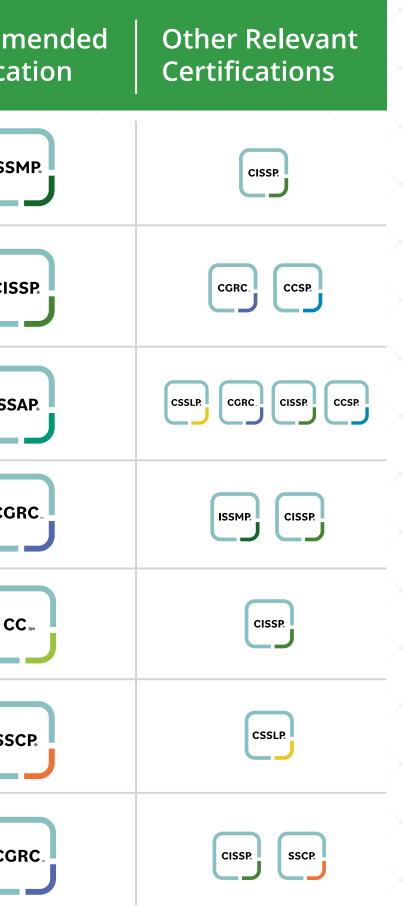
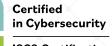
# ISC2 Certification Coverage of ECSF Roles

This table makes recommendations for learners seeking to understand which ISC2 certifications will help them acquire the knowledge and skills required for roles under ENISA's European Cybersecurity Skills Framework (ECSF). The recommendations are based on the coverage of knowledge and skills topics for each role, rather than coverage of tasks, and limited to roles where ISC2 certifications provide a high level of coverage.

ECSF Profil	Recomr Certifica	
	Chief Information Security Officer	ISS
<b>∆°</b> ∆	Cyber Legal Policy and Compliance Officer	CI
(ē)	Cybersecurity Architect	IS
P	Cybersecurity Auditor	cc
	Cybersecurity Educator	C
08	Cybersecurity Implementer	SS
	Cybersecurity Risk Manager	CC





CC sm

ISC2 Certification





ENTRY-LEVEL	SECURITY ADMINISTRATOR	GOVERNANCE, RISK & COMPLIANCE	SOFTWARE SECURITY	CLOUD SECURITY
Designed as a starting point for students, young professionals and career-changers, this entry-level cybersecurity certification demonstrates knowledge in the key foundational concepts in information security and requires no work experience - just a passion for cybersecurity and the desire to dive into an exciting field that protects the world from cyber threats.	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. It demonstrates advanced technical skills and knowledge to implement, monitor and administer IT infrastructure using security best practices, policies and procedures.	The CGRC is ideal for IT, information security and information assurance practitioners who work in Governance, Risk and Compliance (GRC) roles and have a need to understand, apply and implement a risk management program for IT systems within an organization. It demonstrates advanced knowledge and technical skills to formalize processes to assess risk and establish security documentation.	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 demonstrates advanced knowledge and technical skills to effectively design, develop and implement security practices within each phase of the software lifecycle.	The CCSP is ideal for IT and information security leaders seeking to prove their understanding of cybersecurity and securing critical assets in the cloud. It demonstrates advanced technical skills and knowledge to design, manage and secure data, applications and infrastructure in the cloud.
Required experience	Required experience	Required experience	Required experience	Required experience
There are no specific prerequisites to take the exam. No work experience in cybersecurity or formal educational diploma/degree is required.	To qualify for the SSCP, candidates must pass the exam and have at least one year of cumulative, paid work experience in one or more of the seven domains of the ISC2 SSCP Common Body of Knowledge (CBK®).	To qualify for the CGRC, candidates must pass the exam and have at least two years of cumulative, paid work experience in one or more of the seven domains of the ISC2 CGRC Common Body of Knowledge (CBK®).	To qualify for the CSSLP, candidates must pass the exam and have at least four years of cumulative, paid work experience as a software development lifecycle professional in one or more of the eight domains of the ISC2 CSSLP Common Body of Knowledge (CBK <sup>®</sup> ).	To qualify for the CCSP, candidates must pass the exam and have at least five years of 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 ISC2 CCSP Common Body of Knowledge (CBK®).
Typically pursue CC	Jobs that typically use SSCP	Jobs that typically use CGRC	Jobs that typically use CSSLP	Jobs that typically use CCSP
<ul> <li>IT professionals</li> <li>Career-changers</li> <li>College students or recent graduates</li> <li>Board-level executives seeking foundational knowledge in cybersecurity</li> </ul>	<ul> <li>Network Security Engineer</li> <li>IT/Systems/Network Administrator</li> <li>Security Analyst</li> <li>Systems Engineer</li> <li>Security Consultant/Specialist</li> <li>Security Administrator</li> <li>Systems/Network Analyst</li> <li>Database Administrator</li> <li>Individuals operating in a security operations center (SOC) environment performing the role of incident handler, SIEM analyst, forensics specialist, threat intel researcher, etc.</li> </ul>	<ul> <li>Authorizing Official</li> <li>Cyber GRC Manager</li> <li>Cybersecurity Auditor/Assessor</li> <li>Cybersecurity Compliance Officer</li> <li>Cybersecurity Architect</li> <li>GRC Architect</li> <li>GRC Information Technology Manager</li> <li>GRC Manager</li> <li>Cybersecurity Risk &amp; Compliance Project Manager</li> <li>Cybersecurity Risk &amp; Controls Analyst</li> <li>Cybersecurity Third Party Risk Manager</li> <li>Enterprise Risk Manager</li> <li>GRC Director</li> <li>GRC Security Analyst</li> <li>System Security Manager</li> <li>System Security Officer</li> <li>Information Assurance Manager</li> <li>Cybersecurity Consultant</li> </ul>	<ul> <li>Software Architect</li> <li>Software Engineer</li> <li>Software Developer</li> <li>Application Security Specialist/Manager/Architect</li> <li>Software Program Manager</li> <li>Quality Assurance Tester</li> <li>Penetration Tester/Testing Manager</li> <li>Software Procurement Analyst</li> <li>Project Manager</li> <li>Security Manager</li> <li>IT Director/Manager</li> </ul>	<ul> <li>Cloud Architect</li> <li>Chief Information Security Officer (CISO)</li> <li>Chief Information Officer (CIO)</li> <li>Chief Technology Officer</li> <li>Engineer/Developer/Manager</li> <li>DevOps</li> <li>Enterprise Architect</li> <li>IT Contract Negotiator</li> <li>IT Risk and Compliance Manager</li> <li>Security Administrator</li> <li>Security Analyst</li> <li>Security Architect</li> <li>Security Consultant</li> <li>Security Engineer</li> <li>Systems Architect</li> <li>Systems Engineer</li> <li>SecOps</li> </ul>
Domains covered	Domains covered	Domains covered	Domains covered	Domains covered
<ol> <li>Security Principles</li> <li>Business Continuity (BC), Disaster Recovery (DR) &amp; Incident Response Concepts</li> <li>Access Control Concepts</li> <li>Network Security</li> <li>Security Operations</li> </ol>	<ol> <li>Security Operations and Administration</li> <li>Access Controls</li> <li>Risk Identification, Monitoring and Analysis</li> <li>Incident Response and Recovery</li> <li>Cryptography</li> <li>Network and Communications Security</li> <li>Systems and Application Security</li> </ol>	<ol> <li>Information Security Risk Management Program</li> <li>Scope of the Information System</li> <li>Selection and Approval of Security and Privacy Controls</li> <li>Implementation of Security and Privacy Controls</li> <li>Assessment/Audit of Security and Privacy Controls</li> <li>Authorization/Approval of Information System</li> <li>Continuous Monitoring</li> </ol>	<ol> <li>Secure Software Concepts</li> <li>Secure Software Requirements</li> <li>Secure Software Architecture and Design</li> <li>Secure Software Implementation</li> <li>Secure Software Testing</li> <li>Secure Software Lifecycle Management</li> <li>Secure Software Deployment, Operations, Maintenance</li> <li>Secure Software Supply Chain</li> </ol>	<ol> <li>Cloud Concepts, Architecture and Design</li> <li>Cloud Data Security</li> <li>Cloud Platform &amp; Infrastructure Security</li> <li>Cloud Application Security</li> <li>Cloud Security Operations</li> <li>Legal, Risk and Compliance</li> </ol>



**Certified Cloud** Security Professional

ISC2 Certification



**Certified Information** Systems Security Professional **ISC2** Certification



Information Systems Security Management Professional **ISC2** Certification

Information Systems Security Architecture Professional ISSAP. **ISC2** Certification

LEADERSHIP & OPERATIONS	SECURITY MANAGEMENT	SECURITY ARCHITECTURE	SECURITY
The CISSP is ideal for information security leaders seeking to prove their understanding of cybersecurity strategy and hands-on implementation. It demonstrates advanced knowledge and technical skills to design, develop and manage an organization's overall security posture.	The Information Systems Security Management Professional (ISSMP) recognizes cybersecurity leaders with expertise in information systems security management. It demonstrates deep management and leadership skills and the advanced knowledge to establish, present and govern information security programs.	The Information Systems Security Architecture Professional (ISSAP) recognizes cybersecurity leaders with expertise in information systems security architecture. It demonstrates the knowledge and skills to develop, design and analyze security solutions and provide risk-based guidance to meet organizational goals.	The Informati (ISSEP) recogn information sy the knowledg applications,
Required experience	Required experience	Required experience	Required
To qualify for the CISSP, candidates must pass the exam and have at least five years of cumulative, paid work experience in two or more of the eight domains of the ISC2 CISSP Common Body of Knowledge (CBK®).	There are two ways to earn the ISSMP. Path 1: CISSPs in good standing must have a minimum of two years of cumulative full- time experience in one or more of the six domains in the current ISSMP exam outline. Path 2: All other candidates must have a minimum of seven years of cumulative full-time experience in two or more of the six domains in the current ISSMP exam outline.	There are two ways to earn the ISSAP. Path 1: CISSPs in good standing must have a minimum of two years of cumulative full-time experience in one or more of the six domains in the current ISSAP exam outline. Path 2: All other candidates must have a minimum of seven years of cumulative full-time experience in two or more of the six domains in the current ISSAP exam outline.	There are two standing mus time experien ISSEP exam o minimum of s or more of the
Jobs that typically use CISSP	Jobs that typically use ISSMP	Jobs that typically use ISSAP	Jobs that
<ul> <li>Chief Information Officer</li> <li>Chief Information Security Officer</li> <li>Chief Technology Officer</li> <li>Compliance Manager/Officer</li> <li>Director of Security</li> <li>Information Architect</li> <li>Information Manager/Information Risk Manager or Consultant</li> <li>IT Specialist/Director/Manager</li> <li>Network/System Administrator</li> <li>Security Administrator</li> <li>Security Architect/Security Analyst</li> <li>Security Manager</li> <li>Security Manager</li> <li>Security Systems Engineer/Security Engineer</li> </ul>	<ul> <li>Chief Information Officer</li> <li>Chief Information Security Officer</li> <li>Chief Technology Officer</li> <li>Senior Security Executive</li> </ul>	<ul> <li>System Architect</li> <li>Chief Information Security Officer (CISO)</li> <li>Chief Information Officer (CIO)</li> <li>Chief Technology Officer (CTO)</li> <li>System and Network Designer</li> <li>Business Analyst</li> <li>Chief Security Officer</li> </ul>	<ul> <li>Senior</li> <li>Securi</li> <li>Securi</li> <li>Senior</li> </ul>
Domains covered	Domains covered	Domains covered	Domains of
<ol> <li>Security and Risk Management</li> <li>Asset Security</li> <li>Security Architecture and Engineering</li> <li>Communication and Network Security</li> <li>Identity and Access Management (IAM)</li> <li>Security Assessment and Testing</li> <li>Security Operations</li> <li>Software Development Security</li> </ol>	<ol> <li>Leadership and Business Management</li> <li>Systems Lifecycle Management</li> <li>Risk Management</li> <li>Threat Intelligence and Incident Management</li> <li>Contingency Management</li> <li>Law, Ethics and Security Compliance Management</li> </ol>	<ol> <li>Architect for Governance, Compliance and Risk Management</li> <li>Security Architecture Modeling</li> <li>Infrastructure Security Architecture</li> <li>Identity and Access Management (IAM) Architecture</li> <li>Architect for Application Security</li> <li>Security Operations Architecture</li> </ol>	<ol> <li>Systems Se</li> <li>Risk Manag</li> <li>Security Pl.</li> <li>Systems In</li> <li>Secure Op and Disposition</li> </ol>

## ISSEP.

Information Systems Security Engineering Professional

**ISC2** Certification

### TY ENGINEERING

ation Systems Security Engineering Professional ognizes cybersecurity leaders with expertise in n systems security engineering. It demonstrates dge and skills to incorporate security into projects, ns, business processes and information systems.

#### d experience

wo ways to earn the ISSEP. Path 1: CISSPs in good ust have a minimum of two years of cumulative fullience in one or more of the five domains in the current outline. Path 2: All other candidates must have a f seven years of cumulative full-time experience in two the five domains in the current ISSEP exam outline.

#### at typically use ISSEP

ior Systems Engineer urity Systems Engineer urity Officer ior Security Analyst

#### s covered

Security Engineering Foundations

nagement

Planning and Design

Implementation, Verification and Validation

Operations, Change Management

oosal

Get Official Training from ISC2 at isc2.org/enterprise