

SFIA 9 and CompTIA

Mappings



This document shows the SFIA skills that could be expected to be exhibited by professionals who have obtained CompTIA qualifications.

Levels of Responsibility and Generic Attributes

SFIA first defines seven generic levels of responsibility:

1. Follow
2. Assist
3. Apply
4. Enable
5. Ensure/Advise
6. Initiate/Influence
7. Set Strategy/Inspire/Mobilise

Level 1 is the lowest level of responsibility within the SFIA structure.

Each of these levels is characterised by five attributes:

- Autonomy
- Influence
- Complexity
- Business Skills/Behavioural Factors
- Knowledge

Specific professional skills

In addition to the generic levels of responsibility, SFIA 9 defines 147 specific professional skills. Each skill is described at one or more of the seven levels, reflecting the varying degrees of proficiency observed in the workplace. For each skill, there is an overall description, along with guidance notes and detailed descriptions for each level at which the skill can be recognised.

Mapping between SFIA and CompTIA

This document shows the overall skill description and the differential description for the appropriate level(s) for each of the SFIA skills attributed to a CompTIA certification. CompTIA certifications are based on job roles. Individuals who obtain the CompTIA A+ will have minimum SFIA skills at Level 2 and will be well on their way to Level 3. Other CompTIA certifications are placed higher, and Level 3 is shown as the probable minimum for some skills.

Full definitions of all the levels at which these skills are recognised can be found on the SFIA website: <https://www.sfia-online.org>

The certifications covered below are:

Core	Tech+	A+	Network+	Security+
Infrastructure	Cloud+	Linux+	Server+	CloudNetX
Cybersecurity	CySA+	PenTest+	SecurityX	
Data and Analytics	Data+	DataSys+	DataX	
Additional Professional	Cloud Essentials+	Project+		

CompTIA Tech+ (FCO-U71)

Code/level	Skill name	Overall description, and Description at the specified level(s)
ITOP	<p>Infrastructure operations Overall description</p> <p>Level 1</p> <p>Level 2</p>	<p>Provisioning, deploying, configuring, operating, and optimising technology infrastructure across physical, virtual, and cloud-based environments.</p> <p>Supports routine infrastructure tasks and basic troubleshooting under close supervision. Monitors infrastructure health and reports on component status to support operational continuity.</p> <p>Executes operational procedures, runs automation scripts and performs routine maintenance, installation and monitoring of infrastructure components. Adjusts automation tasks as instructed to meet operational standards. Reports on infrastructure performance and security events, addressing issues directly when possible or escalating them to others for resolution.</p>
DBAD	<p>Database administration Overall description</p> <p>Level 2</p>	<p>Installing, configuring, monitoring, maintaining databases and data stores, ensuring performance and security while adapting to evolving technologies.</p> <p>Executes operational procedures, runs automation scripts and performs routine maintenance and monitoring of databases. Adjusts automation tasks as instructed to meet operational standards for databases. Reports on database performance, addresses issues directly when possible, or escalates to others for resolution.</p>
PROG	<p>Programming/software development Overall description</p> <p>Level 2</p>	<p>Developing software components to deliver value to stakeholders.</p> <p>Designs, codes, verifies, tests, documents, amends and refactors simple programs/scripts. Applies agreed standards, tools and basic security practices to achieve a well-engineered result. Reviews own work.</p>

CompTIA Tech+ (FCO-U71) – continued

Code/level	Skill name	Overall description, and Description at the specified level(s)
HSIN	<p>Systems installation and removal Overall description</p> <p>Level 1</p> <p>Level 2</p>	<p>Installing and testing, or decommissioning and removing, systems or system components.</p> <p>Follows agreed procedures to perform simple installations, replace consumable items and check the correct working of installations. Documents and reports on work done.</p> <p>Installs or removes system components using supplied installation instructions and tools. Conducts standard tests and contributes to investigations of problems and faults. Confirms the correct working of installations. Documents results in accordance with agreed procedures.</p>
NTAS	<p>Network support Overall description</p> <p>Level 1</p> <p>Level 2</p>	<p>Providing maintenance and support services for communications networks.</p> <p>Supports routine network tasks under close supervision. Monitors basic network health and reports on the status of network components. Assists with straightforward troubleshooting and follows established procedures to maintain operational continuity. Escalates issues as necessary to higher levels of support</p> <p>Assists in the operational configuration of network components and the investigation and resolution of network problems. Assists in the implementation of basic scripting and automation tools to streamline network support tasks. Assists with specified maintenance procedures and follows established safety, security and quality standards. Provides first-line support and guidance to network users, escalating issues as necessary.</p>

CompTIA Tech+ (FCO-U71) – continued

Code/level	Skill name	Overall description, and Description at the specified level(s)
SCAD	<p>Security operations Overall description</p> <p>Level 1</p> <p>Level 2</p>	<p>Manages and administers security measures, using tools and intelligence to protect assets, ensuring compliance and operational integrity.</p> <p>Performs simple security administration tasks. Maintains relevant records and documentation, contributing to overall data integrity.</p> <p>Receives and responds to routine requests for security support. Maintains records and effectively communicates actions taken. Assists in the investigation and resolution of issues relating to security systems using basic diagnostic tools and techniques. Documents incident and event information and generates reports on exceptions and security events. Contributes to management reporting processes.</p>
USUP	<p>Incident management Overall description</p> <p>Level 1</p>	<p>Coordinating responses to a diverse range of incidents to minimise negative impacts and quickly restore services.</p> <p>Follows agreed procedures to identify, register and categorise incidents. Uses provided tools and technologies to support the incident management process. Collects information as instructed to assist in incident resolution and allocates incidents as directed. Assists in monitoring incident queues and escalates issues according to procedures.</p>
PBMG	<p>Problem management Overall description</p> <p>Level 2</p> <p>Level 3</p>	<p>Managing the lifecycle of all problems that have occurred or could occur in delivering a service.</p> <p>Assists with problem management tasks under routine supervision. Helps document problems and maintain relevant records. Assists in detecting, logging, classifying, and prioritising problems in systems, processes, and services.</p> <p>Investigates problems in systems, processes and services. Contributes to the implementation of agreed remedies and preventative measures.</p>

CompTIA Tech+ (FCO-U71) – continued

Code/level	Skill name	Overall description, and Description at the specified level
ASUP	Application Support Overall Description Level 2	Delivering management, technical and administrative services to support and maintain live applications. Assists with specified maintenance procedures. Assists in the investigation and resolution of issues relating to applications.
DBDS	Database design Overall description Level 2	Specifying, designing and maintaining mechanisms for storing and accessing data across various environments and platforms. Assists in creating and documenting detailed database designs under routine supervision. Follows established procedures and guidelines. Helps create and maintain documentation.

A+ Core Series (220-1101 & 220-1102)

Code/level	Skill name	Overall description, and Description at the specified level
ITOP	<p>Infrastructure operations Overall description</p> <p>Level 1</p> <p>Level 2</p> <p>Level 3</p>	<p>Provisioning, deploying, configuring, operating, and optimising technology infrastructure across physical, virtual, and cloud-based environments.</p> <p>Supports routine infrastructure tasks and basic troubleshooting under close supervision. Monitors infrastructure health and reports on component status to support operational continuity.</p> <p>Executes operational procedures, runs automation scripts and performs routine maintenance, installation and monitoring of infrastructure components. Adjusts automation tasks as instructed to meet operational standards. Reports on infrastructure performance and security events, addressing issues directly when possible or escalating them to others for resolution.</p> <p>Provisions, deploys, and configures infrastructure services and components. Monitors infrastructure for load, performance and security events. Reports metrics and resolves operational issues. Executes standard operational procedures, including backups and restorations. Carries out agreed system software maintenance tasks. Automates routine system administration tasks to specifications using standard tools and basic scripting.</p>
NTDS	<p>Network design Overall description</p> <p>Level 2</p> <p>Level 3</p>	<p>Designing communication networks to meet business requirements, ensuring scalability, reliability, security and alignment with strategic objectives.</p> <p>Assists with defining configurations for networks and network components under routine supervision. Follows established network architectures, standards, and security protocols. Assists in documenting network configurations and producing detailed network specifications under guidance, incorporating relevant security aspects.</p> <p>Specifies the technical configurations and components required for a small network or a network segment in a more complex infrastructure. Follows organisational architectures, standards, and security guidelines.</p>

A+ Core Series (220-1101 & 220-1102) – continued

Code/level	Skill name	Overall description, and Description at the specified level
HSIN	<p>Systems installation and removal Overall description</p> <p>Level 1</p> <p>Level 2</p> <p>Level 3</p>	<p>Installing and testing, or decommissioning and removing, systems or system components.</p> <p>Follows agreed procedures to perform simple installations, replace consumable items and check the correct working of installations. Documents and reports on work done.</p> <p>Installs or removes system components using supplied installation instructions and tools. Conducts standard tests and contributes to investigations of problems and faults. Confirms the correct working of installations. Documents results in accordance with agreed procedures.</p> <p>Installs or removes hardware and/or software, using supplied installation instructions and tools, including handover to the client. Uses standard procedures and diagnostic tools to test installations, correct problems, and document results. Records details of all components that have been installed and removed. Assists users and follows agreed procedures for further help or escalation. Contributes to the development of installation procedures and standards.</p>
USUP	<p>Incident management Overall description</p> <p>Level 1</p> <p>Level 2</p>	<p>Coordinating responses to a diverse range of incidents to minimise negative impacts and quickly restore services.</p> <p>Follows agreed procedures to identify, register and categorise incidents. Uses provided tools and technologies to support the incident management process. Collects information as instructed to assist in incident resolution and allocates incidents as directed. Assists in monitoring incident queues and escalates issues according to procedures.</p> <p>Provides first line investigation and gathers information to enable incident resolution and allocate incidents. Gathers information to enable incident resolution and allocates incidents according to established procedures. Escalates incidents as necessary. Advises relevant people of actions taken. Communicates with users and stakeholders to provide updates on incident status. Assists in maintaining records and documentation related to incidents.</p>

SFIA 9 and CompTIA Mappings



	Level 3	<p>Prioritises and diagnoses incidents applying agreed procedures and tools.</p> <p>Investigates causes of incidents and seeks resolution.</p> <p>Escalates unresolved incidents to higher levels or specialist teams. Coordinates with stakeholders to ensure timely resolution.</p> <p>Facilitates recovery, following resolution of incidents. Documents, communicates outcomes and closes resolved incidents.</p>
--	---------	---

A+ Core Series (220-1101 & 220-1102) – continued

Code/level	Skill name	Overall description, and Description at the specified level
<p>NTAS</p>	<p>Network support Overall description</p> <p>Level 1</p> <p>Level 2</p> <p>Level 3</p>	<p>Providing maintenance and support services for communications networks.</p> <p>Supports routine network tasks under close supervision. Monitors basic network health and reports on the status of network components. Assists with straightforward troubleshooting and follows established procedures to maintain operational continuity. Escalates issues as necessary to higher levels of support</p> <p>Assists in the operational configuration of network components and the investigation and resolution of network problems. Assists in the implementation of basic scripting and automation tools to streamline network support tasks. Assists with specified maintenance procedures and follows established safety, security and quality standards. Provides first-line support and guidance to network users, escalating issues as necessary.</p> <p>Executes agreed network maintenance tasks and specified operational configuration of network components. Identifies and diagnoses network problems/faults using the required troubleshooting tools and network management software, including addressing security-related issues. Implements and maintains scripts, automation tools and orchestration platforms to optimise network support processes. Collects performance and traffic statistics and collaborates with others to ensure network effectiveness and resolve issues</p>
<p>PBMG</p>	<p>Problem management Overall description</p> <p>Level 2</p> <p>Level 3</p>	<p>Managing the lifecycle of all problems that have occurred or could occur in delivering a service.</p> <p>Assists with problem management tasks under routine supervision. Helps document problems and maintain relevant records. Assists in detecting, logging, classifying, and prioritising problems in systems, processes, and services.</p> <p>Investigates problems in systems, processes and services. Contributes to the implementation of agreed remedies and preventative measures.</p>

SFIA 9 and CompTIA Mappings



A+ Core Series (220-1101 & 220-1102) – continued

Code/level	Skill name	Overall description, and Description at the specified level
SCAD	<p>Security operations Overall description</p> <p>Level 1</p> <p>Level 2</p>	<p>Manages and administers security measures, using tools and intelligence to protect assets, ensuring compliance and operational integrity.</p> <p>Performs simple security administration tasks. Maintains relevant records and documentation, contributing to overall data integrity.</p> <p>Receives and responds to routine requests for security support. Maintains records and effectively communicates actions taken. Assists in the investigation and resolution of issues relating to security systems using basic diagnostic tools and techniques. Documents incident and event information and generates reports on exceptions and security events. Contributes to management reporting processes.</p>
PROG	<p>Programming/software development Overall description</p> <p>Level 2</p>	<p>Developing software components to deliver value to stakeholders.</p> <p>Designs, codes, verifies, tests, documents, amends and refactors simple programs/scripts. Applies agreed standards, tools and basic security practices to achieve a well-engineered result. Reviews own work.</p>

A+ Core Series (220-1101 & 220-1102) – continued

Code/level	Skill name	Overall description, and Description at the specified level
RFEN	<p>Radio frequency engineering Overall description</p> <p>Level 2</p> <p>Level 3</p>	<p>Designing, installing and maintaining radio frequency based devices and software.</p> <p>Assists with setting up, tuning and functional checks of radio frequency devices and software. Resolves faults down to line replaceable unit level or escalates according to given procedures. Carries out user confidence checks and escalates faults according to given procedures. Integrates RF devices with software applications using static configurations.</p> <p>Deploys, sets up, tunes and calibrates RF devices and software following maintenance schedules and using appropriate tools and test equipment. Incorporates hardware/firmware modifications. Interprets automatic fault/performance indications and resolves faults down to discrete component level or escalates according to given procedures. Implements communication protocols between system elements in accordance with defined standards. Integrates RF devices with software applications, incorporating dynamic reconfiguration of elements under software control to optimise their operational performance.</p>
ASUP	<p>Application support Overall description</p> <p>Level 2</p>	<p>Delivering management, technical and administrative services to support and maintain live applications.</p> <p>Assists with specified maintenance procedures. Assists in the investigation and resolution of issues relating to applications.</p>

A+ Core Series (220-1101 & 220-1102) – continued

Code/level	Skill name	Overall description, and Description at the specified level
SYSP	<p>System software administration Overall description</p> <p>Level 2</p> <p>Level 3</p>	<p>Installing, managing and maintaining operating systems, data management, office automation and utility software across various infrastructure environments.</p> <p>Assists with system software administration tasks under routine supervision. Supports the installation and configuration of system software. Helps monitor system performance and resource usage. Assists in documenting system software settings and updates.</p> <p>Monitors operational systems for resource usage and failure rates, to inform and facilitate system software tuning. Applies system software settings to optimise performance, enabling maximum throughput and efficient resource utilisation. Installs and tests new versions of system software. Assists in creating software implementation procedures, including fallback contingency plans.</p>
STMG	<p>Storage management Overall description</p> <p>Level 2</p> <p>Level 3</p>	<p>Provisioning, configuring and optimising on-premises and cloud-based storage solutions, ensuring data availability, security and alignment with business objectives.</p> <p>Assists with storage management tasks such as provisioning. Supports the setup and configuration of storage systems, incorporating standard security practices. Helps monitor storage performance and capacity, and documents storage utilisation.</p> <p>Executes routine storage management tasks following established procedures and using standard tools. Implements documented configurations for allocation of storage, installation and maintenance of secure storage systems using the agreed operational procedures. Identifies operational problems, including security-related issues, and contributes to their resolution. Uses standard management and reporting tools to collect and report on storage utilisation, performance and backup statistics.</p>

A+ Core Series (220-1101 & 220-1102) – continued

Code/level	Skill name	Overall description, and Description at the specified level
CIPM	<p>Organisational change management Overall description</p> <p>Level 2</p> <p>Level 3</p>	<p>Planning, designing and implementing activities to transition the organisation and people to the required future state.</p> <p>Assists with organisational change management tasks under routine supervision. Supports the collection and analysis of data related to change readiness and impact. Helps document and communicate change management plans and activities.</p> <p>Follows standard techniques to investigate and analyse the size, nature and impact of changes to operational activities. Contributes to change management plans and actions, focusing on the procedural execution of change. Supports implementation and engages with stakeholders under direction.</p>
CHMG	<p>Change control Overall description</p> <p>Level 2</p>	<p>Assessing risks associated with proposed changes and ensuring changes to products, services or systems are controlled and coordinated.</p> <p>Administers, tracks, logs, reports on change requests, using appropriate tools, techniques and processes. Provides assistance to implement standard low-risk changes, in accordance with defined change control procedures.</p>

A+ Core Series (220-1101 & 220-1102) – continued

Code/level	Skill name	Overall description, and Description at the specified level
CSMG	<p>Customer service support Overall description</p> <p>Level 1</p> <p>Level 2</p>	<p>Managing and operating customer service or service desk functions.</p> <p>Receives and handles routine customer inquiries and requests, following established procedures. Accurately records customer interactions and maintains relevant records. Escalates complex issues to appropriate team members or departments.</p> <p>Responds to common customer service requests, providing information to enable fulfilment or resolution. Allocates unresolved calls, requests, or issues to appropriate functions. Contributes to the maintenance of customer service knowledge bases and documentation. Assists in monitoring customer satisfaction metrics.</p>
DEPL	<p>Deployment Overall Description</p> <p>Level 2</p> <p>Level 3</p>	<p>Transitioning software from development to live usage, managing risks and ensuring it works as intended.</p> <p>Assists in deploying software releases and updates under routine supervision. Executes defined deployment processes and procedures using deployment tools and techniques. Monitors deployed applications and reports issues. Assists in rolling back deployments when necessary.</p> <p>Deploys software releases and updates to production environments. Uses deployment tools and techniques to ensure consistent deployments. Monitors and troubleshoots deployment processes. Performs rollbacks of deployments in case of issues or failures. Collaborates with release management and operations teams.</p>

A+ Core Series (220-1101 & 220-1102) – continued

Code/level	Skill name	Overall description, and Description at the specified level
IAMT	<p>Identity and Access Management Overall Description</p> <p>Level 1</p> <p>Level 2</p>	<p>Manages identity verification and access permissions within organisational systems and environments.</p> <p>Performs basic identity and access management tasks, including user account lifecycle management, under supervision. Maintains accurate records and follows established identity and access management protocols.</p> <p>Provides assistance for identity and access management operations, including automated role allocation and access control management. Engages in user identity lifecycle management, including account creation and deletion. Facilitates operation of identity and access management tools and self-service portals.</p>

A+ Core Series (220-1201 & 220-1202) – Releasing 2025

Code/level	Skill name	Overall description, and Description at the specified level
ITOP	<p>Infrastructure operations</p> <p>Overall description</p> <p>Level 1</p> <p>Level 2</p> <p>Level 3</p>	<p>Provisioning, deploying, configuring, operating, and optimising technology infrastructure across physical, virtual, and cloud-based environments.</p> <p>Supports routine infrastructure tasks and basic troubleshooting under close supervision. Monitors infrastructure health and reports on component status to support operational continuity.</p> <p>Executes operational procedures, runs automation scripts and performs routine maintenance, installation and monitoring of infrastructure components. Adjusts automation tasks as instructed to meet operational standards. Reports on infrastructure performance and security events, addressing issues directly when possible or escalating them to others for resolution.</p> <p>Provisions, deploys, and configures infrastructure services and components. Monitors infrastructure for load, performance and security events. Reports metrics and resolves operational issues. Executes standard operational procedures, including backups and restorations. Carries out agreed system software maintenance tasks. Automates routine system administration tasks to specifications using standard tools and basic scripting.</p>
NTDS	<p>Network design</p> <p>Overall description</p> <p>Level 2</p> <p>Level 3</p>	<p>Designing communication networks to meet business requirements, ensuring scalability, reliability, security and alignment with strategic objectives.</p> <p>Assists with defining configurations for networks and network components under routine supervision. Follows established network architectures, standards, and security protocols. Assists in documenting network configurations and producing detailed network specifications under guidance, incorporating relevant security aspects.</p> <p>Specifies the technical configurations and components required for a small network or a network segment in a more complex infrastructure. Follows organisational architectures, standards, and security guidelines.</p>

A+ Core Series (220-1201 & 220-1202) – continued

Code/level	Skill name	Overall description, and Description at the specified level
HSIN	<p>Systems installation and removal Overall description</p> <p>Level 1</p> <p>Level 2</p> <p>Level 3</p>	<p>Installing and testing, or decommissioning and removing, systems or system components.</p> <p>Follows agreed procedures to perform simple installations, replace consumable items and check the correct working of installations. Documents and reports on work done.</p> <p>Installs or removes system components using supplied installation instructions and tools. Conducts standard tests and contributes to investigations of problems and faults. Confirms the correct working of installations. Documents results in accordance with agreed procedures.</p> <p>Installs or removes hardware and/or software, using supplied installation instructions and tools, including handover to the client. Uses standard procedures and diagnostic tools to test installations, correct problems, and document results. Records details of all components that have been installed and removed. Assists users and follows agreed procedures for further help or escalation. Contributes to the development of installation procedures and standards.</p>
USUP	<p>Incident management Overall description</p> <p>Level 1</p> <p>Level 2</p>	<p>Coordinating responses to a diverse range of incidents to minimise negative impacts and quickly restore services.</p> <p>Follows agreed procedures to identify, register and categorise incidents. Uses provided tools and technologies to support the incident management process. Collects information as instructed to assist in incident resolution and allocates incidents as directed. Assists in monitoring incident queues and escalates issues according to procedures.</p> <p>Provides first line investigation and gathers information to enable incident resolution and allocate incidents. Gathers information to enable incident resolution and allocates incidents according to established procedures. Escalates incidents as necessary. Advises relevant people of actions taken. Communicates with users and stakeholders to provide updates on incident status. Assists in maintaining records and documentation related to incidents.</p>

SFIA 9 and CompTIA Mappings



	Level 3	<p>Prioritises and diagnoses incidents applying agreed procedures and tools.</p> <p>Investigates causes of incidents and seeks resolution.</p> <p>Escalates unresolved incidents to higher levels or specialist teams. Coordinates with stakeholders to ensure timely resolution.</p> <p>Facilitates recovery, following resolution of incidents. Documents, communicates outcomes and closes resolved incidents.</p>
--	---------	---

A+ Core Series (220-1201 & 220-1202) – continued

Code/level	Skill name	Overall description, and Description at the specified level
NTAS	<p>Network support Overall description</p> <p>Level 1</p> <p>Level 2</p> <p>Level 3</p>	<p>Providing maintenance and support services for communications networks.</p> <p>Supports routine network tasks under close supervision. Monitors basic network health and reports on the status of network components. Assists with straightforward troubleshooting and follows established procedures to maintain operational continuity. Escalates issues as necessary to higher levels of support</p> <p>Assists in the operational configuration of network components and the investigation and resolution of network problems. Assists in the implementation of basic scripting and automation tools to streamline network support tasks. Assists with specified maintenance procedures and follows established safety, security and quality standards. Provides first-line support and guidance to network users, escalating issues as necessary.</p> <p>Executes agreed network maintenance tasks and specified operational configuration of network components. Identifies and diagnoses network problems/faults using the required troubleshooting tools and network management software, including addressing security-related issues. Implements and maintains scripts, automation tools and orchestration platforms to optimise network support processes. Collects performance and traffic statistics and collaborates with others to ensure network effectiveness and resolve issues</p>
PBMG	<p>Problem management Overall description</p> <p>Level 2</p> <p>Level 3</p>	<p>Managing the lifecycle of all problems that have occurred or could occur in delivering a service.</p> <p>Assists with problem management tasks under routine supervision. Helps document problems and maintain relevant records. Assists in detecting, logging, classifying, and prioritising problems in systems, processes, and services.</p> <p>Investigates problems in systems, processes and services. Contributes to the implementation of agreed remedies and preventative measures.</p>

SFIA 9 and CompTIA Mappings



A+ Core Series (220-1201 & 220-1202) – continued

Code/level	Skill name	Overall description, and Description at the specified level
SCAD	<p>Security operations Overall description</p> <p>Level 1</p> <p>Level 2</p>	<p>Manages and administers security measures, using tools and intelligence to protect assets, ensuring compliance and operational integrity.</p> <p>Performs simple security administration tasks. Maintains relevant records and documentation, contributing to overall data integrity.</p> <p>Receives and responds to routine requests for security support. Maintains records and effectively communicates actions taken. Assists in the investigation and resolution of issues relating to security systems using basic diagnostic tools and techniques. Documents incident and event information and generates reports on exceptions and security events. Contributes to management reporting processes.</p>
PROG	<p>Programming/software development Overall description</p> <p>Level 2</p>	<p>Developing software components to deliver value to stakeholders.</p> <p>Designs, codes, verifies, tests, documents, amends and refactors simple programs/scripts. Applies agreed standards, tools and basic security practices to achieve a well-engineered result. Reviews own work.</p>

A+ Core Series (220-1201 & 220-1202) – continued

Code/level	Skill name	Overall description, and Description at the specified level
RFEN	<p>Radio frequency engineering Overall description</p> <p>Level 2</p> <p>Level 3</p>	<p>Designing, installing and maintaining radio frequency based devices and software.</p> <p>Assists with setting up, tuning and functional checks of radio frequency devices and software. Resolves faults down to line replaceable unit level or escalates according to given procedures. Carries out user confidence checks and escalates faults according to given procedures. Integrates RF devices with software applications using static configurations.</p> <p>Deploys, sets up, tunes and calibrates RF devices and software following maintenance schedules and using appropriate tools and test equipment. Incorporates hardware/firmware modifications. Interprets automatic fault/performance indications and resolves faults down to discrete component level or escalates according to given procedures. Implements communication protocols between system elements in accordance with defined standards. Integrates RF devices with software applications, incorporating dynamic reconfiguration of elements under software control to optimise their operational performance.</p>
ASUP	<p>Application support Overall description</p> <p>Level 2</p>	<p>Delivering management, technical and administrative services to support and maintain live applications.</p> <p>Assists with specified maintenance procedures. Assists in the investigation and resolution of issues relating to applications.</p>

A+ Core Series (220-1201 & 220-1202) – continued

Code/level	Skill name	Overall description, and Description at the specified level
SYSP	<p>System software administration Overall description</p> <p>Level 2</p> <p>Level 3</p>	<p>Installing, managing and maintaining operating systems, data management, office automation and utility software across various infrastructure environments.</p> <p>Assists with system software administration tasks under routine supervision. Supports the installation and configuration of system software. Helps monitor system performance and resource usage. Assists in documenting system software settings and updates.</p> <p>Monitors operational systems for resource usage and failure rates, to inform and facilitate system software tuning. Applies system software settings to optimise performance, enabling maximum throughput and efficient resource utilisation. Installs and tests new versions of system software. Assists in creating software implementation procedures, including fallback contingency plans.</p>
STMG	<p>Storage management Overall description</p> <p>Level 2</p> <p>Level 3</p>	<p>Provisioning, configuring and optimising on-premises and cloud-based storage solutions, ensuring data availability, security and alignment with business objectives.</p> <p>Assists with storage management tasks such as provisioning. Supports the setup and configuration of storage systems, incorporating standard security practices. Helps monitor storage performance and capacity, and documents storage utilisation.</p> <p>Executes routine storage management tasks following established procedures and using standard tools. Implements documented configurations for allocation of storage, installation and maintenance of secure storage systems using the agreed operational procedures. Identifies operational problems, including security-related issues, and contributes to their resolution. Uses standard management and reporting tools to collect and report on storage utilisation, performance and backup statistics.</p>

A+ Core Series (220-1201 & 220-1202) – continued

SFIA 9 and CompTIA Mappings



Code/level	Skill name	Overall description, and Description at the specified level
CIPM	Organisational change management Overall description Level 2 Level 3	<p>Planning, designing and implementing activities to transition the organisation and people to the required future state.</p> <p>Assists with organisational change management tasks under routine supervision. Supports the collection and analysis of data related to change readiness and impact. Helps document and communicate change management plans and activities.</p> <p>Follows standard techniques to investigate and analyse the size, nature and impact of changes to operational activities. Contributes to change management plans and actions, focusing on the procedural execution of change. Supports implementation and engages with stakeholders under direction.</p>
CHMG	Change control Overall description Level 2	<p>Assessing risks associated with proposed changes and ensuring changes to products, services or systems are controlled and coordinated.</p> <p>Administers, tracks, logs, reports on change requests, using appropriate tools, techniques and processes. Provides assistance to implement standard low-risk changes, in accordance with defined change control procedures.</p>

A+ Core Series (220-1201 & 220-1202) – continued

Code/level	Skill name	Overall description, and Description at the specified level
CSMG	<p>Customer service support Overall description</p> <p>Level 1</p> <p>Level 2</p>	<p>Managing and operating customer service or service desk functions.</p> <p>Receives and handles routine customer inquiries and requests, following established procedures. Accurately records customer interactions and maintains relevant records. Escalates complex issues to appropriate team members or departments.</p> <p>Responds to common customer service requests, providing information to enable fulfilment or resolution. Allocates unresolved calls, requests, or issues to appropriate functions. Contributes to the maintenance of customer service knowledge bases and documentation. Assists in monitoring customer satisfaction metrics.</p>
DEPL	<p>Deployment Overall Description</p> <p>Level 2</p> <p>Level 3</p>	<p>Transitioning software from development to live usage, managing risks and ensuring it works as intended.</p> <p>Assists in deploying software releases and updates under routine supervision. Executes defined deployment processes and procedures using deployment tools and techniques. Monitors deployed applications and reports issues. Assists in rolling back deployments when necessary.</p> <p>Deploys software releases and updates to production environments. Uses deployment tools and techniques to ensure consistent deployments. Monitors and troubleshoots deployment processes. Performs rollbacks of deployments in case of issues or failures. Collaborates with release management and operations teams.</p>

A+ Core Series (220-1201 & 220-1202) – continued

Code/level	Skill name	Overall description, and Description at the specified level
IAMT	<p>Identity and Access Management Overall Description</p> <p>Level 1</p> <p>Level 2</p>	<p>Manages identity verification and access permissions within organisational systems and environments.</p> <p>Performs basic identity and access management tasks, including user account lifecycle management, under supervision. Maintains accurate records and follows established identity and access management protocols.</p> <p>Provides assistance for identity and access management operations, including automated role allocation and access control management. Engages in user identity lifecycle management, including account creation and deletion. Facilitates operation of identity and access management tools and self-service portals.</p>

Network+ (N10-009)

Code/level	Skill name	Overall description, and Description at the specified level
NTDS	<p>Network design Overall description</p> <p>Level 2</p> <p>Level 3</p>	<p>Designing communication networks to meet business requirements, ensuring scalability, reliability, security and alignment with strategic objectives.</p> <p>Assists with defining configurations for networks and network components under routine supervision. Follows established network architectures, standards, and security protocols. Assists in documenting network configurations and producing detailed network specifications under guidance, incorporating relevant security aspects.</p> <p>Specifies the technical configurations and components required for a small network or a network segment in a more complex infrastructure. Follows organisational architectures, standards, and security guidelines..</p>
ITOP	<p>Infrastructure operations Overall description</p> <p>Level 1</p> <p>Level 2</p> <p>Level 3</p>	<p>Provisioning, deploying, configuring, operating and optimising technology infrastructure across physical, virtual and cloud-based environments.</p> <p>Supports routine infrastructure tasks and basic troubleshooting under close supervision. Monitors infrastructure health and reports on component status to support operational continuity.</p> <p>Executes operational procedures, runs automation scripts and performs routine maintenance, installation and monitoring of infrastructure components. Adjusts automation tasks as instructed to meet operational standards. Reports on infrastructure performance and security events, addressing issues directly when possible or escalating them to others for resolution.</p> <p>Provisions, deploys, and configures infrastructure services and components. Monitors infrastructure for load, performance and security events. Reports metrics and resolves operational issues. Executes standard operational procedures, including backups and restorations. Carries out agreed system software maintenance tasks. Automates routine system administration tasks to specifications using standard tools and basic scripting.</p>

Network+ (N10-009) – continued

Code/level	Skill name	Overall description, and Description at the specified level
NTAS	<p>Network support Overall description</p> <p>Level 1</p> <p>Level 2</p> <p>Level 3</p> <p>Level 4</p>	<p>Providing maintenance and support services for communications networks.</p> <p>Supports routine network tasks under close supervision. Monitors basic network health and reports on the status of network components. Assists with straightforward troubleshooting and follows established procedures to maintain operational continuity. Escalates issues as necessary to higher levels of support</p> <p>Assists in the operational configuration of network components and the investigation and resolution of network problems. Assists in the implementation of basic scripting and automation tools to streamline network support tasks. Assists with specified maintenance procedures and follows established safety, security and quality standards. Provides first-line support and guidance to network users, escalating issues as necessary.</p> <p>Executes agreed network maintenance tasks and specified operational configuration of network components. Identifies and diagnoses network problems/faults using the required troubleshooting tools and network management software, including addressing security-related issues. Implements and maintains scripts, automation tools and orchestration platforms to optimise network support processes. Collects performance and traffic statistics and collaborates with others to ensure network effectiveness and resolve issues.</p> <p>Applies technical expertise to maintain and optimise network infrastructure, executing updates and employing automation tools. Uses network management tools to monitor load, performance, and security statistics. Investigates and enables the resolution of network-related operational and security issues. Configures tools and/or creates scripts to automate network tasks. Maintains operational procedures and checks that they are followed. Provides reports and proposals for improvement to stakeholders. Contributes to the planning and implementation of network maintenance, updates, and security enhancements. Implements agreed network changes and maintenance routines.</p>

SFIA 9 and CompTIA Mappings



SCAD	<p>Security operations Overall description</p> <p>Level 1</p> <p>Level 2</p> <p>Level 3</p>	<p>Manages and administers security measures, using tools and intelligence to protect assets, ensuring compliance and operational integrity.</p> <p>Performs simple security administration tasks. Maintains relevant records and documentation, contributing to overall data integrity.</p> <p>Receives and responds to routine requests for security support. Maintains records and effectively communicates actions taken. Assists in the investigation and resolution of issues relating to security systems using basic diagnostic tools and techniques. Documents incident and event information and generates reports on exceptions and security events. Contributes to management reporting processes.</p> <p>Investigates minor security breaches using established procedures, incorporating analytical tools and techniques. Performs non-standard operational security tasks adapting to evolving technologies and threat landscapes. Addresses and resolves a variety of security events to maintain system integrity and operational continuity.</p>
------	--	---

Network+ (N10-009) – continued

Code/level	Skill name	Overall description, and Description at the specified level
USUP	<p>Incident management Overall description</p> <p>Level 1</p> <p>Level 2</p> <p>Level 3</p>	<p>Coordinating responses to a diverse range of incidents to minimise negative impacts and quickly restore services.</p> <p>Follows agreed procedures to identify, register and categorise incidents. Uses provided tools and technologies to support the incident management process. Collects information as instructed to assist in incident resolution and allocates incidents as directed. Assists in monitoring incident queues and escalates issues according to procedures.</p> <p>Provides first line investigation and gathers information to enable incident resolution and allocate incidents. Gathers information to enable incident resolution and allocates incidents according to established procedures. Escalates incidents as necessary. Advises relevant people of actions taken. Communicates with users and stakeholders to provide updates on incident status. Assists in maintaining records and documentation related to incidents.</p> <p>Prioritises and diagnoses incidents applying agreed procedures and tools. Investigates causes of incidents and seeks resolution. Escalates unresolved incidents to higher levels or specialist teams. Coordinates with stakeholders to ensure timely resolution. Facilitates recovery, following resolution of incidents. Documents, communicates outcomes and closes resolved incidents.</p>
PBMG	<p>Problem management Overall description</p> <p>Level 2</p> <p>Level 3</p>	<p>Managing the lifecycle of all problems that have occurred or could occur in delivering a service.</p> <p>Assists with problem management tasks under routine supervision. Helps document problems and maintain relevant records. Assists in detecting, logging, classifying, and prioritising problems in systems, processes, and services.</p> <p>Investigates problems in systems, processes and services. Contributes to the implementation of agreed remedies and preventative measures.</p>

SFIA 9 and CompTIA Mappings



Network+ (N10-009) – continued

Code/level	Skill name	Overall description, and Description at the specified level
HSIN	<p>Systems installation and removal Overall description</p> <p>Level 1</p> <p>Level 2</p> <p>Level 3</p>	<p>Installing and testing, or decommissioning and removing, systems or system components.</p> <p>Follows agreed procedures to perform simple installations, replace consumable items and check the correct working of installations. Documents and reports on work done.</p> <p>Installs or removes system components using supplied installation instructions and tools. Conducts standard tests and contributes to investigations of problems and faults. Confirms the correct working of installations. Documents results in accordance with agreed procedures.</p> <p>Installs or removes hardware and/or software, using supplied installation instructions and tools, including handover to the client. Uses standard procedures and diagnostic tools to test installations, correct problems, and document results. Records details of all components that have been installed and removed. Assists users and follows agreed procedures for further help or escalation. Contributes to the development of installation procedures and standards.</p>
RFEN	<p>Radio frequency engineering Overall description</p> <p>Level 2</p> <p>Level 3</p>	<p>Designing, installing and maintaining radio frequency based devices and software.</p> <p>Assists with setting up, tuning and functional checks of radio frequency devices and software. Resolves faults down to line replaceable unit level or escalates according to given procedures. Carries out user confidence checks and escalates faults according to given procedures. Integrates RF devices with software applications using static configurations.</p> <p>Deploys, sets up, tunes and calibrates RF devices and software following maintenance schedules and using appropriate tools and test equipment.</p>

SFIA 9 and CompTIA Mappings



		<p>Incorporates hardware/firmware modifications. Interprets automatic fault/performance indications and resolves faults down to discrete component level or escalates according to given procedures.</p> <p>Implements communication protocols between system elements in accordance with defined standards.</p> <p>Integrates RF devices with software applications, incorporating dynamic reconfiguration of elements under software control to optimise their operational performance.</p>
--	--	---

Network+ (N10-009) – continued

Code/level	Skill name	Overall description, and Description at the specified level
CHMG	<p>Change control Overall description</p> <p>Level 2</p> <p>Level 3</p>	<p>Assessing risks associated with proposed changes and ensuring changes to products, services or systems are controlled and coordinated.</p> <p>Administers, tracks, logs, reports on change requests, using appropriate tools, techniques and processes. Provides assistance to implement standard low-risk changes, in accordance with defined change control procedures.</p> <p>Develops, documents and implements changes based on requests for change. Applies change control processes and procedures.</p> <p>Applies tools, techniques and processes to manage and report on change requests.</p>
BURM	<p>Risk management Overall description</p> <p>Level 2</p> <p>Level 3</p>	<p>Planning and implementing processes for managing risk across the enterprise, aligned with organisational strategy and governance frameworks.</p> <p>Assists in collecting and reporting data to support risk management activities under routine supervision. Helps create and maintain documentation of risks and risk management activities. Helps identify and report issues and discrepancies.</p> <p>Undertakes basic risk management activities. Maintains documentation of risks, threats, vulnerabilities and mitigation actions.</p>

Network+ (N10-009) – continued

Code/level	Skill name	Overall description, and Description at the specified level
CIPM	<p>Organisational change management Overall description</p> <p>Level 2</p> <p>Level 3</p>	<p>Planning, designing and implementing activities to transition the organisation and people to the required future state.</p> <p>Assists with organisational change management tasks under routine supervision. Supports the collection and analysis of data related to change readiness and impact. Helps document and communicate change management plans and activities.</p> <p>Follows standard techniques to investigate and analyse the size, nature and impact of changes to operational activities. Contributes to change management plans and actions, focusing on the procedural execution of change. Supports implementation and engages with stakeholders under direction.</p>
IAMT	<p>Identity and Access Management Overall Description</p> <p>Level 1</p> <p>Level 2</p>	<p>Manages identity verification and access permissions within organisational systems and environments.</p> <p>Performs basic identity and access management tasks, including user account lifecycle management, under supervision. Maintains accurate records and follows established identity and access management protocols.</p> <p>Provides assistance for identity and access management operations, including automated role allocation and access control management. Engages in user identity lifecycle management, including account creation and deletion. Facilitates operation of identity and access management tools and self-service portals.</p>

Network+ (N10-009) – continued

Code/level	Skill name	Overall description, and Description at the specified level
IFDN	Infrastructure Design Overall Description Level 2	Designing technology infrastructure to meet business requirements, ensuring scalability, reliability, security and alignment with strategic objectives. Assists in developing preliminary infrastructure design specifications under routine supervision. Uses established standards and security protocols to contribute to infrastructure design activities. Helps draft design documents and diagrams. Documents design-related issues.

Security+ (SY0-701)

Code/level	Skill name	Overall description, and Description at the specified level
SCTY	<p>Information security Overall description</p> <p>Level 2</p> <p>Level 3</p>	<p>Defining and operating a framework of security controls and security management strategies.</p> <p>Assists with implementing and monitoring security policies and protocols across different systems. Contributes to identifying and addressing potential risks in security governance and compliance. Supports the analysis of documented security incidents, escalating where appropriate. Assists in the review of access controls and permissions, ensuring adherence to security policies.</p> <p>Applies and maintains specific security controls as required by organisational policy and local risk assessments. Communicates security risks and issues to business managers and others. Performs basic risk assessments for small information systems. Contributes to the identification of risks that arise from potential technical solution architectures. Suggests alternate solutions or countermeasures to mitigate risks. Defines secure systems configurations in compliance with intended architectures. Supports investigation of suspected attacks and security breaches.</p>

Security+ (SY0-701) – continued

Code/level	Skill name	Overall description, and Description at the specified level
SCAD	<p>Security operations Overall description</p> <p>Level 1</p> <p>Level 2</p> <p>Level 3</p>	<p>Manages and administers security measures, using tools and intelligence to protect assets, ensuring compliance and operational integrity.</p> <p>Performs simple security administration tasks. Maintains relevant records and documentation, contributing to overall data integrity.</p> <p>Receives and responds to routine requests for security support. Maintains records and effectively communicates actions taken. Assists in the investigation and resolution of issues relating to security systems using basic diagnostic tools and techniques. Documents incident and event information and generates reports on exceptions and security events. Contributes to management reporting processes.</p> <p>Investigates minor security breaches using established procedures, incorporating analytical tools and techniques. Performs non-standard operational security tasks adapting to evolving technologies and threat landscapes. Addresses and resolves a variety of security events to maintain system integrity and operational continuity.</p>
VURE	<p>Vulnerability research Overall description</p> <p>Level 2</p> <p>Level 3</p>	<p>Conducting applied research to discover, evaluate and mitigate new or unknown security vulnerabilities and weaknesses.</p> <p>Assists with vulnerability research tasks under routine supervision. Helps document and report findings from vulnerability research activities.</p> <p>Applies standard techniques and tools for vulnerability research. Uses available resources to update knowledge of relevant specialism. Participates in research communities. Analyses and reports on activities and results.</p>

Security+ (SY0-701) – continued

Code/level	Skill name	Overall description, and Description at the specified level
NTAS	<p>Network support Overall description</p> <p>Level 1</p> <p>Level 2</p> <p>Level 3</p>	<p>Providing maintenance and support services for communications networks.</p> <p>Supports routine network tasks under close supervision. Monitors basic network health and reports on the status of network components. Assists with straightforward troubleshooting and follows established procedures to maintain operational continuity. Escalates issues as necessary to higher levels of support</p> <p>Assists in the operational configuration of network components and the investigation and resolution of network problems. Assists in the implementation of basic scripting and automation tools to streamline network support tasks. Assists with specified maintenance procedures and follows established safety, security and quality standards. Provides first-line support and guidance to network users, escalating issues as necessary.</p> <p>Executes agreed network maintenance tasks and specified operational configuration of network components. Identifies and diagnoses network problems/faults using the required troubleshooting tools and network management software, including addressing security-related issues. Implements and maintains scripts, automation tools and orchestration platforms to optimise network support processes. Collects performance and traffic statistics and collaborates with others to ensure network effectiveness and resolve issues</p>

Security+ (SY0-701) – continued

<p>DGFS</p>	<p>Digital forensics Overall description</p> <p>Level 2</p> <p>Level 3</p> <p>Level 4</p>	<p>Recovering and investigating material found in digital devices.</p> <p>Assists with digital forensic investigations under routine supervision. Supports the recovery of damaged, deleted or hidden data from digital devices. Helps collect and preserve digital information and evidence according to established protocols.</p> <p>Applies standard forensic tools and techniques to examine digital devices. Recovers and analyses damaged, deleted or hidden data from various digital sources and devices. Maintains the integrity of digital evidence and ensures its collection adheres to legal admissibility standards.</p> <p>Designs and executes complex digital forensic examinations. Specifies requirements for specialised forensic tools and resources. Provides guidance on advanced data recovery techniques and artefact analysis. Processes and analyses digital evidence in line with organisational policies and industry standards. Develops procedures for handling emerging technologies in forensic contexts. Contributes to forensic reports detailing technical findings.</p>
-------------	--	--

Security+ (SY0-701) – continued

Code/level	Skill name	Overall description, and Description at the specified level
USUP	<p>Incident management Overall description</p> <p>Level 1</p> <p>Level 2</p> <p>Level 3</p>	<p>Coordinating responses to a diverse range of incidents to minimise negative impacts and quickly restore services.</p> <p>Follows agreed procedures to identify, register and categorise incidents. Uses provided tools and technologies to support the incident management process. Collects information as instructed to assist in incident resolution and allocates incidents as directed. Assists in monitoring incident queues and escalates issues according to procedures.</p> <p>Provides first line investigation and gathers information to enable incident resolution and allocate incidents. Gathers information to enable incident resolution and allocates incidents according to established procedures. Escalates incidents as necessary. Advises relevant people of actions taken. Communicates with users and stakeholders to provide updates on incident status. Assists in maintaining records and documentation related to incidents.</p> <p>Prioritises and diagnoses incidents applying agreed procedures and tools. Investigates causes of incidents and seeks resolution. Escalates unresolved incidents to higher levels or specialist teams. Coordinates with stakeholders to ensure timely resolution. Facilitates recovery, following resolution of incidents. Documents, communicates outcomes and closes resolved incidents.</p>
THIN	<p>Threat intelligence Overall description</p> <p>Level 2</p>	<p>Developing and sharing actionable insights on current and potential security threats to the success or integrity of an organisation.</p> <p>Contributes to routine threat intelligence gathering tasks. Monitors and detects potential security threats and escalates in accordance with relevant procedures and standards.</p>

Security+ (SY0-701) – continued

Code/level	Skill name	Overall description, and Description at the specified level
BURM	<p>Risk management</p> <p>Overall description</p> <p>Level 2</p> <p>Level 3</p> <p>Level 4</p>	<p>Planning and implementing processes for managing risk across the enterprise, aligned with organisational strategy and governance frameworks.</p> <p>Assists in collecting and reporting data to support risk management activities under routine supervision. Helps create and maintain documentation of risks and risk management activities. Helps identify and report issues and discrepancies.</p> <p>Undertakes basic risk management activities. Maintains documentation of risks, threats, vulnerabilities and mitigation actions.</p> <p>Carries out risk management activities within a specific function, technical area or project of medium complexity. Identifies risks and vulnerabilities, assesses their impact and probability, develops mitigation strategies and reports to the business. Involves specialists and domain experts as necessary.</p>
AUDT	<p>Audit</p> <p>Overall description</p> <p>Level 2</p> <p>Level 3</p>	<p>Delivering independent, risk-based assessments of the effectiveness of processes, the controls and the compliance environment of an organisation.</p> <p>Assists in collecting evidence and conducting audit activities under routine supervision. Maintains documentation and audit trails. Helps identify and report issues and discrepancies.</p> <p>Adopts a structured approach to executing and documenting audit fieldwork, following agreed standards. Maintains integrity of records to support and satisfy audit trails. Identifies typical risk indicators and explains prevention measures.</p>

Security+ (SY0-701) – continued

Code/level	Skill name	Overall description, and Description at the specified level
NTDS	<p>Network design Overall description</p> <p>Level 2</p> <p>Level 3</p>	<p>Designing communication networks to meet business requirements, ensuring scalability, reliability, security and alignment with strategic objectives.</p> <p>Assists with defining configurations for networks and network components under routine supervision. Follows established network architectures, standards, and security protocols. Assists in documenting network configurations and producing detailed network specifications under guidance, incorporating relevant security aspects.</p> <p>Specifies the technical configurations and components required for a small network or a network segment in a more complex infrastructure. Follows organisational architectures, standards, and security guidelines.</p>
RFEN	<p>Radio frequency engineering Overall description</p> <p>Level 2</p>	<p>Designing, installing and maintaining radio frequency based devices and software.</p> <p>Assists with setting up, tuning and functional checks of radio frequency devices and software. Resolves faults down to line replaceable unit level or escalates according to given procedures. Carries out user confidence checks and escalates faults according to given procedures. Integrates RF devices with software applications using static configurations.</p>

Security+ (SY0-701) – continued

Code/level	Skill name	Overall description, and Description at the specified level
HSIN	<p>Systems installation and removal Overall description</p> <p>Level 1</p> <p>Level 2</p> <p>Level 3</p>	<p>Installing and testing, or decommissioning and removing, systems or system components.</p> <p>Follows agreed procedures to perform simple installations, replace consumable items and check the correct working of installations. Documents and reports on work done.</p> <p>Installs or removes system components using supplied installation instructions and tools. Conducts standard tests and contributes to investigations of problems and faults. Confirms the correct working of installations. Documents results in accordance with agreed procedures.</p> <p>Installs or removes hardware and/or software, using supplied installation instructions and tools, including handover to the client. Uses standard procedures and diagnostic tools to test installations, correct problems, and document results. Records details of all components that have been installed and removed. Assists users and follows agreed procedures for further help or escalation. Contributes to the development of installation procedures and standards.</p>
PENT	<p>Penetration testing Overall description</p> <p>Level 2</p>	<p>Testing the effectiveness of security controls by emulating the tools and techniques of likely attackers.</p> <p>Assists with penetration testing tasks under routine supervision. Supports the execution of standard penetration tests on systems, networks and applications. Helps document and report on test results, findings and potential security risks.</p>

Security+ (SY0-701) – continued

Code/level	Skill name	Overall description, and Description at the specified level
PEDP	<p>Information and Data Compliance Overall description</p> <p>Level 4</p>	<p>Implementing and promoting compliance with information and data management legislation.</p> <p>Supports the implementation of policy, standards and guidelines related to information and data legislation and compliance requirements. Monitors the implementation of effective controls for internal delegation, audit and control relating to information management. Reports on the consolidated status of information controls to inform effective decision-making. Identifies risks around the use of information and data that is subject to specific legislation. Recommends remediation actions as required.</p>
CHMG	<p>Change control Overall description</p> <p>Level 2</p> <p>Level 3</p>	<p>Assessing risks associated with proposed changes and ensuring changes to products, services or systems are controlled and coordinated.</p> <p>Administers, tracks, logs, reports on change requests, using appropriate tools, techniques and processes. Provides assistance to implement standard low-risk changes, in accordance with defined change control procedures.</p> <p>Develops, documents and implements changes based on requests for change. Applies change control processes and procedures. Applies tools, techniques and processes to manage and report on change requests.</p>

Security+ (SY0-701) – continued

Code/level	Skill name	Overall description, and Description at the specified level
CIPM	<p>Organisational change management Overall description</p> <p>Level 2</p>	<p>Planning, designing and implementing activities to transition the organisation and people to the required future state.</p> <p>Assists with organisational change management tasks under routine supervision. Supports the collection and analysis of data related to change readiness and impact. Helps document and communicate change management plans and activities.</p>
IAMT	<p>Identity and access management Overall description</p> <p>Level 1</p> <p>Level 2</p> <p>Level 3</p>	<p>Manages identity verification and access permissions within organisational systems and environments.</p> <p>Performs basic identity and access management tasks, including user account lifecycle management, under supervision. Maintains accurate records and follows established identity and access management protocols.</p> <p>Provides assistance for identity and access management operations, including automated role allocation and access control management. Engages in user identity lifecycle management, including account creation and deletion. Facilitates operation of identity and access management tools and self-service portals.</p> <p>Administers standard identity and access management services, implementing policies and resolving related issues. Manages monitoring, audits and logging for identity and access management systems. Investigates minor security breaches in accordance with established procedures related to identity and access management. Assists users in defining their access rights and privileges. Designs and implements simple identity and access management solutions, enhancing user access security. Contributes to the enhancement and optimisation of existing identity and access management processes and systems.</p>

Security+ (SY0-701) – continued

Code/level	Skill name	Overall description, and Description at the specified level
IFDN	<p>Infrastructure design Overall description</p> <p>Level 2</p>	<p>Designing technology infrastructure to meet business requirements, ensuring scalability, reliability, security and alignment with strategic objectives.</p> <p>Assists in developing preliminary infrastructure design specifications under routine supervision. Uses established standards and security protocols to contribute to infrastructure design activities. Helps draft design documents and diagrams. Documents design-related issues.</p>
INAS	<p>Information assurance Overall description</p> <p>Level 2</p> <p>Level 3</p> <p>Level 4</p>	<p>Protecting against and managing risks related to the use, storage and transmission of data and information systems.</p> <p>Assists with information assurance activities under routine supervision. Helps perform basic risk assessments and supports the implementation of information assurance measures. Assists in maintaining records and documentation related to information assurance.</p> <p>Follows standard approaches for the technical assessment of information systems against information assurance policies and business objectives. Makes routine accreditation decisions. Recognises decisions that are beyond their scope and responsibility level and escalates according. Reviews and performs risk assessments and risk treatment plans. Identifies typical risk indicators and explains prevention measures. Maintains integrity of records to support and justify decisions.</p> <p>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.</p>

Cloud+ (CV0-004)

Code/level	Skill name	Overall description, and Description at the specified level
ITOP	<p>Infrastructure operations</p> <p>Overall description</p> <p>Level 1</p> <p>Level 2</p> <p>Level 3</p>	<p>Provisioning, deploying, configuring, operating, and optimising technology infrastructure across physical, virtual, and cloud-based environments.</p> <p>Supports routine infrastructure tasks and basic troubleshooting under close supervision. Monitors infrastructure health and reports on component status to support operational continuity.</p> <p>Executes operational procedures, runs automation scripts and performs routine maintenance, installation and monitoring of infrastructure components. Adjusts automation tasks as instructed to meet operational standards. Reports on infrastructure performance and security events, addressing issues directly when possible or escalating them to others for resolution.</p> <p>Provisions, deploys, and configures infrastructure services and components. Monitors infrastructure for load, performance and security events. Reports metrics and resolves operational issues. Executes standard operational procedures, including backups and restorations. Carries out agreed system software maintenance tasks. Automates routine system administration tasks to specifications using standard tools and basic scripting.</p>

Cloud+ (CV0-004) – continued

Code/level	Skill name	Overall description, and Description at the specified level
STMG	<p>Storage management Overall description</p> <p>Level 2</p> <p>Level 3</p>	<p>Provisioning, configuring and optimising on-premises and cloud-based storage solutions, ensuring data availability, security and alignment with business objectives.</p> <p>Assists with storage management tasks such as provisioning. Supports the setup and configuration of storage systems, incorporating standard security practices. Helps monitor storage performance and capacity, and documents storage utilisation.</p> <p>Executes routine storage management tasks following established procedures and using standard tools. Implements documented configurations for allocation of storage, installation and maintenance of secure storage systems using the agreed operational procedures. Identifies operational problems, including security-related issues, and contributes to their resolution. Uses standard management and reporting tools to collect and report on storage utilisation, performance and backup statistics.</p>
SINT	<p>Systems integration and build Overall description</p> <p>Level 2</p>	<p>Planning, implementing and controlling activities to integrate system elements, subsystems and interfaces to create operational systems, products or services.</p> <p>Produces builds from system components using appropriate build automation tools and processes. Conducts tests as defined in an integration test specification and records the details of any failures. Analyses and reports on integration test activities and results. Identifies and reports issues and risks.</p>

Cloud+ (CV0-004) – continued

Code/level	Skill name	Overall description, and Description at the specified level
AVMT	<p>Availability management Overall description</p> <p>Level 3</p> <p>Level 4</p>	<p>Ensuring services deliver agreed levels of availability to meet the current and future needs of the business.</p> <p>Performs defined availability management tasks, such as routine monitoring and data collection. Tests disaster recovery procedures under direction and contributes to the documentation of recovery plans. Assists with the operation of availability management tools and processes. Monitors service components against agreed performance standards and reports any deviations.</p> <p>Analyses service and component availability, reliability, maintainability and serviceability. Contributes to the availability management process and its operation. Monitors and maintains services and components to ensure ongoing compliance with agreed performance targets and service levels. Implements disaster recovery arrangements and documents recovery procedures. Conducts testing of recovery procedures.</p>
HSIN	<p>Systems installation and removal Overall description</p> <p>Level 1</p> <p>Level 2</p> <p>Level 3</p>	<p>Installing and testing, or decommissioning and removing, systems or system components.</p> <p>Follows agreed procedures to perform simple installations, replace consumable items, and check the correct working of installations. Documents and reports on work done.</p> <p>Installs or removes system components using supplied installation instructions and tools. Conducts standard tests and contributes to investigations of problems and faults. Confirms the correct working of installations. Documents results in accordance with agreed procedures.</p> <p>Installs or removes hardware and/or software, using supplied installation instructions and tools, including handover to the client. Uses standard procedures and diagnostic tools to test installations, correct problems, and document results.</p>

SFIA 9 and CompTIA Mappings



		Records details of all components that have been installed and removed. Assists users and follows agreed procedures for further help or escalation. Contributes to the development of installation procedures and standards.
--	--	---

Cloud+ (CV0-004) – continued

Code/level	Skill name	Overall description, and Description at the specified level
DESN	<p>Systems design Overall description</p> <p>Level 2</p> <p>Level 3</p>	<p>Designing systems to meet specified requirements and agreed systems architectures.</p> <p>Assists in the creation and documentation of system design elements under routine supervision. Follows established procedures and guidelines. Helps create and maintain documentation.</p> <p>Follows standard approaches and established design patterns to create new designs for simple systems or system components. Identifies and resolves minor design issues. Identifies alternative design options and seeks guidance when deviating from established design patterns.</p>
SCAD	<p>Security operations Overall description</p> <p>Level 1</p> <p>Level 2</p>	<p>Manages and administers security measures, using tools and intelligence to protect assets, ensuring compliance and operational integrity.</p> <p>Performs simple security administration tasks. Maintains relevant records and documentation, contributing to overall data integrity.</p> <p>Receives and responds to routine requests for security support. Maintains records and effectively communicates actions taken. Assists in the investigation and resolution of issues relating to security systems using basic diagnostic tools and techniques. Documents incident and event information and generates reports on exceptions and security events. Contributes to management reporting processes.</p>

Cloud+ (CV0-004) – continued

Code/level	Skill name	Overall description, and Description at the specified level
NTAS	<p>Network support Overall description</p> <p>Level 1</p> <p>Level 2</p> <p>Level 3</p>	<p>Providing maintenance and support services for communications networks.</p> <p>Supports routine network tasks under close supervision. Monitors basic network health and reports on the status of network components. Assists with straightforward troubleshooting and follows established procedures to maintain operational continuity. Escalates issues as necessary to higher levels of support</p> <p>Assists in the operational configuration of network components and the investigation and resolution of network problems. Assists in the implementation of basic scripting and automation tools to streamline network support tasks. Assists with specified maintenance procedures and follows established safety, security and quality standards. Provides first-line support and guidance to network users, escalating issues as necessary.</p> <p>Executes agreed network maintenance tasks and specified operational configuration of network components. Identifies and diagnoses network problems/faults using the required troubleshooting tools and network management software, including addressing security-related issues. Implements and maintains scripts, automation tools and orchestration platforms to optimise network support processes. Collects performance and traffic statistics and collaborates with others to ensure network effectiveness and resolve issues</p>
ARCH	<p>Solution architecture Overall description</p> <p>Level 4</p>	<p>Developing and communicating a multi-dimensional solution architecture to deliver agreed business outcomes.</p> <p>Contributes to the development of solution architectures in specific business, infrastructure or functional areas. Identifies and evaluates alternative architectures and the trade-offs in cost, performance and scalability. Determines and documents architecturally significant decisions. Produces specifications of cloud-based or on-premises components, tiers and interfaces, for translation into detailed designs using selected services and products. Supports projects or change initiatives through the preparation of technical plans and application of design principles. Aligns solutions with enterprise and solution architecture standards (including security).</p>

SFIA 9 and CompTIA Mappings



Cloud+ (CV0-004) – continued

Code/level	Skill name	Overall description, and Description at the specified level
<p>PEDP</p>	<p>Information and data compliance Overall description</p> <p>Level 4</p>	<p>Implementing and promoting compliance with information and data management legislation.</p> <p>Supports the implementation of policy, standards and guidelines related to information and data legislation and compliance requirements. Monitors the implementation of effective controls for internal delegation, audit and control relating to information management. Reports on the consolidated status of information controls to inform effective decision-making. Identifies risks around the use of information and data that is subject to specific legislation. Recommends remediation actions as required.</p>
<p>DEPL</p>	<p>Deployment Overall description</p> <p>Level 2</p>	<p>Transitioning software from development to live usage, managing risks and ensuring it works as intended.</p> <p>Assists in deploying software releases and updates under routine supervision. Executes defined deployment processes and procedures using deployment tools and techniques. Monitors deployed applications and reports issues. Assists in rolling back deployments when necessary.</p>

Cloud+ (CV0-004) – continued

Code/level	Skill name	Overall description, and Description at the specified level
IAMT	<p>Identity and access management Overall description</p> <p>Level 2</p> <p>Level 3</p>	<p>Manages identity verification and access permissions within organisational systems and environments.</p> <p>Performs basic identity and access management tasks, including user account lifecycle management, under supervision. Maintains accurate records and follows established identity and access management protocols.</p> <p>Provides assistance for identity and access management operations, including automated role allocation and access control management. Engages in user identity lifecycle management, including account creation and deletion. Facilitates operation of identity and access management tools and self-service portals.</p>
CFMG	<p>Configuration management Overall description</p> <p>Level 2</p>	<p>Planning, identifying, controlling, accounting for and auditing of configuration items (CIs) and their interrelationships.</p> <p>Applies tools, techniques and processes to administer, track, log, report on and correct configuration items, components and changes. Assists with audits to check the accuracy of the information and undertakes any necessary corrective action under direction.</p>

Linux+ (XKO-005)

Code/level	Skill name	Overall description, and Description at the specified level
SYSP	<p>System software administration Overall description</p> <p>Level 2</p> <p>Level 3</p>	<p>Installing, managing and maintaining operating systems, data management, office automation and utility software across various infrastructure environments.</p> <p>Assists with system software administration tasks under routine supervision. Supports the installation and configuration of system software. Helps monitor system performance and resource usage. Assists in documenting system software settings and updates.</p> <p>Monitors operational systems for resource usage and failure rates, to inform and facilitate system software tuning. Applies system software settings to optimise performance, enabling maximum throughput and efficient resource utilisation. Installs and tests new versions of system software. Assists in creating software implementation procedures, including fallback contingency plans.</p>
HSIN	<p>Systems installation and removal Overall description</p> <p>Level 1</p> <p>Level 2</p> <p>Level 3</p>	<p>Installing and testing, or decommissioning and removing, systems or system components.</p> <p>Follows agreed procedures to perform simple installations, replace consumable items, and check the correct working of installations. Documents and reports on work done.</p> <p>Installs or removes system components using supplied installation instructions and tools. Conducts standard tests and contributes to investigations of problems and faults. Confirms the correct working of installations. Documents results in accordance with agreed procedures.</p> <p>Installs or removes hardware and/or software, using supplied installation instructions and tools, including handover to the client. Uses standard procedures and diagnostic tools to test installations, correct problems, and document results. Records details of all components that have been installed and removed. Assists users and follows agreed procedures for further help or escalation.</p>

SFIA 9 and CompTIA Mappings



		Contributes to the development of installation procedures and standards.
--	--	--

Linux+ (XK0-005) – continued

Code/level	Skill name	Overall description, and Description at the specified level
ITOP	<p>Infrastructure operations Overall description</p> <p>Level 1</p> <p>Level 2</p> <p>Level 3</p>	<p>Provisioning, deploying, configuring, operating, and optimising technology infrastructure across physical, virtual, and cloud-based environments.</p> <p>Supports routine infrastructure tasks and basic troubleshooting under close supervision. Monitors infrastructure health and reports on component status to support operational continuity.</p> <p>Executes operational procedures, runs automation scripts and performs routine maintenance, installation and monitoring of infrastructure components. Adjusts automation tasks as instructed to meet operational standards. Reports on infrastructure performance and security events, addressing issues directly when possible or escalating them to others for resolution.</p> <p>Provisions, deploys, and configures infrastructure services and components. Monitors infrastructure for load, performance and security events. Reports metrics and resolves operational issues. Executes standard operational procedures, including backups and restorations. Carries out agreed system software maintenance tasks. Automates routine system administration tasks to specifications using standard tools and basic scripting.</p>

Linux+ (XK0-005) – continued

Code/level	Skill name	Overall description, and Description at the specified level
SCAD	<p>Security operations Overall description</p> <p>Level 1</p> <p>Level 2</p>	<p>Manages and administers security measures, using tools and intelligence to protect assets, ensuring compliance and operational integrity.</p> <p>Performs simple security administration tasks. Maintains relevant records and documentation, contributing to overall data integrity.</p> <p>Receives and responds to routine requests for security support. Maintains records and effectively communicates actions taken. Assists in the investigation and resolution of issues relating to security systems using basic diagnostic tools and techniques. Documents incident and event information and generates reports on exceptions and security events. Contributes to management reporting processes.</p>
PROG	<p>Programming/software development Overall description</p> <p>Level 2</p>	<p>Developing software components to deliver value to stakeholders.</p> <p>Designs, codes, verifies, tests, documents, amends and refactors simple programs/scripts. Applies agreed standards, tools and basic security practices to achieve a well-engineered result. Reviews own work.</p>

Linux+ (XK0-005) – continued

Code/level	Skill name	Overall description, and Description at the specified level
IAMT	<p>Identity and access management Overall description</p> <p>Level 1</p> <p>Level 2</p>	<p>Manages identity verification and access permissions within organisational systems and environments.</p> <p>Performs basic identity and access management tasks, including user account lifecycle management, under supervision. Maintains accurate records and follows established identity and access management protocols.</p> <p>Provides assistance for identity and access management operations, including automated role allocation and access control management. Engages in user identity lifecycle management, including account creation and deletion. Facilitates operation of identity and access management tools and self-service portals.</p>
DEPL	<p>Deployment Overall description</p> <p>Level 2</p>	<p>Transitioning software from development to live usage, managing risks and ensuring it works as intended.</p> <p>Assists in deploying software releases and updates under routine supervision. Executes defined deployment processes and procedures using deployment tools and techniques. Monitors deployed applications and reports issues. Assists in rolling back deployments when necessary.</p>

Server+ (SK0-005)

Code/level	Skill name	Overall description, and Description at the specified level
<p>HSIN</p>	<p>Systems installation and removal Overall description</p> <p>Level 1</p> <p>Level 2</p> <p>Level 3</p>	<p>Installing and testing, or decommissioning and removing, systems or system components.</p> <p>Follows agreed procedures to perform simple installations, replace consumable items, and check the correct working of installations. Documents and reports on work done.</p> <p>Installs or removes system components using supplied installation instructions and tools. Conducts standard tests and contributes to investigations of problems and faults. Confirms the correct working of installations. Documents results in accordance with agreed procedures.</p> <p>Installs or removes hardware and/or software, using supplied installation instructions and tools, including handover to the client. Uses standard procedures and diagnostic tools to test installations, correct problems, and document results. Records details of all components that have been installed and removed. Assists users and follows agreed procedures for further help or escalation. Contributes to the development of installation procedures and standards.</p>
<p>AVMT</p>	<p>Availability management Overall description</p> <p>Level 3</p> <p>Level 4</p>	<p>Ensuring services deliver agreed levels of availability to meet the current and future needs of the business.</p> <p>Performs defined availability management tasks, such as routine monitoring and data collection. Tests disaster recovery procedures under direction and contributes to the documentation of recovery plans. Assists with the operation of availability management tools and processes. Monitors service components against agreed performance standards and reports any deviations.</p> <p>Analyses service and component availability, reliability, maintainability and serviceability. Contributes to the availability management process and its operation. Monitors and maintains services and components to ensure ongoing compliance with agreed performance targets and service levels.</p>

SFIA 9 and CompTIA Mappings



		Implements disaster recovery arrangements and documents recovery procedures. Conducts testing of recovery procedures.
--	--	---

Server+ (SK0-005) – continued

Code/level	Skill name	Overall description, and Description at the specified level
SCAD	<p>Security operations Overall description</p> <p>Level 1</p> <p>Level 2</p> <p>Level 3</p>	<p>Manages and administers security measures, using tools and intelligence to protect assets, ensuring compliance and operational integrity.</p> <p>Performs simple security administration tasks. Maintains relevant records and documentation, contributing to overall data integrity.</p> <p>Receives and responds to routine requests for security support. Maintains records and effectively communicates actions taken. Assists in the investigation and resolution of issues relating to security systems using basic diagnostic tools and techniques. Documents incident and event information and generates reports on exceptions and security events. Contributes to management reporting processes.</p> <p>Investigates minor security breaches using established procedures, incorporating analytical tools and techniques. Performs non-standard operational security tasks adapting to evolving technologies and threat landscapes. Addresses and resolves a variety of security events to maintain system integrity and operational continuity.</p>

Server+ (SK0-005) – continued

Code/level	Skill name	Overall description, and Description at the specified level
SYSP	<p>System software administration Overall description</p> <p>Level 2</p> <p>Level 3</p> <p>Level 4</p>	<p>Installing, managing and maintaining operating systems, data management, office automation and utility software across various infrastructure environments.</p> <p>Assists with system software administration tasks under routine supervision. Supports the installation and configuration of system software. Helps monitor system performance and resource usage. Assists in documenting system software settings and updates.</p> <p>Monitors operational systems for resource usage and failure rates, to inform and facilitate system software tuning. Applies system software settings to optimise performance, enabling maximum throughput and efficient resource utilisation. Installs and tests new versions of system software. Assists in creating software implementation procedures, including fallback contingency plans.</p> <p>Monitors system software metrics and adjusts configurations for optimum availability and performance. Applies technical expertise to investigate and resolve complex system software issues, requesting action from supplier if required. Analyses system software updates and determines which ones require actions. Develops comprehensive software implementation procedures with robust contingency plans.</p>

Server+ (SK0-005) – continued

Code/level	Skill name	Overall description, and Description at the specified level
ITOP	<p>Infrastructure operations Overall description</p> <p>Level 1</p> <p>Level 2</p> <p>Level 3</p>	<p>Provisioning, deploying, configuring, operating, and optimising technology infrastructure across physical, virtual, and cloud-based environments.</p> <p>Supports routine infrastructure tasks and basic troubleshooting under close supervision. Monitors infrastructure health and reports on component status to support operational continuity.</p> <p>Executes operational procedures, runs automation scripts and performs routine maintenance, installation and monitoring of infrastructure components. Adjusts automation tasks as instructed to meet operational standards. Reports on infrastructure performance and security events, addressing issues directly when possible or escalating them to others for resolution.</p> <p>Provisions, deploys, and configures infrastructure services and components. Monitors infrastructure for load, performance and security events. Reports metrics and resolves operational issues. Executes standard operational procedures, including backups and restorations. Carries out agreed system software maintenance tasks. Automates routine system administration tasks to specifications using standard tools and basic scripting.</p>

Server+ (SK0-005) – continued

Code/level	Skill name	Overall description, and Description at the specified level
STMG	<p>Storage management Overall description</p> <p>Level 2</p> <p>Level 3</p>	<p>Provisioning, configuring and optimising on-premises and cloud-based storage solutions, ensuring data availability, security and alignment with business objectives.</p> <p>Assists with storage management tasks such as provisioning. Supports the setup and configuration of storage systems, incorporating standard security practices. Helps monitor storage performance and capacity, and documents storage utilisation.</p> <p>Executes routine storage management tasks following established procedures and using standard tools. Implements documented configurations for allocation of storage, installation and maintenance of secure storage systems using the agreed operational procedures. Identifies operational problems, including security-related issues, and contributes to their resolution. Uses standard management and reporting tools to collect and report on storage utilisation, performance and backup statistics.</p>
PBMG	<p>Problem management Overall description</p> <p>Level 2</p> <p>Level 3</p>	<p>Managing the lifecycle of all problems that have occurred or could occur in delivering a service.</p> <p>Assists with problem management tasks under routine supervision. Helps document problems and maintain relevant records. Assists in detecting, logging, classifying, and prioritising problems in systems, processes, and services.</p> <p>Investigates problems in systems, processes and services. Contributes to the implementation of agreed remedies and preventative measures.</p>

Server+ (SK0-005) – continued

Code/level	Skill name	Overall description, and Description at the specified level
COPL	<p>Continuity management Overall description</p> <p>Level 2</p> <p>Level 3</p>	<p>Developing, implementing and testing a business continuity framework.</p> <p>Maintains records of all related testing and training and ensures the availability of all documentation. Records the actions taken and the consequences following an incident or live testing of a continuity plan for a lessons-learned report.</p> <p>Applies a structured approach to develop and document the detail for a continuity plan. Maintains documentation of business continuity and disaster recovery plans. Supports the development of a test plan and implementation of continuity management exercises.</p>
PEDP	<p>Information and data compliance Overall description</p> <p>Level 4</p>	<p>Implementing and promoting compliance with information and data management legislation.</p> <p>Supports the implementation of policy, standards and guidelines related to information and data legislation and compliance requirements. Monitors the implementation of effective controls for internal delegation, audit and control relating to information management. Reports on the consolidated status of information controls to inform effective decision-making. Identifies risks around the use of information and data that is subject to specific legislation. Recommends remediation actions as required.</p>

Server+ (SK0-005) – continued

Code/level	Skill name	Overall description, and Description at the specified level
CHMG	<p>Change control Overall description</p> <p>Level 2</p> <p>Level 3</p>	<p>Assessing risks associated with proposed changes and ensuring changes to products, services or systems are controlled and coordinated.</p> <p>Administers, tracks, logs, reports on change requests, using appropriate tools, techniques and processes. Provides assistance to implement standard low-risk changes, in accordance with defined change control procedures.</p> <p>Develops, documents and implements changes based on requests for change. Applies change control processes and procedures. Applies tools, techniques and processes to manage and report on change requests.</p>
BURM	<p>Risk management Overall description</p> <p>Level 2</p> <p>Level 3</p>	<p>Planning and implementing processes for managing risk across the enterprise, aligned with organisational strategy and governance frameworks.</p> <p>Assists in collecting and reporting data to support risk management activities under routine supervision. Helps create and maintain documentation of risks and risk management activities. Helps identify and report issues and discrepancies.</p> <p>Undertakes basic risk management activities. Maintains documentation of risks, threats, vulnerabilities and mitigation actions.</p>

Server+ (SK0-005) – continued

Code/level	Skill name	Overall description, and Description at the specified level
CIPM	<p>Organisational change management Overall description</p> <p>Level 2</p> <p>Level 3</p>	<p>Planning, designing and implementing activities to transition the organisation and people to the required future state.</p> <p>Assists with organisational change management tasks under routine supervision. Supports the collection and analysis of data related to change readiness and impact. Helps document and communicate change management plans and activities.</p> <p>Follows standard techniques to investigate and analyse the size, nature and impact of changes to operational activities. Contributes to change management plans and actions, focusing on the procedural execution of change. Supports implementation and engages with stakeholders under direction.</p>
DEPL	<p>Deployment Overall description</p> <p>Level 2</p> <p>Level 3</p>	<p>Transitioning software from development to live usage, managing risks and ensuring it works as intended.</p> <p>Assists in deploying software releases and updates under routine supervision. Executes defined deployment processes and procedures using deployment tools and techniques. Monitors deployed applications and reports issues. Assists in rolling back deployments when necessary.</p> <p>Deploys software releases and updates to production environments. Uses deployment tools and techniques to ensure consistent deployments. Monitors and troubleshoots deployment processes. Performs rollbacks of deployments in case of issues or failures. Collaborates with release management and operations teams.</p>

Server+ (SK0-005) – continued

Code/level	Skill name	Overall description, and Description at the specified level
ASMG	<p>Asset Management Overall description</p> <p>Level 2</p> <p>Level 3</p>	<p>Managing the full life cycle of assets from acquisition, operation, maintenance to disposal.</p> <p>Uses agreed procedures to create and maintain an accurate register of assets. Performs activities related to the administration of assets. Produces routine reports to assist asset management activities and decision-making.</p> <p>Applies tools, techniques and processes to create and maintain an accurate asset register. Produces reports and analysis to support asset management activities and aid decision-making.</p>
AUDT	<p>Audit Overall description</p> <p>Level 2</p>	<p>Delivering independent, risk-based assessments of the effectiveness of processes, the controls and the compliance environment of an organisation.</p> <p>Assists in collecting evidence and conducting audit activities under routine supervision. Maintains documentation and audit trails. Helps identify and report issues and discrepancies.</p>
IAMT	<p>Identity and access management Overall description</p> <p>Level 1</p>	<p>Manages identity verification and access permissions within organisational systems and environments.</p> <p>Performs basic identity and access management tasks, including user account lifecycle management, under supervision. Maintains accurate records and follows established identity and access management protocols.</p>

CloudNetX (CN1-001)

Code/level	Skill name	Overall description, and Description at the specified level
CIPM	<p>Organisational change management Overall description</p> <p>Level 2</p> <p>Level 3</p>	<p>Planning, designing and implementing activities to transition the organisation and people to the required future state.</p> <p>Assists with organisational change management tasks under routine supervision. Supports the collection and analysis of data related to change readiness and impact. Helps document and communicate change management plans and activities.</p> <p>Follows standard techniques to investigate and analyse the size, nature and impact of changes to operational activities. Contributes to change management plans and actions, focusing on the procedural execution of change. Supports implementation and engages with stakeholders under direction.</p>
CFMG	<p>Configuration management Overall description</p> <p>Level 2</p> <p>Level 3</p>	<p>Planning, identifying, controlling, accounting for and auditing of configuration items (CIs) and their interrelationships.</p> <p>Applies tools, techniques and processes to administer, track, log, report on and correct configuration items, components and changes. Assists with audits to check the accuracy of the information and undertakes any necessary corrective action under direction.</p> <p>Applies tools, techniques and processes to track, log and correct information related to configuration items. Verifies and approves changes to protect assets and components from unauthorised change, diversion and inappropriate use. Supports user compliance with identification standards for object types, environments, processes, lifecycles, documentation, versions, formats, baselines, releases and templates. Performs audits to check the accuracy of the information and undertakes any necessary corrective action under direction.</p>

SFIA 9 and CompTIA Mappings



CloudNetX (CN1-001) - continued

Code/level	Skill name	Overall description, and Description at the specified level
IAMT	<p>Identity and access management Overall description</p> <p>Level 1</p> <p>Level 2</p> <p>Level 3</p> <p>Level 4</p>	<p>Manages identity verification and access permissions within organisational systems and environments.</p> <p>Performs basic identity and access management tasks, including user account lifecycle management, under supervision. Maintains accurate records and follows established identity and access management protocols.</p> <p>Provides assistance for identity and access management operations, including automated role allocation and access control management. Engages in user identity lifecycle management, including account creation and deletion. Facilitates operation of identity and access management tools and self-service portals.</p> <p>Administers standard identity and access management services, implementing policies and resolving related issues. Manages monitoring, audits and logging for identity and access management systems. Investigates minor security breaches in accordance with established procedures related to identity and access management. Assists users in defining their access rights and privileges. Designs and implements simple identity and access management solutions, enhancing user access security. Contributes to the enhancement and optimisation of existing identity and access management processes and systems.</p> <p>Designs and implements complex identity and access management solutions, focusing on automated access control and role allocation. Oversees the integration of identity and access management services with new technologies. Provides specialised support for complex identity and access management operations and supports implementation of policies and standards. Collaborates with stakeholders to align identity and access management with business objectives and emerging security trends.</p>

CloudNetX (CN1-001) - continued

Code/level	Skill name	Overall description, and Description at the specified level
NTDS	<p>Network design Overall description</p> <p>Level 2</p> <p>Level 3</p> <p>Level 4</p> <p>Level 5</p>	<p>Designing communication networks to meet business requirements, ensuring scalability, reliability, security and alignment with strategic objectives.</p> <p>Assists with defining configurations for networks and network components under routine supervision. Follows established network architectures, standards, and security protocols. Assists in documenting network configurations and producing detailed network specifications under guidance, incorporating relevant security aspects.</p> <p>Specifies the technical configurations and components required for a small network or a network segment in a more complex infrastructure. Follows organisational architectures, standards, and security guidelines.</p> <p>Designs specific network components using agreed architectures, design standards, patterns and methodology. Translates logical designs into physical designs that meet specified operational parameters for capacity and performance. Reviews and verifies network designs against non-functional requirements, including validation and error correction procedures, access, security and audit controls. Contributes to the development of recovery routines and contingency procedures. Contributes to alternative network architectures, networking topologies and design options.</p> <p>Produces, or approves network providers', network architectures, topologies and configuration databases for own area of responsibility. Specifies design parameters for network connectivity, capacity, speed, interfacing, security and access, in line with business requirements. Assesses network-related risks and specifies recovery routines and contingency procedures. Creates multiple design views to address the different stakeholders' concerns and to handle both functional and non-functional requirements.</p>

CloudNetX (CN1-001) - continued

Code/level	Skill name	Overall description, and Description at the specified level
NTAS	<p>Network support Overall description</p> <p>Level 1</p> <p>Level 2</p> <p>Level 3</p> <p>Level 4</p>	<p>Providing maintenance and support services for communications networks.</p> <p>Supports routine network tasks under close supervision. Monitors basic network health and reports on the status of network components. Assists with straightforward troubleshooting and follows established procedures to maintain operational continuity. Escalates issues as necessary to higher levels of support</p> <p>Assists in the operational configuration of network components and the investigation and resolution of network problems. Assists in the implementation of basic scripting and automation tools to streamline network support tasks. Assists with specified maintenance procedures and follows established safety, security and quality standards. Provides first-line support and guidance to network users, escalating issues as necessary.</p> <p>Executes agreed network maintenance tasks and specified operational configuration of network components. Identifies and diagnoses network problems/faults using the required troubleshooting tools and network management software, including addressing security-related issues. Implements and maintains scripts, automation tools and orchestration platforms to optimise network support processes. Collects performance and traffic statistics and collaborates with others to ensure network effectiveness and resolve issues.</p> <p>Executes agreed network maintenance tasks and specified operational configuration of network components. Identifies and diagnoses network problems/faults using the required troubleshooting tools and network management software, including addressing security-related issues. Implements and maintains scripts, automation tools and orchestration platforms to optimise network support processes. Collects performance and traffic statistics and collaborates with others to ensure network effectiveness and resolve issues</p>

SFIA 9 and CompTIA Mappings



CloudNetX (CN1-001) - continued

Code/level	Skill name	Overall description, and Description at the specified level
ITOP	<p>Infrastructure operations Overall description</p> <p>Level 1</p> <p>Level 2</p> <p>Level 3</p> <p>Level 4</p>	<p>Provisioning, deploying, configuring, operating, and optimising technology infrastructure across physical, virtual, and cloud-based environments.</p> <p>Supports routine infrastructure tasks and basic troubleshooting under close supervision. Monitors infrastructure health and reports on component status to support operational continuity.</p> <p>Executes operational procedures, runs automation scripts and performs routine maintenance, installation and monitoring of infrastructure components. Adjusts automation tasks as instructed to meet operational standards. Reports on infrastructure performance and security events, addressing issues directly when possible or escalating them to others for resolution.</p> <p>Provisions, deploys, and configures infrastructure services and components. Monitors infrastructure for load, performance and security events. Reports metrics and resolves operational issues. Executes standard operational procedures, including backups and restorations. Carries out agreed system software maintenance tasks. Automates routine system administration tasks to specifications using standard tools and basic scripting.</p> <p>Applies technical expertise to maintain and optimise technology infrastructure, executing updates and employing automation tools. Configures tools and/or creates scripts to automate infrastructure tasks. Maintains operational procedures and checks that they are followed, including adherence to security policies. Uses infrastructure management tools to monitor load, performance, and security metrics. Investigates and enables the resolution of operational and security-related issues. Provides reports and proposals for improvement to stakeholders. Contributes to the planning and implementation of infrastructure maintenance and updates. Implements agreed infrastructure changes and maintenance routines.</p>

CloudNetX (CN1-001) - continued

Code/level	Skill name	Overall description, and Description at the specified level
SINT	<p>Systems integration and build Overall description</p> <p>Level 2</p> <p>Level 3</p>	<p>Planning, implementing and controlling activities to integrate system elements, subsystems and interfaces to create operational systems, products or services.</p> <p>Produces builds from system components using appropriate build automation tools and processes. Conducts tests as defined in an integration test specification and records the details of any failures. Analyses and reports on integration test activities and results. Identifies and reports issues and risks.</p> <p>Defines the modules and components and dependencies needed for an integration build and produces a build definition. Accepts completed modules and components, checking that they meet defined criteria. Produces builds from system components for loading onto target environments. Configures the hardware, software and infrastructure environment as required by the system being integrated. Produces integration test specifications, conducts tests and records and reports on outcomes. Diagnoses faults and documents the results of tests. Produces system integration reports.</p>
AVMT	<p>Availability management Overall description</p> <p>Level 3</p> <p>Level 4</p>	<p>Ensuring services deliver agreed levels of availability to meet the current and future needs of the business.</p> <p>Performs defined availability management tasks, such as routine monitoring and data collection. Tests disaster recovery procedures under direction and contributes to the documentation of recovery plans. Assists with the operation of availability management tools and processes. Monitors service components against agreed performance standards and reports any deviations.</p> <p>Analyses service and component availability, reliability, maintainability and serviceability. Contributes to the availability management process and its operation. Monitors and maintains services and components to ensure ongoing compliance with agreed performance targets and service levels. Implements disaster recovery arrangements and documents recovery procedures. Conducts testing of recovery procedures.</p>

CloudNetX (CN1-001) - continued

Code/level	Skill name	Overall description, and Description at the specified level
HSIN	<p>Systems installation and removal Overall description</p> <p>Level 1</p> <p>Level 2</p> <p>Level 3</p>	<p>Installing and testing, or decommissioning and removing, systems or system components.</p> <p>Follows agreed procedures to perform simple installations, replace consumable items, and check the correct working of installations. Documents and reports on work done.</p> <p>Installs or removes system components using supplied installation instructions and tools. Conducts standard tests and contributes to investigations of problems and faults. Confirms the correct working of installations. Documents results in accordance with agreed procedures.</p> <p>Installs or removes hardware and/or software, using supplied installation instructions and tools, including handover to the client. Uses standard procedures and diagnostic tools to test installations, correct problems, and document results. Records details of all components that have been installed and removed. Assists users and follows agreed procedures for further help or escalation. Contributes to the development of installation procedures and standards.</p>
DESN	<p>Systems design Overall description</p> <p>Level 2</p> <p>Level 3</p>	<p>Designing systems to meet specified requirements and agreed systems architectures.</p> <p>Assists in the creation and documentation of system design elements under routine supervision. Follows established procedures and guidelines. Helps create and maintain documentation.</p> <p>Follows standard approaches and established design patterns to create new designs for simple systems or system components. Identifies and resolves minor design issues. Identifies alternative design options and seeks guidance when deviating from established design patterns.</p>

SFIA 9 and CompTIA Mappings



CloudNetX (CN1-001) - continued

Code/level	Skill name	Overall description, and Description at the specified level
BURM	<p>Risk management Overall description</p> <p>Level 2</p> <p>Level 3</p> <p>Level 4</p>	<p>Planning and implementing processes for managing risk across the enterprise, aligned with organisational strategy and governance frameworks.</p> <p>Assists in collecting and reporting data to support risk management activities under routine supervision. Helps create and maintain documentation of risks and risk management activities. Helps identify and report issues and discrepancies.</p> <p>Undertakes basic risk management activities. Maintains documentation of risks, threats, vulnerabilities and mitigation actions.</p> <p>Carries out risk management activities within a specific function, technical area or project of medium complexity. Identifies risks and vulnerabilities, assesses their impact and probability, develops mitigation strategies and reports to the business. Involves specialists and domain experts as necessary.</p>
ARCH	<p>Solution architecture Overall description</p> <p>Level 4</p>	<p>Developing and communicating a multi-dimensional solution architecture to deliver agreed business outcomes.</p> <p>Contributes to the development of solution architectures in specific business, infrastructure or functional areas. Identifies and evaluates alternative architectures and the trade-offs in cost, performance and scalability. Determines and documents architecturally significant decisions. Produces specifications of cloud-based or on-premises components, tiers and interfaces, for translation into detailed designs using selected services and products. Supports projects or change initiatives through the preparation of technical plans and application of design principles. Aligns solutions with enterprise and solution architecture standards (including security).</p>

CloudNetX (CN1-001) - continued

Code/level	Skill name	Overall description, and Description at the specified level
IFDN	<p>Infrastructure design Overall description</p> <p>Level 2</p> <p>Level 3</p> <p>Level 4</p>	<p>Designing technology infrastructure to meet business requirements, ensuring scalability, reliability, security and alignment with strategic objectives.</p> <p>Assists in developing preliminary infrastructure design specifications under routine supervision. Uses established standards and security protocols to contribute to infrastructure design activities. Helps draft design documents and diagrams. Documents design-related issues.</p> <p>Performs varied infrastructure design tasks, including complex and non-routine assignments, using standard methods. Develops design specifications and diagrams for infrastructure components, integrating hardware, software, network elements, and cloud services, and addressing security requirements. Collaborates with others to align infrastructure design with organisational objectives and resolve design issues. Suggests improvements to enhance infrastructure performance and reliability.</p> <p>Leads the design of complex infrastructure systems to deliver comprehensive design solutions. Develops detailed architectural frameworks and ensures integration of all infrastructure components, including cloud services. Provides guidance on recommended practices and design standards. Reviews and validates design specifications and documentation. Checks that designs are scalable, reliable and secure, aligning with business and technical requirements.</p>

CloudNetX (CN1-001) - continued

Code/level	Skill name	Overall description, and Description at the specified level
SCAD	<p>Security operations Overall description</p> <p>Level 1</p> <p>Level 2</p>	<p>Manages and administers security measures, using tools and intelligence to protect assets, ensuring compliance and operational integrity.</p> <p>Performs simple security administration tasks. Maintains relevant records and documentation, contributing to overall data integrity.</p> <p>Receives and responds to routine requests for security support. Maintains records and effectively communicates actions taken. Assists in the investigation and resolution of issues relating to security systems using basic diagnostic tools and techniques. Documents incident and event information and generates reports on exceptions and security events. Contributes to management reporting processes.</p>

CySA+ Cybersecurity Analyst (CS0-003)

Code/level	Skill name	Overall description, and Description at the specified level
SCTY	<p>Information security Overall description</p> <p>Level 2</p> <p>Level 3</p>	<p>Defining and operating a framework of security controls and security management strategies.</p> <p>Assists with implementing and monitoring security policies and protocols across different systems. Contributes to identifying and addressing potential risks in security governance and compliance. Supports the analysis of documented security incidents, escalating where appropriate. Assists in the review of access controls and permissions, ensuring adherence to security policies.</p> <p>Applies and maintains specific security controls as required by organisational policy and local risk assessments. Communicates security risks and issues to business managers and others. Performs basic risk assessments for small information systems. Contributes to the identification of risks that arise from potential technical solution architectures. Suggests alternate solutions or countermeasures to mitigate risks. Defines secure systems configurations in compliance with intended architectures. Supports investigation of suspected attacks and security breaches.</p>

CySA+ Cybersecurity Analyst (CS0-003) – continued

Code/level	Skill name	Overall description, and Description at the specified level
THIN	<p>Threat intelligence Overall description</p> <p>Level 2</p> <p>Level 3</p> <p>Level 4</p>	<p>Developing and sharing actionable insights on current and potential security threats to the success or integrity of an organisation.</p> <p>Contributes to routine threat intelligence gathering tasks. Monitors and detects potential security threats and escalates in accordance with relevant procedures and standards.</p> <p>Performs routine threat intelligence gathering tasks. Transforms collected information into a data format that can be used for operational security activities. Cleans and converts quantitative information into consistent formats.</p> <p>Collates and analyses information for threat intelligence requirements from a variety of sources. Contributes to reviewing, ranking and categorising qualitative threat intelligence information. Creates threat intelligence reports. Evaluates the value, usefulness and impact of threat intelligence sources.</p>

CySA+ Cybersecurity Analyst (CS0-003) – continued

Code/level	Skill name	Overall description, and Description at the specified level
SCAD	<p>Security operations Overall description</p> <p>Level 1</p> <p>Level 2</p> <p>Level 3</p> <p>Level 4</p>	<p>Manages and administers security measures, using tools and intelligence to protect assets, ensuring compliance and operational integrity.</p> <p>Performs simple security administration tasks. Maintains relevant records and documentation, contributing to overall data integrity.</p> <p>Receives and responds to routine requests for security support. Maintains records and effectively communicates actions taken. Assists in the investigation and resolution of issues relating to security systems using basic diagnostic tools and techniques. Documents incident and event information and generates reports on exceptions and security events. Contributes to management reporting processes.</p> <p>Investigates minor security breaches using established procedures, incorporating analytical tools and techniques. Performs non-standard operational security tasks adapting to evolving technologies and threat landscapes. Addresses and resolves a variety of security events to maintain system integrity and operational continuity.</p> <p>Maintains and optimises operational security processes. Checks that all requests for support are dealt with according to established protocols, including for cloud-based and automated systems. Provides advice on implementing and managing physical, procedural and technical security encompassing both physical and digital assets. Investigates security breaches in accordance with established procedures using advanced tools and techniques and recommends necessary corrective actions. Enables effective implementation of recommended security measures and monitors their performance.</p>

CySA+ Cybersecurity Analyst (CS0-003) – continued

Code/level	Skill name	Overall description, and Description at the specified level
TECH	<p>Specialist advice Overall description</p> <p>Level 4</p>	<p>Providing authoritative, professional advice and direction in a specialist area.</p> <p>Provides detailed and specific advice to support the organisation's planning and operations, typically related to the immediate area of responsibility. Actively maintains recognised expert level knowledge in one or more identifiable specialisms. Recognises and identifies the boundaries of their own specialist knowledge. Where appropriate, collaborates with other specialists to ensure advice given is professionally sound and appropriate to the organisation's needs.</p>
USUP	<p>Incident management Overall description</p> <p>Level 1</p> <p>Level 2</p> <p>Level 3</p>	<p>Coordinating responses to a diverse range of incidents to minimise negative impacts and quickly restore services.</p> <p>Follows agreed procedures to identify, register and categorise incidents. Uses provided tools and technologies to support the incident management process. Collects information as instructed to assist in incident resolution and allocates incidents as directed. Assists in monitoring incident queues and escalates issues according to procedures.</p> <p>Provides first line investigation and gathers information to enable incident resolution and allocate incidents. Gathers information to enable incident resolution and allocates incidents according to established procedures. Escalates incidents as necessary. Advises relevant people of actions taken. Communicates with users and stakeholders to provide updates on incident status. Assists in maintaining records and documentation related to incidents.</p> <p>Prioritises and diagnoses incidents applying agreed procedures and tools. Investigates causes of incidents and seeks resolution. Escalates unresolved incidents to higher levels or specialist teams. Coordinates with stakeholders to ensure timely resolution. Facilitates recovery, following resolution of incidents. Documents, communicates outcomes and closes resolved incidents.</p>

SFIA 9 and CompTIA Mappings



	Level 4	<p>Monitors and manages incident queues to ensure incidents are handled according to procedures and service levels. Contributes to developing, testing and improving incident management procedures. Uses analytics tools to track trends.</p> <p>Ensures resolved incidents are properly documented and closed.</p> <p>Supports team members in the correct use of the incident process.</p>
--	---------	---

CySA+ Cybersecurity Analyst (CS0-003) – continued

Code/level	Skill name	Overall description, and Description at the specified level
DGFS	<p>Digital forensics Overall description</p> <p>Level 2</p> <p>Level 3</p>	<p>Recovering and investigating material found in digital devices.</p> <p>Assists with digital forensic investigations under routine supervision. Supports the recovery of damaged, deleted or hidden data from digital devices. Helps collect and preserve digital information and evidence according to established protocols.</p> <p>Applies standard forensic tools and techniques to examine digital devices. Recovers and analyses damaged, deleted or hidden data from various digital sources and devices. Maintains the integrity of digital evidence and ensures its collection adheres to legal admissibility standards.</p>
BURM	<p>Risk management Overall description</p> <p>Level 2</p> <p>Level 3</p>	<p>Planning and implementing processes for managing risk across the enterprise, aligned with organisational strategy and governance frameworks.</p> <p>Assists in collecting and reporting data to support risk management activities under routine supervision. Helps create and maintain documentation of risks and risk management activities. Helps identify and report issues and discrepancies.</p> <p>Undertakes basic risk management activities. Maintains documentation of risks, threats, vulnerabilities and mitigation actions.</p>

CySA+ Cybersecurity Analyst (CS0-003) – continued

Code/level	Skill name	Overall description, and Description at the specified level
ITOP	<p>Infrastructure operations Overall description</p> <p>Level 1</p> <p>Level 2</p> <p>Level 3</p> <p>Level 4</p>	<p>Provisioning, deploying, configuring, operating, and optimising technology infrastructure across physical, virtual, and cloud-based environments.</p> <p>Supports routine infrastructure tasks and basic troubleshooting under close supervision. Monitors infrastructure health and reports on component status to support operational continuity.</p> <p>Executes operational procedures, runs automation scripts and performs routine maintenance, installation and monitoring of infrastructure components. Adjusts automation tasks as instructed to meet operational standards. Reports on infrastructure performance and security events, addressing issues directly when possible or escalating them to others for resolution.</p> <p>Provisions, deploys, and configures infrastructure services and components. Monitors infrastructure for load, performance and security events. Reports metrics and resolves operational issues. Executes standard operational procedures, including backups and restorations. Carries out agreed system software maintenance tasks. Automates routine system administration tasks to specifications using standard tools and basic scripting.</p> <p>Applies technical expertise to maintain and optimise technology infrastructure, executing updates and employing automation tools. Configures tools and/or creates scripts to automate infrastructure tasks. Maintains operational procedures and checks that they are followed, including adherence to security policies. Uses infrastructure management tools to monitor load, performance, and security metrics. Investigates and enables the resolution of operational and security-related issues. Provides reports and proposals for improvement to stakeholders. Contributes to the planning and implementation of infrastructure maintenance and updates. Implements agreed infrastructure changes and maintenance routines.</p>

CySA+ Cybersecurity Analyst (CS0-003) – continued

Code/level	Skill name	Overall description, and Description at the specified level
VUAS	<p>Vulnerability assessment Overall description</p> <p>Level 2</p> <p>Level 3</p> <p>Level 4</p>	<p>Identifying and classifying security vulnerabilities in networks, systems and applications and mitigating or eliminating their impact.</p> <p>Undertakes low-complexity routine vulnerability assessments using automated and semi-automated tools. Escalates issues where appropriate. Contributes to documenting the scope and evaluating the results of vulnerability assessments.</p> <p>Follows standard approaches to perform basic vulnerability assessments for small information systems. Supports creation of catalogues of information and technology assets for vulnerability assessment.</p> <p>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.</p>
PEDP	<p>Information and data compliance Overall description</p> <p>Level 4</p>	<p>Implementing and promoting compliance with information and data management legislation.</p> <p>Supports the implementation of policy, standards and guidelines related to information and data legislation and compliance requirements. Monitors the implementation of effective controls for internal delegation, audit and control relating to information management. Reports on the consolidated status of information controls to inform effective decision-making. Identifies risks around the use of information and data that is subject to specific legislation. Recommends remediation actions as required.</p>

PenTest+ (PT0-003)

Code/level	Skill name	Overall description, and Description at the specified level
PENT	<p>Penetration testing Overall description</p> <p>Level 2</p> <p>Level 3</p> <p>Level 4</p> <p>Level 5</p>	<p>Testing the effectiveness of security controls by emulating the tools and techniques of likely attackers.</p> <p>Assists with penetration testing tasks under routine supervision. Supports the execution of standard penetration tests on systems, networks and applications. Helps document and report on test results, findings and potential security risks.</p> <p>Follows standard approaches to design and execute penetration testing activities. Researches and investigates attack techniques and recommends ways to defend against them. Analyses and reports on penetration testing activities, results, issues and risks.</p> <p>Selects appropriate testing approaches using in-depth technical analysis of risks and typical vulnerabilities. Produces test scripts, materials and test packs and tests new and existing networks, systems or applications. Provides advice on penetration testing to support others. Records and analyses actions and results and modifies tests if necessary. Provides reports on progress, anomalies, risks and issues associated with the overall project.</p> <p>Plans and drives penetration testing within a defined area of business activity. Delivers objective insights into the existence of vulnerabilities, the effectiveness of defences and mitigating controls. Takes responsibility for the integrity of testing activities and coordinates the execution of these activities. Provides authoritative advice and guidance on all aspects of penetration testing. Identifies needs and implements new approaches for penetration testing. Contributes to security testing standards.</p>

PenTest+ (PT0-003) – continued

Code/level	Skill name	Overall description, and Description at the specified level
TECH	<p>Specialist advice Overall description</p> <p>Level 4</p>	<p>Providing authoritative, professional advice and direction in a specialist area.</p> <p>Provides detailed and specific advice to support the organisation's planning and operations, typically related to the immediate area of responsibility. Actively maintains recognised expert level knowledge in one or more identifiable specialisms. Recognises and identifies the boundaries of their own specialist knowledge. Where appropriate, collaborates with other specialists to ensure advice given is professionally sound and appropriate to the organisation's needs.</p>
OCOP	<p>Offensive cyber operations Overall description</p> <p>Level 2</p>	<p>Plans, executes and manages offensive cybersecurity operations, including target selection, electronic target folders and post-operation analysis.</p> <p>Supports offensive cyber operations under supervision. Assists in creating electronic target folders based on provided intelligence. Participates in basic operational tasks, following established security protocols. Assists in documenting operations and outcomes, contributing to post-operation reviews.</p>

PenTest+ (PT0-003) – continued

Code/level	Skill name	Overall description, and Description at the specified level
VURE	<p>Vulnerability research Overall description</p> <p>Level 2</p> <p>Level 3</p>	<p>Conducting applied research to discover, evaluate and mitigate new or unknown security vulnerabilities and weaknesses.</p> <p>Assists with vulnerability research tasks under routine supervision. Helps document and report findings from vulnerability research activities.</p> <p>Applies standard techniques and tools for vulnerability research. Uses available resources to update knowledge of relevant specialism. Participates in research communities. Analyses and reports on activities and results.</p>
BURM	<p>Risk management Overall description</p> <p>Level 2</p> <p>Level 3</p>	<p>Planning and implementing processes for managing risk across the enterprise, aligned with organisational strategy and governance frameworks.</p> <p>Assists in collecting and reporting data to support risk management activities under routine supervision. Helps create and maintain documentation of risks and risk management activities. Helps identify and report issues and discrepancies.</p> <p>Undertakes basic risk management activities. Maintains documentation of risks, threats, vulnerabilities and mitigation actions.</p>

PenTest+ (PT0-003) – continued

Code/level	Skill name	Overall description, and Description at the specified level
VUAS	<p>Vulnerability assessment Overall description</p> <p>Level 2</p> <p>Level 3</p> <p>Level 4</p> <p>Level 5</p>	<p>Identifying and classifying security vulnerabilities in networks, systems and applications and mitigating or eliminating their impact.</p> <p>Undertakes low-complexity routine vulnerability assessments using automated and semi-automated tools. Escalates issues where appropriate. Contributes to documenting the scope and evaluating the results of vulnerability assessments.</p> <p>Follows standard approaches to perform basic vulnerability assessments for small information systems. Supports creation of catalogues of information and technology assets for vulnerability assessment.</p> <p>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.</p> <p>Plans and manages vulnerability assessment activities within the organisation. Evaluates, selects and 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.</p>

CompTIA SecurityX (CAS-005)

Code/level	Skill name	Overall description, and Description at the specified level
SCAD	<p>Security operations Overall description</p> <p>Level 1</p> <p>Level 2</p> <p>Level 3</p> <p>Level 4</p> <p>Level 5</p>	<p>Manages and administers security measures, using tools and intelligence to protect assets, ensuring compliance and operational integrity.</p> <p>Performs simple security administration tasks. Maintains relevant records and documentation, contributing to overall data integrity.</p> <p>Receives and responds to routine requests for security support. Maintains records and effectively communicates actions taken. Assists in the investigation and resolution of issues relating to security systems using basic diagnostic tools and techniques. Documents incident and event information and generates reports on exceptions and security events. Contributes to management reporting processes.</p> <p>Investigates minor security breaches using established procedures, incorporating analytical tools and techniques. Performs non-standard operational security tasks adapting to evolving technologies and threat landscapes. Addresses and resolves a variety of security events to maintain system integrity and operational continuity.</p> <p>Maintains and optimises operational security processes. Checks that all requests for support are dealt with according to established protocols, including for cloud-based and automated systems. Provides advice on implementing and managing physical, procedural and technical security encompassing both physical and digital assets. Investigates security breaches in accordance with established procedures using advanced tools and techniques and recommends necessary corrective actions. Enables effective implementation of recommended security measures and monitors their performance.</p> <p>Oversees security operations procedures, ensuring adherence and effectiveness, including cloud security practices and automated threat responses. Reviews actual or potential security breaches and vulnerabilities and ensures they are promptly and thoroughly investigated. Recommends actions and appropriate control improvements.</p>

SFIA 9 and CompTIA Mappings



		<p>Ensures the integrity and completeness of security records, ensuring timely support and adherence to established procedures.</p> <p>Contributes to the creation and maintenance of security policies, standards and procedures integrating new compliance requirements and technology advances.</p>
--	--	--

CompTIA SecurityX (CAS-005) – continued

Code/level	Skill name	Overall description, and Description at the specified level
SCTY	<p>Information security Overall description</p> <p>Level 2</p> <p>Level 3</p> <p>Level 4</p>	<p>Defining and operating a framework of security controls and security management strategies.</p> <p>Assists with implementing and monitoring security policies and protocols across different systems. Contributes to identifying and addressing potential risks in security governance and compliance. Supports the analysis of documented security incidents, escalating where appropriate. Assists in the review of access controls and permissions, ensuring adherence to security policies.</p> <p>Applies and maintains specific security controls as required by organisational policy and local risk assessments. Communicates security risks and issues to business managers and others. Performs basic risk assessments for small information systems. Contributes to the identification of risks that arise from potential technical solution architectures. Suggests alternate solutions or countermeasures to mitigate risks. Defines secure systems configurations in compliance with intended architectures. Supports investigation of suspected attacks and security breaches.</p> <p>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 manage identified risks. Investigates suspected attacks and supports security incident management.</p>

CompTIA SecurityX (CAS-005) – continued

Code/level	Skill name	Overall description, and Description at the specified level
BURM	<p>Business risk management Overall description</p> <p>Level 2</p> <p>Level 3</p> <p>Level 4</p> <p>Level 5</p>	<p>Planning and implementing processes for managing risk across the enterprise, aligned with organisational strategy and governance frameworks.</p> <p>Assists in collecting and reporting data to support risk management activities under routine supervision. Helps create and maintain documentation of risks and risk management activities. Helps identify and report issues and discrepancies.</p> <p>Undertakes basic risk management activities. Maintains documentation of risks, threats, vulnerabilities and mitigation actions.</p> <p>Carries out risk management activities within a specific function, technical area or project of medium complexity. Identifies risks and vulnerabilities, assesses their impact and probability, develops mitigation strategies and reports to the business. Involves specialists and domain experts as necessary.</p> <p>Plans and implements complex and substantial risk management activities within a specific function, technical area, project or programme. Establishes consistent risk management processes and reporting mechanisms aligned with governance frameworks. Engages specialists and domain experts as necessary. Advises on the organisation's approach to risk management.</p>

CompTIA SecurityX (CAS-005) – continued

Code/level	Skill name	Overall description, and Description at the specified level
NTDS	<p>Network design Overall description</p> <p>Level 2</p> <p>Level 3</p> <p>Level 4</p>	<p>Designing communication networks to meet business requirements, ensuring scalability, reliability, security and alignment with strategic objectives.</p> <p>Assists with defining configurations for networks and network components under routine supervision. Follows established network architectures, standards, and security protocols. Assists in documenting network configurations and producing detailed network specifications under guidance, incorporating relevant security aspects.</p> <p>Specifies the technical configurations and components required for a small network or a network segment in a more complex infrastructure. Follows organisational architectures, standards, and security guidelines.</p> <p>Designs specific network components using agreed architectures, design standards, patterns and methodology. Translates logical designs into physical designs that meet specified operational parameters for capacity and performance. Reviews and verifies network designs against non-functional requirements, including validation and error correction procedures, access, security and audit controls. Contributes to the development of recovery routines and contingency procedures. Contributes to alternative network architectures, networking topologies and design options.</p>

CompTIA SecurityX (CAS-005) – continued

Code/level	Skill name	Overall description, and Description at the specified level
VUAS	<p>Vulnerability assessment Overall description</p> <p>Level 2</p> <p>Level 3</p> <p>Level 4</p> <p>Level 5</p>	<p>Identifying and classifying security vulnerabilities in networks, systems and applications and mitigating or eliminating their impact.</p> <p>Undertakes low-complexity routine vulnerability assessments using automated and semi-automated tools. Escalates issues where appropriate. Contributes to documenting the scope and evaluating the results of vulnerability assessments.</p> <p>Follows standard approaches to perform basic vulnerability assessments for small information systems. Supports creation of catalogues of information and technology assets for vulnerability assessment.</p> <p>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.</p> <p>Plans and manages vulnerability assessment activities within the organisation. Evaluates, selects and 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.</p>

CompTIA SecurityX (CAS-005) – continued

Code/level	Skill name	Overall description, and Description at the specified level
PEDP	<p>Information and data compliance Overall description</p> <p>Level 4</p> <p>Level 5</p>	<p>Implementing and promoting compliance with information and data management legislation.</p> <p>Supports the implementation of policy, standards and guidelines related to information and data legislation and compliance requirements. Monitors the implementation of effective controls for internal delegation, audit and control relating to information management. Reports on the consolidated status of information controls to inform effective decision-making. Identifies risks around the use of information and data that is subject to specific legislation. Recommends remediation actions as required.</p> <p>Contributes to policies, standards and guidelines for information and data compliance. Provides authoritative advice on implementing compliance controls in products, services and systems. Investigates breaches and recommends control improvements. Maintains an inventory of legislated data, conducts risk assessments and specifies necessary changes. Ensures formal requests and complaints are handled following procedures. Prepares and submits reports to relevant authorities, ensuring all compliance requirements are met.</p>

CompTIA SecurityX (CAS-005) – continued

Code/level	Skill name	Overall description, and Description at the specified level
THIN	<p>Threat intelligence Overall description</p> <p>Level 2</p> <p>Level 3</p> <p>Level 4</p>	<p>Developing and sharing actionable insights on current and potential security threats to the success or integrity of an organisation.</p> <p>Contributes to routine threat intelligence gathering tasks. Monitors and detects potential security threats and escalates in accordance with relevant procedures and standards.</p> <p>Performs routine threat intelligence gathering tasks. Transforms collected information into a data format that can be used for operational security activities. Cleans and converts quantitative information into consistent formats.</p> <p>Collates and analyses information for threat intelligence requirements from a variety of sources. Contributes to reviewing, ranking and categorising qualitative threat intelligence information. Creates threat intelligence reports. Evaluates the value, usefulness and impact of threat intelligence sources.</p>
AIDE	<p>AI and data ethics Overall description</p> <p>Level 3</p>	<p>Implementing and promoting ethical practices in the design, development, deployment and use of AI and data technologies.</p> <p>Supports ethical reviews and conducts basic impact assessments under direction. Gathers and analyses information for assessments. Reports on ethical issues and compliance with guidance from others. Documents findings from audits and reviews. Assists with documentation and communication of ethical policies. Supports others in responding to incidents.</p>

CompTIA SecurityX (CAS-005) – continued

Code/level	Skill name	Overall description, and Description at the specified level
DAAN	<p>Data analytics Overall description</p> <p>Level 2</p> <p>Level 3</p>	<p>Enabling data-driven decision making by extracting, analysing and communicating insights from structured and unstructured data.</p> <p>Assists in data preparation and analysis activities under direction. Processes and validates data to support analytics. Generates standard reports and insights using established tools and methods.</p> <p>Supports data analytics by gathering and preparing data from multiple sources. Applies analytical and statistical methods and software tools to analyse data and develop reports. Assists in identifying trends, patterns and insights that inform business decisions. Collaborates with team members to refine analysis techniques and maintain data quality.</p>

CompTIA SecurityX (CAS-005) – continued

Code/level	Skill name	Overall description, and Description at the specified level
IAMT	<p>Identity and access management Overall description</p> <p>Level 1</p> <p>Level 2</p> <p>Level 3</p> <p>Level 4</p>	<p>Manages identity verification and access permissions within organisational systems and environments.</p> <p>Performs basic identity and access management tasks, including user account lifecycle management, under supervision. Maintains accurate records and follows established identity and access management protocols.</p> <p>Provides assistance for identity and access management operations, including automated role allocation and access control management. Engages in user identity lifecycle management, including account creation and deletion. Facilitates operation of identity and access management tools and self-service portals.</p> <p>Administers standard identity and access management services, implementing policies and resolving related issues. Manages monitoring, audits and logging for identity and access management systems. Investigates minor security breaches in accordance with established procedures related to identity and access management. Assists users in defining their access rights and privileges. Designs and implements simple identity and access management solutions, enhancing user access security. Contributes to the enhancement and optimisation of existing identity and access management processes and systems.</p> <p>Designs and implements complex identity and access management solutions, focusing on automated access control and role allocation. Oversees the integration of identity and access management services with new technologies. Provides specialised support for complex identity and access management operations and supports implementation of policies and standards. Collaborates with stakeholders to align identity and access management with business objectives and emerging security trends.</p>

CompTIA SecurityX (CAS-005) – continued

Code/level	Skill name	Overall description, and Description at the specified level
IRMG	<p>Information management Overall description</p> <p>Level 3</p> <p>Level 4</p>	<p>Enabling the effective management and use of information assets.</p> <p>Supports teams and individuals to identify and organise information assets and repositories in line with policy and practices. Conducts routine searches for non-sensitive information needed to support organisational decision making. Supports users to find and access information resources based on their requirements and approved access.</p> <p>Enables the organisation to organise, control and discover information assets. Supports the organisation to identify, catalogue and categorise information types and information repositories in line with information management strategies and practices. Enables users to find information through appropriate use of metadata and search tools. Provides advice and guidance to enable good information management practices to be adopted across the organisation.</p>
DATM	<p>Data management Overall description</p> <p>Level 2</p>	<p>Developing and implementing plans, policies and practices that control, protect and optimise the value and governance of data assets.</p> <p>Assists in implementing data management activities under close guidance and supervision. Helps create and maintain documentation of data management activities. Helps identify and report issues and discrepancies.</p>

CompTIA SecurityX (CAS-005) – continued

Code/level	Skill name	Overall description, and Description at the specified level
CFMG	Configuration management Overall description Level 2	Planning, identifying, controlling, accounting for and auditing of configuration items (CIs) and their interrelationships. Applies tools, techniques and processes to administer, track, log, report on and correct configuration items, components and changes. Assists with audits to check the accuracy of the information and undertakes any necessary corrective action under direction.

CompTIA SecurityX (CAS-005) – continued

Code/level	Skill name	Overall description, and Description at the specified level
DESN	<p>Systems design Overall description</p> <p>Level 2</p> <p>Level 3</p> <p>Level 4</p>	<p>Designing systems to meet specified requirements and agreed systems architectures.</p> <p>Assists in the creation and documentation of system design elements under routine supervision. Follows established procedures and guidelines. Helps create and maintain documentation.</p> <p>Follows standard approaches and established design patterns to create new designs for simple systems or system components. Identifies and resolves minor design issues. Identifies alternative design options and seeks guidance when deviating from established design patterns.</p> <p>Designs system components using appropriate modelling techniques following agreed architectures, design standards, patterns and methodology. Identifies and evaluates alternative design options and trade-offs. Creates multiple design views to address the concerns of the different stakeholders and to handle functional and non-functional requirements. Models, simulates or prototypes the behaviour of proposed system components to enable approval by stakeholders. Produces detailed design specifications to form the basis for the construction of systems. Reviews, verifies and improves own designs against specifications.</p>
GOVN	<p>Governance Overall description</p> <p>Level 6</p>	<p>Defining and operating frameworks for decision-making, risk management, stakeholder relationships and compliance with organisational and regulatory obligations.</p> <p>Implements the governance framework to enable governance activity to be conducted. Within a defined area of accountability, determines the requirements for appropriate governance reflecting the organisation's values, ethics, risk appetite and wider governance frameworks. Communicates delegated authority, benefits, opportunities, costs and risks. Leads reviews of governance practices with appropriate and sufficient independence from management activity. Acts as the organisation's contact for relevant regulatory authorities and ensures proper relationships between the organisation and external stakeholders.</p>

SFIA 9 and CompTIA Mappings



CompTIA SecurityX (CAS-005) – continued

Code/level	Skill name	Overall description, and Description at the specified level
CIPM	<p>Organisational change management Overall description</p> <p>Level 2</p> <p>Level 3</p>	<p>Planning, designing and implementing activities to transition the organisation and people to the required future state.</p> <p>Assists with organisational change management tasks under routine supervision. Supports the collection and analysis of data related to change readiness and impact. Helps document and communicate change management plans and activities.</p> <p>Follows standard techniques to investigate and analyse the size, nature and impact of changes to operational activities. Contributes to change management plans and actions, focusing on the procedural execution of change. Supports implementation and engages with stakeholders under direction.</p>

CompTIA SecurityX (CAS-005) – continued

Code/level	Skill name	Overall description, and Description at the specified level
INAS	<p>Information assurance Overall description</p> <p>Level 2</p> <p>Level 3</p> <p>Level 4</p>	<p>Protecting against and managing risks related to the use, storage and transmission of data and information systems.</p> <p>Assists with information assurance activities under routine supervision. Helps perform basic risk assessments and supports the implementation of information assurance measures. Assists in maintaining records and documentation related to information assurance.</p> <p>Follows standard approaches for the technical assessment of information systems against information assurance policies and business objectives. Makes routine accreditation decisions. Recognises decisions that are beyond their scope and responsibility level and escalates according. Reviews and performs risk assessments and risk treatment plans. Identifies typical risk indicators and explains prevention measures. Maintains integrity of records to support and justify decisions.</p> <p>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.</p>

Data+ (DA0-001)

Code/level	Skill name	Overall description, and Description at the specified level
DATS	<p>Data science Overall description</p> <p>Level 2</p>	<p>Applying mathematics, statistics, data mining and predictive modelling techniques to gain insights, predict behaviours and generate value from data.</p> <p>Under routine supervision, applies specified data science techniques to data. Analyses and reports findings and addresses simple issues, using algorithms included within standard software frameworks and tools.</p>
NUAN	<p>Numerical analysis Overall description</p> <p>Level 4</p>	<p>Creating, analysing, implementing, testing and improving algorithms for numerically solving mathematical problems.</p> <p>Creates moderately complex algorithms using a range of mathematical techniques and with sensitivity to the limitations of the techniques. Uses sophisticated scientific computing and visualisation environments. Assesses the stability, accuracy and efficiency of algorithms and makes or recommends improvements to them. Iterates and improves models using feedback from experts as appropriate.</p>

Data+ (DA0-001) – continued

Code/level	Skill name	Overall description, and Description at the specified level
DATM	<p>Data management Overall description</p> <p>Level 2</p> <p>Level 3</p>	<p>Developing and implementing plans, policies and practices that control, protect and optimise the value and governance of data assets.</p> <p>Assists in implementing data management activities under close guidance and supervision. Helps create and maintain documentation of data management activities. Helps identify and report issues and discrepancies.</p> <p>Implements standard data management practices based on detailed organisational requirements. Monitors and maintains data quality through regular reviews and validation checks. Communicates the details of data management procedures to others, helping with their understanding and compliance.</p>
DTAN	<p>Data modelling and design Overall description</p> <p>Level 2</p>	<p>Developing models and diagrams to represent, communicate and manage data requirements and data assets.</p> <p>Establishes, modifies or maintains simple data structures and associated components. Uses specific data modelling and design techniques under guidance.</p>
BINT	<p>Business intelligence Overall description</p> <p>Level 2</p>	<p>Developing, producing and delivering regular and one-off management information to provide insights and aid decision-making.</p> <p>Assists with the creation of regular business intelligence reports using standard tools. Supports data preparation from existing sources.</p>

Data+ (DA0-001) – continued

Code/level	Skill name	Overall description, and Description at the specified level
DAAN	<p>Data analytics Overall description</p> <p>Level 2</p> <p>Level 3</p> <p>Level 4</p>	<p>Enabling data-driven decision making by extracting, analysing and communicating insights from structured and unstructured data.</p> <p>Assists in data preparation and analysis activities under direction. Processes and validates data to support analytics. Generates standard reports and insights using established tools and methods.</p> <p>Supports data analytics by gathering and preparing data from multiple sources. Applies analytical and statistical methods and software tools to analyse data and develop reports. Assists in identifying trends, patterns and insights that inform business decisions. Collaborates with team members to refine analysis techniques and maintain data quality.</p> <p>Conducts end-to-end data analysis, defining data requirements and ensuring data integrity. Applies advanced analytical and statistical techniques to extract meaningful insights and develop predictive models. Communicates complex findings to stakeholders in an understandable manner. Contributes to the development of data analytics processes and standards. Identifies opportunities for improving data analytics practices.</p>

Data+ (DA0-001) – continued

Code/level	Skill name	Overall description, and Description at the specified level
VISL	<p>Data visualisation Overall description</p> <p>Level 2</p> <p>Level 3</p> <p>Level 4</p>	<p>Facilitating understanding of data by displaying concepts, ideas, and facts using graphical representations.</p> <p>Creates standard data visuals using established products, tools and techniques, under routine supervision. Assists in updating and refining existing data visualisations to maintain effective representation of concepts, ideas and facts.</p> <p>Uses visualisation products, as guided, to design and create data visuals. Selects appropriate visualisation techniques from the options available. Engages with the target user to prototype and refine specified visualisations. Assists in developing narratives around data sets to support understanding and decision-making.</p> <p>Applies a variety of visualisation techniques and designs the content and appearance of data visuals. Operationalises and automates activities for efficient and timely production of data visuals. Selects appropriate visualisation approaches from a range of applicable options. Develops narratives around data sets to guide decision-making processes and enhance understanding of key insights. Contributes to exploration and experimentation in data visualisation.</p>
ANCC	<p>Analytical classification and coding Overall description</p> <p>Level 2</p> <p>Level 3</p>	<p>Interpreting information and assigning classifications or labels based on domain-specific knowledge, standards and guidelines to enable data analysis and use.</p> <p>Independently assigns accurate classifications/labels to a broad range of information. Interprets complex information and chooses appropriate classifications/labels. Participates in team quality improvement initiatives. Advises and guides others on classification/labelling practices.</p> <p>Assigns classifications/labels to highly complex information. Performs quality assurance checks on the work of others. Investigates and corrects complex classification/labelling errors. Delivers training to team members. Contributes to the development of classification/labelling processes and guidelines.</p>

SFIA 9 and CompTIA Mappings



DataSys+ (DS0-001)

Code/level	Skill name	Overall description, and Description at the specified level
DBAD	<p>Database administration Overall description</p> <p>Level 2</p> <p>Level 3</p> <p>Level 4</p>	<p>Installing, configuring, monitoring, maintaining databases and data stores, ensuring performance and security while adapting to evolving technologies.</p> <p>Executes operational procedures, runs automation scripts and performs routine maintenance and monitoring of databases. Adjusts automation tasks as instructed to meet operational standards for databases. Reports on database performance, addresses issues directly when possible, or escalates to others for resolution.</p> <p>Provisions, installs, configures and ensures the maintenance and reliability of databases. Monitors databases for load, performance and security events. Reports metrics and resolves operational issues. Executes standard operational procedures, including database backups and restorations. Automates routine database administration tasks to specifications using standard scripts and tools.</p> <p>Applies technical expertise to maintain and optimise databases, executing updates and employing automation tools. Configures tools and/or creates scripts to automate database tasks. Maintains operational procedures and checks that they are followed, including compliance with security policies. Uses database management tools to monitor load and performance statistics. Investigates and enables the resolution of database operational and security issues. Provides reports and proposals for improvement to stakeholders. Contributes to the planning and implementation of database maintenance and updates. Implements agreed database changes and maintenance routines.</p>

DataSys+ (DS0-001) – continued

Code/level	Skill name	Overall description, and Description at the specified level
DBDS	<p>Database design Overall description</p> <p>Level 2</p> <p>Level 3</p> <p>Level 4</p>	<p>Specifying, designing and maintaining mechanisms for storing and accessing data across various environments and platforms.</p> <p>Assists in creating and documenting detailed database designs under routine supervision. Follows established procedures and guidelines. Helps create and maintain documentation.</p> <p>Interprets installation standards to meet project needs and produces database or data warehouse component specifications. Develops physical database or data warehouse design elements, within set policies, to meet data requirements.</p> <p>Implements physical database designs to support transactional data requirements for performance and availability. Develops and maintains specialist knowledge of database and data warehouse concepts, design principles, architectures, software and facilities. Assesses proposed changes to object/data structures and evaluates alternative options. Implements data warehouse designs that support business intelligence and data analytics.</p>
COPL	<p>Continuity management Overall description</p> <p>Level 2</p> <p>Level 3</p>	<p>Developing, implementing and testing a business continuity framework.</p> <p>Maintains records of all related testing and training and ensures the availability of all documentation. Records the actions taken and the consequences following an incident or live testing of a continuity plan for a lessons-learned report.</p> <p>Applies a structured approach to develop and document the detail for a continuity plan. Maintains documentation of business continuity and disaster recovery plans. Supports the development of a test plan and implementation of continuity management exercises.</p>

DataSys+ (DS0-001) – continued

Code/level	Skill name	Overall description, and Description at the specified level
DATM	<p>Data management Overall description</p> <p>Level 2</p> <p>Level 3</p>	<p>Developing and implementing plans, policies and practices that control, protect and optimise the value and governance of data assets.</p> <p>Assists in implementing data management activities under close guidance and supervision. Helps create and maintain documentation of data management activities. Helps identify and report issues and discrepancies.</p> <p>Implements standard data management practices based on detailed organisational requirements. Monitors and maintains data quality through regular reviews and validation checks. Communicates the details of data management procedures to others, helping with their understanding and compliance.</p>
IAMT	<p>Identity and access management Overall description</p> <p>Level 2</p>	<p>Manages identity verification and access permissions within organisational systems and environments.</p> <p>Performs basic identity and access management tasks, including user account lifecycle management, under supervision. Maintains accurate records and follows established identity and access management protocols.</p>

DataSys+ (DS0-001) – continued

Code/level	Skill name	Overall description, and Description at the specified level
DTAN	<p>Data modelling and design Overall description</p> <p>Level 2</p> <p>Level 3</p> <p>Level 4</p>	<p>Developing models and diagrams to represent, communicate and manage data requirements and data assets.</p> <p>Establishes, modifies or maintains simple data structures and associated components. Uses specific data modelling and design techniques under guidance.</p> <p>Applies standard data modelling and design techniques based upon a detailed understanding of organisational requirements. Establishes, modifies and maintains data structures and associated components. Communicates and explain the details of data structures and components to others.</p> <p>Investigates enterprise data requirements where there is some complexity and ambiguity. Plans data modelling and design activities, selecting appropriate techniques and levels of detail to meet objectives. Provides advice and guidance to others using the data structures and associated components.</p>
SCTY	<p>Information security Overall description</p> <p>Level 2</p>	<p>Defining and operating a framework of security controls and security management strategies.</p> <p>Assists with implementing and monitoring security policies and protocols across different systems. Contributes to identifying and addressing potential risks in security governance and compliance. Supports the analysis of documented security incidents, escalating where appropriate. Assists in the review of access controls and permissions, ensuring adherence to security policies.</p>

DataSys+ (DS0-001) – continued

Code/level	Skill name	Overall description, and Description at the specified level
PROG	<p>Programming/software development Overall description</p> <p>Level 2</p>	<p>Developing software components to deliver value to stakeholders.</p> <p>Designs, codes, verifies, tests, documents, amends and refactors simple programs/scripts. Applies agreed standards, tools and basic security practices to achieve a well-engineered result. Reviews own work.</p>
SCAD	<p>Security operations Overall description</p> <p>Level 1</p>	<p>Manages and administers security measures, using tools and intelligence to protect assets, ensuring compliance and operational integrity.</p> <p>Performs simple security administration tasks. Maintains relevant records and documentation, contributing to overall data integrity.</p>

DataSys+ (DS0-001) – continued

Code/level	Skill name	Overall description, and Description at the specified level
STMG	<p>Storage management Overall description</p> <p>Level 2</p> <p>Level 3</p> <p>Level 4</p>	<p>Provisioning, configuring and optimising on-premises and cloud-based storage solutions, ensuring data availability, security and alignment with business objectives.</p> <p>Assists with storage management tasks such as provisioning. Supports the setup and configuration of storage systems, incorporating standard security practices. Helps monitor storage performance and capacity, and documents storage utilisation.</p> <p>Executes routine storage management tasks following established procedures and using standard tools. Implements documented configurations for allocation of storage, installation and maintenance of secure storage systems using the agreed operational procedures. Identifies operational problems, including security-related issues, and contributes to their resolution. Uses standard management and reporting tools to collect and report on storage utilisation, performance and backup statistics.</p> <p>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.</p>

DataX (DY0-001)

Code/level	Skill name	Overall description, and Description at the specified level
DAAN	<p>Data analytics Overall description</p> <p>Level 2</p> <p>Level 3</p> <p>Level 4</p> <p>Level 5</p>	<p>Enabling data-driven decision making by extracting, analysing and communicating insights from structured and unstructured data.</p> <p>Assists in data preparation and analysis activities under direction. Processes and validates data to support analytics. Generates standard reports and insights using established tools and methods.</p> <p>Supports data analytics by gathering and preparing data from multiple sources. Applies analytical and statistical methods and software tools to analyse data and develop reports. Assists in identifying trends, patterns and insights that inform business decisions. Collaborates with team members to refine analysis techniques and maintain data quality.</p> <p>Conducts end-to-end data analysis, defining data requirements and ensuring data integrity. Applies advanced analytical and statistical techniques to extract meaningful insights and develop predictive models. Communicates complex findings to stakeholders in an understandable manner. Contributes to the development of data analytics processes and standards. Identifies opportunities for improving data analytics practices.</p> <p>Manages data analytics activities, establishing frameworks and methodologies aligned with business objectives and data governance policies. Leads the implementation of data analytics solutions. Translates business needs into analytics requirements and identifies data-driven solutions. Guides the selection and application of advanced analytical techniques. Communicates insights and recommendations to senior stakeholders, influencing strategic decisions.</p>

DataX (DY0-001) – continued

Code/level	Skill name	Overall description, and Description at the specified level
DATM	<p>Data management Overall description</p> <p>Level 2</p> <p>Level 3</p> <p>Level 4</p> <p>Level 5</p>	<p>Developing and implementing plans, policies and practices that control, protect and optimise the value and governance of data assets.</p> <p>Assists in implementing data management activities under close guidance and supervision. Helps create and maintain documentation of data management activities. Helps identify and report issues and discrepancies.</p> <p>Implements standard data management practices based on detailed organisational requirements. Monitors and maintains data quality through regular reviews and validation checks. Communicates the details of data management procedures to others, helping with their understanding and compliance.</p> <p>Devises and implements data governance and master data management processes for specific subsets of data. Assesses the integrity of data from multiple sources. Advises on transformation of data between formats or media. Maintains and implements data handling procedures. Enables data availability, integrity and searchability through formal data and metadata structures and protection measures.</p> <p>Devises and implements data governance and master data management processes. Derives data management structures and metadata to support consistent data retrieval, integration, analysis, pattern recognition and interpretation across the organisation. Independently validates external information from multiple sources. Plans effective data storage, sharing and publishing practices within the organisation. Identifies and addresses issues preventing optimal use of information assets. Provides expert advice to maximise data asset value, ensuring data quality and compliance.</p>

DataX (DY0-001) – continued

Code/level	Skill name	Overall description, and Description at the specified level
MLNG	<p>Machine learning Overall description</p> <p>Level 2</p> <p>Level 3</p> <p>Level 4</p> <p>Level 5</p>	<p>Developing systems that learn from data and experience, improving performance, accuracy and adaptability in dynamic environments.</p> <p>Assists in data preparation, model training and evaluation tasks under routine supervision. Uses standard machine learning frameworks and tools to develop basic models for well-defined problems. Documents results and contributes to maintaining machine learning solutions.</p> <p>Applies established machine learning techniques and algorithms to solve business problems. Selects and prepares data for model training and evaluation. Trains, optimises and validates machine learning models using standard tools and frameworks. Deploys models into production and monitors their performance. Communicates results and limitations to stakeholders.</p> <p>Assesses the suitability of machine learning and designs and develops solutions for a range of business problems. Selects and applies appropriate techniques and algorithms based on data characteristics and business requirements. Provides guidance to others. Engineers features and optimises model performance. Implements algorithms and contributes to development, evaluation, monitoring and deployment. Applies industry-specific rules and guidelines, anticipating risks and implications. Collaborates with cross-functional teams to integrate machine learning models into production systems. Conducts in-depth performance analysis and troubleshoots issues.</p> <p>Leads the development and implementation of machine learning solutions for complex, high-impact business problems. Architects end-to-end machine learning pipelines and systems, incorporating MLOps practices. Evaluates and selects tools, frameworks and infrastructure for machine learning projects. Establishes practices and standards for machine learning development and operations. Provides expert advice and guidance on machine learning techniques and applications. Collaborates with stakeholders to align machine learning initiatives with organisational goals.</p>

SFIA 9 and CompTIA Mappings



DataX (DY0-001) – continued

Code/level	Skill name	Overall description, and Description at the specified level
DATS	<p>Data science Overall description</p> <p>Level 2</p> <p>Level 3</p> <p>Level 4</p>	<p>Applying mathematics, statistics, data mining and predictive modelling techniques to gain insights, predict behaviours and generate value from data.</p> <p>Under routine supervision, applies specified data science techniques to data. Analyses and reports findings and addresses simple issues, using algorithms included within standard software frameworks and tools.</p> <p>Applies standard data science techniques to new problems and datasets using specialised programming techniques. Identifies and selects appropriate data sources and prepares data to be used by data science models. Evaluates the outcomes and performance of data science models. Identifies and implements opportunities to train and improve models and the data they use. Publishes and reports on model outputs to meet customer needs and conform to agreed standards.</p> <p>Investigates problems and datasets to assess the usefulness of data science solutions. Applies diverse data science techniques and specialised programming languages. Understands and applies rules and guidelines specific to the industry and business, and anticipates risks and other implications of modelling. Selects, acquires and integrates data for analysis. Formulates hypotheses and evaluates data science models. Advises on the effectiveness of specific techniques based on analysis findings and research. Contributes to the development, evaluation, monitoring and deployment of data science solutions.</p>

DataX (DY0-001) – continued

Code/level	Skill name	Overall description, and Description at the specified level
VISL	<p>Data visualisation Overall description</p> <p>Level 2</p> <p>Level 3</p> <p>Level 4</p>	<p>Facilitating understanding of data by displaying concepts, ideas, and facts using graphical representations.</p> <p>Creates standard data visuals using established products, tools and techniques, under routine supervision. Assists in updating and refining existing data visualisations to maintain effective representation of concepts, ideas and facts.</p> <p>Uses visualisation products, as guided, to design and create data visuals. Selects appropriate visualisation techniques from the options available. Engages with the target user to prototype and refine specified visualisations. Assists in developing narratives around data sets to support understanding and decision-making.</p> <p>Applies a variety of visualisation techniques and designs the content and appearance of data visuals. Operationalises and automates activities for efficient and timely production of data visuals. Selects appropriate visualisation approaches from a range of applicable options. Develops narratives around data sets to guide decision-making processes and enhance understanding of key insights. Contributes to exploration and experimentation in data visualisation.</p>

DataX (DY0-001) – continued

Code/level	Skill name	Overall description, and Description at the specified level
DTAN	<p>Data modelling and design Overall description</p> <p>Level 2</p> <p>Level 3</p> <p>Level 4</p> <p>Level 5</p>	<p>Developing models and diagrams to represent, communicate and manage data requirements and data assets.</p> <p>Establishes, modifies or maintains simple data structures and associated components. Uses specific data modelling and design techniques under guidance.</p> <p>Applies standard data modelling and design techniques based upon a detailed understanding of organisational requirements. Establishes, modifies and maintains data structures and associated components. Communicates and explain the details of data structures and components to others.</p> <p>Investigates enterprise data requirements where there is some complexity and ambiguity. Plans data modelling and design activities, selecting appropriate techniques and levels of detail to meet objectives. Provides advice and guidance to others using the data structures and associated components.</p> <p>Sets standards for data modelling and design tools and techniques, advises on their application and ensures compliance. Manages the investigation of enterprise data requirements based on a detailed understanding of information requirements. Coordinates the application of analysis, design and modelling techniques to establish, modify or maintain data structures and their associated components. Manages the iteration, review and maintenance of data requirements and data models.</p>

DataX (DY0-001) – continued

Code/level	Skill name	Overall description, and Description at the specified level
DENG	<p>Data engineering Overall description</p> <p>Level 2</p> <p>Level 3</p> <p>Level 4</p>	<p>Designing, building, operationalising, securing and monitoring data pipelines and data stores.</p> <p>Assist in developing and implementing data pipelines and data stores. Performs administrative tasks to provide accessibility, retrievability, security and protection of data.</p> <p>Follows standard approaches and established design patterns to create and implement simple data pipelines and data stores to acquire and prepare data. Applies data engineering standards and tools to create and maintain data pipelines and extract, transform and load data. Carries out routine data quality checks and remediation.</p> <p>Designs, implements, and maintains complex data engineering solutions to acquire and prepare data. Creates and maintains data pipelines to connect data within and between data stores, applications and organisations. Carries out complex data quality checking and remediation.</p>
ANCC	<p>Analytical classification and coding Overall description</p> <p>Level 2</p> <p>Level 3</p>	<p>Interpreting information and assigning classifications or labels based on domain-specific knowledge, standards and guidelines to enable data analysis and use.</p> <p>Independently assigns accurate classifications/labels to a broad range of information. Interprets complex information and chooses appropriate classifications/labels. Participates in team quality improvement initiatives. Advises and guides others on classification/labelling practices.</p> <p>Assigns classifications/labels to highly complex information. Performs quality assurance checks on the work of others. Investigates and corrects complex classification/labelling errors. Delivers training to team members. Contributes to the development of classification/labelling processes and guidelines.</p>

DataX (DY0-001) – continued

Code/level	Skill name	Overall description, and Description at the specified level
NUAN	<p>Numerical analysis Overall description</p> <p>Level 4</p> <p>Level 5</p>	<p>Creating, analysing, implementing, testing and improving algorithms for numerically solving mathematical problems.</p> <p>Creates moderately complex algorithms using a range of mathematical techniques and with sensitivity to the limitations of the techniques. Uses sophisticated scientific computing and visualisation environments. Assesses the stability, accuracy and efficiency of algorithms and makes or recommends improvements to them. Iterates and improves models using feedback from experts as appropriate.</p> <p>Creates, tests and improves complex algorithms that numerically solve real-world problems. Develops mathematical and computational techniques to assist with numerical analysis. Communicates limitations such as uncertainty and systematic errors. Reviews algorithms for their conformance to design and performance standards.</p>
ARCH	<p>Solution architecture Overall description</p> <p>Level 4</p>	<p>Developing and communicating a multi-dimensional solution architecture to deliver agreed business outcomes.</p> <p>Contributes to the development of solution architectures in specific business, infrastructure or functional areas. Identifies and evaluates alternative architectures and the trade-offs in cost, performance and scalability. Determines and documents architecturally significant decisions. Produces specifications of cloud-based or on-premises components, tiers and interfaces, for translation into detailed designs using selected services and products. Supports projects or change initiatives through the preparation of technical plans and application of design principles. Aligns solutions with enterprise and solution architecture standards (including security).</p>

DataX (DY0-001) – continued

Code/level	Skill name	Overall description, and Description at the specified level
DESN	<p>Systems design Overall description</p> <p>Level 2</p> <p>Level 3</p> <p>Level 4</p>	<p>Designing systems to meet specified requirements and agreed systems architectures.</p> <p>Assists in the creation and documentation of system design elements under routine supervision. Follows established procedures and guidelines. Helps create and maintain documentation.</p> <p>Follows standard approaches and established design patterns to create new designs for simple systems or system components. Identifies and resolves minor design issues. Identifies alternative design options and seeks guidance when deviating from established design patterns.</p> <p>Designs system components using appropriate modelling techniques following agreed architectures, design standards, patterns and methodology. Identifies and evaluates alternative design options and trade-offs. Creates multiple design views to address the concerns of the different stakeholders and to handle functional and non-functional requirements. Models, simulates or prototypes the behaviour of proposed system components to enable approval by stakeholders. Produces detailed design specifications to form the basis for the construction of systems. Reviews, verifies and improves own designs against specifications.</p>

Cloud Essentials+ (CLO-002)

Code/level	Skill name	Overall description, and Description at the specified level
<p>BUSA</p>	<p>Business situation analysis Overall description</p> <p>Level 2</p> <p>Level 3</p>	<p>Investigating business situations to define recommendations for improvement action.</p> <p>Assists in investigating business situations to help identify and analyse problems and opportunities, under routine supervision. Helps collect and organise data and information to support recommendations.</p> <p>Investigates straightforward business situations to identify and analyse problems and opportunities. Contributes to the recommendation of improvements. Follows agreed standards and techniques to investigate, analyse and document business situations. Engages with stakeholders under direction.</p>
<p>BURM</p>	<p>Risk management Overall description</p> <p>Level 2</p> <p>Level 3</p>	<p>Planning and implementing organisation-wide processes and procedures for the management of risk to the success or integrity of the enterprise.</p> <p>Assists in collecting and reporting data to support risk management activities under routine supervision. Helps create and maintain documentation of risks and risk management activities. Helps identify and report issues and discrepancies.</p> <p>Undertakes basic risk management activities. Maintains documentation of risks, threats, vulnerabilities and mitigation actions.</p>

Cloud Essentials+ (CLO-002) – continued

Code/level	Skill name	Overall description, and Description at the specified level
SORC	<p>Sourcing Overall description</p> <p>Level 2</p>	<p>Managing, or providing advice on, the procurement or commissioning of products and services.</p> <p>Assists in the preparation of pre-qualification questionnaires and tender invitations in response to business cases. Assembles relevant information for tenders. Produces detailed evaluation criteria for simple tender criteria. Assists in the evaluation of tenders.</p>
FEAS	<p>Feasibility assessment Overall description</p> <p>Level 2</p> <p>Level 3</p>	<p>Defining, evaluating and describing business change options for financial, technical and business feasibility and strategic alignment.</p> <p>Assists in feasibility assessment tasks under routine supervision. Helps gather information required for feasibility assessments. Supports the identification and documentation of options for business change.</p> <p>Supports option identification and feasibility assessment. Selects and employs standard techniques to get the information required for feasibility assessment. Supports identification of tangible costs and benefits, and development of business cases.</p>
DESN	<p>Systems design Overall description</p> <p>Level 2</p> <p>Level 3</p>	<p>Designing systems to meet specified requirements and agreed systems architectures.</p> <p>Assists in the creation and documentation of system design elements under routine supervision. Follows established procedures and guidelines. Helps create and maintain documentation.</p> <p>Follows standard approaches and established design patterns to create new designs for simple systems or system components. Identifies and resolves minor design issues. Identifies alternative design options and seeks guidance when deviating from established design patterns.</p>

Cloud Essentials+ (CLO-002) – continued

SFIA 9 and CompTIA Mappings



Code/level	Skill name	Overall description, and Description at the specified level
CHMG	Change control Overall description Level 2 Level 3	Assessing risks associated with proposed changes and ensuring changes to products, services or systems are controlled and coordinated. Administers, tracks, logs, reports on change requests, using appropriate tools, techniques and processes. Provides assistance to implement standard low-risk changes, in accordance with defined change control procedures. Develops, documents and implements changes based on requests for change. Applies change control processes and procedures. Applies tools, techniques and processes to manage and report on change requests.
INAS	Information assurance Overall description Level 2	Protecting against and managing risks related to the use, storage and transmission of data and information systems. Assists with information assurance activities under routine supervision. Helps perform basic risk assessments and supports the implementation of information assurance measures. Assists in maintaining records and documentation related to information assurance.

Cloud Essentials+ (CLO-002) – continued

Code/level	Skill name	Overall description, and Description at the specified level
BUDF	<p>Budgeting and forecasting</p> <p>Overall description</p> <p>Level 2</p> <p>Level 3</p>	<p>Developing and managing financial budgets and forecasts to enable effective decision-making and resource allocation.</p> <p>Assists in gathering financial data and preparing basic budget templates under supervision. Supports the budgeting and forecasting process by completing assigned tasks.</p> <p>Performs specified tasks in the budgeting and forecasting process, including data analysis and report preparation, using standard methods. Identifies and resolves routine budgeting and forecasting issues. Communicates budget and forecast information to relevant stakeholders.</p>

Project+ (PK0-005)

Code/level	Skill name	Overall description, and Description at the specified level
PRMG	<p>Project management Overall description</p> <p>Level 4</p> <p>Level 5</p>	<p>Delivering agreed outcomes from projects using appropriate management techniques, collaboration, leadership and governance.</p> <p>Defines, documents and executes small projects or sub-projects. Works alone or with a small team actively participating in all phases of the project. Applies appropriate project management methods and tools. Identifies, assesses and manages risks effectively. Agrees project approach with stakeholders and prepares realistic project plans (including scope, schedule, quality, risk and communication plans). Tracks activities against the project schedule, managing stakeholder involvement as appropriate. Monitors costs, times, quality and resources used takes action where these exceed agreed tolerances.</p> <p>Takes full responsibility for the definition, approach, facilitation and satisfactory completion of medium-scale projects. Provides effective leadership to the project team. Adopts appropriate project management methods and tools. Manages the change control process and assesses and manages risks. Ensures that realistic project plans are maintained and delivers regular and accurate communication to stakeholders. Ensures project and product quality reviews occur on schedule and according to procedure. Ensures that project deliverables are completed within agreed cost, timescale and resource budgets, and are formally accepted, by appropriate stakeholders. Monitors costs, times, quality and resources used and takes action where performance deviates from agreed tolerances.</p>

Project+ (PK0-005) – continued

Code/level	Skill name	Overall description, and Description at the specified level
PROF	<p>Portfolio, programme and project support Overall description</p> <p>Level 2</p> <p>Level 3</p>	<p>Providing support and guidance on portfolio, programme and project management processes, procedures, tools and techniques.</p> <p>Assists with the compilation of reports for projects, programmes, or portfolios. Maintains programme and project files from supplied actual and forecast data. Works under supervision to support the administrative needs of project teams, contributing to routine project activities.</p> <p>Provides foundational support for projects, programmes, or portfolios. Assists with planning, scheduling, tracking and reporting using established project management tools and processes. Follows recommended solutions to ensure accurate documentation and communication of project progress. Collaborates closely with project teams and stakeholders, gathering updates and information to maintain project records and ensure alignment with project objectives. Participates in project boards, assurance teams and quality review meetings when necessary.</p>
BUSA	<p>Business situation analysis Overall description</p> <p>Level 2</p> <p>Level 3</p>	<p>Investigating business situations to define recommendations for improvement action.</p> <p>Assists in investigating business situations to help identify and analyse problems and opportunities, under routine supervision. Helps collect and organise data and information to support recommendations.</p> <p>Investigates straightforward business situations to identify and analyse problems and opportunities. Contributes to the recommendation of improvements. Follows agreed standards and techniques to investigate, analyse and document business situations. Engages with stakeholders under direction.</p>

Project+ (PK0-005) – continued

Code/level	Skill name	Overall description, and Description at the specified level
RLMT 	Stakeholder relationship management Overall description Level 4	<p>Systematically analysing, managing and influencing stakeholder relationships to achieve mutually beneficial outcomes through structured engagement.</p> <p>Deals with problems and issues, managing resolutions, corrective actions, lessons learned and the collection and dissemination of relevant information. Implements stakeholder engagement/communications plans. Collects and uses feedback from customers and stakeholders to help measure the effectiveness of stakeholder management. Helps develop and enhance customer and stakeholder relationships.</p>
CIPM 	Organisational change management Overall description Level 2 Level 3	<p>Planning, designing and implementing activities to transition the organisation and people to the required future state.</p> <p>Assists with organisational change management tasks under routine supervision. Supports the collection and analysis of data related to change readiness and impact. Helps document and communicate change management plans and activities.</p> <p>Follows standard techniques to investigate and analyse the size, nature and impact of changes to operational activities. Contributes to change management plans and actions, focusing on the procedural execution of change. Supports implementation and engages with stakeholders under direction.</p>

Project+ (PK0-005) – continued

Code/level	Skill name	Overall description, and Description at the specified level
BURM	<p>Risk management Overall description</p> <p>Level 2</p> <p>Level 3</p> <p>Level 4</p>	<p>Planning and implementing processes for managing risk across the enterprise, aligned with organisational strategy and governance frameworks.</p> <p>Assists in collecting and reporting data to support risk management activities under routine supervision. Helps create and maintain documentation of risks and risk management activities. Helps identify and report issues and discrepancies.</p> <p>Undertakes basic risk management activities. Maintains documentation of risks, threats, vulnerabilities and mitigation actions.</p> <p>Carries out risk management activities within a specific function, technical area or project of medium complexity. Identifies risks and vulnerabilities, assesses their impact and probability, develops mitigation strategies and reports to the business. Involves specialists and domain experts as necessary.</p>
CHMG	<p>Change control Overall description</p> <p>Level 2</p> <p>Level 3</p>	<p>Assessing risks associated with proposed changes and ensuring changes to products, services or systems are controlled and coordinated.</p> <p>Administers, tracks, logs, reports on change requests, using appropriate tools, techniques and processes. Provides assistance to implement standard low-risk changes, in accordance with defined change control procedures.</p> <p>Develops, documents and implements changes based on requests for change. Applies change control processes and procedures. Applies tools, techniques and processes to manage and report on change requests.</p>

Project+ (PK0-005) – continued

Code/level	Skill name	Overall description, and Description at the specified level
QUMG	Quality management Overall description Level 2	Defining and operating a management framework of processes and working practices to deliver the organisation's quality objectives. Assists with quality management tasks under routine supervision. Supports the development, maintenance and distribution of quality standards. Helps document and track updates to quality management processes and standards.