ISC2 Certification Mappings to the Skills Framework for the Information Age (SFIA)

12 June 2024 | Document One

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, ISC2 offers a portfolio of credentials that are part of a holistic, pragmatic approach to security. Our association of candidates, associates and members, more than 450,000 strong, is made up of certified cyber, information, software and infrastructure security professionals who are making a difference and helping to advance the industry. Our vision is supported by our commitment to educate and reach the general public through our charitable foundation – The Center for Cyber Safety and Education™.

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

The **CSSLP** is ideal for software development and security professionals responsible for applying best practices to each phase of the software development lifecycle (SDLC). It shows advanced knowledge and the technical skills to effectively design, develop and implement security practices within each phase of the software lifecycle. Jobs that typically use or require the CSSLP include Software Program Manager, IT Director/Manager, Security Manager, Software Architect, Application Security Specialist, Software Engineer, Project Manager and Quality Assurance Tester.

The **CCSP** is ideal for IT and information security leaders seeking to prove their understanding of cybersecurity and securing critical assets in the cloud. It shows advanced technical skills and knowledge to design, manage and secure data, applications and infrastructure in the cloud. Jobs that typically use or require the **CCSP** include Security Architect, Security Manager, Systems Architect, Systems Engineer, Security Consultant, Security Engineer and Security Administrator.

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

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

This document will assist information security practitioners to understand the ISC2 certification mappings to the Skills Framework for the Information Age (SFIA).

Introduction

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

The CISSP and CSSLP certification covers the security aspects of SFIA skills at levels 5-6. The CCSP certification covers the security aspects of SFIA skills at level 5, and the SSCP certification covers SFIA skills at levels 3-4. The certification exam assesses knowledge of these skill attributes and tests against the application of these knowledge areas through scenario-based items.

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

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

2. Primary SFIA Skills

Primary SFIA skills are those which have attributes that can be clearly mapped to the knowledge and skills relevant to the ISC2 certifications.

			🟩	🟨	🟦	🟧
Skills for Security Professionals	Information Security	SCTY	6	5	5	4
	Governance	GOVN	6			
	Risk Management	BURM	5	5	5	3
	Audit	AUDT	5	5	5	4
	Information Assurance	INAS	5		5	4
	Continuity Management	COPL	5		5	4
	Incident Management	USUP	5	5	5	4
	Security Operations	SCAD	5		5	4
	Vulnerability Assessment	VUAS	5	5	5	4
	Digital Forensics	DGFS				4
	Service Level Management	SLMO		5	5	
	Personal Data Protection	PEDP	5	5	5	
Secure Software Development	System and Software Lifecycle Engineering	SLEN	5	6		
	Requirements Definition and Management	REQM		5		
	Solution Architecture	ARCH		5	5	
	Testing	TEST		5		3
Secure Infrastructure	IT Infrustructure	ITOP			5	4
	Network Support	NTAS	5			4
	Asset Management	ASMG	5			4
	Storage Management	STMG	5		5	4
	Supplier Management	SUPP		5	5	
	System Software	SYSP	5	5	5	
	Contract Management	ITCM			5	
Other Security Related Skills	Information Management	IRMG		5		4
	Data Management	DATM	5		5	4

CISSP

CISSP® Certified Information Systems Security Professional
ISC2 Certification

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

Strategy and Architecture

Strategy and Planning

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.

Strategy and Privacy

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

Information Assurance INAS	**Level 5**
Protecting against and managing risks related to the use, storage and transmission of data and information systems.	• Interprets information assurance and security policies and applies these to manage risks • Provides advice and guidance to ensure adoption of and adherence to information assurance architectures, strategies, policies, standards and guidelines • Plans, organises and conducts information assurance and accreditation of complex 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 operating a framework of controls and management strategies to promote compliance with personal data legislation.	• Contributes to the development of policy, standards and guidelines related to personal data legislation • Provides expert advice and guidance on implementing personal data legislation controls in products, services and systems. Investigates major data breaches and recommends appropriate control improvements • Creates and maintains an inventory of data that are subject to personal data legislation. Conducts risk assessments, business impact analysis for complex information systems and specifies any required changes • Ensures that formal requests and complaints are dealt with according to approved procedures. Prepares and submits reports and registrations to relevant authorities

Governance, Risk and Compliance

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

Risk Management BURM	Level 5
Planning and implementing organisation-wide processes and procedures for the management of risk to the success or integrity of the enterprise.	• Plans and implements complex and substantial risk management activities within a specific function, technical area, project or programme • Implements consistent and reliable risk management processes and reporting to key stakeholders • Engages specialists and domain experts as necessary • Advises on the organisation’s approach to risk management

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

Development and Implementation

Systems Development

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

Data and Analytics

Data Management DATM	**Level 5**
Developing and implementing plans, policies, and practices that control, protect and optimise the value of data assets.	• Devises and implements master data management processes. • Derives data management structures and metadata to support consistency of information retrieval, combination, analysis, pattern recognition and interpretation, throughout the organisation • Plans effective data storage, sharing and publishing within the organisation • Independently validates external information from multiple sources • Assesses issues that might prevent the organisation from making maximum use of its information assets • Provides expert advice and guidance to enable the organisation to get maximum value from its data assets

Delivery and Operation

Technology Management

Storage Management STMG	**Level 5**
Planning, implementing and optimising the technologies and processes used for data storage.	• 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

System Software SYSP	**Level 5**
Installing, managing, controlling, deploying and maintaining infrastructure systems software, to meet operational needs and service levels.	• Ensures that system software is provisioned and configured to facilitate the achievement of service objectives • Evaluates new system software and recommends adoption if appropriate. Plans the provisioning and testing of new versions of system software • Investigates and coordinates the resolution of potential and actual service problems • Ensures that operational procedures and diagnostics for system software are current, accessible and well understood

Network Support NTAS	Level 5
Providing maintenance and support services for communications networks.	• Drafts and maintains procedures and documentation for network support and operation • Makes a significant contribution to the investigation, diagnosis and resolution of network problems • Ensures that all requests for support are dealt with according to set standards and procedures

Service Management

Incident Management USUP	Level 5
Coordinating responses to incident reports, minimising negative impacts and restoring service as quickly as possible.	• Develops, maintains and tests incident management procedures in agreement with service owners • Investigates escalated, non-routine and high-impact incidents to responsible service owners and seeks resolution • Facilitates recovery, following resolution of incidents. Ensures that resolved incidents are properly documented and closed • Analyses causes of incidents, and informs service owners to minimise probability of recurrence, and contributes to service improvement • Analyses metrics and reports on the performance of the incident management process

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
Delivering management, technical and administrative services to implement security controls and security management strategies.	• Monitors the application and compliance of security operations procedures • Reviews actual or potential security breaches and vulnerabilities and ensures that they are promptly and thoroughly investigated • Recommends actions and appropriate control improvements • Ensures that security records are accurate and complete and that requests for support are deal with according to agreed procedures • Contributes to the creation and maintenance of policy, standards, procedures and documentation for security

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

CSSLP

CSSLP Certified Secure Software Lifecycle Professional
ISC2 Certification

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

Strategy and Architecture

Strategy and Planning

Information Management IRMG	**Level 5**
Planning, implementing and controlling the full life cycle management of digitally organised information and records.	• Ensures implementation of information and records management policies and standard practice • Communicates the benefits and value of information, both internal and external, that can be mined from business systems and elsewhere • Reviews new change proposals and provides specialist advice on information and records management. Assesses and manages information-related risks • 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 that appropriate technical resources are made available • Ensures that 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 that relevant technical strategies, policies, standards and practices (including security) are applied correctly

Security and Privacy

Information Security SCTY	Level 5
Defining and operating a framework of security controls and security management strategies.	• Develops and communicates corporate information security policy, standards and guidelines • Ensures architectural principles are applied during design to reduce risk • Drives adoption and adherence to policy, standards and guidelines • Contributes to the development of organisational strategies that address information control requirements • Identifies and monitors environmental and market trends and proactively assesses impact on business strategies, benefits and risks • Leads the provision of authoritative advice and guidance on the requirements for security controls in collaboration with subject matter experts

Personal Data Protection PEDP	Level 5
Implementing and operating a framework of controls and management strategies to promote compliance with personal data legislation.	• Contributes to the development of policy, standards and guidelines related to personal data legislation • Provides expert advice and guidance on implementing personal data legislation controls in products, services and systems • Investigates major data breaches and recommends appropriate control improvements • Creates and maintains an inventory of data that are subject to personal data legislation. Conducts risk assessments, business impact analysis for complex information systems and specifies any required changes • Ensures that formal requests and complaints are dealt with according to approved procedures. Prepares and submits reports and registrations to relevant authorities

Governance, Risk and Compliance

Risk Management BURM — Level 5

Planning and implementing organisation-wide processes and procedures for the management of risk to the success or integrity of the enterprise.

- Plans and implements complex and substantial risk management activities within a specific function, technical area, project or programme
- Implements consistent and reliable risk management processes and reporting to key stakeholders
- Engages specialists and domain experts as necessary
- Advises on the organisation’s approach to risk management

Audit AUDT — Level 5

Delivering independent, risk-based assessments of the effectiveness of processes, the controls, and the compliance environment of an organisation.

- Plans, organises and conducts audits of complex domain areas, cross-functional areas, and across the supply chain
- Confirms the scope and objectives of specific audit activity with management. Aligns with the scope of the audit program and organisational policies
- Determines appropriate methods of investigation to achieve the audit objectives. Presents audit findings to management describing the effectiveness and efficiency of control mechanisms
- Provides general and specific audit advice. Collaborates with professionals in related specialisms to develop and integrate findings

Change and Transformation

Change Analysis

Requirements Definition and Management REQM — Level 5

Managing requirements through the entire delivery and operational life cycle.

- Plans and drives scoping, requirements definition and prioritisation activities for large, complex initiatives
- Selects, adopts and adapts appropriate requirements definition and management methods, tools and techniques
- Contributes to the development of organisational methods and standards for requirements management
- Obtains input from, and agreement to requirements from a diverse range of stakeholders. Negotiates with stakeholders to manage competing priorities and conflicts
- Establishes requirements baselines
- Ensures changes to requirements are investigated and managed

Development and Implementation

Systems Development

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

Testing TEST	**Level 5**
Investigating products, systems and services to assess behaviour and whether these meet specified or unspecified requirements and characteristics.	• Plans and drives testing activities across all stages and iterations of product, systems and service development • Provides authoritative advice and guidance on any aspect of test planning and execution. Adopts and adapts appropriate testing methods, automated tools and techniques to solve problems in tools and testing approaches • Measures and monitors applications of standards for testing. Assesses risks and takes preventative action • Identifies improvements and contributes to the development of organisational policies, standards, and guidelines for testing

Delivery and Operation

Technology Management

System Software SYSP	**Level 5**
Installing, managing, controlling, deploying and maintaining infrastructure systems software, to meet operational needs and service levels.	• Ensures that system software is provisioned and configured to facilitate the achievement of service objectives • Evaluates new system software and recommends adoption if appropriate. Plans the provisioning and testing of new versions of system software • Investigates and coordinates the resolution of potential and actual service problems • Ensures that operational procedures and diagnostics for system software are current, accessible and well understood

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 incident reports, minimising negative impacts and restoring service as quickly as possible.	• Develops, maintains and tests incident management procedures in agreement with service owners • Investigates escalated, non-routine and high-impact incidents to responsible service owners and seeks resolution • Facilitates recovery, following resolution of incidents. Ensures that resolved incidents are properly documented and closed • Analyses causes of incidents, and informs service owners to minimise probability of recurrence, and contributes to service improvement • Analyses metrics and reports on the performance of the incident management process

Security Services

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

Relationship and Engagement

Stakeholder Management

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

CCSP

CCSP Certified Cloud Security Professional
ISC2 Certification

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

Strategy and Architecture

Strategy and Planning

Solution Architecture ARCH	**Level 5**
Developing and communicating a multi-dimensional solution architecture to deliver agreed business outcomes.	• Leads the development of solution architectures in specific business, infrastructure or functional areas • Leads the preparation of technical plans and ensures that 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 that relevant technical strategies, policies, standards and practices (including security) are applied correctly

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

Security and Privacy

Information Security SCTY	Level 5
Defining and operating a framework of security controls and security management strategies.	• Develops and communicates corporate information security policy, standards and guidelines • Ensures architectural principles are applied during design to reduce risk • Drives adoption and adherence to policy, standards and guidelines • Contributes to the development of organisational strategies that address information control requirements • Identifies and monitors environmental and market trends and proactively assesses impact on business strategies, benefits and risks • Leads the provision of authoritative advice and guidance on the requirements for security controls in collaboration with subject matter experts

Information Assurance INAS	Level 5
Protecting against and managing risks related to the use, storage and transmission of data and information systems.	• Interprets information assurance and security policies and applies these to manage risks • Provides advice and guidance to ensure adoption of and adherence to information assurance architectures, strategies, policies, standards and guidelines • Plans, organises and conducts information assurance and accreditation of complex 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 operating a framework of controls and management strategies to promote compliance with personal data legislation.	• Contributes to the development of policy, standards and guidelines related to personal data legislation • Provides expert advice and guidance on implementing personal data legislation controls in products, services and systems. Investigates major data breaches and recommends appropriate control improvements • Creates and maintains an inventory of data that are subject to personal data legislation. Conducts risk assessments, business impact analysis for complex information systems and specifies any required changes • Ensures that formal requests and complaints are dealt with according to approved procedures. Prepares and submits reports and registrations to relevant authorities

Governance, Risk and Compliance

Risk Management BURM — Level 5

Planning and implementing organisation-wide processes and procedures for the management of risk to the success or integrity of the enterprise.

- Plans and implements complex and substantial risk management activities within a specific function, technical area, project or programme
- Implements consistent and reliable risk management processes and reporting to key stakeholders
- Engages specialists and domain experts as necessary
- Advises on the organisation’s approach to risk management

Audit AUDT — Level 5

Delivering independent, risk-based assessments of the effectiveness of processes, the controls, and the compliance environment of an organisation.

- Plans, organises and conducts audits of complex domains areas, cross-functional areas, and across the supply chain
- Confirms the scope and objectives of specific audit activity with management
- Aligns with the scope of the audit program and organisational policies
- Determines appropriate methods of investigation to achieve the audit objectives
- Presents audit findings to management describing the effectiveness and efficiency ofcontrol 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 of data assets.

- Devises and implements master data management processes
- Derives data management structures and metadata to support consistency of information retrieval, combination, analysis, pattern recognition and interpretation, throughout the organisation
- Plans effective data storage, sharing and publishing within the organisation
- Independently validates external information from multiple sources
- Assesses issues that might prevent the organisation from making maximum use of its information assets
- Provides expert advice and guidance to enable the organisation to get maximum value from its data assets

Delivery and Operation

Technology Management

IT Infrastructure ITOP	Level 5
Deploying, configuring and operating IT Infrastructure.	• Provides technical leadership to optimise the performance of IT infrastructure • Investigates and manages the adoption of tools, techniques and processes (including automation) for the management of systems and services • 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 that operational procedures and documentation are fit for purpose and kept up to date • Ensures that operational issues are identified, recorded, monitored and resolved • Provides appropriate status and other reports to specialists, users and managers
System Software SYSP	**Level 5**
Installing, managing, controlling, deploying and maintaining infrastructure systems software, to meet operational needs and service levels.	• Ensures that system software is provisioned and configured to facilitate the achievement of service objectives • Evaluates new system software and recommends adoption if appropriate • Plans the provisioning and testing of new versions of system software • Investigates and coordinates the resolution of potential and actual service problems. • Ensures that operational procedures and diagnostics for system software are current accessible and well understood
Storage Management STMG	**Level 5**
Planning, implementing and optimising the technologies and processes used for data storage.	• 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

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 incident reports, minimising negative impacts and restoring service as quickly as possible.	• Develops, maintains and tests incident management procedures in agreement with service owners • Investigates escalated, non-routine and high-impact incidents to responsible service owners and seeks resolution • Facilitates recovery, following resolution of incidents • Ensures that resolved incidents are properly documented and closed • Analyses causes of incidents and informs service owners to minimise probability of recurrence, and contributes to service improvement • Analyses metrics and reports on the performance of the incident management process

Security Services

Security Operations SCAD	Level 5
Delivering management, technical and administrative services to implement security controls and security management strategies.	• Monitors the application and compliance of security operations procedures • Reviews actual or potential security breaches and vulnerabilities and ensures they are promptly and thoroughly investigated • Recommends actions and appropriate control improvements • Ensures security records are accurate and complete and that requests for support are dealt with according to agreed procedures • Contributes to the creation and maintenance of policy, standards, procedures and documentation for security

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

Relationship and Engagement

Stakeholder Management

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

Contract Management ITCM	Level 5
Managing and 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

SSCP

SSCP. Systems Security Certified Practitioner
ISC2 Certification

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

Strategy and Architecture

Strategy and Planning

Information Management IRMG	**Level 4**
Planning, implementing and controlling the full life cycle management of digitally organised information and records.	• Supports the implementation of information and records management policies and standard practice • Monitors the implementation of effective controls for internal delegation, audit and control relating to information and records management • Reports on the consolidated status of information controls to inform effective decision-making • Identifies risks around the use of information • Recommends remediation actions as required
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

Security and Privacy

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

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

Governance, Risk and Compliance

Risk Management BURM	Level 3
Planning and implementing organisation-wide processes and procedures for the management of risk to the success or integrity of the enterprise.	• Undertakes basic risk management activities • Maintains documentation of risks, threats, vulnerabilities and mitigation actions

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

Development and Implementation

Systems Development

Testing TEST	**Level 3**
Investigating products, systems and services to assess behaviour and whether these meet specified or unspecified requirements and characteristics.	• Designs test cases and test scripts under own direction, mapping back to pre-determined criteria, recording and reporting test outcomes • Participates in requirement, design and specification reviews, and uses this information to design test plans and test conditions • Applies agreed standards to specify and perform manual and automated testing • Automates testing tasks and builds test coverage through existing or new infrastructure • Analyses and reports on test activities, results, issues and risks

Data and Analytics

Data Management DATM	**Level 4**
Developing and implementing plans, policies, and practices that control, protect and optimise the value of data assets.	• Devises and implements master data management processes for specific subsets of data • Assesses the integrity of data from multiple sources • Provides advice on the transformation of data from one format/medium to another • Maintains and implements information handling procedures • Enables the availability, integrity and searchability of information through the application of formal data and metadata structures and protection measures

Delivery and Operation

Technology Management

IT Infrastructure ITOP — Level 4

Deploying, configuring and operating IT Infrastructure.

- Provides technical expertise to enable the correct application of operational procedures
- Contributes to the planning and implementation of infrastructure maintenance and updates. Implements agreed upon infrastructure changes and maintenance routines
- Uses infrastructure management tools to determine load and performance statistics. Configures tools and/or creates scripts to automate the provisioning, testing and deployment of new and changed infrastructure
- Maintains operational procedures and checks that they are executed following agreed standards
- Investigates and enables the resolution of operational issues
- Provides reports and proposals for improvement, to specialists, users and managers

Network Support NTAS — Level 4

Installing, managing, controlling, deploying and maintaining infrastructure systems software, to meet operational needs and service levels.

- Maintains the network support process and checks that all requests for support are dealt with according to agreed upon procedures
- Ensures network configurations are applied to meet operational requirements in line with agreed upon procedures
- Uses network management software and tools to investigate and diagnose network problems, collect performance statistics and create reports

Storage Management STMG — Level 4

Planning, implementing and optimising the technologies and processes used for data storage.

- Prepares and maintains operational procedures for storage management
- Monitors capacity, performance, availability and other operational metrics
- Takes appropriate action to ensure corrective and proactive maintenance of storage and backup systems to protect and secure business information
- Creates reports and proposals for improvement
- Contributes to the planning and implementation of new installations and scheduled maintenance and changes of existing systems

Service Management

Incident Management USUP	Level 4
Coordinating responses to incident reports, minimising negative impacts and restoring service as quickly as possible.	• Ensures that incidents are handled according to agreed procedures • Prioritises and diagnoses incidents. Investigates causes of incidents and seeks resolution. Escalates unresolved incidents • Facilitates recovery, following resolution of incidents • Documents and closes resolved incidents • Contributes to testing and improving incident management procedures

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

Delivery and Operation

Security Services

Security Operations SCAD	**Level 4**
Delivering management, technical and administrative services to implement security controls and security management strategies.	• Maintains operational security processes and checks that all requests for support are dealt with according to agreed procedures • Provides advice on defining access rights and the application and operation of elementary physical, procedural and technical security controls • Investigates security breaches in accordance with established procedures and recommends required actions • Provides support and checks that corrective actions are implemented

Vulnerability Assessment VAUS	**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 investigations on devices • Specifies requirements for resources and tools to perform investigations • Processes and analyses evidence in line with policy, standards and guidelines and supports the production of forensics findings and reports

3. Secondary SFIA Skills

Secondary SFIA skills are those which have attributes that can be partially mapped to the Common Body of Knowledge (CBK) for each respective ISC2 certification.

			CISSP	CSSLP	CCSP	SSCP
Security Programmes	Learning Delivery	ETDL				3
	Learning Development and Management	ETMG	5	5	5	
	Stakeholder Relationship Management	RLMT		5	5	
Security Software Development	Systems Development Management	DLMG		5		
	Systems Design	DESN	5	5		
	Software Design	SWDN	5	5		
	Programming/Software Development	PROG		5		4
	Systems Integration and Build	SINT		5		
	Release and Deployment	RELM		5		
	Change Control	CHMG				3
Secure Infrastructure	Technology Service Management	ITMG	5		5	
	Network Design	NTDS	5			
	Capacity Management	CRMG			5	
	Configuration Management	CFMG				3
	Systems Installation and Removal	HSIN		5		
	Sourcing	SORC			5	
	Radio Frequency Engineering	RFEN				3
	Facilities Management	DCMA	5			3
Security Practice Management	Employee Experience	EEXP	5			
	Resourcing	RESC	5			
Other Security Related Skills	Methods and Tools	METL	5			

4. Ancillary SFIA Skills

Ancillary SFIA skills have been mapped to the CISSP, CSSLP and CCSP Common Body of Knowledge (CBK) and have attributes below the knowledge required for SFIA level 5.

			🟩	🟨	🟦
Skills for Security Professionals	Problem Management	PBMG		4	
	Vulnerability Research	VURE	4		
	Threat Intelligence	THIN	4	4	
	Security Operations	SCAD		4	
	Digital Forensics	DGFS	4	4	4
	Penetration Testing	PENT	4	4	
Security Software Development	Solution Architecture	ARCH	4		
	Systems Design	DESN			4
	Programming/Software Development	PROG			3
	Testing	TEST	4		4
	Software Configuration	PORT	4		3
	Systems Intergration and Build	SINT			3
	Release and Deployment	RELM			3
	Change Control	CHMG	4		
Secure Infrastructure	Configuration Management	CFMG	4	4	
	Sourcing	SORC		4	
	Supplier Management	SUPP	4		
	Facilities Management	DCMA			4
Security Practice Management	Quality Assurance	QUAS			3
Other Security Related Skills	Information Management	IRMG	4		4