

A man with dark hair and a beard, wearing a light blue button-down shirt, is smiling broadly and gesturing with his hands as if speaking in a meeting. He is surrounded by other people, some of whom are also smiling. The background is slightly blurred, showing an office or conference room setting. A clear plastic cup is visible on the table in front of him.

(ISC)²

(ISC)² Certifications

Jon France
CISO

This is (ISC)²



Largest nonprofit membership association of certified cybersecurity professionals



Work with businesses and governments to build certifications that meet market needs



Provider of **lifelong professional education**



Global advocate for ethics, growth and success of the cybersecurity profession

We also do other stuff



Security Congress

(ISC)[®] SECURITY CONGRESS
JACKPOT!
 SAVE \$200 with Early Bird Through Sept. 16 [Register Now](#)
 OCT 10 - 12 LAS VEGAS CAESARS PALACE

Secure Summits

<p>Thursday, April 7, 2022 SECURE London BMA House</p>	<p>Thursday, July 14, 2022 SECURE Singapore Shangri-La Singapore</p> <p>Open for Registration</p>	<p>Friday, December 9, 2022 SECURE Washington, DC Renaissance Washington, DC Downtown Hotel</p> <p>Open for Registration</p>
---	--	---



Briefings

(ISC)[®] WEBINARS SECURITY BRIEFINGS
The CIO-CISO Balancing Act In The Cloud
 Guy Raz, Principal Systems Engineer, Extrahop
 Pam Everitt, Head of Advisory Services, Soteria
 Jeff Story, EVP/CISO, The Bankers Bank
 Brandon Dunlap, Moderator
[ExtraHop](#)

(ISC)[®] WEBINARS THINK TANK
Extending Governance to Your First & Third-Party Cloud Environments
 Sakrishna Chavali, Senior Product Marketing Manager, Proofpoint
 Jonathan Kinnitt, CISO, University of Tulsa
 Rex Messier, Principal Consultant, Mandiant
 Brandon Dunlap, Moderator
[proofpoint](#)

(ISC)[®] WEBINARS THINK TANK
Can You Beat the Clock?: The New Regulations on Breach Notification Reporting
 Daniel Schaeffer, CISO & IIR Information Technology, DomainTools
 Jennifer Bink, Director, Controlling & Information Governance, TransPerfect Legal Solutions
 Seth Giordano, Esq., VP, Corporate Privacy and General Counsel, Spin
 Brandon Dunlap, Moderator
[DOMAINTOOLS](#)

Think Tank

(ISC)[®] WEBINARS SECURITY BRIEFINGS
CyberRisk Alliance Global Security Report: Remote Workers Spell Trouble
 Srikrupa Srivatsan, Dir of Product Marketing, Infoblox
 Brandon Dunlap, Moderator
[Infoblox](#)

(ISC)[®] WEBINARS SECURITY BRIEFINGS
DDoS Attack Trends and Predictions for 2022
 David Warburton, Manager Threat Research, FS Labs
 Brandon Dunlap, Moderator
[FS](#)

(ISC)[®] WEBINARS SECURITY BRIEFINGS
Cloud Threat Report: IAM the first line of defense
 Nathaniel Quist, Principal Researcher, Unit 42
 Jay Chen, Principal Researcher Unit 42
 Brandon Dunlap, Moderator
[paloalto](#)



Knowledge Vault

The 'Hottest' IT Security Technologies in 2022
 Hitesh Piplani, CISSP
 Founder & CEO, Cybertage
 Moderator
 Brandon Dunlap
[ISC](#)
 KNOWLEDGE VAULT

Accelerate Your Cybersecurity Career with the **CISSP**
 Online Information Session 2022
 May 27 | 1:00-2:00 p.m. EST
[Sign Up Now](#)

CYBEREDGE GROUP
Insights From CyberEdge's 2022 Cyberthreat Defense Report
 Steve Piper, CISSP
 Founder & CEO
 CyberEdge

Accreditations, Recognitions and Endorsements



ASD Cyber Skills Framework



HM Revenue & Customs



HONG KONG MONETARY AUTHORITY
香港金融管理局



警視庁
Metropolitan Police Department



Earn Your Cybersecurity Certification



Certified in
Cybersecurity
An (ISC)[®] Certification



Systems Security
Certified Practitioner
An (ISC)[®] Certification



Certified Information
Systems Security Professional
An (ISC)[®] Certification



Certified Cloud
Security Professional
An (ISC)[®] Certification



Certified
Authorization Professional
An (ISC)[®] Certification



Certified Secure
Software Lifecycle Professional
An (ISC)[®] Certification



HealthCare Information
Security and Privacy Practitioner
An (ISC)[®] Certification

The Skills Gap



A woman with dark hair and glasses, wearing a light blue top with a floral pattern, is smiling and looking towards a man with a beard. She is holding a yellow notepad. The background is a blurred office or meeting environment with other people.

Yes. We can solve
the workforce
shortage **together.**

Keeping up isn't enough.

2020



2021

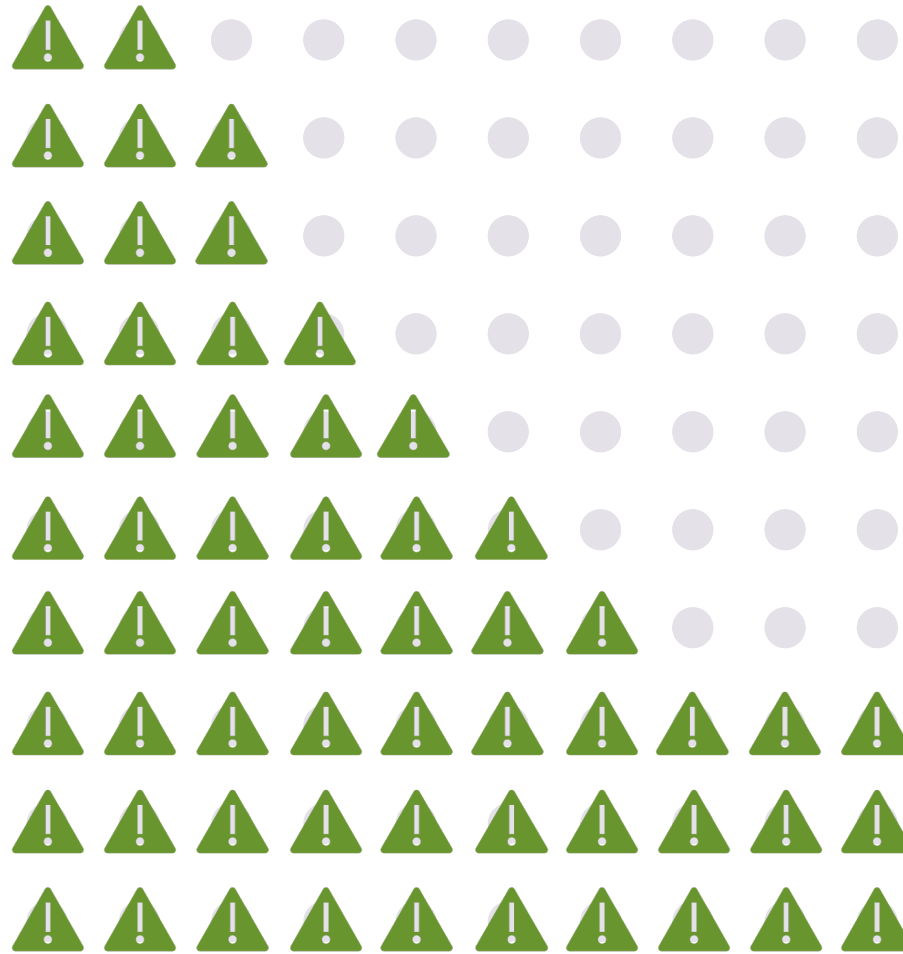


65%

How much the **cybersecurity workforce needs to increase** to close the gap

60%

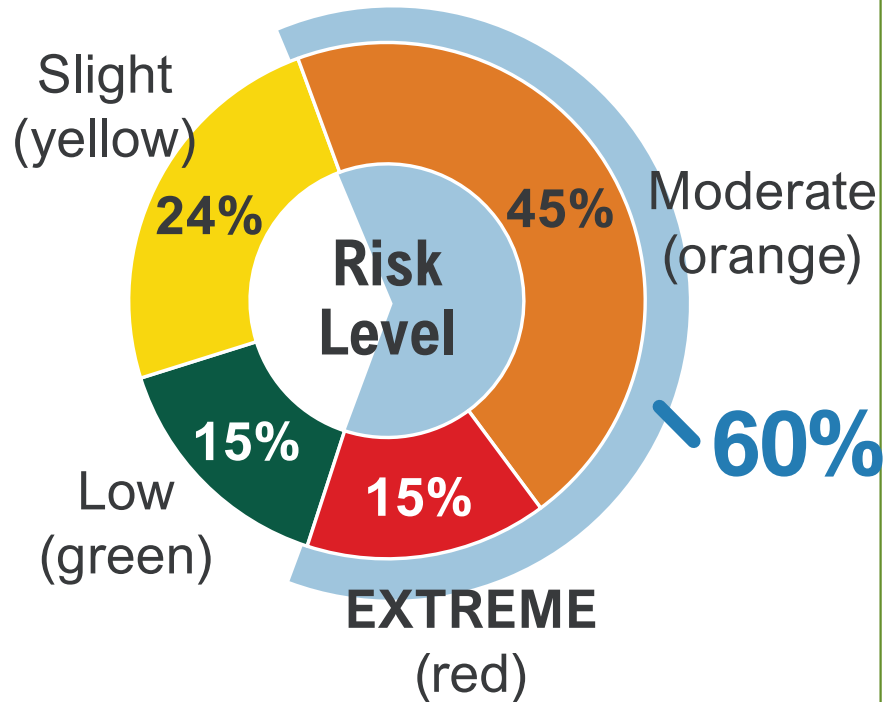
of study participants say
their organizations are at risk
due to staffing shortages



The Gap Puts Organizations at Risk

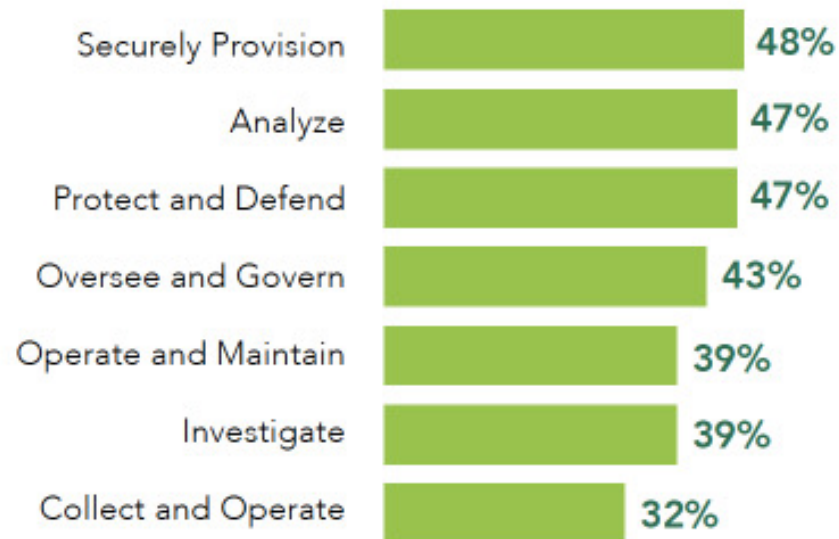
67%

Reported a cybersecurity staffing shortage



Despite another influx of **700,000** professionals into the cybersecurity workforce, the 2021 study shows that global demand for cybersecurity professionals continues to outpace supply

Cyber Staffing shortages by Function Area Worldwide



Real Consequences of Cyber Staff Shortages



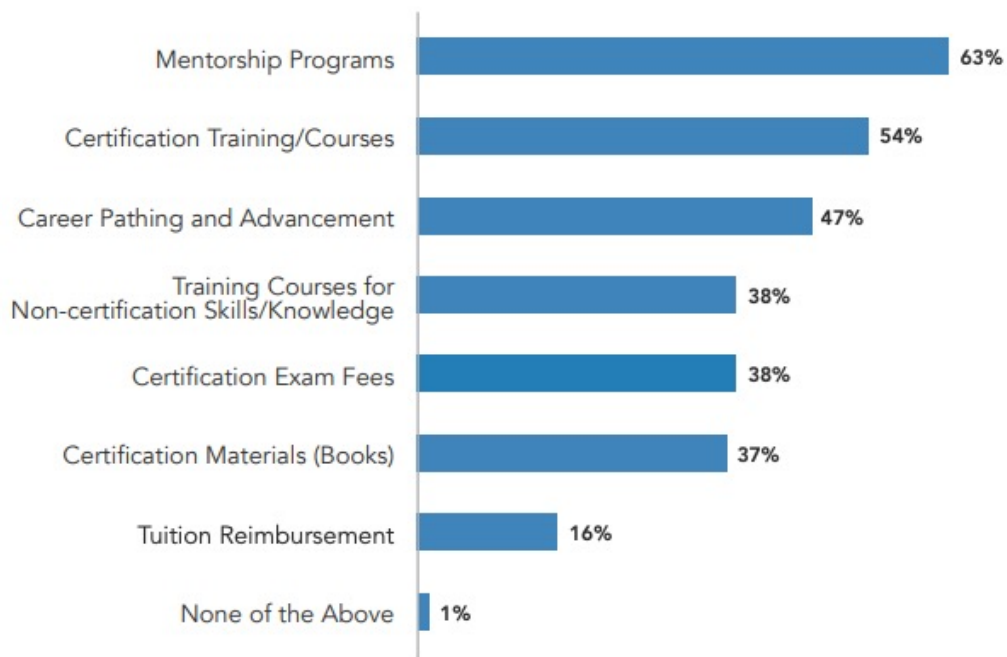


Help Wanted:
Talented people with the potential to succeed.
Deep IT experience *not always required.*

Top People Investments Organizations are Making to Address the Workforce Gap



How Hiring Managers Develop Entry- and Junior-Level Staff



Benefit of Hiring at the Entry Level

Entry Level and Junior Cyber Security staff bring new perspectives, ideas, creativity, critical skills in new technologies, enthusiasm and reinvigorating energy.

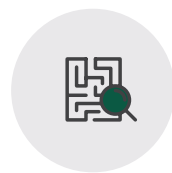
How have entry- or junior-level cybersecurity team members helped your organization?

“They often bring an element of creativity and out-of-the-box thinking to the team.”

Hire for aptitude and attitude. You can teach the rest.



34%
Analytical
thinking



33%
Problem
solving



27%
Critical
thinking



24%
Ability to work
in a team



21%
Creativity



19%
Ability to work
independently



11%
Data
visualization



10%
Business
acumen



Want to make an impact in your organization?
Recruit entry- and junior-level team members.

Time and cost to get entry- and junior-level employees up to speed

37%

of cybersecurity hiring managers surveyed estimate entry- and junior-level professionals are considered “up to speed” after six months or less on the job.

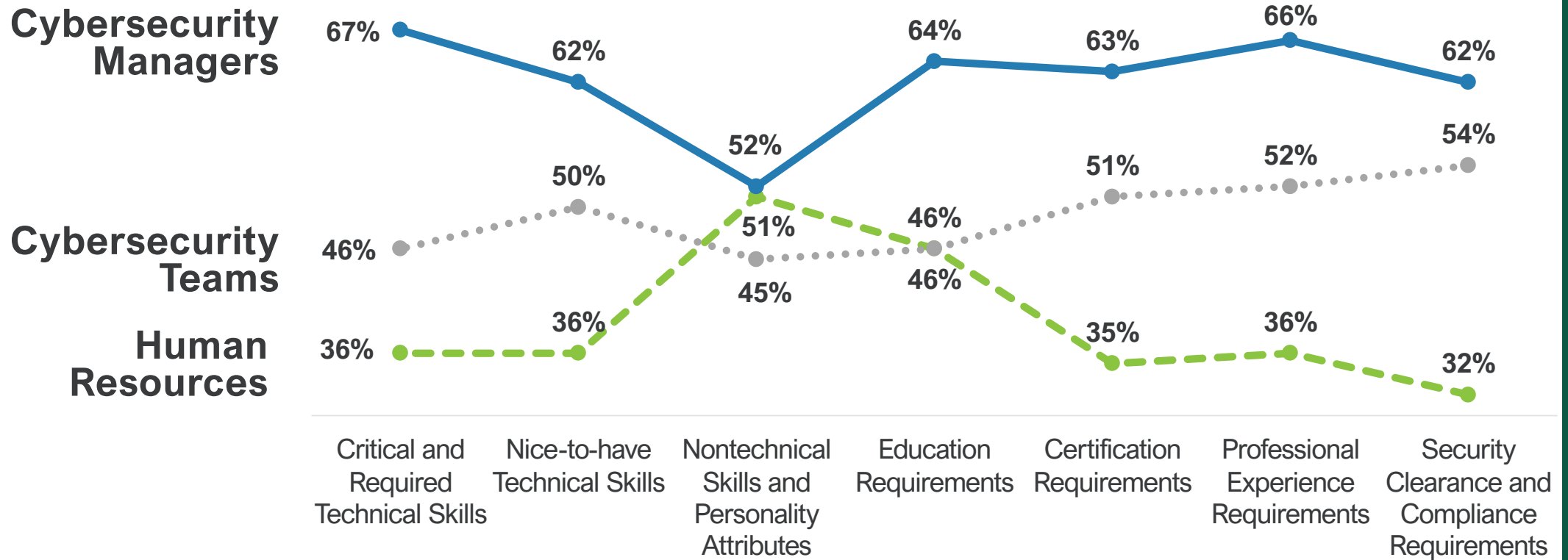
\$500–\$5,000

Cost to develop entry-and junior-level cybersecurity professionals

Source: 2022 (ISC)² Cybersecurity Hiring Managers Report



Who Takes the Lead?



Footnotes and source information goes here. Delete this text box if you're not using it.

IT Experience Not Always the Winning Attribute

92%
of
Cybersecurity Hiring
Managers
prioritize
candidates
with IT
experience




73%
Prioritize
cybersecurity education
but no work
experience



62%
Favor self-
taught
candidates
without work
experience





Establishing a new baseline. Introducing a path into the cybersecurity profession that welcomes a diversity of experience and builds a shared core of skills.



Certified in
Cybersecurity

An (ISC)² Certification

Ideal for People Without Cybersecurity Work Experience

The CC proves to employers that you have the foundational knowledge, skills and abilities necessary for an entry- or junior-level cybersecurity role. It signals your understanding of fundamental security best practices, policies and procedures, and your willingness and ability to learn more and grow on the job.





Certified in
Cybersecurity

An (ISC)² Certification

The CC is ideal for students, incoming professionals and career changers to build confidence and enter their first cybersecurity role prepared for what's next.

IT Professionals

College Students

Advanced High
School Students

Career Changers

Recent College
Graduates

Recent High
School Graduates



Certified in
Cybersecurity

An (ISC)² Certification

The broad spectrum of topics included in the CC Common Body of Knowledge (CBK[®]) ensures its relevancy across all disciplines in the field of information security. Successful candidates are competent in the following five domains:

Security Principles

Business Continuity
(BC), Disaster Recovery
(DR) & Incident
Response Concepts

Access Controls
Concepts

Network Security

Security Operations



Certified in
Cybersecurity

An (ISC)² Certification

There are no specific prerequisites to take the exam. It is recommended that candidates have basic information technology (IT) knowledge. No work experience in cybersecurity or formal educational diploma/degree is required. If you're a problem-solver with an analytical mindset, entry-level cybersecurity certification is right for you.



1 Million Globally

Growing the
Cybersecurity
Workforce

<https://www.isc2.org/landing/1MCC>



Certified in
Cybersecurity

An (ISC)² Certification

Benefits of (ISC)² Certification

Proves you have expertise employers need

Demonstrates you're continually improving your skills

Grants access to resources and educational tools

Provides peer-to-peer networking opportunities

Enables you to command top salaries

Sets you apart

Directly benefits you





Certified Information
Systems Security Professional

An (ISC)² Certification

Ideal for experienced security practitioners, managers and executives

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.





Certified Information
Systems Security Professional

An (ISC)² Certification

The CISSP is ideal for experienced security practitioners, managers and executives interested in proving their knowledge across a wide array of security practices and principles, including people in these positions.

Chief Information
Security Officer

Chief Information
Officer

Security Architect

Network Architect

Director of
Security

Security
Systems Engineer

Security Analyst

IT Director/Mgr.

Security Auditor

Security Manager

Security
Consultant



Certified Information
Systems Security Professional

An (ISC)² Certification

The broad spectrum of topics included in the CISSP CBK ensures its relevancy across all disciplines in the field of information security. Successful candidates are competent in the following eight domains:

Security and Risk
Management

Asset Security

Security
Architecture and
Engineering

Communication
and Network
Security

Identity and
Access
Management
(IAM)

Security
Assessment and
Testing

Security
Operations

Software
Development
Security



Certified Information
Systems Security Professional

An (ISC)² Certification

CISSP Experience Requirements

Candidates must have a minimum of five years' cumulative paid work experience in two or more of the eight domains of the CISSP CBK.1

Earning a four-year college degree or regional equivalent or an additional credential from the (ISC)² approved list will satisfy one year of the required experience.

Education credit will only satisfy one year of experience.

CISSP Concentrations

CISSP®

Certified Information
Systems Security Professional

An (ISC)² Certification

- ISSAP Architecture
- ISSEP Engineering
- ISSMP Management





Certified Information
Systems Security Professional

An (ISC)[®] Certification

ISSAP Architecture

Ideal for Chief Security Architects or Analysts

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. They facilitate the alignment of security solutions within the organization.





Certified Information
Systems Security Professional

An (ISC)² Certification

ISSAP Architecture

The ISSAP is a CISSP who distinguishes in planning security solutions and offering management with risk-based guidance to achieve organizational goals. They are experts in promoting the alignment of security solutions within the organizational context, such as mission, vision, policies, strategy, change, requirements, and external factors.

System Architect

System and
Network Designer

Chief Security
Officer

Chief Technology
Officer

Business Analyst



Certified Information
Systems Security Professional

An (ISC)[®] Certification

ISSAP Architecture

The broad spectrum of topics included in the ISSAP CBK ensures its relevancy across all disciplines in the field of information security. Successful candidates are competent in the following six domains:

Architect for Governance,
Compliance and
Risk Management

Security Architecture
Modeling

Infrastructure Security
Architecture

Identity and Access
Management (IAM)
Architecture

Architect for
Application Security

Security Operations
Architecture



Certified Information
Systems Security Professional

An (ISC)[®] Certification

ISSAP Architecture

CISSP-ISSAP Experience Requirements

Candidates must be a
CISSP in good
standing and have two
years cumulative paid
work experience in one
or more of the six
domains of the CISSP-
ISSAP CBK



Certified Information
Systems Security Professional

An (ISC)[®] Certification

ISSEP Engineering

Ideal for Systems Security Engineering Professionals

Proves your ability in applying security engineering principles into the business processes you support.





Certified Information
Systems Security Professional

An (ISC)[®] Certification

ISSEP Engineering

The ISSEP is ideal for the CISSP who specialize in implementing systems engineering principles and methods to create a security system. The ISSEP wants to build on their expertise in information security engineering.

Senior Systems
Engineer

Information
Assurance Officer

Senior Security
Analyst

Information
Assurance
Systems Engineer

Information
Assurance Analyst



Certified Information
Systems Security Professional

An (ISC)[®] Certification

ISSEP Engineering

The broad spectrum of topics included in the ISSEP CBK ensures its relevancy across all disciplines in the field of security engineering. Successful candidates are competent in the following five domains:

Systems Security
Engineering
Foundations

Risk Management

Security Planning
and Design

Systems Implementation,
Verification and
Validation

Secure Operations,
Change Management
and Disposal



Certified Information
Systems Security Professional

An (ISC)[®] Certification

ISSEP Engineering

CISSP-ISSEP Experience Requirements

Candidates must be a
CISSP in good
standing and have two
years cumulative paid
work experience
in one or more of the
five domains of the
CISSP-ISSEP CBK.



Certified Information
Systems Security Professional

An (ISC)[®] Certification

ISSMP Management

Ideal for CIOs, CISOs, CTOs, and Senior Security Executives

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.





Certified Information
Systems Security Professional

An (ISC)[®] Certification

ISSMP Management

CISSP-ISSMP certification is the executive's confirmation of network safety, which proves your skills to oversee, put forward, and set up data security outlines. Moreover, it helps to demonstrate your well-bred methodology in administration and the board's capabilities. As the name suggests, this certification incorporates zones of security arranging and task the board. The most well-known obligations of an ISSMP are to plan utility, response plans, and consistency.

Chief Information
Officer

Chief Technology
Officer

Chief Information
Security Officer

Senior Security
Executive



Certified Information
Systems Security Professional

An (ISC)[®] Certification

ISSMP Management

The broad spectrum of topics included in the ISSMP CBK ensures its relevancy across all disciplines in the field of information security management. Successful candidates are competent in the following six domains:

Leadership and
Business Management

Systems Lifecycle
Management

Risk Management

Threat Intelligence and
Incident Management

Contingency
Management

Law, Ethics and
Security Compliance
Management



Certified Information
Systems Security Professional

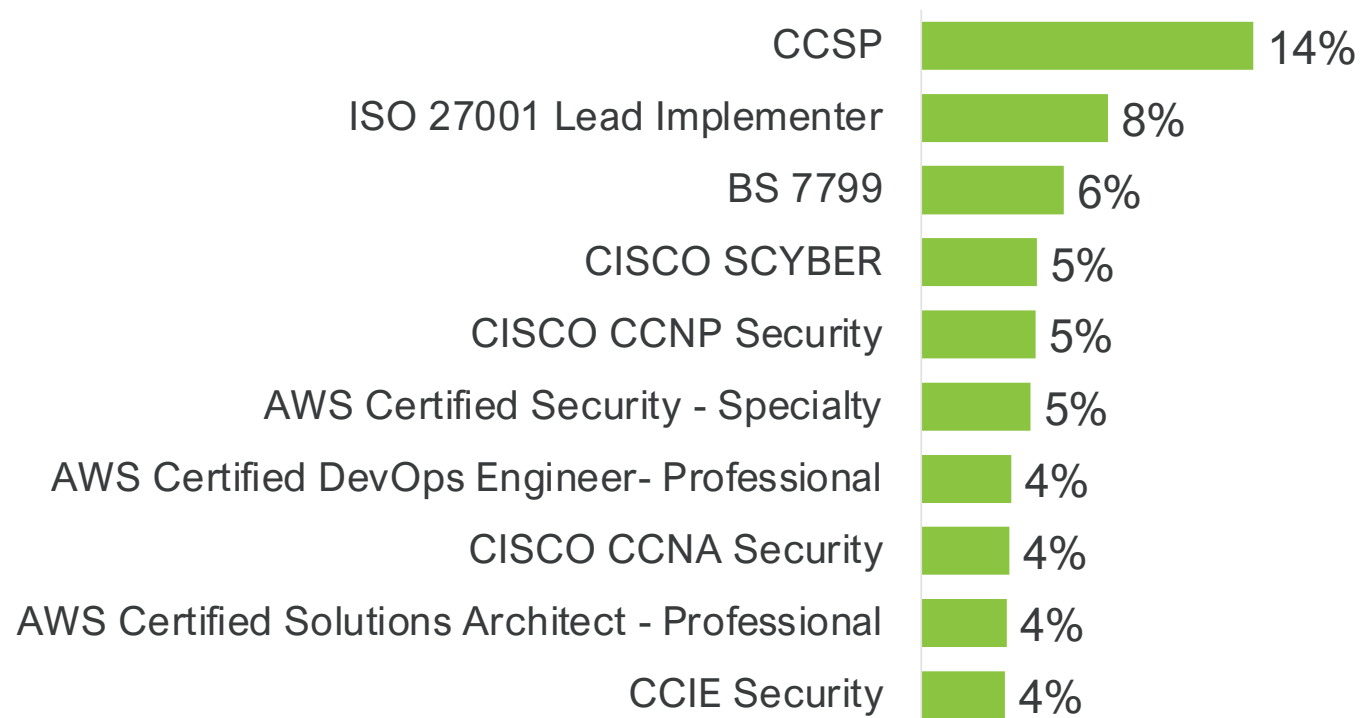
An (ISC)[®] Certification

ISSMP Management

CISSP-ISSMP Experience Requirements

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

Top Certifications and Certificates Pursued in 2021



CCSP®

Certified Cloud
Security Professional

An (ISO)² Certification

Ideal for Cloud Security Professionals

Shows you have the required knowledge, skills, and abilities in cloud security design, implementation, architecture, operations, controls, and compliance with regulatory frameworks.





Certified Cloud
Security Professional

An (ISO)² Certification

The CCSP is ideal for IT and information security leaders responsible for applying best practices to cloud security architecture, design, operations and service orchestration, including people in these positions.

Cloud Architect

Cloud Consultant

Cloud Security
Analyst

Auditor of Cloud
Computing Services

Cloud Engineer

Cloud
Administrator

Cloud Specialist

Professional
Cloud Developer



Certified Cloud
Security Professional

An (ISO)² Certification

The broad spectrum of topics included in the CCSP CBK ensures its relevancy across all disciplines in the field of information security. Successful candidates are competent in the following six domains:

Cloud Concepts,
Architecture and Design

Cloud Data Security

Cloud Platform &
Infrastructure Security

Cloud Security
Operations

Cloud Application
Security

Legal, Risk and
Compliance



Certified Cloud
Security Professional

An (ISC)² Certification

CCSP Experience Requirements

Candidates must have a minimum of five years' cumulative paid work experience in information technology, of which three years must be in information security and one year in one or more of the six domains of the CCSP CBK.

Earning CSA's CCSK certificate can be substituted for one year of experience in one or more of the six domains of the CCSP CBK.

Earning (ISC)²'s CISSP credential can be substituted for the entire CCSP experience requirement.



HealthCare Information
Security and Privacy Practitioner

An (ISC)² Certification

Ideal for Staff Charged with Guarding PHI

Proves ability to successfully implement, manage or assess security and privacy controls for healthcare and patient information.

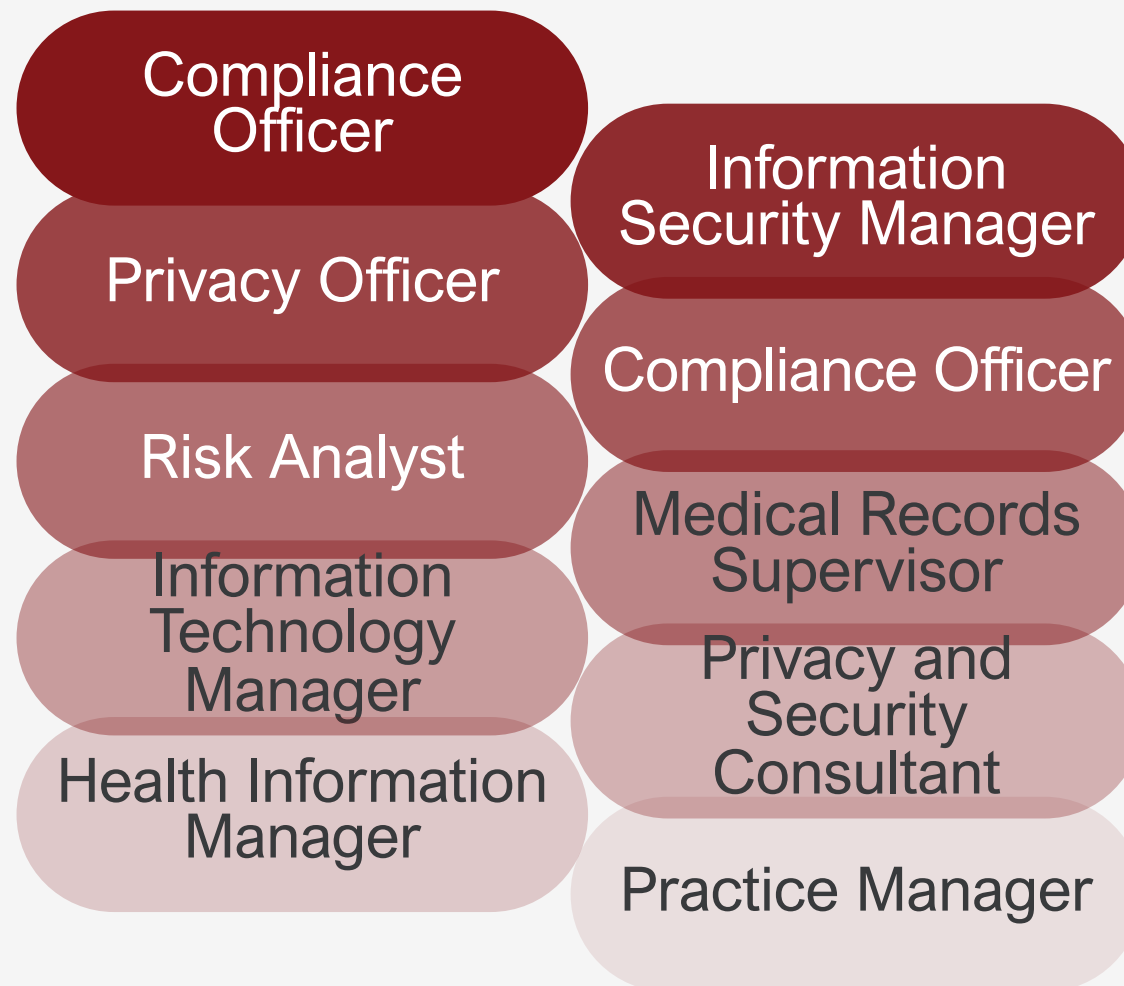




HealthCare Information
Security and Privacy Practitioner

An (ISC)² Certification

The HealthCare Information Security and Privacy Practitioner (HCISPP) is the ideal certification for those with the core knowledge and experience needed to implement, manage or assess the appropriate security and privacy controls of a healthcare organization. HCISPP provides confirmation of a practitioner's knowledge of best practices and techniques to protect organizations and sensitive data against emerging threats and breaches.





HealthCare Information
Security and Privacy Practitioner

An (ISC)² Certification

The broad spectrum of topics included in the HCISPP CBK ensure its relevancy across all disciplines in the field of information security. Successful candidates are competent in the following seven domains:

Healthcare
Industry

Information
Governance in
Healthcare

Information
Technologies in
Healthcare

Regulatory and
Standards
Environment

Privacy and
Security in
Healthcare

Risk Management
and Risk
Assessment

Third-Party Risk
Management



HealthCare Information
Security and Privacy Practitioner

An (ISC)² Certification

HCISPP Experience Requirements

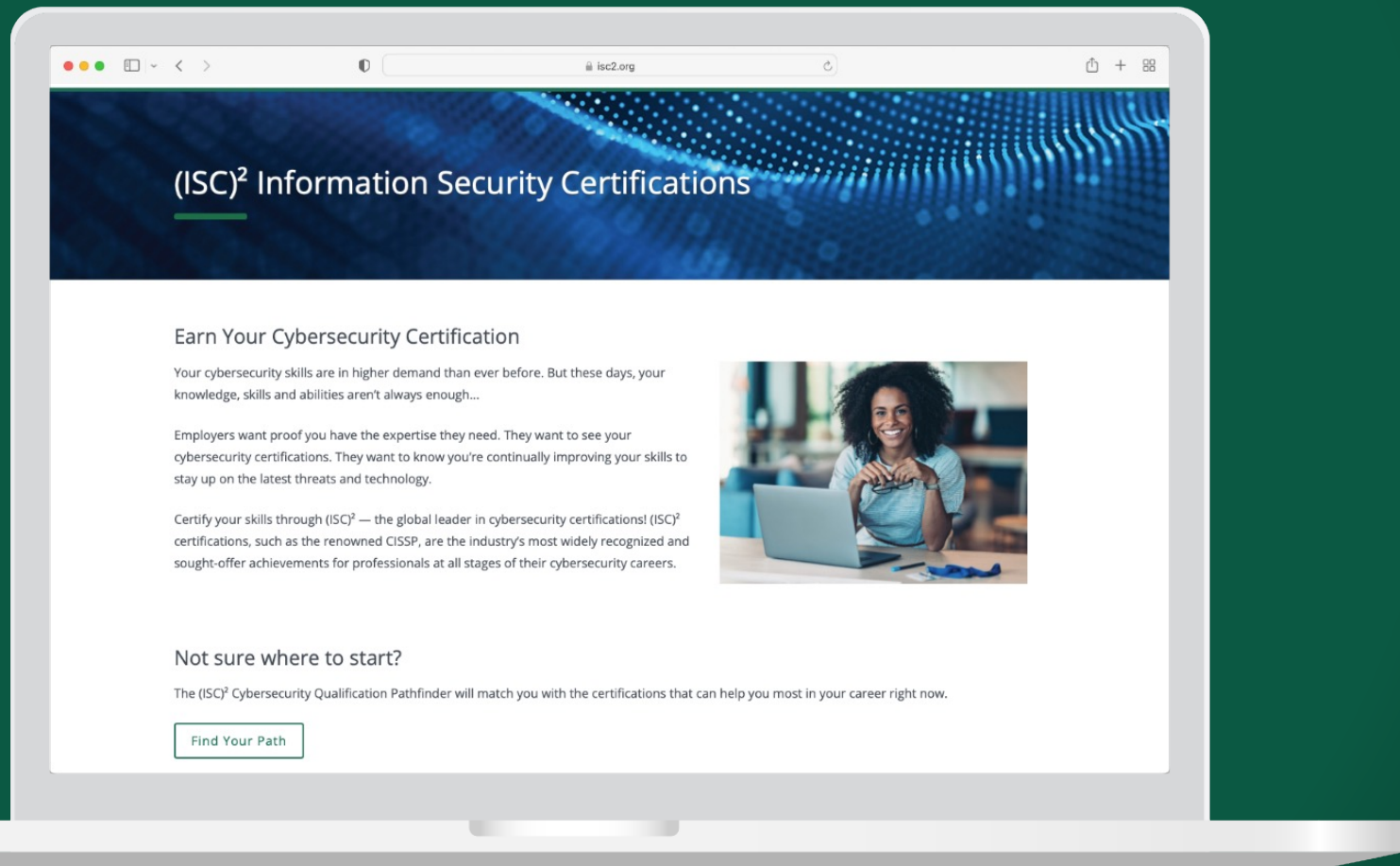
Candidates must have a minimum of two years' cumulative paid work experience in one or more knowledge areas of the HCISPP Common Body of Knowledge (CBK) that includes security, compliance and privacy.

Legal experience may be substituted for compliance and information management experience may be substituted for privacy. Of the two years of experience, one of those years must be in the healthcare industry.

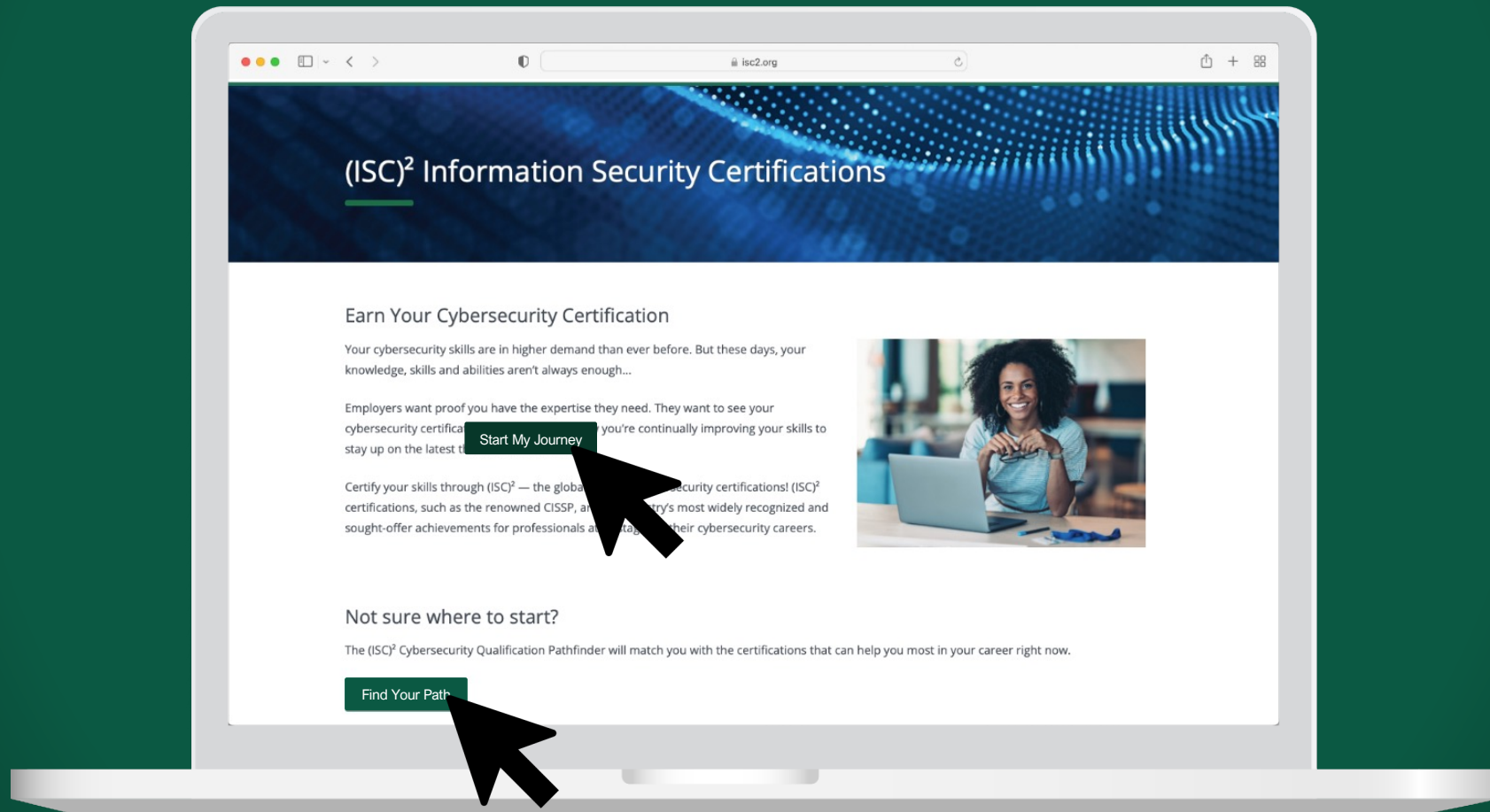


**Earning an (ISC)² certification
opens many doors.**

Learn more about (ISC)² cybersecurity certification at isc2.org/Certifications



Learn more about (ISC)² cybersecurity certification at isc2.org/Certifications



(ISC)²

Thank you!

Questions ?

Jon France

CISO



Appendix

Other Certification Details



Systems Security
Certified Practitioner

An (ISC)² Certification

**Ideal for IT administrators,
managers, directors and network
security professionals**

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.





Systems Security
Certified Practitioner

An (ISC)² Certification

The SSCP is ideal for IT administrators, managers, directors and network security professionals responsible for the hands-on operational security of their organization's critical assets, including people in these positions.

Network Security
Engineer

Security Analyst

Security Consultant/
Specialist

Systems/Network
Analyst

Systems
Administrator

Systems Engineer

Security
Administrator

Database
Administrator



Systems Security
Certified Practitioner

An (ISC)² Certification

The broad spectrum of topics included in the SSCP CBK ensures its relevancy across all disciplines in the field of information security. Successful candidates are competent in the following seven domains:





Systems Security
Certified Practitioner

An (ISC)² Certification

SSCP Experience Requirements

Candidates must have a minimum of one year's cumulative work experience in one or more of the seven domains of the SSCP CBK.

A one-year prerequisite pathway will be granted for candidates who received a degree (bachelors or masters) in a cybersecurity program.²

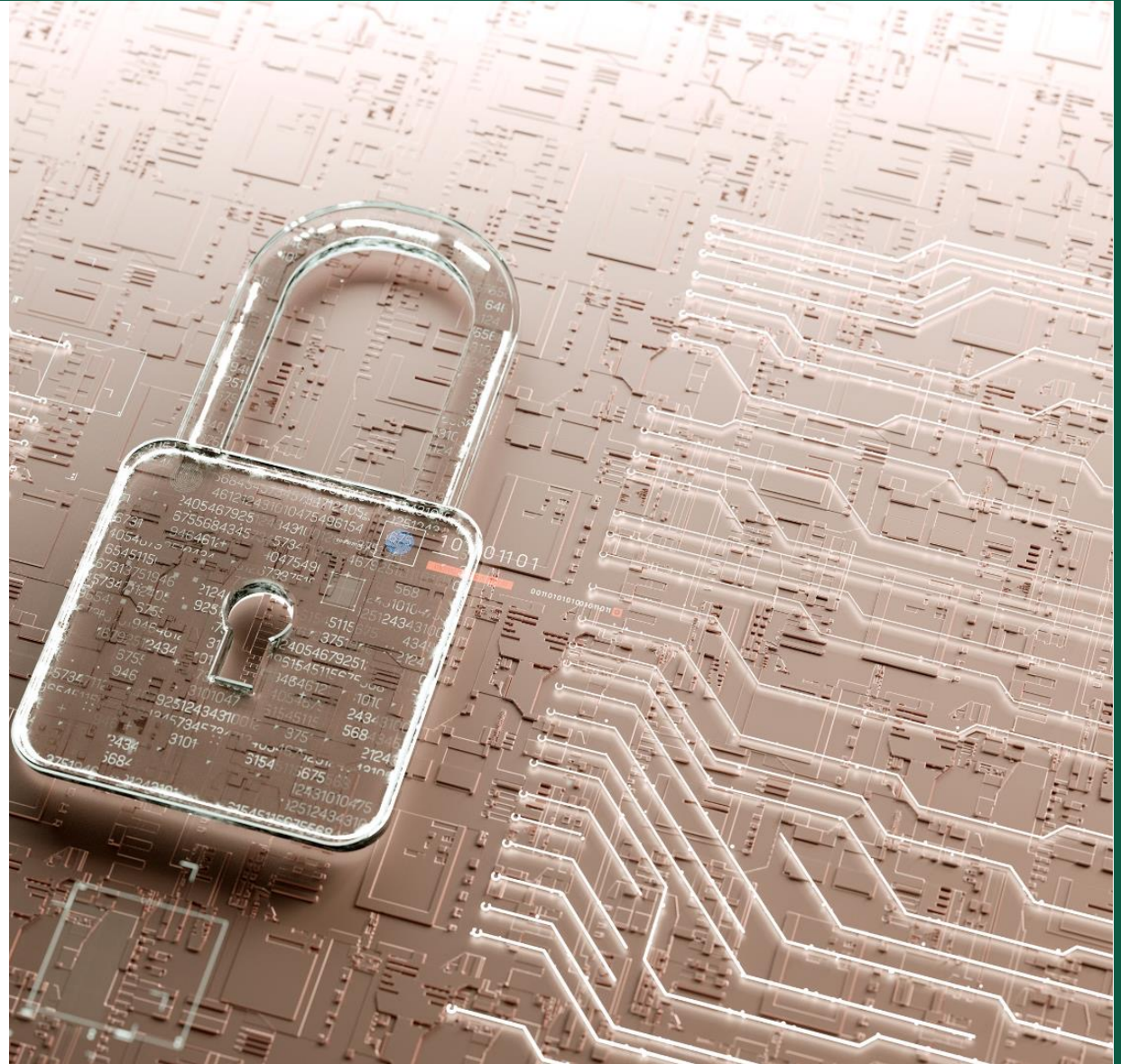


Certified
Authorization Professional

An (ISC)² Certification

Ideal for Security Assessment and Authorizations Staff

The CAP shows employers you have the advanced technical skills and knowledge to understand Governance, Risk and Compliance (GRC) and can authorize and maintain information systems utilizing various risk management frameworks, as well as best practices, policies and procedures.





Certified
Authorization Professional

An (ISC)² Certification

Who Earns the CAP?

The Certified Authorization Professional is an information security practitioner who advocates for security risk management in pursuit of information system authorization to support an organization's mission and operations in accordance with legal and regulatory requirements.

System Security
Officers

Risk Management
Practitioners

Execs Responsible
for Risk

Program
Managers

System Security
Managers

Continuous
Monitoring
Practitioners

Auditors

IT Professionals



Certified
Authorization Professional

An (ISC)² Certification

The broad spectrum of topics included in the CAP CBK ensures its relevancy across all disciplines in the field of information security. Successful candidates are competent in the following seven domains:

Information
Security Risk
Management
Program

Scope of the
Information
System

Selection and
Approval of
Security and
Privacy Controls

Implementation
of Security and
Privacy Controls

Assessment/
Audit of Security
and Privacy
Controls

Authorization/
Approval of
Information
System

Continuous
Monitoring



Certified
Authorization Professional

An (ISC)² Certification

CAP Experience Requirements

Candidates must have a minimum of two years of cumulative work experience in one or more of the seven domains of the CAP CBK.



Certified Secure
Software Lifecycle Professional

An (ISC)² Certification

Ideal for Software Development and Acquisitions Staff

CSSLP certification recognizes leading application security skills. Shows ability to incorporate security practices — authentication, authorization and auditing — into each phase of the software development lifecycle.





Certified Secure
Software Lifecycle Professional

An (ISC)² Certification

The CSSLP is ideal for software development and security professionals responsible for applying best practices to each phase of the SDLC – from software design and implementation to testing and deployment – including those in the following positions:

Software Architect

Software Developer

Software Program Manager

Penetration Tester

Project Manager

IT Director/
Manager

Software Engineer

Application Security Specialist

Quality Assurance Tester

Software Procurement Analyst

Security Manager



Certified Secure
Software Lifecycle Professional

An (ISC)² Certification

The broad spectrum of topics included in the CSSLP CBK ensures its relevancy across all disciplines in the field of information security. Successful candidates are competent in the following eight domains:

Secure Software
Concepts

Secure Software
Requirements

Secure Software
Architecture and
Design

Secure Software
Implementation

Secure Software
Testing

Secure Software
Lifecycle
Management

Secure Software
Deployment,
Operations,
Maintenance

Secure Software
Supply Chain

CSSLP®

Certified Secure
Software Lifecycle Professional

An (ISC)² Certification

CSSLP Experience Requirements

Candidates must have a minimum of four years of cumulative paid Software Development Lifecycle (SDLC) professional work experience in one or more of the eight domains of the CSSLP CBK.

Or three years of cumulative paid SDLC professional work experience in one or more of the eight domains of the CSSLP CBK with a four-year degree leading to a Baccalaureate or regional equivalent in Computer Science, Information Technology (IT) or related fields.