# ISC2 Training Course Mappings to the Skills Framework for the Information Age (SFIA)



12 June 2024 | 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 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 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 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, 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, 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 training covers the security aspects of SFIA skills at levels 5-6. The CCSP 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. Primary SFIA Skills

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

| | | | | | | |
|---|---|---|---|---|---|---|
| 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 | 5 | 4 |
| | Continuity Management | COPL | 5 | 5 | 5 | 4 |
| | Incident Management | USUP | 5 | 5 | 5 | 4 |
| | Problem Management | PBMG | | 5 | | |
| | Security Operations | SCAD | 5 | | 5 | 4 |
| | Vulnerability Assessment | VUAS | 5 | | 5 | 4 |
| | Digital Forensics | DGFS | | 5 | 5 | 4 |
| | System Software | SYSP | 5 | 5 | 5 | 3 |
| | Penetration Testing | PENT | | 5 | | 3 |
| | Service Level Management | SLMO | | 5 | 5 | |
| | Personal Data Protection | PEDP | 5 | 5 | 5 | |
| Security Programmes | Learning Delivery | ETDL | | | | 3 |
| | Learning and Development Management | ETMG | 5 | 5 | 5 | |
| | Stakeholder Relationship Management | RLMT | | | 5 | |
| Secure Software Development | Systems Development Management | DLMG | | 5 | | |
| | Systems and Software Lifecycle Engineering | SLEN | 5 | 6 | | |
| | Requirements Definition and Management | REQM | | 5 | | |
| | Solution Architecture | ARCH | | 5 | 5 | |
| | Systems Design | DESN | 5 | 5 | | |
| | Software Design | SWDN | 5 | 5 | | |
| | Database Design | DBDS | | 5 | | |

Continued

| | | | | | | |
|---|---|---|---|---|---|---|
| | Programming/Software Development | PROG | | 5 | | 4 |
| | Testing | TEST | 5 | 5 | | 3 |
| | Systems Integration and Build | SINT | | 5 | | |
| | Release and Deployment | RELM | | 5 | | |
| | Change Control | CHMG | | | | 3 |
| Secure Infrastructure | Technology Service Management | ITMG | 5 | | 5 | |
| | IT Infrastructure | ITOP | | | 5 | 3 |
| | Network Design | NTDS | 5 | | | |
| | Network Support | NTAS | 5 | | | 4 |
| | Asset Management | ASMG | 5 | | | 4 |
| | Capacity Management | CPMG | | | 5 | |
| | Configuration Management | CFMG | | | | 3 |
| | Systems Installation and Removal | HSIN | | 5 | | |
| | Storage Management | STMG | 5 | | 5 | 4 |
| | Sourcing | SORC | | 5 | 5 | |
| | Radio Frequency Engineering | RFEN | | | | 3 |
| | Supplier Management | SUPP | 5 | 5 | 5 | |
| | Contract Management | ITCM | | | 5 | |
| | Facilities Management | DCMA | 5 | | 5 | 3 |
| Security Practice Management | Employee Experience | EEXP | 5 | | | |
| | Resourcing | RESC | 5 | | | |
| Other Security Related Skills | Methods and Tools | METL | 5 | | | |
| | Acceptance Testing | BPTS | 5 | | | |
| | Information Management | IRMG | | 5 | | 4 |
| | Data Management | DATM | 5 | 5 | 5 | 4 |

# 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 Planning

| **Continuity Management COPL** | **Level 5** |
|---|---|
| Developing, implementing and testing a business continuity framework. | • Manages the development, implementation and testing of continuity management plans<br>• Manages the relationship with individuals and teams who have authority for critical business processes and supporting systems<br>• Evaluates the critical risks and identifies priority areas for improvement<br>• 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<br>• Ensures architectural principles are applied during design to reduce risk. Drives adoption and adherence to policy, standards and guidelines<br>• 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<br>• 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<br>• Provides advice and guidance to ensure adoption of and adherence to information assurance architectures, strategies, policies, standards and guidelines<br>• Plans, organises and conducts information assurance and accreditation of complex domains areas, cross-functional areas, and across the supply chain<br>• 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<br>• 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<br>• Creates and maintains an inventory of data that are subject to personal data legislation<br>• Conducts risk assessments, business impact analysis for complex information systems and specifies any required changes<br>• Ensures that formal requests and complaints are dealt with according to approved procedures.<br>• 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<br>• Within a defined area of accountability, determines the requirements for appropriate governance reflecting the organisation's values, ethics and wider governance frameworks<br>• Communicates delegated authority, benefits, opportunities, costs, and risks<br>• Leads reviews of governance practices with appropriate and sufficient independence from management activity<br>• 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<br>• Implements consistent and reliable risk management processes and reporting to key stakeholders<br>• Engages specialists and domain experts as necessary<br>• 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<br>• Confirms the scope and objectives of specific audit activity with management. Aligns with the scope of the audit programme and organisational policies<br>• Determines appropriate methods of investigation to achieve the audit objectives. Presents audit findings to management describing the effectiveness and efficiency of control mechanisms<br>• 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 |
|---|---|
| Ensuring methods and tools are adopted and used effectively throughout the organisation. | • Provides advice, guidance and expertise to promote adoption of methods and tools and adherence to policies and standards<br>• Evaluates and selects appropriate methods and tools in line with agreed policies and standards<br>• Contributes to organisational policies, standards, and guidelines for methods and tools<br>• 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 |

## Change and Transformation

### Change Analysis

| 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<br>• 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<br>• Ensure tests and results are documented, analysed and reported to stakeholders, and required actions taken. Highlights issues and risks identified during testing to stakeholders<br>• 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<br>• Supports deployment of the working environment for systems and software life cycle working practices<br>• Provides effective feedback to encourage development of the individuals and teams responsible for systems and software life cycle working practices<br>• Provides guidance and makes suggestions to support continual improvement and learning approaches<br>• Contributes to identifying new domains within the organisation 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<br>• Ensures that the system design balances functional and non-functional requirements<br>• Reviews systems designs and ensures that appropriate methods, tools and techniques are applied effectively<br>• Makes recommendations and assesses and manages associated risks<br>• Adopts and adapts system design methods, tools and techniques<br>• Contributes to development of system design policies, standards and selection of architecture components |
| Software Design **SWDN** | **Level 5** |
| Specifying and designing software to meet defined requirements by following agreed design standards and principles. | • Specifies and designs large or complex software applications, components and modules<br>• 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<br>• Evaluates software designs to ensure adherence to standards and identifies corrective action<br>• Ensures that the software design balances functional, quality, security and systems management requirements<br>• Contributes to the development of organisational software design and architecture policies and standards |
| Network Design **NTDS** | **Level 5** |
| Designing communication networks to support strategic and operational requirements and producing network strategies, architectures, policies and related documentation. | • Produces, or approves network providers', network architectures, topologies and configuration databases for own area of responsibility<br>• Specifies design parameters for network connectivity, capacity, speed, interfacing, security and access, in line with business requirements<br>• Assesses network-related risks and specifies recovery routines and contingency procedures<br>• Creates multiple design views to address the different stakeholders' concerns and to handle both functional and non-functional requirements |

| 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<br>• Provides authoritative advice and guidance on any aspect of test planning and execution<br>• Adopts and adapts appropriate testing methods, automated tools and techniques to solve problems in tools and testing approaches<br>• Measures and monitors applications of standards for testing. Assesses risks and takes preventative action<br>• Identifies improvements and contributes to the development of organisational policies, standards, and guidelines for testing |

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

## Delivery and Operation

### Technology Management

| **Technology Service Management ITMG** | **Level 5** |
|---|---|
| Managing the provision of technology-based services to meet defined organisational needs. | • Takes responsibility for managing the design, procurement, installation, upgrading, operation, control, maintenance and effective use of specific technology services.<br>• Leads the delivery of services, ensuring that agreed service levels, security requirements and other quality standards are met. Ensures adherence to relevant policies and procedures.<br>• Ensures that processes and practices are aligned across teams and providers to operate effectively and efficiently.<br>• Monitors the performance of technology services. Provides appropriate status and other reports to managers and senior users |
| **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<br>• Provides expert advice and guidance to implement and improve storage management<br>• Manages storage and backup systems to provide agreed service levels<br>• Creates, improves and supports storage management services with optimal utilisation of storage resources, ensuring security, availability and integrity of data |
| **Systems 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<br>• Evaluates new system software and recommends adoption if appropriate. Plans the provisioning and testing of new versions of system software<br>• Investigates and coordinates the resolution of potential and actual service problems<br>• 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<br>• Makes a significant contribution to the investigation, diagnosis and resolution of network problems<br>• Ensures that all requests for support are dealt with according to set standards and procedures |
| **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<br>• Optimises efficiency in the population of data centre space. Ensures adherence to all relevant policies and processes<br>• Uses data centre management tools to plan, record and manage installed infrastructure, power, space and cooling capabilities<br>• Monitors usage and actions to meet sustainability targets |
| 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<br>• Investigates escalated, non-routine and high-impact incidents to responsible service owners and seeks resolution<br>• Facilitates recovery, following resolution of incidents. Ensures that resolved incidents are properly documented and closed<br>• Analyses causes of incidents, and informs service owners to minimise probability of recurrence, and contributes to service improvement<br>• 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<br>• Identifies, assesses and communicates associated risks<br>• 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<br>• Reviews actual or potential security breaches and vulnerabilities and ensures that they are promptly and thoroughly investigated<br>• Recommends actions and appropriate control improvements<br>• Ensures that security records are accurate and complete and that requests for support are dealt with according to agreed procedures<br>• 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<br>• Evaluates and selects, reviews vulnerability assessment tools and techniques<br>• Provides expert advice and guidance to support the adoption of agreed approaches<br>• Obtains and acts on vulnerability information and conducts security risk assessments, business impact analysis and accreditation on complex information systems |

## 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<br>• Provides guidance to individuals on long-term development goals and career opportunities, considering an individual's strengths and preferences<br>• 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<br>• Maintains awareness of the physical and emotional welfare of employees, and provides counselling when required |
| **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<br>• Maintains, publicises and promotes a catalogue of learning and development activities. Ensures that courses are up to date and accredited (when required)<br>• Arranges facilities and schedules with learning and development providers as appropriate<br>• Uses data to assess and improve the effectiveness of learning or educational activities |
| **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<br>• Defines and manages the implementation of resourcing processes and tools. Advises on available options and customises resourcing approach to meet requirements<br>• Adheres to standards, statutory or external regulations and codes of practice and ensures compliance<br>• Engages with external parties in support of resourcing plans<br>• Measures effectiveness of resourcing processes and implements improvements |

## 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 targets<br>• Manages the operational relationships between suppliers and ensures potential disputes or conflicts are raised and resolved<br>• 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<br>• Manages implementation of supplier service improvement actions<br>• Identifies constraints and opportunities when negotiating or renegotiating contracts |

# CSSLP

Certified Secure Software Lifecycle 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 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<br>• Communicates the benefits and value of information, both internal and external, that can be mined from business systems and elsewhere<br>• Reviews new change proposals and provides specialist advice on information and records management. Assesses and manages information-related risks<br>• 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<br>• Leads the preparation of technical plans and ensures that appropriate technical resources are made available<br>• Ensures that appropriate tools and methods are available, understood and employed in architecture development<br>• Provides technical guidance and governance on solution development and integration<br>• Evaluates requests for changes and deviations from specifications and recommends actions<br>• 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<br>• Manages the relationship with individuals and teams who have authority for critical business processes and supporting systems<br>• Evaluates the critical risks and identifies priority areas for improvement<br>• 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<br>• Ensures architectural principles are applied during design to reduce risk<br>• Drives adoption and adherence to policy, standards and guidelines<br>• Contributes to the development of organisational strategies that address information control requirements<br>• Identifies and monitors environmental and market trends and proactively assesses impact on business strategies, benefits and risks<br>• 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<br>• Provides advice and guidance to ensure adoption of and adherence to information assurance architectures, strategies, policies, standards and guidelines<br>• Plans, organises and conducts information assurance and accreditation of complex domains areas, cross-functional areas, and across the supply chain<br>• 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<br>• Provides expert advice and guidance on implementing personal data legislation controls in products, services and systems<br>• Investigates major data breaches and recommends appropriate control improvements<br>• Creates and maintains an inventory of data that are subject to personal data legislation<br>• Conducts risk assessments, business impact analysis for complex information systems and specifies any required changes<br>• 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<br>• Implements consistent and reliable risk management processes and reporting to key stakeholders<br>• Engages specialists and domain experts as necessary<br>• 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<br>• Confirms the scope and objectives of specific audit activity with management. Aligns with the scope of the audit program and organisational policies<br>• Determines appropriate methods of investigation to achieve the audit objectives<br>• Presents audit findings to management describing the effectiveness and efficiency of control mechanisms<br>• 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<br>• Selects, adopts and adapts appropriate requirements definition and management methods, tools and techniques<br>• Contributes to the development of organisational methods and standards for requirements management<br>• Obtains input from, and agreement to requirements from a diverse range of stakeholders<br>• Negotiates with stakeholders to manage competing priorities and conflicts<br>• Establishes requirements baselines. Ensures changes to requirements are investigated and managed |

## 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<br>• Leads activities to make security and privacy integral to systems development<br>• Identifies and manages the resources necessary for all stages of systems development projects<br>• Ensures that 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 organisational commitment to strategies to deliver systems and software life cycle working practices to achieve business objectives<br>• Works with others to integrate organisational policies, standards and techniques across the full software and systems life cycle<br>• Develops and deploys the working environment supporting systems and software life cycle practices for strategic, large and complex products and services<br>• Leads activities to manage risks associated with systems and software life cycle working practices<br>• 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<br>• Ensures that the system design balances functional and non-functional requirements<br>• Reviews systems designs and ensures that appropriate methods, tools and techniques are applied effectively<br>• Makes recommendations and assesses and manages associated risks<br>• Adopts and adapts system design methods, tools and techniques<br>• Contributes to development of system design policies, standards and selection of architecture components |

| Software Design SWDN | Level 5 |
|---|---|
| Specifying and designing software to meet defined requirements by following agreed design standards and principles. | • Specifies and designs large or complex software applications, components and modules<br>• Adopts and adapts software design methods, tools and techniques<br>• Undertakes impact analysis on major design options, makes recommendations and assesses and manages associated risks<br>• Specifies prototypes/simulations to enable informed decision-making<br>• Evaluates software designs to ensure adherence to standards and identifies corrective action<br>• Ensures that the software design balances functional, quality, security and systems management requirements. Contributes to the development of organisational 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<br>• Plans and drives software construction activities. Adopts and adapts appropriate software development methods, tools and techniques<br>• Measures and monitors applications of project/team standards for software construction, including software security<br>• Contributes to the development of organisational policies, standards, and guidelines for software development |
| **Systems Integration and Build SINT** | **Level 5** |
| Planning, implementing and controlling activities to synthesise system components to create operational systems, products or services. | • Plans and drives activities to develop organisational systems integration and build capabilities including automation and continuous integration<br>• Identifies, evaluates and manages the adoption of tools, techniques and processes to create a robust integration framework<br>• Provides authoritative advice and guidance on any aspect of systems integration<br>• Leads integration work in line with the agreed system and service design<br>• Assesses risks and takes preventative action<br>• Measures and monitors applications of standards<br>• Contributes to the development of organisational policies, standards, and guidelines for systems integration |

| Testing TEST | Level 6 |
|---|---|
| Investigating products, systems and services to assess behaviour and whether these meet specified or unspecified requirements and characteristics. | • Develops organisational policies, standards, and guidelines for testing<br>• Plans and leads strategic, large and complex testing activities. Leads activities to manage risks and opportunities associated with testing<br>• Adapts or develops organisational testing capabilities and methods to solve complex business and engineering problems in tools and testing<br>• Promotes a culture of quality throughout the organisation and drives adoption of and adherence to testing policies and standards |

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

| Database Design DBDS | Level 5 |
|---|---|
| Specifying, designing and maintaining mechanisms for storing and accessing data. | • Provides specialist expertise in the design characteristics of database management systems or data warehouse products/services<br>• Provides expert guidance in the selection, provision and use of database and data warehouse architectures, software and facilities<br>• Ensures that physical database design policy supports transactional data requirements for performance and availability<br>• Ensures that data warehouse design policy supports demands for business intelligence and data analytics |

## 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<br>• Evaluates new system software and recommends adoption if appropriate. Plans the provisioning and testing of new versions of system software<br>• Investigates and coordinates the resolution of potential and actual service problems<br>• Ensures that operational procedures and diagnostics for system software are current accessible and well understood |

| 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<br>• Provides effective team leadership, including information flow to and from the customer during project work<br>• Develops and implements quality plans and method statements<br>• Monitors the effectiveness of installations and ensures that appropriate recommendations for change are made |

| Release and Deployment RELM | Level 5 |
|---|---|
| Applying the processes, systems and functions required to make new and changed services and features available for use. | • Leads the assessment, analysis, planning and design of release packages, including assessment of risk. Liaises with business and technology teams on release scheduling and communication of progress. Conducts post-release reviews<br>• Ensures that release processes and procedures are applied and that releases can be rolled back as needed<br>• Identifies, evaluates and manages the adoption of appropriate release and deployment techniques, processes and automation tools |

| 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<br>• Negotiates service level requirements and agreed service levels with customers<br>• Diagnoses service delivery problems and initiates actions to maintain or improve levels of service<br>• 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<br>• Investigates escalated, non-routine and high-impact incidents to responsible service owners and seeks resolution<br>• Facilitates recovery, following resolution of incidents. Ensures that resolved incidents are properly documented and closed<br>• Analyses causes of incidents, and informs service owners to minimise probability of recurrence, and contributes to service improvement<br>• Analyses metrics and reports on the performance of the incident management process |
| **Problem Management PBMG** | **Level 5** |
| Managing the life cycle of all problems that have occurred or could occur in delivering a service. | • Ensures that appropriate action is taken to anticipate, investigate and resolve problems in systems and services<br>• Ensures that such problems are fully documented within the relevant reporting systems<br>• Enables development of problem solutions. Coordinates the implementation of agreed remedies and preventative measures<br>• Analyses patterns and trends and improves problem management processes |

## Security Services

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

| 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<br>• Delivers objective insights into the existence of vulnerabilities, the effectiveness of defences and mitigating controls<br>• Takes responsibility for the integrity of testing activities and coordinates the execution of these activities.<br>• Provides authoritative advice and guidance on all aspects of penetration testing<br>• 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<br>• Maintains, publicises and promotes a catalogue of learning and development activities. Ensures that courses are up to date and accredited (when required).<br>• Arranges facilities and schedules with learning and development providers as appropriate<br>• 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<br>• 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<br>• Advises on the business case for alternative sourcing models. Advises on policy and procedures covering tendering, the selection of suppliers and procurement<br>• Negotiates with potential partners and suppliers, developing acceptance criteria and procedures. Drafts and laces contracts |

| 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 targets<br>• Manages the operational relationships between suppliers and ensures potential disputes or conflicts are raised and resolved.<br>• Performs benchmarking and makes use of supplier performance data to ensure that performance is adequately monitored and regularly reviewed<br>• Use suppliers' expertise to support and inform development roadmaps<br>• 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 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 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<br>• Leads the preparation of technical plans and ensures that appropriate technical resources are made available<br>• Ensures appropriate tools and methods are available, understood and employed in architecture development<br>• Provides technical guidance and governance on solution development and integration<br>• Evaluates requests for changes and deviations from specifications and recommends actions<br>• 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<br>• Manages the relationship with individuals and teams who have authority for critical business processes and supporting systems<br>• Evaluates the critical risks and identifies priority areas for improvement<br>• 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<br>• Ensures architectural principles are applied during design to reduce risk<br>• Drives adoption and adherence to policy, standards and guidelines<br>• Contributes to the development of organisational strategies that address information control requirements<br>• Identifies and monitors environmental and market trends and proactively assesses impact on business strategies, benefits and risks<br>• 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<br>• Provides advice and guidance to ensure adoption of and adherence to information assurance architectures, strategies, policies, standards and guidelines<br>• Plans, organises and conducts information assurance and accreditation of complex domains areas, cross-functional areas, and across the supply chain<br>• 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<br>• 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<br>• Creates and maintains an inventory of data that are subject to personal data legislation<br>• Conducts risk assessments, business impact analysis for complex information systems and specifies any required changes<br>• 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<br>• Implements consistent and reliable risk management processes and reporting to key stakeholders<br>• Engages specialists and domain experts as necessary<br>• 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<br>• Confirms the scope and objectives of specific audit activity with management. Aligns with the scope of the audit program and organisational policies<br>• Determines appropriate methods of investigation to achieve the audit objectives. Presents audit findings to management describing the effectiveness and efficiency of control mechanisms<br>• 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<br>• Derives data management structures and metadata to support consistency of information retrieval, combination, analysis, pattern recognition and interpretation, throughout the organisation<br>• Plans effective data storage, sharing and publishing within the organisation. Independently validates external information from multiple sources<br>• Assesses issues that might prevent the organisation from making maximum use of its information assets<br>• Provides expert advice and guidance to enable the organisation to get maximum value from its data assets |

## Delivery and Operation

### Technology Management

| Technology Service Management ITMG | Level 5 |
|---|---|
| Managing the provision of technology-based services to meet defined organisational needs. | • Takes responsibility for managing the design, procurement, installation, upgrading, operation, control, maintenance and effective use of specific technology services<br>• Leads the delivery of services, ensuring that agreed service levels, security requirements and other quality standards are met<br>• Ensures adherence to relevant policies and procedures<br>• Ensures that processes and practices are aligned across teams and providers to operate effectively and efficiently<br>• Monitors the performance of technology services. Provides appropriate status and other reports to managers and senior users |
| **IT Infrastructure ITOP** | **Level 5** |
| Deploying, configuring and operating T Infrastructure. | • Provides technical leadership to optimise the performance of IT infrastructure<br>• Investigates and manages the adoption of tools, techniques and processes (including automation) for the management of systems and services<br>• 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<br>• Ensures that operational procedures and documentation are fit for purpose and kept up to date<br>• 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<br>• Evaluates new system software and recommends adoption if appropriate. Plans the provisioning and testing of new versions of system software<br>• Investigates and coordinates the resolution of potential and actual service problems<br>• 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 fo data storage. | • Develops standards and guidelines for implementing data protection and disaster recovery functionality for all business applications and business data<br>• Provides expert advice and guidance to implement and improve storage management<br>• Manages storage and backup systems to provide agreed service levels<br>• 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<br>• Optimises efficiency in the population of data centre space. Ensures adherence to all relevant policies and processes<br>• Uses data centre management tools to plan, record and manage installed infrastructure, power, space and cooling capabilities<br>• 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<br>• Negotiates service level requirements and agreed service levels with customers<br>• Diagnoses service delivery problems and initiates actions to maintain or improve levels of service<br>• Establishes and maintains operational methods, procedures and facilities and reviews them regularly for effectiveness and efficiency |

| 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<br>• Proactively reviews information in conjunction with service level agreements to identify any capacity issues and specifies any required changes<br>• Provides advice to support the design of service components, including designing in flexible and scalable capacity<br>• Works with business representatives to agree and implement short- and medium-term modifications to capacity<br>• Drafts and maintains standards and procedures for service component capacity management<br>• Ensures the correct implementation of standards and procedures |
| **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.<br>• Investigates escalated, non-routine and high-impact incidents to responsible service owners and seeks resolution<br>• Facilitates recovery, following resolution of incidents<br>• Ensures that resolved incidents are properly documented and closed<br>• Analyses causes of incidents and informs service owners to minimise probability of recurrence, and contributes to service improvement<br>• 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<br>• Reviews actual or potential security breaches and vulnerabilities and ensures that they are promptly and thoroughly investigated.<br>• Recommends actions and appropriate control improvements<br>• Ensures security records are accurate and complete and that requests for support are dealt with according to reed procedures<br>• Contributes to the creation and maintenance of policy, standards, procedures and documentation for security |

| Digital Forensics DGFS | Level 5 |
|---|---|
| Recovering and investigating material found in digital devices. | • Conducts investigations to correctly gather, analyse and present findings, including digital evidence, to both business and legal audiences<br>• Collates conclusions and recommendations and presents forensics findings to stakeholders<br>• Plans and manages digital forensics activities within the organisation<br>• Provides expert advice on digital forensics<br>• Contributes to the development of digital forensics policies, standards and guidelines.<br>• 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 organisation.<br>• Evaluates and selects, reviews vulnerability assessment tools and techniques.<br>• Provides expert advice and guidance to support the adoption of agreed approaches.<br>• Obtains and acts on vulnerability information and conducts security risk assessments, business impact analysis and accreditation on complex information systems. |

## 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<br>• Maintains, publicises and promotes a catalogue of learning and development activities. Ensures that courses are up to date and accredited (when required)<br>• Arranges facilities and schedules with learning and development providers as appropriate<br>• 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<br>• Manages tender, evaluation and acquisition processes<br>• Researches suppliers and markets, and maintains a broad understanding of the commercial environment, to inform and develop commercial strategies and sourcing plans<br>• Advises on the business case for alternative sourcing models<br>• Advises on policy and procedures covering tendering, the selection of suppliers and procurement<br>• Negotiates with potential partners and suppliers, developing acceptance criteria and procedures<br>• Drafts and places contracts |
| **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<br>• Manages the operational relationships between suppliers and ensures potential disputes or conflicts are raised and resolved<br>• Performs benchmarking and makes use of supplier performance data to ensure that performance is adequately monitored and regularly reviewed<br>• Use suppliers' expertise to support and inform development roadmaps<br>• Manages implementation of supplier service improvement actions<br>• Identifies constraints and opportunities when negotiating or renegotiating contracts |
| **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<br>• Facilitates open communication and discussion between stakeholders<br>• 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<br>• Facilitates business decision-making processes. Captures and disseminates technical and business information |

| Contract Management ITCM | |
|---|---|
| Managing and controlling the operation of formal contracts for the supply of products and services. | • Oversees and measures the fulfilment of contractual obligations<br>• 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<br>• Identifies where changes are required, evaluates the impact, and advises stakeholders about the implications and consequences. Negotiates variations and seeks appropriate authorisation.<br>• 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

Systems Security Certified Practitioner
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 Planning

| **Information Management IRMG** | **Level 4** |
|---|---|
| Developing, implementing and testing a business continuity framework. | • Supports the implementation of information and records management policies and standard practice<br>• Monitors the implementation of effective controls for internal delegation, audit and control relating to information and records management<br>• Reports on the consolidated status of information controls to inform effective decision-making<br>• 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<br>• Identifies information and communication systems that support critical business processes<br>• Coordinates the business impact analysis and the assessment of risks<br>• 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<br>• Explains the purpose of security controls and performs security risk and business impact analysis for medium complexity information systems<br>• Identifies risks that arise from potential technical solution architectures<br>• Designs alternate solutions or countermeasures and ensures they mitigate identified risks<br>• 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<br>• Identifies risk mitigation measures required in addition to the standard organisation or domain measures<br>• Establishes the requirement for accreditation evidence from delivery partners and communicates accreditation requirements to stakeholders<br>• Contributes to planning and organisation of information assurance and accreditation activities<br>• 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<br>• 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<br>• Identifies and documents risks in detail<br>• Identifies the root cause of issues during an audit, and communicates these effectively as risk insights<br>• Collates evidence regarding the interpretation and implementation of control measures<br>• 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<br>• Contributes to the selection of the software development methods, tools and techniques<br>• Applies agreed standards and tools to achieve well-engineered outcomes<br>• Participates in reviews of own work and leads reviews of colleagues' work |

| 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<br>• Participates in requirement, design and specification reviews, and uses this information to design test plans and test conditions<br>• Applies agreed standards to specify and perform manual and automated testing<br>• Automates testing tasks and builds test coverage through existing or new infrastructure<br>• Analyses and reports on test activities, results, issues and risks |

| 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<br>• Incorporates hardware/firmware modifications. Interprets automatic fault/performance indications and resolves faults down to discrete component level or escalates according to given procedures<br>• Implements communication protocols between system elements in accordance with defined standards<br>• 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 of data assets. | • Devises and implements master data management processes for specific subsets of data<br>• Assesses the integrity of data from multiple sources<br>• Provides advice on the transformation of data from one format/medium to another. Maintains and implements information handling procedures<br>• 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<br>• Contributes to the planning and implementation of infrastructure maintenance and updates. Implements agreed upon infrastructure changes and maintenance routines<br>• 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<br>• Maintains operational procedures and checks that they are executed following agreed standards<br>• Investigates and enables the resolution of operational issues. Provides reports and proposals for improvement, to specialists, users and managers |

| Systems Software SYSP | Level 3 |
|---|---|
| Installing, managing, controlling, deploying and maintaining infrastructure systems software, to meet operational needs and service levels. | • Monitors operational systems for resource usage and failure rates, to inform and facilitate system software tuning<br>• Applies system software parameters to maximise throughput and efficiency<br>• Installs and tests new versions of system software.<br>• Contributes to preparation of software implementation procedures with fall back contingency plans |
| **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<br>• Ensures network configurations are applied to meet operational requirements in line with agreed upon procedures<br>• Uses network management software and tools to investigate and diagnose network problems, collect performance statistics and create reports |
| **Configuration Management CFMG** | **Level 3** |
| Planning, identifying, controlling, accounting for and auditing of configuration items (CIs) and their interrelationships. | • Applies tools, techniques and processes to track, log and correct information related to configuration items<br>• Verifies and approves changes ensuring the protection of assets and components from unauthorised change, diversion and inappropriate use<br>• Ensures that users comply with identification standards for object types, environments, processes, life cycles, documentation, versions, formats, baselines, releases and templates<br>• Performs audits to check the accuracy of the information and undertakes any necessary corrective action under direction |
| **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<br>• 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<br>• Creates reports and proposals for improvement<br>• 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<br>• Grants users required physical accesses and monitors and reports on overall access control |

## 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<br>• Prioritises and diagnoses incidents. Investigates causes of incidents and seeks resolution<br>• Escalates unresolved incidents<br>• Facilitates recovery, following resolution of incidents. Documents and closes resolved incidents<br>• Contributes to testing and improving incident management procedures |

| 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<br>• Applies change control procedures<br>• 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<br>• Produces and analyses registers and histories of authorised assets and verifies that all these assets are in a known state and location<br>• Acts to highlight and resolve potential instances of unauthorised assets |

## 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<br>• Provides advice on defining access rights and the application and operation of elementary physical, procedural and technical security controls<br>• Investigates security breaches in accordance with established procedures and recommends required actions. Provides support and checks that corrective actions are implemented |
| **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<br>• Performs vulnerability assessments and business impact analysis for medium complexity information systems<br>• 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<br>• Specifies requirements for resources and tools to perform investigations<br>• Processes and analyses evidence in line with policy, standards and guidelines and supports the production of forensics findings and reports |
| **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<br>• Researches and investigates attack techniques and recommend ways to defend against them.<br>• 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 a variety of audiences using prepared materials to meet established learning objectives<br>• Uses established guidelines for the preparation of the environment. Assists with the development and maintenance of examples and case study materials<br>• Appropriately uses a range of learning delivery techniques to enable learners to develop skills, capability, techniques and required knowledge<br>• Observes learners performing practical activities and work. Advises and assists where necessary<br>• Provides detailed instruction where necessary and responds to questions, seeking advice in exceptional conditions beyond own experience |

# 3. Ancillary SFIA Skills

Ancillary SFIA skills have been mapped to CISSP, CSSLP and CCSP training courses and have attributes below the knowledge required for SFIA level 5.

| | | | | | |
|---|---|---|---|---|---|
| Skills for Security Professionals | Vulnerability Research | VURE | | 4 | |
| | Threat Intelligence | THIN | 4 | 4 | |
| | Security Operations | SCAD | | 4 | |
| | Digital Forensics | DGFS | 4 | | |
| | Penetration Testing | PENT | 4 | | |
| Security Software Development | Systems and Software Lifecycle Engineering | SLEN | | | 4 |
| | Solution Architecture | ARCH | 4 | | |
| | Systems Design | DESN | | | 4 |
| | Software Configuration | PORT | 4 | | |
| | Change Control | CHMG | 4 | | |
| Secure Infrastructure | Configuration Management | CFMG | 4 | 4 | |
| | Quality Assurance | QUAS | | | |
| | Quality Management | QUMG | | | |
| Other Security Related Skills | Information Management | IRMG | 4 | | 4 |