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 Profile Title	Recommended Certification	Other Relevant Certifications
Chief Information Security Officer	ISSMP	CISSP
Cyber Legal Policy and Compliance Officer	CISSP	CGRC CCSP
Cybersecurity Architect	ISSAP	CSSLP CGRC CISSP CCSP
Cybersecurity Auditor	CGRC	ISSMP CISSP
Cybersecurity Educator	CC	CISSP
Cybersecurity Implementer	SSCP	CSSLP
Cybersecurity Risk Manager	CGRC	CISSP SSCP

CC Certified in Cybersecurity ISC2 Certification	SSCP Systems Security Certified Practitioner ISC2 Certification	CGRC Certified in Governance, Risk and Compliance ISC2 Certification	CSSLP Certified Secure Software Lifecycle Professional ISC2 Certification	CCSP Certified Cloud Security Professional 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®).	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**
• IT professionals • Career-changers • College students or recent graduates • Board-level executives seeking foundational knowledge in cybersecurity	• Network Security Engineer • IT/Systems/Network Administrator • Security Analyst • Systems Engineer • Security Consultant/Specialist • Security Administrator • Systems/Network Analyst • Database Administrator • Individuals operating in a security operations center (SOC) environment performing the role of incident handler, SIEM analyst, forensics specialist, threat intel researcher, etc.	• Authorizing Official • Cyber GRC Manager • Cybersecurity Auditor/Assessor • Cybersecurity Compliance Officer • Cybersecurity Architect • GRC Architect • GRC Information Technology Manager • GRC Manager • Cybersecurity Risk & Compliance Project Manager • Cybersecurity Risk & Controls Analyst • Cybersecurity Third Party Risk Manager • Enterprise Risk Manager • GRC Analyst • GRC Director • GRC Security Analyst • System Security Manager • System Security Officer • Information Assurance Manager • Cybersecurity Consultant	• Software Architect • Software Engineer • Software Developer • Application Security Specialist/Manager/Architect • Software Program Manager • Quality Assurance Tester • Penetration Tester/Testing Manager • Software Procurement Analyst • Project Manager • Security Manager • IT Director/Manager	• Cloud Architect • Chief Information Security Officer (CISO) • Chief Information Officer (CIO) • Chief Technology Officer • Engineer/Developer/Manager • DevOps • Enterprise Architect • IT Contract Negotiator • IT Risk and Compliance Manager • Security Administrator • Security Analyst • Security Architect • Security Consultant • Security Engineer • Security Manager • Systems Architect • Systems Engineer • SecOps
Domains covered	**Domains covered**	**Domains covered**	**Domains covered**	**Domains covered**
1. Security Principles 2. Business Continuity (BC), Disaster Recovery (DR) & Incident Response Concepts 3. Access Control Concepts 4. Network Security 5. Security Operations	1. Security Operations and Administration 2. Access Controls 3. Risk Identification, Monitoring and Analysis 4. Incident Response and Recovery 5. Cryptography 6. Network and Communications Security 7. Systems and Application Security	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	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	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 and Compliance

CISSP Certified Information Systems Security Professional ISC2 Certification	ISSMP Information Systems Security Management Professional ISC2 Certification	ISSAP Information Systems Security Architecture Professional ISC2 Certification	ISSEP Information Systems Security Engineering Professional ISC2 Certification
LEADERSHIP & OPERATIONS	**SECURITY MANAGEMENT**	**SECURITY ARCHITECTURE**	**SECURITY ENGINEERING**
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 Information Systems Security Engineering Professional (ISSEP) recognizes cybersecurity leaders with expertise in information systems security engineering. It demonstrates the knowledge and skills to incorporate security into projects, applications, business processes and information systems.
Required experience	**Required experience**	**Required experience**	**Required experience**
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 ways to earn the ISSEP. Path 1: CISSPs in good standing must have a minimum of two years of cumulative full-time experience in one or more of the five domains in the current ISSEP 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 five domains in the current ISSEP exam outline.
Jobs that typically use CISSP	**Jobs that typically use ISSMP**	**Jobs that typically use ISSAP**	**Jobs that typically use ISSEP**
• Chief Information Officer • Chief Information Security Officer • Chief Technology Officer • Compliance Manager/Officer • Director of Security • Information Architect • Information Manager/Information Risk Manager or Consultant • IT Specialist/Director/Manager • Network/System Administrator • Security Administrator • Security Architect/Security Analyst • Security Consultant • Security Manager • Security Systems Engineer/Security Engineer	• Chief Information Officer • Chief Information Security Officer • Chief Technology Officer • Senior Security Executive	• System Architect • Chief Information Security Officer (CISO) • Chief Information Officer (CIO) • Chief Technology Officer (CTO) • System and Network Designer • Business Analyst • Chief Security Officer	• Senior Systems Engineer • Security Systems Engineer • Security Officer • Senior Security Analyst
Domains covered	**Domains covered**	**Domains covered**	**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	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	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	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

Get Official Training from ISC2 at isc2.org/enterprise