ISC2 Certification Mappings to the SFIA 9 Framework

25 March 2025 | Document One

Table of Contents

Preface	3
1. Introduction	5
2. Primary SFIA Skills	6
CISSP	7
CSSLP	14
CCSP	20
CGRC	27
SSCP	33
CC	39
3. Secondary SFIA Skills	43
4. Ancillary SFIA Skills	44

Preface

ISC2™ 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, ISC2 offers a portfolio of credentials that are part of a holistic, pragmatic approach to security. Our association of candidates, associates and members, more than 450,000 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™.

The **CISSP** recognizes information security leaders who understand cybersecurity strategy and hands-on implementation. It provides evidence that professionals have the knowledge, skills, abilities and experience to design, develop and manage an organisation's overall security posture. Jobs that typically use or require a **CISSP** include Chief Information Officer, Chief Information Security Officer, Director of Security, IT Director/Manager, Network Architect, Security Architect, Security Consultant and Security Manager.

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 advanced knowledge and the technical skills to effectively design, develop and implement security practices within each phase of the software lifecycle. Jobs that typically use or require the **CSSLP** include Software Program Manager, IT Director/Manager, Security Manager, Software Architect, Application Security Specialist, Software Engineer, Project Manager and Quality Assurance Tester.

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 shows advanced technical skills and knowledge to design, manage and secure data, applications and infrastructure in the cloud. Jobs that typically use or require the **CCSP** include Security Architect, Security Manager, Systems Architect, Systems Engineer, Security Consultant, Security Engineer and Security Administrator.

The **CGRC** recognizes an information security practitioner who advocates for security risk management to support an organization's mission and operations in accordance with legal and regulatory requirements. Jobs that typically use or require the **CGRC** include Cybersecurity Auditor, Cybersecurity Compliance Officer, GRC Architect, GRC Manager, Cybersecurity Risk & Compliance Project Manager, Cybersecurity Risk & Controls Analyst and Cybersecurity Third Party Risk Manager.

The **SSCP** is ideal for IT administrators, managers, directors and network security professionals responsible for the hands-on operational security of their organisation's critical assets. It shows you have the advanced technical skills and knowledge to implement, monitor and administer IT infrastructure using security best practices, policies and procedures. Jobs that typically use or require the **SSCP** include Database Administrator, Network Security Engineer, Security Administrator, Security Analyst, Security Consultant/Specialist, Systems Administrator, Systems Engineer and Systems/Network Analyst.

The **CC** certification creates a clear pathway to an exciting and rewarding career in cybersecurity. It breaks down traditional barriers to entry, enabling confidence to be built for entry into a first cybersecurity role. **CC** candidates include IT professionals, career-changers, college students or recent graduates and executives seeking foundational knowledge in cybersecurity.

All ISC2 certification schemes are third-party accredited by ANSI National Accreditation Board under ISO/IEC 17024:2003. ISO/IEC 17024:2003 specifies requirements for a body certifying person against specific requirements, including the development and maintenance of a certification scheme for personnel.

This document will assist information security practitioners to understand the ISC2 certification mappings to the SFIA Framework.

Introduction

CISSP, CSSLP, CGRC, CCSP and SSCP

The SFIA Framework defines the skills and competencies required by professionals who design, develop, implement, manage and protect the data and technology that power the digital world. SFIA gives individuals and organisations a common language to define skills and expertise in a consistent way. The use of clear language, avoidance of technical jargon and acronyms, makes SFIA accessible to all involved in the work as well as people in supporting roles such as human resources, learning and development, organisation design, and procurement. It can solve the common translation issues that hinder communication and effective partnerships within organisations and multi-disciplinary teams.

The CISSP, CSSLP and CGRC certifications cover the security aspects of SFIA skills at levels 5-6. The CCSP certification covers the security aspects of SFIA skills at level 5, and the SSCP certification covers SFIA skills at levels 3-4. The certification exam assesses knowledge of these skill attributes and tests against the application of these knowledge areas through scenario-based items which require judgement to be answered successfully and can only, realistically, be achieved with the experience of practicing the skill.

Following the awarding of this group of ISC2 certifications, a practitioner could reasonably be expected to have demonstrated the knowledge necessary for the SFIA skills related to the areas examined. ISC2 certification schemes require specific prerequisites, (e.g. work experience) prior to a candidate becoming certified. The table in Section 2 indicates the SFIA skills relevant to the knowledge and skills assessed in each of these ISC2 certifications. Once assessed for practice of a SFIA skill, including the SFIA Generic Attributes for the level, in a real working environment a practitioner would then be validated as competent.

The general process for an ISC2 certification requires:

Exam	Successfully complete an ISC2 exam.
Experience	Meet the number of years of cumulative work experience in the required ISC2 Exam Outline domains.
Code of Ethics	Agree to the ISC2 Code of Ethics
Attestation	Have an endorser attest to the years of experience and good standing within the cybersecurity industry

For those information security specialists who are awarded an ISC2 certification there will be a subset of the listed SFIA skills used consistently within their role, depending on individual responsibilities, role descriptions and organisational requirements. For example, a Chief Information Security Officer will have a different set of skills used on a regular basis compared to a Security Architect based on their respective role requirements.

CC

There are no specific work experience prerequisites to becoming CC certified, although it is recommended that candidates have basic information technology (IT) knowledge. Becoming CC certified will demonstrate a foundational level of knowledge in the mapped SFIA skills and may show a degree of skill and capability if previous IT work experience has been undertaken.

2. ISC2 Certifications mapped to SFIA Skills

The table below presents a primary view showing where the knowledge gained from ISC2 certifications map directly to SFIA skills at the levels of responsibility. Additionally, in section 3, a similar table presents a secondary view showing where the knowledge gained from ISC2 certifications partially map to SFIA skills at levels of responsibility below those shown in this table (the primary view).

			CISSP	CSSLP	CCSP	CGRC	SSCP	CC
Cyber security strategy and leadership	Information security	SCTY	6	5	5	6	4	2
	Stakeholder relationship management	RLMT				5		
Cyber security architecture	Requirements definition and management	REQM		5				
	Solution architecture	ARCH		5	5			
	Data management	DATM	5		5		4	2
Cybersecurity governance, risk and compliance	Governance	GOVN	6			6		
	Risk management	BURM	5	5	5	5	3	2
	Audit	AUDT	5	5	5	5	4	
	Information and data compliance	PEDP	5	5	5	5		
	Information management	IRMG		5		5	4	
	Quality assurance	QUAS				5		
	Information assurance	INAS	5		5	5	4	2
Secure software and systems development	Systems and software lifecycle engineering	SLEN	5	6				
	Non-functional testing	NFTS	5	6			3	
Secure supply chain	Supplier management	SUPP		5	5			
	Contract management	ITCM			5			
Secure infrastructure management	Infrastructure operations	ITOP			5		4	
	Network support	NTAS	5				4	1
	Systems installation and removal	HSIN				5		
	Deployment	DEPL		5				
	Storage management	STMG	5		5		4	
	System software administration	SYSP	5	5	5			2
	Service level management	SLMO		5	5	5		2
Cybersecurity resilience	Security operations	SCAD	5		5	5	4	1
	Identity and access management	IAMT	5		5		4	1
	Continuity management	COPL	5		5		4	2
	Incident management	USUP	5	5	5		4	1
	Change control	CHMG				5		
	Asset management	ASMG	5			5	4	
	Vulnerability assessment	VUAS	5	5	5	5	4	
	Digital forensics	DGFS					4	

CISSP

Certified Information Systems Security Professional
ISC2 Certification

Following the awarding of a CISSP certification, a practitioner could reasonably be expected to have demonstrated the knowledge and skills necessary for the SFIA skills listed below, together with the level of responsibility for the SFIA Generic Attributes including behavioral and business skills. The CISSP certification will contribute to the provision of evidence that the practitioner has applied the relevant knowledge and skills and has significant professional experience performing the activities described by SFIA in a professional working environment through the performance of a role, job or function. This table indicates the SFIA skills relevant to the knowledge and skills assessed during the certification process.

Strategy and Architecture

Strategy and Privacy

Information Security SCTY	Level 6
Defining and operating a framework of security controls and security management strategies.	• Develops and communicates corporate information security policy, standards and guidelines. • Ensures architectural principles are applied during design to reduce risk. Drives adoption and adherence to policy, standards and guidelines. • Contributes to the development of organisational strategies that address information control requirements. Identifies and monitors environmental and market trends and proactively assesses impact on business strategies, benefits and risks. • Leads the provision of authoritative advice and guidance on the requirements for security controls in collaboration with subject matter experts.

Information Assurance INAS	Level 5
Protecting against and managing risks related to the use, storage and transmission of data and information systems.	• Interprets information assurance and security policies and applies these to manage risks • Provides advice and guidance to ensure adoption of and adherence to information assurance architectures, strategies, policies, standards and guidelines • Plans, organises and conducts information assurance and accreditation of complex domain areas, cross-functional areas, and across the supply chain • Contributes to the development of policies, standards and guidelines

Information and Data Compliance PEDP	Level 5
Implementing and promoting compliance with information and data management legislation.	• Contributes to policies, standards and guidelines for information and data compliance. • Provides authoritative advice on implementing compliance controls in products, services and systems. • Investigates breaches and recommends control improvements. Maintains an inventory of legislated data, conducts risk assessments and specifies necessary changes. • Ensures formal requests and complaints are handled following procedures. Prepares and submits reports to relevant authorities, ensuring all compliance requirements are met.

Governance, Risk and Compliance

Governance GOVN	Level 6
Defining and operating frameworks for decision-making, risk management, stakeholder relationships and compliance with organisational and regulatory obligations.	• Implements the governance framework to enable governance activity to be conducted • Within a defined area of accountability, determines the requirements for appropriate governance reflecting the organisation's values, ethics, risk appetite and wider governance frameworks. Communicates delegated authority, benefits, opportunities, costs, and risks • Leads reviews of governance practices with appropriate and sufficient independence from management activity • Acts as the organisation's contact for relevant regulatory authorities and ensures proper relationships between the organisation and external stakeholders

Risk Management BURM	Level 5
Planning and implementing processes for managing risk across the enterprise, aligned with organisational strategy and governance frameworks.	• Plans and implements complex and substantial risk management activities within a specific function, technical area, project or programme. • Establishes consistent risk management processes and reporting mechanisms aligned with governance frameworks. • Engages specialists and domain experts as necessary. • Advises on the organisation's approach to risk management.

Audit AUDT	Level 5
Delivering independent, risk-based assessments of the effectiveness of processes, the controls, and the compliance environment of an organisation.	• Plans, organises and conducts audits of complex domains areas, cross-functional areas, and across the supply chain • Confirms the scope and objectives of specific audit activities with management. Aligns with the scope of the audit programme and organisational policies • Determines appropriate methods of investigation to achieve the audit objectives. Presents audit findings to management describing the effectiveness and efficiency of control mechanisms • Provides general and specific audit advice. Collaborates with professionals in related specialisms to develop and integrate findings

Development and Implementation

Systems Development

Systems and Software Lifecycle Engineering SLEN	Level 5
Establishing and deploying an environment for developing, continually improving and securely operating software and systems products and services.	• Collaborates with those responsible for ongoing systems and software life cycle management to select, adopt and adapt working practices • Supports deployment of the working environment for systems and software life cycle working practices • Provides effective feedback to encourage development of the individuals and teams responsible for systems and software life cycle working practices Provides guidance and makes suggestions to support continual improvement and learning approaches • Contributes to identifying new domains within the organisation where systems and software life cycle working practices can be deployed

Non-functional Testing NFTS	Level 5
Assessing systems and services to evaluate performance, security, scalability and other non-functional qualities against requirements or expected standards.	• Plans and drives non-functional testing across all stages, ensuring alignment with requirements and prioritising risk-based strategies. • Provides expert advice on non-functional methods, tools and frameworks. Leads the setup and maintenance of advanced test environments. • Monitors the application of testing standards, ensuring they reflect real-world conditions. Troubleshoots and resolves complex issues, working closely with stakeholders. • Leads efforts to improve the efficiency and reliability of non-functional testing. Identifies improvements and contributes to organisational policies, standards and guidelines for non-functional testing.

Data and Analytics

Data Management DATM	Level 5
Developing and implementing plans, policies and practices that control, protect and optimise the value and governance of data assets.	• Devises and implements data governance and master data management processes. • Derives data management structures and metadata to support consistent data retrieval, integration, analysis, pattern recognition and interpretation across the organisation. • Independently validates external information from multiple sources. Plans effective data storage, sharing and publishing practices within the organisation. • Identifies and addresses issues preventing optimal use of information assets. Provides expert advice to maximise data asset value, ensuring data quality and compliance.

Delivery and Operation

Technology Management

System Software Administration SYSP	Level 5
Installing, managing and maintaining operating systems, data management, office automation and utility software across various infrastructure environments.	• Ensures system software is provisioned and configured to support the achievement of service objectives. • Develops and maintains diagnostic tools and processes for troubleshooting and performance analysis. • Evaluates new system software and recommends adoption if appropriate. Plans the provisioning and testing of new versions of system software. • Ensures operational procedures and diagnostics for system software are current, accessible and well understood. Investigates and coordinates the resolution of potential and actual service problems.

Network Support NTAS	Level 5
Providing maintenance and support services for communications networks.	• Leads network operations to optimise performance. • Oversees planning, installation, maintenance, and acceptance of network components and services, aligning with service expectations, standards, and security requirements. • Ensures network support requests are handled according to set standards and procedures. • Drives the adoption of tools and processes for effective operational management and delivery, ensuring security considerations are addressed. Maintains procedures and documentation. Investigates and resolves complex network problems. Tracks operational issues and reports to stakeholders.
Storage Management STMG	**Level 5**
Provisioning, configuring and optimising on-premises and cloud-based storage solutions, ensuring data availability, security and alignment with business objectives.	• Develops standards and guidelines for implementing data protection and disaster recovery functionality for all business applications and business data. • Provides authoritative advice and guidance to implement and improve storage management. • Manages storage and backup systems to provide agreed service levels. • Creates, improves and supports storage management services with optimal utilisation of storage resources, ensuring security, availability and integrity of data.
Service Management	
Continuity Management COPL	**Level 5**
Developing, implementing and testing a business continuity framework.	• Manages the development, implementation and testing of continuity management plans. • Manages the relationship with individuals and teams who have authority for critical business processes and supporting systems. • Evaluates the critical risks and identifies priority areas for improvement. • Tests continuity management plans and procedures to ensure they address exposure to risk and that agreed levels of continuity can be maintained.

Incident Management USUP	Level 5
Coordinating responses to a diverse range of incidents to minimise negative impacts and quickly restore services.	• Responsible for the operation of the incident management process. • Manages incident communications, ensuring al parties are aware of incidents and their role in the process. • Leads the review of major incidents and informs service owners of outcomes. Ensures incident resolution within service targets. Analyses metrics and reports on the performance of the incident management process. • Develops, maintains and tests incident management policy and procedures. Ensures compliance with regulatory requirements.
Asset Management ASMG	**Level 5**
Managing the full life cycle of assets from acquisition, operation, maintenance to disposal.	• Manages and maintains the service compliance of IT and service assets in line with business and regulatory requirements • Identifies, assesses and communicates associated risks • Ensures asset controllers, infrastructure teams and the business co-ordinate and optimise value, maintain control and maintain appropriate legal compliance
Security Services	
Security Operations SCAD	**Level 5**
Manages and administers security measures, using tools and intelligence to protect assets, ensuring compliance and operational integrity.	• Oversees security operations procedures, ensuring adherence and effectiveness, including cloud security practices and automated threat responses. • Reviews actual or potential security breaches and vulnerabilities and ensures they are promptly and thoroughly investigated. Recommends actions and appropriate control improvements. • Ensures the integrity and completeness of security records, ensuring timely support and adherence to established procedures. • Contributes to the creation and maintenance of security policies, standards and procedures integrating new compliance requirements and technology advances.

Identity and Access Management IAMT	Level 5
Identifying and classifying security vulnerabilities in networks, systems and applications and mitigating or eliminating their impact.	• Plans and manages vulnerability assessment activities within the organisation • Evaluates and selects, reviews vulnerability assessment tools and techniques • Provides expert advice and guidance to support the adoption of agreed approaches • Obtains and acts on vulnerability information and conducts security risk assessments, business impact analysis and accreditation on complex information systems
Vulnerability Assessment VUAS	**Level 5**
Identifying and classifying security vulnerabilities in networks, systems and applications and mitigating or eliminating their impact.	• Plans and manages vulnerability assessment activities within the organisation • Evaluates and selects, reviews vulnerability assessment tools and techniques • Provides expert advice and guidance to support the adoption of agreed approaches • Obtains and acts on vulnerability information and conducts security risk assessments, business impact analysis and accreditation on complex information systems

CSSLP

Certified Secure Software Lifecycle Professional
ISC2 Certification

Following the awarding of a CSSLP certification, a practitioner could reasonably be expected to have demonstrated the knowledge and skills necessary for the SFIA skills listed below, together with the level of responsibility for the SFIA Generic Attributes including behavioral and business skills. The CSSLP certification will contribute to the provision of evidence that the practitioner has applied the relevant knowledge and skills and has significant professional experience performing the activities described by SFIA in a professional working environment through the performance of a role, job or function. This table indicates the SFIA skills relevant to the knowledge and skills assessed during the certification process.

Strategy and Architecture	
Strategy and Planning	
Information Management IRMG	**Level 5**
Enabling the effective management and use of information assets.	• Ensures implementation of information and records management policies and standard practice. Communicates the benefits and value of information management. • Plans effective information storage, sharing and publishing within the organisation. Develops organisational taxonomy for information assets. • Provides expert advice and guidance to enable the organisation to get maximum value from its information assets. • Assesses issues that might prevent the organisation from making maximum use of its information assets. Contributes to the development of policy, standards and procedures for compliance with relevant legislation.
Solution architecture ARCH	**Level 5**
Developing and communicating a multi-dimensional solution architecture to deliver agreed business outcomes.	• Leads the development of solution architectures in specific business, infrastructure or functional areas. • Leads the preparation of technical plans and ensures appropriate technical resources are made available. Ensures appropriate tools and methods are available, understood and employed in architecture development. • Provides technical guidance and governance on solution development and integration. Evaluates requests for changes and deviations from specifications and recommends actions. • Ensures relevant technical strategies, policies, standards and practices (including security and cost management) are applied correctly.

Security and Privacy

Information Security SCTY	Level 5
Defining and operating a framework of security controls and security management strategies.	• Provides advice and guidance on security strategies to manage identified risks and ensure adoption and adherence to standards. • Contributes to development of information security policy, standards and guidelines. • Obtains and acts on vulnerability information and conducts security risk assessments, business impact analysis and accreditation on complex information systems. Investigates major breaches of security and recommends appropriate control improvements. • Develops new architectures that manage the risks posed by new technologies and business practices.

Information and Data Compliance PEDP	Level 5
Implementing and promoting compliance with information and data management legislation.	• Contributes to policies, standards and guidelines for information and data compliance. • Provides authoritative advice on implementing compliance controls in products, services and systems. • Investigates breaches and recommends control improvements. Maintains an inventory of legislated data, conducts risk assessments and specifies necessary changes. • Ensures formal requests and complaints are handled following procedures. Prepares and submits reports to relevant authorities, ensuring all compliance requirements are met.

Governance, Risk and Compliance

Risk Management BURM	Level 5
Planning and implementing processes for managing risk across the enterprise, aligned with organisational strategy and governance frameworks.	• Plans and implements complex and substantial risk management activities within a specific function, technical area, project or programme. • Establishes consistent risk management processes and reporting mechanisms aligned with governance frameworks. • Engages specialists and domain experts as necessary. • Advises on the organisation's approach to risk management.

Audit AUDT	Level 5
Delivering independent, risk-based assessments of the effectiveness of processes, the controls, and the compliance environment of an organisation.	• Plans, organises and conducts audits of complex domain areas, cross-functional areas, and across the supply chain • Confirms the scope and objectives of specific audit activities with management. Aligns with the scope of the audit program and organisational policies • Determines appropriate methods of investigation to achieve the audit objectives. Presents audit findings to management describing the effectiveness and efficiency of control mechanisms • Provides general and specific audit advice. Collaborates with professionals in related specialisms to develop and integrate findings

Change and Transformation

Change Analysis

Requirements Definition and Management REQM	Level 5
Managing requirements through the entire delivery and operational life cycle.	• Plans and drives scoping, requirements definition and prioritisation activities for large, complex initiatives. • Selects, adopts and adapts appropriate requirements definition and management methods, tools and techniques. Contributes to the development of organisational methods and standards for requirements management. • Obtains input and agreement to requirements from a diverse range of stakeholders. Negotiates with stakeholders to manage competing priorities and conflicts. • Establishes requirements baselines or backlogs. Ensures changes to requirements are investigated and managed.

Development and Implementation

Systems Development

Systems and Software Lifecycle Engineering SLEN	Level 6
Establishing and deploying an environment for developing, continually improving, and securely operating software and systems products and services.	• Obtains organisational commitment to strategies to deliver systems and software life cycle working practices to achieve business objectives • Works with others to integrate organisational policies, standards and techniques across the full software and systems life cycle • Develops and deploys the working environment supporting systems and software life cycle practices for strategic, large and complex products and services • Leads activities to manage risks associated with systems and software life cycle working practices. Plans and manages the evaluation or assessment of systems and software life cycle working practices

Non-functional Testing NFTS	Level 6
Assessing systems and services to evaluate performance, security, scalability and other non-functional qualities against requirements or expected standards.	• Develops organisational policies, standards and guidelines for process testing, ensuring they align with business strategy and incorporate a risk-based approach. • Plans and leads strategic, complex testing activities, ensuring they align with overall system quality goals. Manages risks and opportunities, coordinating with other types of testing. • Develops organisational capabilities to address complex quality validation challenges. Drives continuous automation and improvements in test environments. • Promotes a culture of quality in non-functional testing, driving adherence to organisational standards and proactive risk mitigation.

Delivery and Operation

Technology Management

System Software Administration SYSP	Level 5
Installing, managing and maintaining operating systems, data management, office automation and utility software across various infrastructure environments.	• Ensures system software is provisioned and configured to support the achievement of service objectives. • Develops and maintains diagnostic tools and processes for troubleshooting and performance analysis. • Evaluates new system software and recommends adoption if appropriate. Plans the provisioning and testing of new versions of system software. • Ensures operational procedures and diagnostics for system software are current, accessible and well understood. Investigates and coordinates the resolution of potential and actual service problems.

Deployment DEPL	Level 5
Transitioning software from development to live usage, managing risks and ensuring it works as intended.	• Designs and implements deployment approaches, processes and automation tools for the organization. • Oversees the deployment of critical and large-scale software. Ensures deployment processes align with organizational standards and recommended practices. Continuously improves deployment processes and automation capabilities. • Defines monitoring and alert strategies for deployed applications.

Service management

Service Level Management SLMO	Level 5
Agreeing targets for service levels and assessing, monitoring, and managing the delivery of services against the targets.	• Ensures that service delivery meets agreed service levels • Negotiates service level requirements and agreed service levels with customers • Diagnoses service delivery problems and initiates actions to maintain or improve levels of service • Establishes and maintains operational methods, procedures and facilities and reviews them regularly for effectiveness and efficiency

Incident Management USUP	Level 5
Coordinating responses to a diverse range of incidents to minimise negative impacts and quickly restore services.	• Responsible for the operation of the incident management process. • Manages incident communications, ensuring all parties are aware of incidents and their role in the process. • Leads the review of major incidents and informs service owners of outcomes. • Ensures incident resolution within service targets. Analyses metrics and reports on the performance of the incident management process. • Develops, maintains and tests incident management policy and procedures. Ensures compliance with regulatory requirements.

Security Services

Vulnerability Assessment VUAS	Level 5
Identifying and classifying security vulnerabilities in networks, systems and applications and mitigating or eliminating their impact.	• Plans and manages vulnerability assessment activities within the organisation • Evaluates and selects, reviews vulnerability assessment tools and techniques • Provides expert advice and guidance to support the adoption of agreed approaches • Obtains and acts on vulnerability information and conducts security risk assessments, business impact analysis and accreditation on complex information systems

Relationship and Engagement

Stakeholder Management

Supplier Management SUPP	Level 5
Aligning the organisation's supplier performance objectives and activities with sourcing strategies and plans, balancing costs, efficiencies and service quality.	• Manages suppliers to meet key performance indicators and agreed upon targets • Manages the operational relationships between suppliers and ensures potential disputes or conflicts are raised and resolved • Performs bench-marking and makes use of supplier performance data to ensure that performance is adequately monitored and regularly reviewed • Use suppliers' expertise to support and inform development roadmaps • Manages implementation of supplier service improvement actions • Identifies constraints and opportunities when negotiating or renegotiating contracts

CCSP

Certified Cloud Security Professional
ISC2 Certification

Following the awarding of a CCSP certification, a practitioner could reasonably be expected to have demonstrated the knowledge and skills necessary for the SFIA skills listed below, together with the level of responsibility for the SFIA Generic Attributes including behavioral and business skills. The CCSP certification will contribute to the provision of evidence that the practitioner has applied the relevant knowledge and skills and has significant professional experience performing the activities described by SFIA in a professional working environment through the performance of a role, job or function. This table indicates the SFIA skills relevant to the knowledge and skills assessed during the certification process.

Strategy and Architecture	
Strategy and Planning	
Solution Architecture ARCH	**Level 5**
Developing and communicating a multi-dimensional solution architecture to deliver agreed business outcomes.	• Leads the development of solution architectures in specific business, infrastructure or functional areas. • Leads the preparation of technical plans and ensures appropriate technical resources are made available. Ensures appropriate tools and methods are available, understood and employed in architecture development. • Provides technical guidance and governance on solution development and integration. Evaluates requests for changes and deviations from specifications and recommends actions. • Ensures relevant technical strategies, policies, standards and practices (including security and cost management) are applied correctly.
Security and Privacy	
Information Security SCTY	**Level 5**
Defining and operating a framework of security controls and security management strategies.	• Provides advice and guidance on security strategies to manage identified risks and ensure adoption and adherence to standards. • Contributes to development of information security policy, standards and guidelines. • Obtains and acts on vulnerability information and conducts security risk assessments, business impact analysis and accreditation on complex information systems. Investigates major breaches of security and recommends appropriate control improvements. • Develops new architectures that manage the risks posed by new technologies and business practices.

Information Assurance INAS	Level 5
Protecting against and managing risks related to the use, storage and transmission of data and information systems.	• Interprets information assurance and security policies and applies these to manage risks • Provides advice and guidance to ensure adoption of and adherence to information assurance architectures, strategies, policies, standards and guidelines • Plans, organises and conducts information assurance and accreditation of complex domains areas, cross-functional areas, and across the supply chain • Contributes to the development of policies, standards and guidelines
Information and Data Compliance PEDP	**Level 5**
Implementing and promoting compliance with information and data management legislation.	• Contributes to policies, standards and guidelines for information and data compliance. • Provides authoritative advice on implementing compliance controls in products, services and systems. • Investigates breaches and recommends control improvements. Maintains an inventory of legislated data, conducts risk assessments and specifies necessary changes. • Ensures formal requests and complaints are handled following procedures. Prepares and submits reports to relevant authorities, ensuring all compliance requirements are met.

Governance, Risk and Compliance

Risk Management BURM	Level 5
Planning and implementing processes for managing risk across the enterprise, aligned with organisational strategy and governance frameworks.	• Plans and implements complex and substantial risk management activities within a specific function, technical area, project or programme. • Establishes consistent risk management processes and reporting mechanisms aligned with governance frameworks. • Engages specialists and domain experts as necessary. • Advises on the organisation's approach to risk management.

Audit AUDT	Level 5
Delivering independent, risk-based assessments of the effectiveness of processes, the controls, and the compliance environment of an organisation.	• Plans, organises and conducts audits of complex domains areas, cross-functional areas, and across the supply chain • Confirms the scope and objectives of specific audit activities with management. Aligns with the scope of the audit program and organisational policies • Determines appropriate methods of investigation to achieve the audit objectives. Presents audit findings to management describing the effectiveness and efficiency of control mechanisms • Provides general and specific audit advice. Collaborates with professionals in related specialisms to develop and integrate findings

Development and Implementation

Data and Analytics

Data Management DATM	Level 5
Developing and implementing plans, policies and practices that control, protect and optimise the value and governance of data assets.	• Devises and implements data governance and master data management processes. • Derives data management structures and metadata to support consistent data retrieval, integration, analysis, pattern recognition and interpretation across the organisation. • Independently validates external information from multiple sources. Plans effective data storage, sharing and publishing practices within the organisation. • Identifies and addresses issues preventing optimal use of information assets. Provides expert advice to maximise data asset value, ensuring data quality and compliance.

Delivery and Operation

Technology Management

Infrastructure operations ITOP	Level 5
Provisioning, deploying, configuring, operating and optimising technology infrastructure across physical, virtual and cloud-based environments.	• Provides technical leadership to optimise the performance of the technology infrastructure. • Drives the adoption of tools and automated processes for effective operational management and delivery. • Oversees the planning, installation, maintenance and acceptance of new and updated infrastructure components and infrastructure-based services. Aligns to service expectations, security requirements and other quality standards. • Ensures operational procedures and documentation are current and effective, tracks and addresses operational issues and reports to stakeholders.

System Software Administration SYSP	Level 5
Installing, managing and maintaining operating systems, data management, office automation and utility software across various infrastructure environments.	• Ensures system software is provisioned and configured to support the achievement of service objectives. • Develops and maintains diagnostic tools and processes for troubleshooting and performance analysis. • Evaluates new system software and recommends adoption if appropriate. Plans the provisioning and testing of new versions of system software. • Ensures operational procedures and diagnostics for system software are current, accessible and well understood. Investigates and coordinates the resolution of potential and actual service problems.

Storage Management STMG	Level 5
Provisioning, configuring and optimising on-premises and cloud-based storage solutions, ensuring data availability, security and alignment with business objectives.	• Develops standards and guidelines for implementing data protection and disaster recovery functionality for all business applications and business data. • Provides authoritative advice and guidance to implement and improve storage management. • Manages storage and backup systems to provide agreed service levels. • Creates, improves and supports storage management services with optimal utilisation of storage resources, ensuring security, availability and integrity of data.

Service Management

Service Level Management SLMO	Level 5
Agreeing targets for service levels and assessing, monitoring, and managing the delivery of services against the targets.	• Ensures that service delivery meets agreed service levels • Negotiates service level requirements and agreed service levels with customers • Diagnoses service delivery problems and initiates actions to maintain or improve levels of service • Establishes and maintains operational methods, procedures and facilities and reviews them regularly for effectiveness and efficiency

Continuity Management COPL	Level 5
Developing, implementing and testing a business continuity framework.	• Manages the development, implementation and testing of continuity management plans • Manages the relationship with individuals and teams who have authority for critical business processes and supporting systems • Evaluates the critical risks and identifies priority areas for improvement • Tests continuity management plans and procedures to ensure they address exposure to risk and that agreed levels of continuity can be maintained

Incident Management USUP	Level 5
Coordinating responses to a diverse range of incidents to minimise negative impacts and quickly restore services.	• Responsible for the operation of the incident management process. • Manages incident communications, ensuring al parties are aware of incidents and their role in the process. • Leads the review of major incidents and informs service owners of outcomes. Ensures incident resolution within service targets. Analyses metrics and reports on the performance of the incident management process. • Develops, maintains and tests incident management policy and procedures. Ensures compliance with regulatory requirements.

Security Services

Security Operations SCAD	Level 5
Manages and administers security measures, using tools and intelligence to protect assets, ensuring compliance and operational integrity.	• Oversees security operations procedures, ensuring adherence and effectiveness, including cloud security practices and automated threat responses. • Reviews actual or potential security breaches and vulnerabilities and ensures they are promptly and thoroughly investigated. Recommends actions and appropriate control improvements. • Ensures the integrity and completeness of security records, ensuring timely support and adherence to established procedures. • Contributes to the creation and maintenance of security policies, standards and procedures integrating new compliance requirements and technology advances.

Identity and Access Management IAMT	Level 5
Manages identity verification and access permissions within organisational systems and environments.	• Offers authoritative advice on identity and access management, ensuring services align with and support evolving business needs and security protocols. • Manages large-scale identity and access management initiatives and oversees the integration of identity and access management services with new technologies, enhancing security and operational efficiency. • Leads operational planning for identity and access management, anticipating future trends and preparing the organisation for scalable growth. • Ensures compliance of identity and access management systems and oversees advanced monitoring and audit processes.

Vulnerability Assessment VUAS	Level 5
Identifying and classifying security vulnerabilities in networks, systems and applications and mitigating or eliminating their impact.	• Plans and manages vulnerability assessment activities within the organisation. • Evaluates and selects, reviews vulnerability assessment tools and techniques. • Provides expert advice and guidance to support the adoption of agreed approaches. • Obtains and acts on vulnerability information and conducts security risk assessments, business impact analysis and accreditation on complex information systems

Relationship and Engagement

Stakeholder Management

Supplier Management SUPP	Level 5
Aligning the organisation's supplier performance objectives and activities with sourcing strategies and plans, balancing costs, efficiencies and service quality.	• Manages suppliers to meet key performance indicators and agreed upon targets • Manages the operational relationships between suppliers and ensures potential disputes or conflicts are raised and resolved • Performs benchmarking and makes use of supplier performance data to ensure that performance is adequately monitored and regularly reviewed • Use suppliers' expertise to support and inform development roadmaps • Manages implementation of supplier service improvement actions • Identifies constraints and opportunities when negotiating or renegotiating contracts

Contract Management ITCM	Level 5
Managing and operating formal contracts, addressing supplier and client needs in product and service provision.	• Oversees and measures the fulfilment of contractual obligations • Uses key performance indicators to monitor and challenge performance and identify opportunities for continual improvement • Develops strategies to address under-performance and compliance failures, including the application of contract terms • Identifies where changes are required, evaluates the impact, and advises stakeholders about the implications and consequences • Negotiates variations and seeks appropriate authorisation • Actively supports and engages with experts and stakeholders to ensure continual improvements are identified through review and benchmarking processes • Develops and implements change management protocols

Following the awarding of a CGRC certification, a practitioner could reasonably be expected to have demonstrated the knowledge and skills necessary for the SFIA skills listed below, together with the level of responsibility for the SFIA Generic Attributes including behavioral and business skills. The CGRC certification will contribute to the provision of evidence that the practitioner has applied the relevant knowledge and skills and has significant professional experience performing the activities described by SFIA in a professional working environment through the performance of a role, job or function. This table indicates the SFIA skills relevant to the knowledge and skills assessed during the certification process.

Strategy and Architecture	
Strategy and Planning	
Information Management IRMG	**Level 5**
Enabling the effective management and use of information assets.	• Ensures implementation of information and records management policies and standard practice. Communicates the benefits and value of information management. • Plans effective information storage, sharing and publishing within the organisation. Develops organisational taxonomy for information assets. • Provides expert advice and guidance to enable the organisation to get maximum value from its information assets. • Assesses issues that might prevent the organisation from making maximum use of its information assets. Contributes to the development of policy, standards and procedures for compliance with relevant legislation.
Strategy and Privacy	
Information Security SCTY	**Level 6**
Defining and operating a framework of security controls and security management strategies.	• Develops and communicates corporate information security policy, standards and guidelines. • Ensures architectural principles are applied during design to reduce risk. Drives adoption and adherence to policy, standards and guidelines. • Contributes to the development of organisational strategies that address information control requirements. Identifies and monitors environmental and market trends and proactively assesses impact on business strategies, benefits and risks. • Leads the provision of authoritative advice and guidance on the requirements for security controls in collaboration with subject matter experts.

Information Assurance INAS	Level 5
Protecting against and managing risks related to the use, storage and transmission of data and information systems.	• Interprets information assurance and security policies and applies these to manage risks • Provides advice and guidance to ensure adoption of and adherence to information assurance architectures, strategies, policies, standards and guidelines • Plans, organises and conducts information assurance and accreditation of complex domain areas, cross-functional areas, and across the supply chain • Contributes to the development of policies, standards and guidelines

Information and Data Compliance PEDP	Level 5
Implementing and promoting compliance with information and data management legislation.	• Contributes to policies, standards and guidelines for information and data compliance. • Provides authoritative advice on implementing compliance controls in products, services and systems. • Investigates breaches and recommends control improvements. Maintains an inventory of legislated data, conducts risk assessments and specifies necessary changes. • Ensures formal requests and complaints are handled following procedures. Prepares and submits reports to relevant authorities, ensuring all compliance requirements are met.

Strategy and Architecture

Governance, Risk and Compliance

Governance GOVN	Level 6
Defining and operating frameworks for decision-making, risk management, stakeholder relationships and compliance with organisational and regulatory obligations.	• Implements the governance framework to enable governance activity to be conducted • Within a defined area of accountability, determines the requirements for appropriate governance reflecting the organisation's values, ethics, risk appetite and wider governance frameworks. Communicates delegated authority, benefits, opportunities, costs, and risks • Leads reviews of governance practices with appropriate and sufficient independence from management activity • Acts as the organisation's contact for relevant regulatory authorities and ensures proper relationships between the organisation and external stakeholders

Risk Management BURM	Level 5
Planning and implementing processes for managing risk across the enterprise, aligned with organisational strategy and governance frameworks.	• Plans and implements complex and substantial risk management activities within a specific function, technical area, project or programme. • Establishes consistent risk management processes and reporting mechanisms aligned with governance frameworks. • Engages specialists and domain experts as necessary. • Advises on the organisation's approach to risk management.
Audit AUDT	**Level 5**
Delivering independent, risk-based assessments of the effectiveness of processes, the controls, and the compliance environment of an organisation.	• Plans, organises and conducts audits of complex domains areas, cross-functional areas, and across the supply chain • Confirms the scope and objectives of specific audit activities with management. Aligns with the scope of the audit programme and organisational policies • Determines appropriate methods of investigation to achieve the audit objectives. Presents audit findings to management describing the effectiveness and efficiency of control mechanisms • Provides general and specific audit advice. Collaborates with professionals in related specialisms to develop and integrate findings
Quality Assurance QUAS	**Level 5**
Assuring, through ongoing and periodic assessments and reviews, that the organisation’s quality objectives are being met.	• Plans, organises and conducts formal reviews and assessments of complex domains areas, cross-functional areas and across the supply chain. • Evaluates, appraises and identifies non-compliances with organisational standards and determines the underlying reasons for non-compliance. • Prepares and reports on assessment findings and associated risks. Ensures appropriate owners for corrective actions are identified. Identifies opportunities to improve organisational control mechanisms. • Oversees the assurance activities of others, providing advice and expertise to support assurance activity.

Delivery and Operation

Technology Management

Systems Installation and Removal HSIN	Level 5
Installing and testing, or decommissioning and removing, systems or system components.	• Takes responsibility for installation and/or decommissioning projects. • Provides effective team leadership, including information flow to and from the customer during project work. • Develops and implements quality plans and method statements. • Monitors the effectiveness of installations and ensures appropriate recommendations for change are made.

Service management

Service Level Management SLMO	Level 5
Agreeing targets for service levels and assessing, monitoring, and managing the delivery of services against the targets.	• Ensures that service delivery meets agreed service levels • Negotiates service level requirements and agreed service levels with customers • Diagnoses service delivery problems and initiates actions to maintain or improve levels of service • Establishes and maintains operational methods, procedures and facilities and reviews them regularly for effectiveness and efficiency

Asset Management ASMG	Level 5
Managing the full life cycle of assets from acquisition, operation, maintenance to disposal.	• Manages and maintains the service compliance of IT and service assets in line with business and regulatory requirements. Identifies, assesses and communicates associated risks. • Ensures asset controllers, infrastructure teams and the business co-ordinate and optimize value, maintain control and maintain appropriate legal compliance.

Change Control CHMG	Level 5
Assessing risks associated with proposed changes and ensuring changes to products, services or systems are controlled and coordinated.	• Leads the assessment, analysis, development, documentation and implementation of changes. • Develops implementation plans for complex requests for change. • Reviews proposed implementations and evaluates the risks to the integrity of the product and service environment. Ensures appropriate change approval is applied to changes. • Reviews the effectiveness of change implementation. Identifies, evaluates and manages the adoption of appropriate tools, techniques and processes for change control.

Security Services

Security Operations SCAD	Level 5
Manages and administers security measures, using tools and intelligence to protect assets, ensuring compliance and operational integrity.	• Oversees security operations procedures, ensuring adherence and effectiveness, including cloud security practices and automated threat responses. • Reviews actual or potential security breaches and vulnerabilities and ensures they are promptly and thoroughly investigated. Recommends actions and appropriate control improvements. • Ensures the integrity and completeness of security records, ensuring timely support and adherence to established procedures. • Contributes to the creation and maintenance of security policies, standards and procedures integrating new compliance requirements and technology advances.

Vulnerability Assessment VUAS	Level 5
Identifying and classifying security vulnerabilities in networks, systems and applications and mitigating or eliminating their impact.	• Plans and manages vulnerability assessment activities within the organisation • Evaluates and selects, reviews vulnerability assessment tools and techniques • Provides expert advice and guidance to support the adoption of agreed approaches • Obtains and acts on vulnerability information and conducts security risk assessments, business impact analysis and accreditation on complex information systems

Relationship and Engagement

Stakeholder Management

Stakeholder Relationship Management RLMT	Level 5
Systematically analysing, managing and influencing stakeholder relationships to achieve mutually beneficial outcomes through structured engagement.	• Identifies the communications and relationship needs of stakeholder groups. Translates communications/stakeholder engagement strategies into specific activities and deliverables. • Facilitates open communication and discussion between stakeholders. • Acts as a single point of contact by developing, maintaining and working to stakeholder engagement strategies and plans. Provides informed feedback to assess and promote understanding. • Facilitates business decision-making processes. Captures and disseminates technical and business information.

SSCP

Following the awarding of a SSCP certification, a practitioner could reasonably be expected to have demonstrated the knowledge and skills necessary for the SFIA skills listed below, together with the level of responsibility for the SFIA Generic Attributes including behavioral and business skills. The SSCP certification will contribute to the provision of evidence that the practitioner has applied the relevant knowledge and skills and has significant professional experience performing the activities described by SFIA in a professional working environment through the performance of a role, job or function. This table indicates the SFIA skills relevant to the knowledge and skills assessed during the certification process.

Strategy and Architecture	
Strategy and Planning	
Information Management IRMG	**Level 4**
Enabling the effective management and use of information assets.	• Enables the organisation to organise, control and discover information assets. • Supports the organisation to identify, catalogue and categorise information types and information repositories in line with information management strategies and practices. • Enables users to find information through appropriate use of metadata and search tools. • Provides advice and guidance to enable good information management practices to be adopted across the organisation.

Security and Privacy

Information Security SCTY	Level 4
Defining and operating a framework of security controls and security management strategies.	• Provides guidance on the application and operation of elementary physical, procedural and technical security controls • Explains the purpose of security controls and performs security risk and business impact analysis for medium complexity information systems • Identifies risks that arise from potential technical solution architectures • Designs alternate solutions or countermeasures and ensures they mitigate identified risks • Investigates suspected attacks and supports security incident management

Information Assurance INAS	Level 4
Protecting against and managing risks related to the use, storage and transmission of data and information systems.	• Performs technical assessments and/or accreditation of complex or higher-risk information systems • Identifies risk mitigation measures required in addition to the standard organisation or domain measures • Establishes the requirement for accreditation evidence from delivery partners and communicates accreditation requirements to stakeholders • Contributes to planning and organisation of information assurance and accreditation activities. Contributes to development of and implementation of information assurance processes

Governance, Risk and Compliance

Risk Management BURM	Level 3
Planning and implementing processes for managing risk across the enterprise, aligned with organisational strategy and governance frameworks.	• Undertakes basic risk management activities. Maintains documentation of risks, threats, vulnerabilities and mitigation actions

Audit AUDT	Level 4
Delivering independent, risk-based assessments on the effectiveness of processes, the controls, and the compliance environment of an organisation.	• Contributes to planning and executing of risk-based audit of existing and planned processes, products, systems and services • Identifies and documents risks in detail • Identifies the root cause of issues during an audit, and communicates these effectively as risk insights • Collates evidence regarding the interpretation and implementation of control measures. Prepares and communicates reports to stakeholders, providing a factual basis for findings

Development and Implementation

Systems Development

Non-functional testing NFTS	Level 3
Assessing specified or unspecified functional requirements and characteristics of products, systems and services through investigation and testing.	• Designs non-functional test cases and scripts, mapping to pre-set criteria for system qualities and characteristics. • Prepares and manages test data to reflect real-world scenarios. Configures test environments, collaborates with stakeholders to clarify requirements and automates repeatable tests. • Participates in requirement reviews to refine comprehensive test plans. Undertakes exploratory tests to investigate unusual behaviours. • Executes tests, troubleshooting issues as they arise. Analyses and reports on test activities, providing thorough coverage of non-functional attributes.

Data and Analytics

Data Management DATM	Level 4
Developing and implementing plans, policies and practices that control, protect and optimise the value and governance of data assets.	• Devises and implements data governance and master data management processes. • Derives data management structures and metadata to support consistent data retrieval, integration, analysis, pattern recognition and interpretation across the organisation. • Independently validates external information from multiple sources. Plans effective data storage, sharing and publishing practices within the organisation. • Identifies and addresses issues preventing optimal use of information assets. Provides expert advice to maximise data asset value, ensuring data quality and compliance.

Delivery and Operation

Technology Management

Infrastructure Operations ITOP	Level 4
Provisioning, deploying, configuring, operating and optimising technology infrastructure across physical, virtual and cloud-based environments.	• Applies technical expertise to maintain and optimise technology infrastructure, executing updates and employing automation tools. Configures tools and/or creates scripts to automate infrastructure tasks. • Maintains operational procedures and checks that they are followed, including adherence to security policies. Uses infrastructure management tools to monitor load, performance, and security metrics. • Investigates and enables the resolution of operational and security-related issues. Provides reports and proposals for improvement to stakeholders. • Contributes to the planning and implementation of infrastructure maintenance and updates. Implements agreed infrastructure changes and maintenance routines.

Network Support NTAS	Level 4
Installing, managing, controlling, deploying and maintaining infrastructure systems software, to meet operational needs and service levels.	• Applies technical expertise to maintain and optimise network infrastructure, executing updates and employing automation tools. Uses network management tools to monitor load, performance, and security statistics. Investigates and enables the resolution of network-related operational and security issues. Configures tools and/or creates scripts to automate network tasks. Maintains operational procedures and checks that they are followed. Provides reports and proposals for improvement to stakeholders. • Contributes to the planning and implementation of network maintenance, updates, and security enhancements. Implements agreed network changes and maintenance routines.

Storage Management STMG	Level 4
Provisioning, configuring and optimising on-premises and cloud-based storage solutions, ensuring data availability, security and alignment with business objectives.	• Prepares and maintains operational procedures for storage management. • Monitors capacity, performance, availability and other operational metrics. Takes appropriate action to ensure corrective and proactive maintenance of storage and backup systems to protect and secure business information. • Creates reports and proposals for improvement. • Contributes to the planning and implementation of new installations and scheduled maintenance and changes of existing systems.

Service Management

Continuity Management COPL	Level 4
Developing, implementing and testing a business continuity framework.	• Contributes to the development of continuity management plans • Identifies information and communication systems that support critical business processes • Coordinates the business impact analysis and the assessment of risks • Coordinates the planning, designing, and testing of contingency plans

Incident Management USUP	Level 4
Coordinating responses to a diverse range of incidents to minimise negative impacts and quickly restore services.	• Monitors and manages incident queues to ensure incidents are handled according to procedures and service levels. • Contributes to developing, testing and improving incident management procedures. Uses analytics tools to track trends. • Ensures resolved incidents are properly documented and closed. • Supports team members in the correct use of the incident process.

Asset Management ASMG	Level 4
Managing the full life cycle of assets from acquisition, operation, maintenance to disposal.	• Controls assets in one or more significant areas ensuring that administration of full life cycle of assets is carried out • Produces and analyses registers and histories of authorised assets and verifies that all these assets are in a known state and location • Acts to highlight and resolve potential instances of unauthorised assets

Delivery and Operation

Security Services

Security Operations SCAD	Level 4
Manages and administers security measures, using tools and intelligence to protect assets, ensuring compliance and operational integrity.	• Maintains and optimises operational security processes. Checks that all requests for support are dealt with according to established protocols, including for cloud-based and automated systems. • Provides advice on implementing and managing physical, procedural and technical security encompassing both physical and digital assets. • Investigates security breaches in accordance with established procedures using advanced tools and techniques and recommends necessary corrective actions. • Enables effective implementation of recommended security measures and monitors their performance.
Identity and Access Management IAMT	**Level 4**
Manages identity verification and access permissions within organizational systems and environments.	• Designs and implements complex identity and access management solutions, focusing on automated access control and role allocation. • Oversees the integration of identity and access management services with new technologies. Provides specialized support for complex identity and access management operations and supports implementation of policies and standards. • Collaborates with stakeholders to align identity and access management with business objectives and emerging security trends.
Vulnerability Assessment VUAS	**Level 4**
Identifying and classifying security vulnerabilities in networks, systems and applications and mitigating or eliminating their impact.	• Collates and analyses catalogues of information and technology assets for vulnerability assessment • Performs vulnerability assessments and business impact analysis for medium complexity information systems • Contributes to selection and deployment of vulnerability assessment tools and techniques
Digital Forensics DGFS	**Level 4**
Recovering and investigating material found in digital devices.	• Designs and executes complex digital forensic examinations. • Specifies requirements for specialised forensic tools and resources. Provides guidance on advanced data recovery techniques and artefact analysis. • Processes and analyses digital evidence in line with organisational policies and industry standards. Develops procedures for handling emerging technologies in forensic contexts. • Contributes to forensic reports detailing technical findings.

CC

Certified in Cybersecurity
ISC2 Certification

Following the awarding of a CC certification, a practitioner could reasonably be expected to have demonstrated the knowledge necessary for the SFIA skills listed below within the context of a security role, and this would also be a significant contributor for the practice of the skill in other roles as well. The CC certification will contribute to the provision of evidence that the practitioner has attained the relevant knowledge required for the performance of a role, job or function. This table indicates the SFIA skills relevant to the knowledge assessed during the certification process.

Strategy and Architecture

Security and Privacy

Information Security SCTY	Level 2
Defining and operating a framework of security controls and security management strategies.	• Assists with implementing and monitoring security policies and protocols across different systems. • Contributes to identifying and addressing potential risks in security governance and compliance. • Supports the analysis of documented security incidents, escalating where appropriate. • Assists in the review of access controls and permissions, ensuring adherence to security policies.

Information Assurance INAS	Level 2
Protecting against and managing risks related to the use, storage and transmission of data and information systems.	• Assists with information assurance activities under routine supervision. • Helps perform basic risk assessments and supports the implementation of information assurance measures. • Assists in maintaining records and documentation related to information assurance.

Governance, Risk and Compliance

Risk Management BURM	Level 2
Planning and implementing processes for managing risk across the enterprise, aligned with organizational strategy and governance frameworks.	• Assists in collecting and reporting data to support risk management activities under routine supervision. • Helps create and maintain documentation of risks and risk management activities. • Helps identify and report issues and discrepancies.

Development and Implementation

Data and Analytics

Data Management DATM	Level 2
Developing and implementing plans, policies and practices that control, protect and optimise the value and governance of data assets.	• Assists in implementing data management activities under close guidance and supervision. • Helps create and maintain documentation of data management activities. • Helps identify and report issues and discrepancies.

Delivery and Operation

Technology Management

System Software Administration SYSP	Level 2
Installing, managing and maintaining operating systems, data management, office automation and utility software across various infrastructure environments.	• Assists with system software administration tasks under routine supervision. • Supports the installation and configuration of system software. • Helps monitor system performance and resource usage. • Assists in documenting system software settings and updates.

Network Support NTAS	Level 1
Providing maintenance and support services for communications networks.	• Supports routine network tasks under close supervision. • Monitors basic network health and reports on the status of network components. • Assists with straightforward troubleshooting and follows established procedures to maintain operational continuity. • Escalates issues as necessary to higher levels of support

Service Management

Service Level Management SLMO	Level 2
Agreeing targets for service levels and assessing, monitoring and managing the delivery of services against the targets.	• Monitors and logs the actual service provided. • Compares delivered service to service level agreements, identifying any deviations or areas for improvement.

Continuity Management COPL	Level 2
Developing, implementing and testing a business continuity framework.	• Maintains records of all related testing and training and ensures the availability of all documentation. • Records the actions taken and the consequences following an incident or live testing of a continuity plan for a lessons-learned report.

Incident Management USUP	Level 1
Coordinating responses to a diverse range of incidents to minimize negative impacts and quickly restore services.	• Follows agreed procedures to identify, register and categorize incidents. • Uses provided tools and technologies to support the incident management process. • Collects information as instructed to assist in incident resolution and allocates incidents as directed. • Assists in monitoring incident queues and escalates issues according to procedures.

Security Services	
Security Operations SCAD	**Level 1**
Manages and administers security measures, using tools and intelligence to protect assets, ensuring compliance and operational integrity.	• Performs simple security administration tasks. • Maintains relevant records and documentation, contributing to overall data integrity.
Identity and Access Management IAMT	**Level 1**
Manages identity verification and access permissions within organizational systems and environments.	• Performs basic identity and access management tasks, including user account lifecycle management, under supervision. • Maintains accurate records and follows established identity and access management protocols.

2. Secondary SFIA Skills

The table below shows the secondary view illustrating how the knowledge gained from the CISSP, CSSLP, CCSP and CGRC certifications partially map to SFIA skills.

			CISSP	CSSLP	CCSP	CGRC	SSCP	CC
Secure software and systems development	Systems Development Management	DLMG		5				
	Systems and Software Lifecycle Engineering	SLEN				5		
	Systems Design	DESN	5	5				
	Software Design	SWDN	5	5				
	Network Design	NTDS	5					2
	Delivery Management	DEMG	5	5	5			
	Programming/Software Development	PROG		5			4	
	Systems Integration and Build	SINT		5				
	Infrastructure Design	IFDN	5		5			
	Radio Frequency Engineering	RFEN					3	
Secure supply chain	Sourcing	SORC			5			
Secure infrastructure management	Infrastructure Operations	ITOP						1
	Technology Service Management	ITMG	5		5			
	Release Management	RELM		5				
	Capacity Management	CPMG			5			
	Configuration Management	CFMG					3	2
	Systems installation and removal	HSIN		5				
	Facilities Management	DCMA	5				3	2
	Methods and Tools	METL	5					
Cybersecurity resilience	Change Control	CHMG					3	2
	Identity and Access Management	IAMT		5				
	Cybercrime investigation	CRIM	5		5		4	
Cybersecurity talent management	Resourcing	RESC	5					
	Employee Experience	EEXP	5					
Cybersecurity education and training	Learning Development and Management	ETMG	5	5	5			
	Learning Delivery	ETDL					3	

3. Ancillary SFIA Skills

The table below shows the ancillary view illustrating how the knowledge gained from the CISSP, CSSLP, CCSP and CGRC Common Body of Knowledge (CBK) map directly to SFIA skills at levels of responsibility below SFIA level 5.

			CISSP	CSSLP	CCSP	CGRC
Cyber security architecture	Solution Architecture	ARCH	4			
Cybersecurity research and intelligence	Threat Intelligence	THIN	4	4		
Cybersecurity governance, risk and compliance	Information Management	IRMG	4		4	
	Quality Assurance	QUAS			3	
Secure Software and Systems Development	Systems Design	DESN			4	
	Programming/Software Development	PROG			3	
	Systems Integration and Build	SINT			3	
	Non-Functional Testing	NFTS			4	4
	Delivery Management	DEMG		4		
	Software Configuration	PORT	4		3	
	Penetration Testing	PENT	4	4		
Secure supply chain	Sourcing	SORC		4		
	Supplier Management	SUPP	4			
Secure Infrastructure	Infrastructure Operations	ITOP				4
	Release Management	RELM			3	
	Deployment	DEPL		4		
	Configuration Management	CFMG	4	4		
	Facilities Management	DCMA			4	
Cybersecurity resilience	Security Operations	SCAD		4		
	Problem Management	PBMG		4		
	Change Control	CHMG	4			
	Vulnerability Assessment	VUAS	4			
	Digital Forensics	DGFS	4	4	4	
	Offensive cyber operations	OCOP	4			