ISC2 Training Course Mappings to the SFIA 9 Framework

20 February 2025 | Document Two

Table of Contents

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, (ISC)² 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 organization'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 organization'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.

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 training mappings to the Skills Framework for the Information Age (SFIA).

Introduction

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 organizations a common language to define skills and expertise in a consistent way. The use of clear language, avoiding 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, organization design, and procurement. It can solve the common translation issues that hinder communication and effective partnerships within organizations and multi-disciplinary teams.

The CISSP and CSSLP training covers the security aspects of SFIA skills at levels 5-6. The CCSP and CGRC training covers the security aspects of SFIA skills at level 5, and the SSCP training covers SFIA skills at levels 3-4. The training material provides the knowledge to enable a solid foundation for practitioners to continue to develop their skill attributes and understand the concepts which underpin the ISC2 certification exams.

Following the completion of an ISC2 training course, a practitioner could reasonably be expected to have been provided with the knowledge necessary for the SFIA skills related to the training. The table in Section 2 indicates the SFIA skills relevant to the knowledge provided in each ISC2 training course.

2. ISC2 Training Course mappings to SFIA Skills

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

			CISSP	CSSLP	CCSP	CGRC	SSCP
Cyber security strategy and leadership	Information security	SCTY	6	5	5	6	4
	Stakeholder relationship management	RLMT			5	5	
Cyber security architecture	Requirements definition and management	REQM		5			
	Solution architecture	ARCH		5	5		
	Data management	DATM	5		5		4
Cybersecurity governance, risk and compliance	Governance	GOVN	6			6	
	Risk management	BURM	5	5	5	5	3
	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	5	4
Secure software and systems development	Systems development management	DLMG		6			
	Systems and software lifecycle engineering	SLEN	5	6		5	
	Systems design	DESN	5	5			
	Software design	SWDN	5	5			
	Database design	DBDS		5			
	Programming/software development	PROG		5			4
	Systems integration and build	SINT		5			
	Penetration testing	PENT		5			3
	Non-functional testing	NFTS	5	6		5	4
	User acceptance testing	BPTS	5	5			
	Radio frequency engineering	RFEN					3
Secure supply chain	Sourcing	SORC		5	5		
	Supplier management	SUPP	5	5	5		
	Contract management	ITCM			5		

Continued

			CISSP	CSSLP	CCSP	CGRC	SSCP
Secure infrastructure management	Technology service management	ITMG	5		5		
	Infrastructure operations	ITOP			5	5	4
	Network design	NTDS	5				
	Network support	NTAS	5				4
	Capacity management	CPMG			5		
	Configuration management	CFMG					3
	Systems installation and removal	HSIN		5		5	
	Storage management	STMG	5		5		4
	System software administration	SYSP	5	5	5	5	
	Service level management	SLMO		5	5	5	
	Facilities management	DCMA	5		5		3
	Contract management	ITCM			5		
Cybersecurity resilience	Security operations	SCAD	5		5	5	4
	Identity and access management	IAMT	5	5	5		4
	Continuity management	COPL	5	5	5		4
	Incident management	USUP	5	5	5	5	4
	Problem management	PBMG		5			
	Change control	CHMG				5	3
	Asset management	ASMG	5			5	4
	Vulnerability assessment	VUAS	5	5	5	5	4
	Digital forensics	DGFS		5	5		4
	Cybercrime investigation	CRIM	5		5		4
	Methods and Tools	METL	5				
Cybersecurity talent management	Resourcing	RESC	5				
	Employee experience	EEXP	5				
Cybersecurity education and training	Learning delivery	ETDL					3
	Learning development and management	ETMG	5	5	5		

CISSP

Certified Information Systems Security Professional
ISC2 Certification

Following the completion of a CISSP training course, a practitioner could reasonably be expected to have been provided with 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 CISSP training course will contribute to the provision of the relevant knowledge a practitioner would require for the performance of a role, job or function. This table indicates the SFIA skills relevant to the knowledge provided in the training course.

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 organizational 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 domains areas, cross-functional areas, and across the supply chain • Contributes to the development of policies, standards and guidelines

Personal Data Protection 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 organizational 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 organization'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 organization's contact for relevant regulatory authorities and ensures proper relationships between the organization and external stakeholders

Risk Management BURM	Level 5
Planning and implementing processes for managing risk across the enterprise, aligned with organizational 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 organization'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 organization.	• 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 activity with management. Aligns with the scope of the audit programme and organizational 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

Advice and Guidance

Methods and Tools METL	Level 5
Leads the adoption, management and optimisation of methods and tools, ensuring effective use and alignment with organizational objectives.	• Provides authoritative advice and leadership to promote adoption of methods and tools and adherence to policies and standards. • Evaluates and selects appropriate methods and tools in line with agreed policies and standards. Contributes to organizational policies, standards and guidelines for methods and tools. • Implements methods and tools at programme, project and team levels including selection and tailoring in line with agreed standards. • Manages reviews of the benefits and value of methods and tools. Identifies and recommends improvements that support broader organizational goals.

Change and Transformation

Change Analysis

User Acceptance Testing BPTS	Level 5
Validating systems, products, business processes or services to determine whether the acceptance criteria have been satisfied.	• Plans and manages acceptance testing activity • Specifies the acceptance testing environment for systems, products, business processes and services. Manages the creation of acceptance test cases and scenarios. Ensures that defined tests reflect realistic operational conditions and required level of coverage • Ensure tests and results are documented, analysed and reported to stakeholders, and required actions taken. Highlights issues and risks identified during testing to stakeholders • Provides authoritative advice and guidance on planning and execution of acceptance tests

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 organization where systems and software life cycle working practices can be deployed

Systems Design DESN	Level 5
Designing systems to meet specified requirements and agreed systems architectures.	• Designs large or complex systems and undertakes impact analysis on major design options and trade-offs. • Ensures the system design balances functional and non-functional requirements. • Reviews systems designs and ensures appropriate methods, tools and techniques are applied effectively. Makes recommendations and assesses and manages associated risks. • Adopts and adapts system design methods, tools and techniques. Contributes to development of system design policies, standards and selection of architecture components.
Software Design SWDN	**Level 5**
Architecting and designing software to meet specified requirements, ensuring adherence to established standards and principles.	• Specifies, designs and architects large or complex software applications, components and modules. • Adopts and adapts software design methods, tools and techniques. Undertakes impact analysis on major design options, makes recommendations and assesses and manages associated risks. Specifies prototypes/simulations to enable informed decision-making. • Evaluates software designs to ensure adherence to standards and identifies corrective action. Ensures the software design balances functional, quality, security and systems management requirements. • Contributes to the development of organizational software design and architecture policies and standards.
Network Design NTDS	**Level 5**
Designing communication networks to meet business requirements, ensuring scalability, reliability, security and alignment with strategic objectives.	• Produces, or approves network providers', network architectures, topologies and configuration databases for own area of responsibility. • Specifies design parameters for network connectivity, capacity, speed, interfacing, security and access, in line with business requirements. • Assesses network-related risks and specifies recovery routines and contingency procedures. • Creates multiple design views to address the different stakeholders' concerns and to handle both functional and non-functional requirements.

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 organizational 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 organization. • Independently validates external information from multiple sources. Plans effective data storage, sharing and publishing practices within the organization. • 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

Technology Service Management ITMG	Level 5
Managing the provision of technology-based services to meet defined organizational needs.	• Takes responsibility for managing the design, procurement, installation, upgrading, operation, control, maintenance and effective use of specific technology services. • Leads service delivery, ensuring agreed service levels, security requirements and other quality standards are met. Ensures adherence to relevant policies and procedures. • Ensures processes, procedures and practices are aligned across teams and providers to operate effectively and efficiently. • Monitors technology services performance. Provides appropriate status and other reports to managers and senior users.

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.
Facilities Management DCMA	**Level 5**
Planning, designing and managing the buildings, space and facilities which, collectively, make up the IT estate.	• Develops and maintains the standards, processes and documentation for data centres • Optimises efficiency in the population of data centre space. Ensures adherence to all relevant policies and processes • Uses data centre management tools to plan, record and manage installed infrastructure, power, space and cooling capabilities • Monitors usage and actions to meet sustainability targets
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
Manages identity verification and access permissions within organizational 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 organization 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 organization • 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
Cybercrime Investigation CRIM	**Level 5**
Investigates cybercrimes, collects evidence, determines incident impacts and collaborates with legal teams to protect digital assets.	• Manages complex cybercrime investigations, overseeing all stages from detection to resolution. • Evaluates incidents involving advanced threats or significant breaches. • Develops and implements procedures for evidence handling and documentation. Collaborates with legal teams to ensure evidence supports potential legal proceedings. • Leads the development of response strategies, assessing vulnerabilities and operational capabilities. Oversees the implementation of tools and automation to enhance investigative processes.

People and Skills

People Management

Employee Experience EEXP	Level 5
Enhancing employee engagement and ways of working, empowering employees and supporting their health and wellbeing.	• Implements working practices that motivate employees and support their health and wellbeing • Provides guidance to individuals on long-term development goals and career opportunities, considering an individual's strengths and preferences • Communicates business direction, policy and purpose where these may drive or affect employee engagement. Ensures clear communication of delegated tasks and provides sufficient autonomy to motivate and empower individuals • Maintains awareness of the physical and emotional welfare of employees, and provides counselling when required

Resourcing RESC	Level 5
Acquiring, deploying and onboarding resources.	• Plans and manages the acquisition and deployment of resources to meet specific needs and ongoing demand • Defines and manages the implementation of resourcing processes and tools. Advises on available options and customises resourcing approach to meet requirements • Adheres to standards, statutory or external regulations and codes of practice and ensures compliance • Engages with external parties in support of resourcing plans • Measures effectiveness of resourcing processes and implements improvements

Skills Management

Learning and Development Management ETMG	Level 5
Delivering management, advisory and administrative services to support the development of knowledge, skills and competencies.	• Manages the provision of learning and development, ensuring optimum use of resources. • Maintains, publicises and promotes a catalogue of learning and development activities. Ensures courses are up to date and accredited (when required). • Arranges facilities and schedules with learning and development providers as appropriate. • Uses data to assess and improve the effectiveness of learning or educational activities.

Relationship and Engagement

Stakeholder Management

Supplier Management SUPP	Level 5
Aligning the organization’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 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 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.

CSSLP

Certified Secure Software Lifecycle Professional
ISC2 Certification

Following the completion of a CSSLP training course, a practitioner could reasonably be expected to have been provided with 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 CSSLP training course will contribute to the provision of the relevant knowledge a practitioner would require for the performance of a role, job or function. This table indicates the SFIA skills relevant to the knowledge provided in the training course.

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 organization. Develops organizational taxonomy for information assets. • Provides expert advice and guidance to enable the organization to get maximum value from its information assets. • Assesses issues that might prevent the organization 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 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

Personal Data Protection 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 organizational 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 organization'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 organization.	• 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 activity with management. Aligns with the scope of the audit programme and organizational 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 lifecycle.	• 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 organizational 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.

User Acceptance Testing BPTS	Level 5
Validating systems, products, business processes or services to determine whether the acceptance criteria have been satisfied.	• Plans and manages acceptance testing activity • Specifies the acceptance testing environment for systems, products, business processes and services. Manages the creation of acceptance test cases and scenarios. Ensures that defined tests reflect realistic operational conditions and required level of coverage • Ensure tests and results are documented, analysed and reported to stakeholders, and required actions taken. Highlights issues and risks identified during testing to stakeholders • Provides authoritative advice and guidance on planning and execution of acceptance tests

Development and Implementation

Systems Development

Systems Development Management DLMG	Level 6
Planning, estimating and executing systems development work to time, budget and quality targets.	• Sets policy and drives adherence to standards for systems development. • Leads activities to make security and privacy integral to systems development. • Identifies and manages the resources necessary for all stages of systems development projects. • Ensures technical, financial and quality targets are met.

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 organizational commitment to strategies to deliver systems and software life cycle working practices to achieve business objectives • Works with others to integrate organizational 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
Systems Design DESN	**Level 5**
Designing systems to meet specified requirements and agreed systems architectures.	• Designs large or complex systems and undertakes impact analysis on major design options and trade-offs. • Ensures the system design balances functional and non-functional requirements. • Reviews systems designs and ensures appropriate methods, tools and techniques are applied effectively. Makes recommendations and assesses and manages associated risks. • Adopts and adapts system design methods, tools and techniques. Contributes to development of system design policies, standards and selection of architecture components.

Software Design SWDN	Level 5
Architecting and designing software to meet specified requirements, ensuring adherence to established standards and principles.	• Specifies, designs and architects large or complex software applications, components and modules. • Adopts and adapts software design methods, tools and techniques. Undertakes impact analysis on major design options, makes recommendations and assesses and manages associated risks. Specifies prototypes/simulations to enable informed decision-making. • Evaluates software designs to ensure adherence to standards and identifies corrective action. Ensures the software design balances functional, quality, security and systems management requirements. • Contributes to the development of organizational software design and architecture policies and standards.
Programming/Software Development PROG	**Level 5**
Developing software components to deliver value to stakeholders.	• Takes technical responsibility across all stages and iterations of software development. • Plans and drives software construction activities. Adopts and adapts appropriate software development methods, tools and techniques. • Measures and monitors applications of project/team standards for software construction, including software security. • Contributes to the development of organizational policies, standards and guidelines for software development.
Systems Integration and Build SINT	**Level 5**
Planning, implementing and controlling activities to integrate system elements, subsystems and interfaces to create operational systems, products or services.	• Plans and drives activities to develop organizational systems integration and build capabilities including automation and continuous integration. • Identifies, evaluates and manages the adoption of tools, techniques and processes to create a robust integration framework. Provides authoritative advice and guidance on any aspect of systems integration. • Leads integration work in line with the agreed system and service design. Assesses risks and takes preventative action. Measures and monitors applications of standards. • Contributes to the development of organizational policies, standards and guidelines for systems integration.

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 organizational 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 organizational 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 organizational standards and proactive risk mitigation.

Data and Analytics

Database Design DBDS	Level 5
Specifying, designing and maintaining mechanisms for storing and accessing data across various environments and platforms.	• Provides specialist expertise in the design characteristics of database management systems or data warehouse products/services. • Provides expert guidance in the selection, provision and use of database and data warehouse architectures, software and facilities. • Ensures design policies optimise transactional data systems for performance and availability while meeting the needs of business intelligence and analytics platforms.

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.

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 that 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
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.

Problem Management PBMG	Level 5
Managing the life cycle of all problems that have occurred or could occur in delivering a service.	• Ensures appropriate action is taken to anticipate, investigate and resolve problems in systems and services. • Ensures problems are fully documented within the relevant reporting systems. • Enables development of problem solutions. Coordinates the implementation of agreed remedies and preventative measures. • Analyses patterns and trends and improves problem management processes.

Security Services

Identity and Access Management IAMT	Level 5
Manages identity verification and access permissions within organizational 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 organization for scalable growth. • Ensures compliance of identity and access management systems and oversees advanced monitoring and audit processes.

Digital Forensics DGFS	Level 5
Recovering and investigating material found in digital devices.	• Leads investigations to correctly gather, analyse and present findings, including digital evidence, to both business and legal audiences. • Collates conclusions and recommendations and presents forensic findings to stakeholders. • Plans and manages digital forensics activities within the organization. Provides expert advice on digital forensics. • Contributes to the development of digital forensics policies, standards and guidelines. Evaluates and selects digital forensics tools and techniques.

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 organization • 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

Penetration Testing PENT	Level 5
Testing the effectiveness of security controls by emulating the tools and techniques of likely attackers.	• Plans and drives penetration testing within a defined area of business activity • Delivers objective insights into the existence of vulnerabilities, the effectiveness of defences and mitigating controls • Takes responsibility for the integrity of testing activities and coordinates the execution of these activities. • Provides authoritative advice and guidance on all aspects of penetration testing • Identifies needs and implements new approaches for penetration testing. Contributes to security testing standards

People and Skills

Skills Management

Learning and Development Management ETMG	Level 5
Delivering management, advisory and administrative services to support the development of knowledge, skills and competencies.	• Manages the provision of learning and development, ensuring optimum use of resources • Maintains, publicises and promotes a catalogue of learning and development activities. Ensures that courses are up to date and accredited (when required). • Arranges facilities and schedules with learning and development providers as appropriate • Uses data to assess and improve the effectiveness of learning or educational activities

Relationship and Engagement

Stakeholder Management

Sourcing SORC	Level 5
Managing, or providing advice on, the procurement or commissioning of products and services.	• Plans and manages procurement activities • Manages tender, evaluation and acquisition processes. Researches suppliers and markets, and maintains a broad understanding of the commercial environment, to inform and develop commercial strategies and sourcing plans • Advises on the business case for alternative sourcing models. Advises on policy and procedures covering tendering, the selection of suppliers and procurement • Negotiates with potential partners and suppliers, developing acceptance criteria and procedures. Drafts and laces contracts

Supplier Management SUPP	Level 5
Aligning the organization’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 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 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 completion of a CCSP training course, a practitioner could reasonably be expected to have been provided with 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 CCSP training course will contribute to the provision of the relevant knowledge a practitioner would require for the performance of a role, job or function. This table indicates the SFIA skills relevant to the knowledge provided in the training course.

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
Personal Data Protection 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 organizational 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 organization'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 organization.	• 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 activity with management. Aligns with the scope of the audit programme and organizational 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 organization. • Independently validates external information from multiple sources. Plans effective data storage, sharing and publishing practices within the organization. • 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

Technology Service Management ITMG	Level 5
Managing the provision of technology-based services to meet defined organizational needs.	• Takes responsibility for managing the design, procurement, installation, upgrading, operation, control, maintenance and effective use of specific technology services. • Leads service delivery, ensuring agreed service levels, security requirements and other quality standards are met. Ensures adherence to relevant policies and procedures. • Ensures processes, procedures and practices are aligned across teams and providers to operate effectively and efficiently. • Monitors technology services performance. Provides appropriate status and other reports to managers and senior users.

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 expert 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
Facilities Management DCMA	**Level 5**
Planning, designing and managing the buildings, space and facilities which, collectively, make up the IT estate.	• Develops and maintains the standards, processes and documentation for data centres • Optimises efficiency in the population of data centre space. Ensures adherence to all relevant policies and processes • Uses data centre management tools to plan, record and manage installed infrastructure, power, space and cooling capabilities • Monitors usage and actions to meet sustainability targets
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
Capacity Management CPMG	**Level 5**
Ensuring that service components have the capacity and performance to meet current and planned business needs.	• Manages capacity modelling and forecasting activities • Proactively reviews information in conjunction with service level agreements to identify any capacity issues and specifies any required changes • Provides advice to support the design of service components, including designing in flexible and scalable capacity • Works with business representatives to agree and implement short- and medium-term modifications to capacity • Drafts and maintains standards and procedures for service component capacity management • Ensures the correct implementation of standards and procedures
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 organizational 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 organization 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 organization. • 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.

Digital Forensics DGFS	Level 5
Recovering and investigating material found in digital devices.	• Leads investigations to correctly gather, analyse and present findings, including digital evidence, to both business and legal audiences. • Collates conclusions and recommendations and presents forensic findings to stakeholders. • Plans and manages digital forensics activities within the organization. Provides expert advice on digital forensics. • Contributes to the development of digital forensics policies, standards and guidelines. Evaluates and selects digital forensics tools and techniques.

Cybercrime Investigation CRIM	Level 5
Investigates cybercrimes, collects evidence, determines incident impacts and collaborates with legal teams to protect digital assets.	• Manages complex cybercrime investigations, overseeing all stages from detection to resolution. • Evaluates incidents involving advanced threats or significant breaches. • Develops and implements procedures for evidence handling and documentation. Collaborates with legal teams to ensure evidence supports potential legal proceedings. • Leads the development of response strategies, assessing vulnerabilities and operational capabilities. Oversees the implementation of tools and automation to enhance investigative processes.

People and Skills

People Management

Learning and Development Management ETMG	Level 5
Delivering management, advisory and administrative services to support the development of knowledge, skills and competencies.	• Manages the provision of learning and development, ensuring optimum use of resources • Maintains, publicises and promotes a catalogue of learning and development activities. Ensures that courses are up to date and accredited (when required) • Arranges facilities and schedules with learning and development providers as appropriate • Uses data to assess and improve the effectiveness of learning or educational activities

Relationship and Engagement

Stakeholder Management

Sourcing SORC	Level 5
Managing, or providing advice on, the procurement or commissioning of products and services.	• Plans and manages procurement activities • Manages tender, evaluation and acquisition processes. Researches suppliers and markets, and maintains a broad understanding of the commercial environment, to inform and develop commercial strategies and sourcing plans • Advises on the business case for alternative sourcing models. Advises on policy and procedures covering tendering, the selection of suppliers and procurement • Negotiates with potential partners and suppliers, developing acceptance criteria and procedures. Drafts and places contracts

Supplier Management SUPP	Level 5
Aligning the organization'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 controlling the operation of formal contracts for the supply of products and services	• 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
Stakeholder Relationship Management RLMT	**Level 5**
Influencing stakeholder attitudes, decisions, and actions for mutual benefit.	• 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

Following the completion of a CGRC training course, a practitioner could reasonably be expected to have been provided with 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 CGRC training course will contribute to the provision of the relevant knowledge a practitioner would require for the performance of a role, job or function. This table indicates the SFIA skills relevant to the knowledge provided in the training course.

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 organization. Develops organizational taxonomy for information assets. Provides expert advice and guidance to enable the organization to get maximum value from its information assets. • Assesses issues that might prevent the organization from making maximum use of its information assets. Contributes to the development of policy, standards and procedures for compliance with relevant legislation.

Security 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 organizational 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 organizational 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 organization'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 organization's contact for relevant regulatory authorities and ensures proper relationships between the organization and external stakeholders

Risk Management BURM	Level 5
Planning and implementing processes for managing risk across the enterprise, aligned with organizational 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 organization'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 organization.	• 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 organizational 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 organization’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 organizational 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 organizational control mechanisms. • Oversees the assurance activities of others, providing advice and expertise to support assurance activity.

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 organization 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 organizational policies, standards and guidelines for non-functional testing.

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.

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
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.

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.

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.

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 organization • 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

Systems Security Certified Practitioner
ISC2 Certification

Following the completion of a SSCP training course, a practitioner could reasonably be expected to have been provided with 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 SSCP training course will contribute to the provision of the relevant knowledge a practitioner would require for the performance of a role, job or function. This table indicates the SFIA skills relevant to the knowledge provided in the training course.

Strategy and Architecture

Strategy and Planning

Information Management IRMG	Level 4
Developing, implementing and testing a business continuity framework.	• Enables the organization to organise, control and discover information assets. • Supports the organization 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 organization.

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 organization or domain measures • Establishes the requirement for accreditation evidence from delivery partners and communicates accreditation requirements to stakeholders • Contributes to planning and organization 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 organizational 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 of the effectiveness of processes, the controls, and the compliance environment of an organization.	• 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

Programming/Software Development PROG	Level 4
Developing software components to deliver value to stakeholders.	• Designs, codes, verifies, tests, documents, amends and refactors complex programs/scripts and integration software services. • Contributes to the selection of the software development methods, tools, techniques, and security practices. • Applies agreed standards, tools, and security measures to achieve well-engineered outcomes. • Participates in reviews of own work and leads reviews of colleagues' work.
Non-functional Testing NFTS	**Level 4**
Assessing systems and services to evaluate performance, security, scalability and other non-functional qualities against requirements or expected standards.	• Designs detailed functional test cases and scripts, covering various scenarios and boundary values. • Actively participates in requirement and design reviews, refining test plans based on insights gained. • Undertakes structured exploratory testing to investigate and verify functionality. • Prepares test data, configures environments and automates repeatable tests. Executes tests, logs defects with detailed information and analyses results to assess system functionality.
Radio Frequency Engineering RFEN	**Level 3**
Designing, installing and maintaining radio frequency based devices and software.	• Deploys, sets up, tunes and calibrates RF devices and software following maintenance schedules and using appropriate tools and test equipment • Incorporates hardware/firmware modifications. Interprets automatic fault/performance indications and resolves faults down to discrete component level or escalates according to given procedures • Implements communication protocols between system elements in accordance with defined standards • Integrates RF devices with software applications, incorporating dynamic reconfiguration of elements under software control to optimise their operational performance

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 for specific subsets of data. • Assesses the integrity of data from multiple sources. • Advises on transformation of data between formats or media. Maintains and implements data handling procedures. • Enables data availability, integrity and searchability through formal data and metadata structures and protection measures.

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.

Configuration Management CFMG	Level 3
Planning, identifying, controlling, accounting for and auditing of configuration items (CIs) and their interrelationships.	• Plans the capture and management of CIs and related information. • Agrees scope of configuration management processes and the configuration items (CIs) and related information to be controlled. • Identifies, evaluates and manages the adoption of appropriate tools, techniques and processes (including automation) for configuration management. • Contributes to the development of configuration management strategies, policies, standards and guidelines.
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.
Facilities Management DCMA	**Level 3**
Planning, designing and managing the buildings, space and facilities which, collectively, make up the IT estate.	• Monitors compliance against agreed processes and investigates, assesses and resolves incidents of non-compliance, escalating where necessary. • Processes physical access requests, monitors access control systems and reports on access-related activities.

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.
Change Control CHMG	**Level 3**
Assessing risks associated with proposed changes and ensuring changes to products, services or systems are controlled and coordinated.	• Develops, documents and implements changes based on requests for change. • Applies change control processes and procedures. • Applies tools, techniques and processes to manage and report on change requests.
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

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 specialised 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 organizational policies and industry standards. Develops procedures for handling emerging technologies in forensic contexts. • Contributes to forensic reports detailing technical findings.
Cybercrime Investigation CRIM	**Level 4**
Investigates cybercrimes, collects evidence, determines incident impacts and collaborates with legal teams to protect digital assets.	• Oversees mid-level investigations, coordinating evidence collection and forensic analyses. • Assesses target vulnerabilities and operational impacts of cyber incidents. • Provides comprehensive reports and expert analysis for stakeholders. • Conducts interviews and interrogations, identifying potential legal implications and collaborating with legal professionals.
Penetration Testing PENT	**Level 3**
Testing the effectiveness of security controls by emulating the tools and techniques of likely attackers.	• Follows standard approaches to design and execute penetration testing activities • Researches and investigates attack techniques and recommend ways to defend against them. • Analyses and reports on penetration testing activities, results, issues and risks

People and Skills

Stakeholder Management

Learning Delivery ETDL	Level 3
Transferring knowledge, developing skills and changing behaviours using a range of techniques, resources and media.	• Delivers learning activities to various audiences using prepared materials aligned with established learning objectives. • Follows established guidelines to prepare the learning environment. Assists in developing and maintaining relevant examples and case studies. • Uses a range of delivery techniques to develop learner skills and knowledge. • Observes learners performing practical activities and work. Advises and assists where necessary. Provides detailed instruction where necessary and responds to questions, seeking advice in exceptional conditions beyond own experience.

3. Ancillary SFIA Skills

The table below shows the ancillary view illustrating how the knowledge gained from the CISSP, CSSLP, CCSP and CGRC training course map directly to SFIA skills at levels of responsibility below SFIA Level 5 as shown in the Primary view in Section 2.

			CISSP	CSSLP	CCSP	CGRC
Cybersecurity Architecture	Solution Architecture	ARCH	4			
Cybersecurity Research and Intelligence	Vulnerability Research	VURE		4		
	Threat Intelligence	THIN	4	4		
Cybersecurity Governance, Risk and Compliance	Information Management	IRMG	4		4	
Secure Software and Systems Development	Systems and Software Lifecycle Engineering	SLEN			4	
	Systems Design	DESN			4	
	Non-functional Testing	NFTS			4	
	Software Configuration	PORT	4			
	Penetration Testing	PENT	4			
Secure Infrastructure	Infrastructure Operations	ITOP				4
	Configuration Management	CFMG	4	4		
Cybersecurity Resilience	Security Operations	SCAD		4		
	Change Control	CHMG	4			
	Asset Management	ASMG				4
	Digital Forensics	DGFS	4			
	Offensive Cyber Operations	OCOP	4			