolutely cripple control systems that can be accessed via the internet.

The knowledge I acquired while pursuing the CSSLP informed me of many of the vulnerabilities that can occur and how they can be mitigated. More importantly, it laid a foundation for approaching security by design at the earliest stages of development and throughout the product lifecycle.

The biggest benefit to obtaining the CSSLP was that it broadened my perspective when it came to product design. It added security as an important factor to consider in any design, in addition to all of the other requirements. This adds confidence as we bring new products to market."

Tim Riesch

Senior Embedded Software Engineer
PDQ Manufacturing
De Pere, WI

Rigorous Quality Assurance Testing

"Years ago, a new version of security software developed by third-party developers and managed by my project team was to be integrated with commercial off-the-shelf software.

Unfortunately, a software defect resulted in an unauthorized disclosure of information to an unauthenticated user. Old bugs that were fixed in the earlier versions resurfaced in the new version. Through the investigation, it was revealed that the developers did not properly test the software prior releasing it to us for deployment.

Through CSSLP certification, we learned the importance of enforcing a rigorous software quality assurance testing regime, especially integration testing with COTS software and regression testing.

CSSLP gives me a fundamental understanding of what is required for a holistic, secure software development lifecycle, covering people, processes and technology in each phase. In fact, in today's paradigm shift to cloud, the principles and concepts covered in the CSSLP study materials continue to be relevant when applying them in the context of DevSecOps."

Yew Hoong Wong

ISSAP, ISSEP, ISSMP, CISSP, CCSP, CSSLP, CGRC

Senior Assistant Director, CSA

Singapore

Holistic End-to-End Testing

"When I started my first job as a programmer, I was developing an enterprise workflow application with just on-the-job training, learning as I go both in programming and coding practices. Secure coding was not front-and-center of the job.

The first version of the application was so buggy that whenever the user keyed nonnumeric input into numeric fields, it would not work, and in worst-case scenarios, it would hang the system.

The CSSLP exam outline provides a holistic end-to-end view of the secure software development lifecycle. It helps me in connecting the dots in all the integral parts of the end-to-end product and service offerings to customers. Having a seamless customer experience completes the product offering, which delights customers and builds trust.

CSSLP certification provides holders with industry recognition as an expert in the secure software development lifecycle. It has given me the confidence to carry out my job by understanding the concepts, technology and solutions presented by solutions architects and security architects."

Kevin Wu

CSSLP
Senior Program Manager, KATIM
Abu Dhabi, UAE

Fostering a Culture of Security

"One of the most interesting stories I can share is one of my oldest. A manager introduced application security training to the organization, but the training was not well-received. It was later discovered that passwords were not being correctly encrypted in a database. Once the problem was corrected, they began to view application security more seriously.

That event helped to foster a cultural change in the organization; they decided to appoint a CISO and move to a proactive approach to security.

The CSSLP exam outline covers a lot of topics, from basic to advanced. It collects the information in a series of clear categories and is structured in a way that simply makes sense. One of the most useful pieces of knowledge I gathered from CSSLP is a strong understanding of security principles. After years, I still use it every day.

CSSLP has represented an opportunity to complete my knowledge with important concepts I missed and a way to learn more vendor-independent language.

Simone Curzi

CSSLP

Senior Technical Program Manager, Microsoft

Umbria, Italy

Building Trust Between Teams

"AI makes life easier and quicker for software development. It can improve infrastructure monitoring by analyzing historical data and logs from various sources to formulate a baseline of normal patterns. Businesses can also understand the sophisticated compliance requirements (what) and then obtain best practices (how) handfully.

However, AI brings along other security risks. For example, the accuracy, integrity and trustworthiness of AI-generated codes are new challenges.

CSSLP knowledge helps us ensure security is thoroughly considered and tested in each phase of the development cycle, no matter how rapid it becomes. More importantly, CSSLP doesn't simply tell me what to do to build secure software, it enables me to understand how to build software securely.

Before gaining my CSSLP, my work focused more on infrastructure, which was important but far from complete in terms of security. The knowledge obtained through CSSLP helped me understand the software development process and communicate the need for security to developers. This facilitated cooperation and enabled the building of trust between security and development teams."

Alan Chan

CSSLP

Deputy General Manager, Information Security

Providing Effective Advisory Services

"As a professional security consultant, I have been involved in the full range of software development spectrums, from secure by design to absence of any security concept.

However, the advent of AI has changed the security landscape. For example, AI simplifies compliance by automating data classification, monitoring and reporting. Natural language processing assists in analyzing complex legal texts to identify applicable requirements.

AI tools facilitate comprehensive assessments of infrastructure by analyzing system performance, identifying vulnerabilities and predicting potential threats with precision. This proactive approach strengthens resilience, ensuring that organizations can adapt swiftly to evolving cybersecurity landscapes.

However, AI also brings new challenges.

CSSLP certification equips professionals with a framework to embed security into the software development lifecycle. This foundation is crucial for AI, where dynamic data and adaptive algorithms heighten security challenges. The emphasis on risk management and secure coding ensures that AI-assisted systems are resilient and ethical, fostering user trust and compliance with emerging standards.

With the CSSLP credential, I am appreciated, and it pleases me to apply the skills to my valued customers. This security mindset plays a major role in recognition, acknowledgment and implementation in the cybersecurity industry."

Nop Phoomthaisong

ISSAP, CISSP, CSSLP

CEO, Mayaseven Co., Ltd.

Bangkok, Thailand

Fostering Professionalism

"The domains of the CSSLP exam outline enable IT organizations to have a clear vision in all aspects of secure IT application systems. This is very important because it helps organizations set up associated policies and guidelines in application development.

For example, CSSLP certification provides a broad domain knowledge of best practices and security principles for secure AI application systems development. Applying and integrating these practices and principles allows AI application systems to be developed and used to protect sensitive data and ensure the AI operates ethically and without bias.

The biggest benefit to me in gaining CSSLP certification is the ability to foster professionalism in secure software systems development. It provides me with domain knowledge to evaluate and recommend secure software systems development processes to my clients.

Secure software engineering is a discipline, and the CSSLP helps to maintain that discipline."

Patrick Eulogius Yau

CISSP, CSSLP

Senior Specialist - Technology Controls and Governance, AIA Australia

Victoria, Australia

Security On Day One

“AI tools provide insights through data-driven assessments, identifying vulnerabilities, inefficiencies and areas requiring improvement in real time. AI also evaluates compliance with security standards and readiness for emerging technologies, enabling faster, more informed decision-making.

The knowledge obtained through CSSLP helps everyone in the creation chain to see the bigger picture when it comes to cybersecurity features in modern software. It gives these stakeholders the necessary tools to integrate cybersecurity into software products from day one.

CSSLP principles helped me improve the secure development and use of AI-assisted applications in software development and AI-assisted software.

My expertise ensures that both AI-driven tools and the software they create are reliable, ethical and secure, mitigating risks from dependency vulnerabilities, data bias and evolving threats while maintaining accountability and trust throughout the process.

I treat any certification or training opportunity as a way to improve my fundamentals in a specific domain. Experience alone isn’t sufficient, especially when dealing with emerging technologies.

The CSSLP credential, through its continuous professional education requirements, has helped me remain relevant in the field of software security.”

Sergiu Seche

CSSLP

Project Leader, Boston Consulting Group

London, UK

Cost Avoidance

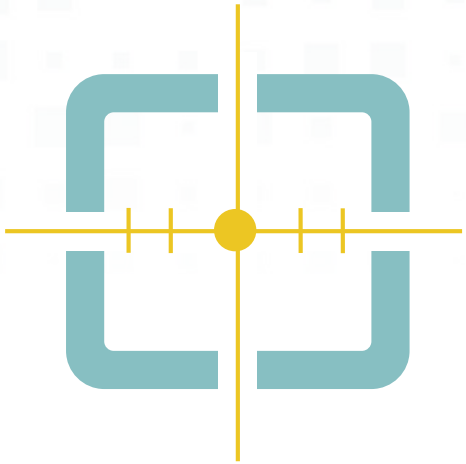
“One of the most significant software failures that I remember happened when there was a decision to migrate critical hardware components that were designed to operate on a legacy technology without involving the security team. Security was dismissed as an unimportant factor. This migration opened up many new vulnerabilities for the system, including data spoofing and alteration. The confidentiality, integrity and availability of the data was subject to being compromised. That particular system has since been redesigned, but the redesign of the subsystem resulted in additional costs and overruns.”

Thomas Jackson

CISSP, CCSP, CSSLP

Principal Systems Architect - Cybersecurity

TACTICS



Equip yourself with modern tools and techniques, such as AI-driven threat modelling and automated security testing, to proactively mitigate risks and adapt to dynamic environments.

Security Increases Quality

"A widely held thought process is that security is the final checklist to review as an addendum to other forms of acceptance testing. Unfortunately, this approach has led to overwhelming levels of technical debts that are costly to resolve – and that is the best-case scenario.

The most impactful thing I gained in preparing for the CSSLP is the concept of the software supply chain. It isn't enough to run a static and a dynamic code scan and say your code is secure. We must vet and thoroughly test the entire software development lifecycle – including our entire supply chain: anyone and anything that is a dependency in our process.

The same is valid for AI systems. We secure an AI system the same way we secure any other software system: by breaking it down into individual components and examining what could be exploited within each component. We need to think in terms of the supply chain or anything that goes into the development of that system.

The biggest benefit to earning the CSSLP was gaining a deep understanding of the relationship between software security and quality. Also, I gained insights in helping an organization set up cybersecurity checkpoints throughout the software development lifecycle to ensure that security is as integrated as functionality, not impeding progress but rather enhancing it."

Brian J. Barber

CISSP, CSSLP

Senior Cybersecurity Engineer (AppSec), Raft

McLane, VA

Situational Awareness

"AI systems are software by nature, and most of them use specific technologies, programming languages and libraries.

CSSLP certification gives me deep knowledge of software security management. With that knowledge changing continuously over the years and focusing more on supply chain vulnerabilities and mitigations, it has become an ally in addressing the challenges of AI-based systems.

It allows me to be more aware and better advise my clients on best practices for secure development and deployment.

The biggest benefit derived from earning the CSSLP credential is elevated reputation. Certification is a huge advantage, not only because of the status it gives to me as a software security expert but due to the fact that I must keep it up to date through continuous learning."

Cristián Rojas

CSSLP
Cybersecurity Auditor, Professor and Speaker
Santiago, Chile

Secure Codebases for High-End Projects

"In a company I worked for previously, we did pen testing on various applications before release to customers. One such test was on a mobile application that handled medical information for insurance customers. The developers writing the code were inexperienced and had no formal training in secure development methodologies, making the application exceedingly vulnerable to even the most basic pen testing attacks on mobile applications. The end result for these errors was a six-month delay while the code was rewritten.

I use the knowledge I gained from CSSLP certification in both my own projects, as well as in consulting with customers for my company.

For software developers working on projects that are high-end or stretch over a long time, CSSLP helps both in writing more secure code and maintaining a secure codebase as the project moves along.

Having the CSSLP credential gives me a lot more weight when I'm advising customers on their development projects. The certification is something potential employers use as a differentiator, and it makes you much more eligible for more interesting software development projects."

Tom Madsen
CISSP, CSSLP
GRC Security Advisor, KMD
Ballerup, Denmark

Security as an Ever Thought

"In one of my early teams, we were building software, and I thought it was important for the team to know what the software was doing. So I trained them on various exploits and how they worked. At some point, I demonstrated SQL injections — what they are, how they work and how simple it is to run them. Upon seeing this, one of the lead database developers turned white and left the room. He later informed me that he was concerned, and the software needed to be fixed immediately.

The problem in particular with security is that developers who are not exposed to it early don't know to consider it from the beginning. Security needs to be an ever-thought, not an afterthought. To my knowledge, nobody ever took advantage of the obvious issue in the software.

I've been a CSSLP for a long time, and being able to connect with others who are securing software and services where I am just learning about them has been a huge benefit to me. Additionally, organizations continue to view certifications as a benefit."

Margaret Layton

CISSP, CSSLP

Security Architecture and Engineering, Children's National Hospital
Nokesville, VA

Security Point of Contact

"I was involved in testing a third-party mobile application and we uncovered a number of issues, including the ability to take over other user accounts. The source was excessive data exposure from the underlying API. This is a common issue and should ideally be found much earlier in API development, but instead was found just before it was released.

The CSSLP improves knowledge around key areas, such as common vulnerabilities, utilizing major industry resources to focus on recurring patterns. This helps highlight the ways vulnerabilities can be introduced and looks at aspects like threat modelling that can tease out potential vulnerabilities before the code is written.

Initially, the CSSLP credential moved me from being one of the developers on the team to being a security point of contact. The exam outline helped me learn other areas of security, which led me to offensive security. I now work as part of a red team, which includes testing software, and my development background and knowledge from CSSLP certification are still really useful."

Gavin Johnson-Lynn

CSSLP

Principal Offensive Security Specialist, Sage

Newcastle Upon Tyne, UK

Competitive Advantage

"I worked for a company that suffered a cyberattack to their accounting system that resulted in the system being down for two days, which impacted their global business operations. After an investigation, it was shown that the internet-facing system with a web interface allowed unauthorized access to financial data. The main contributing factor was that the system was over 10 years old so there was no security considered at the outset of the development. In addition, the security patches were not updated.

CSSLP expertise could have helped prevent this attack by reviewing the application through threat modeling, applying it in the design phase of the software development process, and by reinforcing hardening in software deployment phase and security testing.

CSSLP professionals not only demonstrate professional knowledge applicable to any company but also realize a competitive advantage in the job market."

Kenji Chang

CISSP, CSSLP

Head of Information Security, DFI Retail Group

Hong Kong

A Structured Approach

"Most of our customers are performing security audits of every software they use. By using AI-powered tools we can receive information on the software bill of materials, vulnerabilities and deployments. These tools analyze our systems to highlight potential security issues and help focus on the most important areas that need attention. This makes it easier to prioritize fixes and improve overall security.

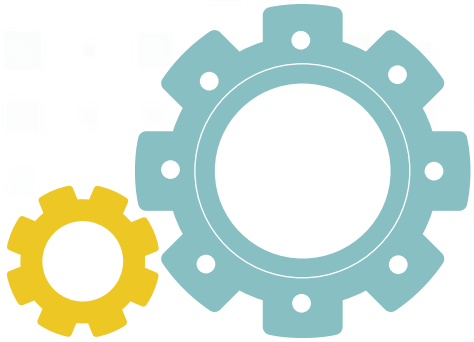
However, we mustn't forget that AI is still software. Due to the nature and power of AI technologies, the risks and challenges are much greater.

For example, AI training requires as much data as possible to be accurate, so data protection becomes even more important. Hence, the knowledge gained from the CSSLP certification is not only relevant but essential.

CSSLP certification provides a structured approach for dealing with security at all development stages. It provides both formal recognition and opens new types of opportunities. It provided me with the opportunity to learn the security language, which allows me to communicate with partners and customers effectively."

Erez Pasternak, CSSLP
Principal Lead Product Architect, Akamai Technologies
Tel Aviv, Israel

EXECUTION



Implement your vision with precision, ensuring seamless collaboration between teams and the integration of security practices at every stage of the software development lifecycle.

Multiple Methods to Solve Problems

"In a previous job, I witnessed the lack of proper constraint testing for a customer-facing web application that resulted in a large-scale denial of service attack, brought on by an exploit that utilized a successful cross-site scripting attack. This is of course avoidable today, given the knowledge I've gained through CSSLP training and certification.

By applying knowledge gained through study for the CSSLP exam, I've been able to understand and properly apply multiple methods, including constraint testing and proper security architecture development, most importantly understanding the need for properly protecting databases utilized by applications.

The largest benefit of earning CSSLP certification has been understanding how to implement an end-to-end framework, in conjunction with application development and security departments working together. That encompasses secure software implementation, testing and secure software lifecycle management."

Jim Rutt

CISSP, CCSP, CSSLP, SSCP, ISSAP, ISSEP, ISSMP

CIO & CISO, The Dana Foundation

New York, NY

Guidelines for Everyday Decisions

“The most valuable knowledge gained in the CSSLP learning process has been finding out about secure design principles. The CSSLP exam utline offers good guidelines that help in making decisions during the everyday software development process.

Let’s consider the use of AI, for example. Despite AI-based tools generating code fast and relatively easily, it’s important that software solutions stay maintainable now and in the future and cause no problems in business continuity.

CSSLP knowledge ensures compliance with privacy regulations, secure deployment and resilience against vulnerabilities in software systems. It helps to understand why it’s important to do coding reviews by developers and run automated testing.

Earning the CSSLP credential was valuable to me, as it has helped me in my everyday job, improving my software design and development skills and helping me to understand the importance of software systems in the context of business.”

Reimo Reisberg

CISSP, CSSLP

Lead Developer, Helmes

Tallinn, Estonia

Keeping the Numbers Correct

"When developing a daily credit card billing run, our team neglected to implement unit testing, leaving it as an afterthought. This led to a rounding error that resulted in dozens of erroneous charges to clients in production. This had severe consequences as a security issue when viewed from the confidentiality, integrity and availability perspective. The integrity of the customer's purchase was violated, and incorrect data was exposed.

CSSLP, with its emphasis on the software development lifecycle security components, clearly defines the role of multiple testing and quality assurance approaches, providing a testing-first mentality and approach to software development. Any one or all of these methods would have served to at least catch the rounding error and many more potential blunders.

I have seen three or four times more recruiter traffic in response to my LinkedIn profile since becoming CSSLP-certified. It attracts attention and has created many opportunities for conversation and consulting."

Alan Young
CISSP, CSSLP
Lead IAM Engineer, Booz Allen Hamilton
Menifee, CA

Strengthened Skills

“In a project that consisted of implementing various business processes on a software suite, we had a security failure that led to the configuration and permissions being modified. This granted unauthorized access to unauthorized administrative functionalities. The solution was to rebuild all the information from scratch to ensure correct operation.

Within the knowledge that corresponds to CSSLP, the security practices are understood within each phase of the development cycle. These practices invite us to approach security from the initial definition of the software to be implemented.

The knowledge related to CSSLP certification strengthens my skills within the tasks I perform. Now, I have the security capabilities and a holistic vision throughout the development lifecycle. This is an important role in the industry. It allows me to obtain quality results and guarantee software to clients and users with controlled and low-security risks.”

Carlos Fajardo

CSSLP
IT Project Manager, BBVA
Bogotá, Colombia

Refined Software Security Skills

"The knowledge obtained from the CSSLP exam outline facilitates the security evangelism necessary to implement a security-aware culture throughout the software development process. It solicits active inquiry into the identification and rationalization of strong software security requirements in the development of AI-assisted applications and software-based systems. The conceptualization of software security demands programming competency and technological foresight on emerging trends. Software security requirements further elicit tactical steps for rationalizing security concepts.

CSSLP certification formalized and refined the software security skills I gained in practicum. However, the biggest benefit is the framework it codifies, which can be used to educate students and practitioners on the breadth and depth of software security fundamentals.

The competencies gained from this education is monumental in developing the next generation of software security practitioners and will serve to continuously strengthen the overall security posture of software."

Jenelle Davis

CISSP, CSSLP

Principal Consultant and Adjunct Professor

Atlanta, GA

Risk Mitigation Competencies

"I recall one instance of a front-end development project where a wrong software library was installed, leading to the possibility of unintended data leakage.

The CSSLP exam outline addresses ways to prevent trivial design faults that can lead to breach events. Particularly, the sections of secure software design, secure software implementation and secure software testing are unmatched in their informational and educational value.

CSSLP training is unique in both system and application software design. The knowledge areas of implementation, testing and production enable me to prevent and mitigate huge cybersecurity risks."

Dr. Daniel Ng
Director

Professional Confidence for Performance

"Knowing and understanding the appropriate places to look and how applications can be attacked has been priceless to keeping out of the spotlight. I don't consider myself omniscient, but I always look for ways to defend in depth.

Attaining knowledge of application security and keeping up with the latest practices help reduce the likelihood of exposed vulnerabilities.

Security in software is of the utmost importance. AI is not any different in this regard. CSSLP gives you the structure and knowledge to address any type of software security, regardless of the technology. In this case, for AI-assisted applications and software-based systems, it is important to first understand the threat exposure of the system and consider an in-depth defense approach.

Looking for defenses in depth at the different application layers and evaluating threats during the design helps to better secure applications.

I started as a software developer in my career and only a little later did I realize the necessity to better understand security within applications. I realized that, as hacking sophistication grew, those controls were no longer adequate. At that point, I realized I needed to learn about securing applications. I took to the CSSLP exam to gain the confidence that I needed to be a better software developer."

Scott Brookhart

CISSP, CCSP, CSSLP

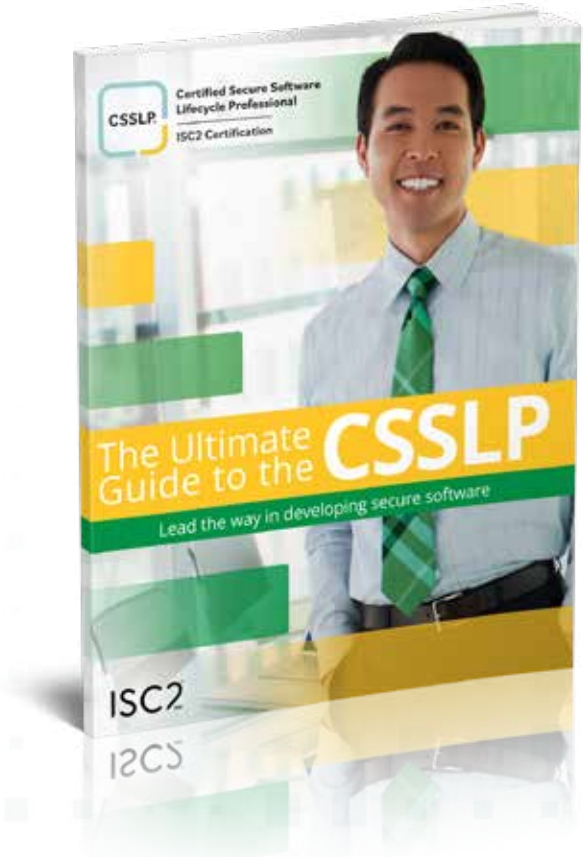
Problem Manager, Employees Retirement System of Texas

Austin, TX

How CSSLP Certification Helps

Earning CSSLP certification from ISC2 is a proven way to build your career and demonstrate your expertise and ability to incorporate security practices – authentication, authorization and auditing – into each phase of the software development lifecycle.

Begin your journey toward CSSLP by becoming an **ISC2 Candidate**. You'll join the world's leading cybersecurity professional organization and access a full range of benefits and discounts. **Sign up now** - your first year is free.



Next Step: Get the Ultimate Guide

Take your next step toward certification with **The Ultimate Guide to the CSSLP**. It covers everything you need to know about CSSLP certification. Find out how CSSLP and ISC2 can help you discover your certification path, create your pan and acquire knowledge and skills for a successful career.

Get Your Guide

About ISC2

ISC2 is the world's leading member organization for cybersecurity professionals, driven by our vision of a safe and secure cyber world. Our more than 265,000 certified members, and associates, are a force for good, safeguarding the way we live. Our award-winning certifications – including cybersecurity's premier certification, the CISSP® – enable professionals to demonstrate their knowledge, skills and abilities at every stage of their careers. ISC2 strengthens the influence, diversity and vitality of the cybersecurity profession through advocacy, expertise and workforce empowerment that accelerates cyber safety and security in an interconnected world. Our charitable foundation, **The Center for Cyber Safety and Education**, helps create more access to cyber careers and educates those most vulnerable. Learn more, get involved or become an ISC2 Candidate to build your cyber career at **ISC2.org**. Connect with us on **X**, **Facebook** and **LinkedIn**.

CC. SSCP. CISSP. CCSP. CGRC. CSSLP. ISSAP. ISSEP. ISSMP.