

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

Generic levels of responsibility

SFIA first defines seven generic levels of responsibility, with 5 attributes (Autonomy, Influence, Complexity, Business Skills and Knowledge) defined at each of the 7 levels within the SFIA structure, with level 1 being the lowest level.

Specific professional skills

On top of the foundation of the generic levels of responsibility attributes, SFIA 8 also provides definitions for 121 specific professional skills, with each skill being described at one or more of the 7 levels, reflecting the different levels of these skills that are found practiced in the working environment. For each skill there is an overall description, supported by guidance notes and differential descriptions for each of the levels at which the skill can be recognised.

Mapping between SFIA and CompTIA

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

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

The certifications covered below are:

Core:	ITF+	A+	Network+	Security+
Infrastructure:	Cloud+	Linux+	Server+	
Cybersecurity:	CySA+	PenTest+	CASP+	
Data and Analytics:	Data+			
Additional Professional:	CTT+	Cloud Essentials+	Project+	

ITF+ CompTIA IT Fundamentals (FCO-U61)

Code/level	Skill name	Overall description, and Description at the specified level(s)
ITOP	IT Infrastructure Overall description Level 1 Level 2	Deploying, configuring and operating IT Infrastructure. Contributes, under supervision, to routine infrastructure operation. Gains understanding of infrastructure components and services by following the activities of experienced colleagues. Carries out routine operational procedures, including the execution of specified automation tools/scripts. Amends existing automation tasks under supervision to gain a basic understanding of the scripting language/automation tools. Contributes to maintenance and installation. Monitors and reports on infrastructure performance to enable service delivery. Resolves issues or refers to others for assistance.
DBAD	Database administration Overall description Level 2	Overall description - Installing, configuring, monitoring, maintaining and improving the performance of databases and data stores. Assists in database support activities.
PROG	Programming / software development Overall description Level 2	Developing software components to deliver value to stakeholders. Designs, codes, verifies, tests, documents, amends and refactors simple programs/scripts. Applies agreed standards and tools to achieve a well-engineered result. Reviews own work.

ITF+ CompTIA IT Fundamentals (FCO-U61) – 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 2</p>	<p>Providing maintenance and support services for communications networks.</p> <p>Contributes to the operational configuration of network components. Assists in the investigation and resolution of network problems. Assists with specified maintenance procedures.</p>

ITF+ CompTIA IT Fundamentals (FCO-U61) – continued

Code/level	Skill name	Overall description, and Description at the specified level(s)
SCAD	Security operations Overall description Level 1 Level 2	<p>Delivering management, technical and administrative services to implement security controls and security management strategies.</p> <p>Performs simple security administration tasks. Maintains relevant records and documentation.</p> <p>Receives and responds to routine requests for security support. Maintains records and advises relevant persons of actions taken. Assists in the investigation and resolution of issues relating to access controls and security systems. Documents incident and event information and produces incident, exception, and management reports.</p>
USUP	Incident management Overall description Level 2	<p>Coordinating responses to incident reports, minimising negative impacts and restoring service as quickly as possible.</p> <p>Follows agreed procedures to identify, register and categorise incidents. Gathers information to enable incident resolution and allocates incidents as appropriate.</p>
PBMG	Problem management Overall description Level 3	<p>Managing the life cycle of all problems that have occurred or could occur in delivering a service.</p> <p>Investigates problems in systems, processes and services. Assists with the implementation of agreed remedies and preventative measures.</p>

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

Code/level	Skill name	Overall description, and Description at the specified level
ITOP	<p>IT infrastructure Overall description</p> <p>Level 1</p> <p>Level 2</p> <p>Level 3</p>	<p>Deploying, configuring and operating IT Infrastructure.</p> <p>Contributes, under supervision, to routine infrastructure operation. Gains understanding of infrastructure components and services by following the activities of experienced colleagues.</p> <p>Carries out routine operational procedures, including the execution of specified automation tools/scripts. Amends existing automation tasks under supervision to gain a basic understanding of the scripting language/automation tools. Contributes to maintenance and installation. Monitors and reports on infrastructure performance to enable service delivery. Resolves issues or refers to others for assistance.</p> <p>Provisions/installs, configures and maintains infrastructure services and components. Monitors, measures and reports on infrastructure load, performance and security events. Identifies operational issues and contributes to their resolution. Carries out agreed operational procedures, including backup/restore, using supplied infrastructure tools and scripts. 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 3</p>	<p>Designing communication networks to support strategic and operational requirements and producing network strategies, architectures, policies and related documentation.</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 and standards.</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 2</p> <p>Level 3</p>	<p>Coordinating responses to incident reports, minimising negative impacts and restoring service as quickly as possible.</p> <p>Follows agreed procedures to identify, register and categorise incidents. Gathers information to enable incident resolution and allocates incidents as appropriate.</p> <p>Provides first line investigation and gathers information to enable incident resolution and allocate incidents. Advises relevant persons of actions taken.</p>

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

Code/level	Skill name	Overall description, and Description at the specified level
NTAS	Network support Overall description Level 2 Level 3	Providing maintenance and support services for communications networks. Contributes to the operational configuration of network components. Assists in the investigation and resolution of network problems. Assists with specified maintenance procedures. Carries out agreed network maintenance tasks and specified operational configuration of network components. Establish and diagnose network problems/faults using the required troubleshooting methodology and tools. Uses network management software and tools to collect agreed performance and traffic statistics.
PBMG	Problem management Overall description Level 3	Managing the life cycle of all problems that have occurred or could occur in delivering a service. Investigates problems in systems, processes and services. Assists with the implementation of agreed remedies and preventative measures.
SCAD	Security operations Overall description Level 1 Level 2	Delivering management, technical and administrative services to implement security controls and security management strategies. Performs simple security administration tasks. Maintains relevant records and documentation. Receives and responds to routine requests for security support. Maintains records and advises relevant persons of actions taken. Assists in the investigation and resolution of issues relating to access controls and security systems. Documents incident and event information and produces incident, exception, and management reports.

A+ Core Series (220-1101 & 220-1102) – 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 and tools to achieve a well-engineered result. Reviews own work.</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. 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 Overall description</p> <p>Level 3</p>	<p>Installing, managing, controlling, deploying and maintaining infrastructure systems software, to meet operational needs and service levels.</p> <p>Monitors operational systems for resource usage and failure rates, to inform and facilitate system software tuning. Applies system software parameters to maximise throughput and efficiency. Installs and tests new versions of system software. Contributes to preparation of software implementation procedures with fall back contingency plans.</p>
STMG	<p>Storage management Overall description</p> <p>Level 3</p>	<p>Planning, implementing and optimising the technologies and processes used for data storage.</p> <p>Performs regular high-performance, scalable backups and restores on a schedule and tracks offsite storage. Implements documented configurations for allocation of storage, installation and maintenance of secure storage systems using the agreed operational procedures. Identifies operational problems and contributes to their resolution. Uses standard management and reporting tools to collect and report on storage utilisation, performance and backup statistics.</p>
CIPM	<p>Organisational change management Overall description</p> <p>Level 3</p>	<p>Planning, designing and implementing activities to transition the organisation and people to the required future state.</p> <p>Follows standard techniques to investigate and analyse the size, nature and impact of changes to operational activities. Contributes to the recommendations for change management plans and actions. Supports implementation and engages with stakeholders under direction.</p>

A+ Core Series (220-1101 & 220-1102) – 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>Assessing risks associated with proposed changes and ensuring changes to products, services or systems are controlled and coordinated.</p> <p>Applies tools, techniques and processes to administer, track, log, report on change requests. Applies change control procedures for standard, low-risk changes.</p>
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 requests for service, following agreed procedures. Promptly allocates calls as appropriate. Logs incidents and service requests and maintains relevant records.</p> <p>Responds to common requests for service by providing information to enable fulfilment. Promptly allocates unresolved calls as appropriate. Maintains records, informs users about the process and advises relevant persons of actions taken.</p>

Network+ (N10-008)

Code/level	Skill name	Overall description, and Description at the specified level
NTDS Level 3	Network design Overall description	Designing communication networks to support strategic and operational requirements and producing network strategies, architectures, policies and related documentation. Specifies the technical configurations and components required for a small network or a network segment in a more complex infrastructure. Follows organisational architectures and standards.
ITOP Level 3	IT infrastructure Overall description	Deploying, configuring and operating IT Infrastructure. Provisions/installs, configures and maintains infrastructure services and components. Monitors, measures and reports on infrastructure load, performance and security events. Identifies operational issues and contributes to their resolution. Carries out agreed operational procedures, including backup/restore, using supplied infrastructure tools and scripts. Carries out agreed system software maintenance tasks. Automates routine system administration tasks to specifications using standard tools and basic scripting.
NTAS Level 3	Network support Overall description	Providing maintenance and support services for communications networks. Carries out agreed network maintenance tasks and specified operational configuration of network components. Establish and diagnose network problems/faults using the required troubleshooting methodology and tools. Uses network management software and tools to collect agreed performance and traffic statistics.

Network+ (N10-008) – continued

Code/level	Skill name	Overall description, and Description at the specified level
SCAD	Security operations Overall description Level 1 Level 2 Level 3	<p>Delivering management, technical and administrative services to implement security controls and security management strategies.</p> <p>Performs simple security administration tasks. Maintains relevant records and documentation.</p> <p>Receives and responds to routine requests for security support. Maintains records and advises relevant persons of actions taken. Assists in the investigation and resolution of issues relating to access controls and security systems. Documents incident and event information and produces incident, exception, and management reports.</p> <p>Investigates minor security breaches in accordance with established procedures. Assists users in defining their access rights and privileges. Performs non-standard operational security tasks. Resolves security events and operational security issues.</p>
USUP	Incident management Overall description Level 3	<p>Coordinating responses to incident reports, minimising negative impacts and restoring service as quickly as possible.</p> <p>Provides first line investigation and gathers information to enable incident resolution and allocate incidents. Advises relevant persons of actions taken.</p>
PBMG	Problem management Overall description Level 3	<p>Managing the life cycle of all problems that have occurred or could occur in delivering a service.</p> <p>Investigates problems in systems, processes and services. Assists with the implementation of agreed remedies and preventative measures.</p>

Network+ (N10-008) – continued

Code/level	Skill name	Overall description, and Description at the specified level
HSIN	Systems installation and removal Overall description Level 2 Level 3	<p>Installing and testing, or decommissioning and removing, systems or system components.</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	Radio frequency engineering Overall description Level 2 Level 3	<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>

Network+ (N10-008) – 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>Applies tools, techniques and processes to administer, track, log, report on change requests. Applies change control procedures for standard, low-risk changes.</p> <p>Develops, documents and implements changes based on requests for change. Applies change control procedures. Applies tools, techniques and processes to manage and report on change requests.</p>
BURM	<p>Risk management Overall description</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>Undertakes basic risk management activities. Maintains documentation of risks, threats, vulnerabilities and mitigation actions.</p>
CIPM	<p>Organisational change management Overall description</p> <p>Level 3</p>	<p>Planning, designing and implementing activities to transition the organisation and people to the required future state.</p> <p>Follows standard techniques to investigate and analyse the size, nature and impact of changes to operational activities. Contributes to the recommendations for change management plans and actions. Supports implementation and engages with stakeholders under direction.</p>

Security+ (SY0-601)

Code/level	Skill name	Overall description, and Description at the specified level
SCTY	Information security Overall description Level 3	Defining and operating a framework of security controls and security management strategies. 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.
SCAD	Security operations Overall description Level 3	Delivering management, technical and administrative services to implement security controls and security management strategies. Investigates minor security breaches in accordance with established procedures. Assists users in defining their access rights and privileges. Performs non-standard operational security tasks. Resolves security events and operational security issues.
VURE	Vulnerability research Overall description Level 3	Conducting applied research to discover, evaluate and mitigate new or unknown security vulnerabilities and weaknesses. 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.

Security+ (SY0-601) – continued

Code/level	Skill name	Overall description, and Description at the specified level
NTAS	Network support Overall description Level 3	Providing maintenance and support services for communications networks. Carries out agreed network maintenance tasks and specified operational configuration of network components. Establish and diagnose network problems/faults using the required troubleshooting methodology and tools. Uses network management software and tools to collect agreed performance and traffic statistics.
DGFS	Digital forensics Overall description Level 4	Recovering and investigating material found in digital devices. Designs and executes complex digital forensic investigations on devices. Specifies requirements for resources and tools to perform investigations. Processes and analyses evidence in line with policy, standards and guidelines and supports the production of forensics findings and reports.
USUP	Incident management Overall description Level 3	Coordinating responses to incident reports, minimising negative impacts and restoring service as quickly as possible. Provides first line investigation and gathers information to enable incident resolution and allocate incidents. Advises relevant persons of actions taken.

Security+ (SY0-601) – continued

Code/level	Skill name	Overall description, and Description at the specified level
THIN	Threat intelligence Overall description Level 2	Developing and sharing actionable insights on current and potential security threats to the success or integrity of an organisation. Contributes to routine threat intelligence gathering tasks. Monitors and detects potential security threats and escalates in accordance with relevant procedures and standards.
BURM	Risk management Overall description Level 3 Level 4	Planning and implementing organisation-wide processes and procedures for the management of risk to the success or integrity of the enterprise. Undertakes basic risk management activities. Maintains documentation of risks, threats, vulnerabilities and mitigation actions. 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.
AUDT	Audit Overall description Level 3	Delivering independent, risk-based assessments of the effectiveness of processes, the controls, and the compliance environment of an organisation. 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.

Security+ (SY0-601) – continued

Code/level	Skill name	Overall description, and Description at the specified level
NTDS	<p>Network design Overall description</p> <p>Level 3</p> <p>Level 4</p>	<p>Designing communication networks to support strategic and operational requirements and producing network strategies, architectures, policies and related documentation.</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 and standards.</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>
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+ (SY0-601) – 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 3</p>	<p>Testing the effectiveness of security controls by emulating the tools and techniques of likely attackers.</p> <p>Follows standard approaches to design and execute penetration testing activities. Researches and investigates attack techniques and recommend ways to defend against them. Analyses and reports on penetration testing activities, results, issues and risks.</p>

Security+ (SY0-601) – continued

Code/level	Skill name	Overall description, and Description at the specified level
BURM	Risk management Overall description Level 3 Level 4	<p>Planning and implementing organisation-wide processes and procedures for the management of risk to the success or integrity of the enterprise.</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>
PEDP	Personal data protection Overall description Level 5	<p>Implementing and operating a framework of controls and management strategies to promote compliance with personal data legislation.</p> <p>Contributes to the development of policy, standards and guidelines related to personal data legislation. Provides expert advice and guidance on implementing personal data legislation controls in products, services and systems. Investigates major data breaches and recommends appropriate control improvements. Creates and maintains an inventory of data that are subject to personal data legislation. Conducts risk assessments, business impact analysis for complex information systems and specifies any required changes. Ensures that formal requests and complaints are dealt with according to approved procedures. Prepares and submits reports and registrations to relevant authorities.</p>

Security+ (SY0-601) – 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>Applies tools, techniques and processes to administer, track, log, report on change requests. Applies change control procedures for standard, low-risk changes.</p> <p>Develops, documents and implements changes based on requests for change. Applies change control procedures. Applies tools, techniques and processes to manage and report on change requests.</p>
CIPM	<p>Organisational change management Overall description</p> <p>Level 3</p>	<p>Planning, designing and implementing activities to transition the organisation and people to the required future state.</p> <p>Follows standard techniques to investigate and analyse the size, nature and impact of changes to operational activities. Contributes to the recommendations for change management plans and actions. Supports implementation and engages with stakeholders under direction.</p>

Cloud+ (CV0-003)

Code/level	Skill name	Overall description, and Description at the specified level
ITOP	IT infrastructure Overall description Level 3	Deploying, configuring and operating IT Infrastructure. Provisions/installs, configures and maintains infrastructure services and components. Monitors, measures and reports on infrastructure load, performance and security events. Identifies operational issues and contributes to their resolution. Carries out agreed operational procedures, including backup/restore, using supplied infrastructure tools and scripts. Carries out agreed system software maintenance tasks. Automates routine system administration tasks to specifications using standard tools and basic scripting.
STMG	Storage management Overall description Level 3	Planning, implementing and optimising the technologies and processes used for data storage. Performs regular high-performance, scalable backups and restores on a schedule and tracks offsite storage. Implements documented configurations for allocation of storage, installation and maintenance of secure storage systems using the agreed operational procedures. Identifies operational problems and contributes to their resolution. Uses standard management and reporting tools to collect and report on storage utilisation, performance and backup statistics.
SINT	Systems integration and build Overall description Level 2	Planning, implementing and controlling activities to synthesise system components to create operational systems, products or services. Produces software builds from software source code. 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.

Cloud+ (CV0-003) – continued

Code/level	Skill name	Overall description, and Description at the specified level
AVMT	Availability management Overall description Level 4	<p>Ensuring that services deliver agreed levels of availability to meet the current and future needs of the business.</p> <p>Analyses service and component availability, reliability, maintainability and serviceability. Contributes to the availability management process and its operation. Performs defined availability management tasks. Ensures that services and components meet and continue to meet all of their agreed performance targets and service levels. Implements arrangements for disaster recovery and documents recovery procedures. Conducts testing of recovery procedures.</p>
HSIN	Systems installation and removal Overall description Level 3	<p>Installing and testing, or decommissioning and removing, systems or system components.</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	Systems design Overall description Level 3	<p>Designing systems to meet specified requirements and agreed systems architectures.</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+ (CV0-003) – continued

Code/level	Skill name	Overall description, and Description at the specified level
SCAD	<p>Security operations Overall description</p> <p>Level 2</p>	<p>Delivering management, technical and administrative services to implement security controls and security management strategies.</p> <p>Receives and responds to routine requests for security support. Maintains records and advises relevant persons of actions taken. Assists in the investigation and resolution of issues relating to access controls and security systems. Documents incident and event information and produces incident, exception, and management reports.</p>
NTAS	<p>Network support Overall description</p> <p>Level 3</p>	<p>Providing maintenance and support services for communications networks.</p> <p>Carries out agreed network maintenance tasks and specified operational configuration of network components. Establish and diagnose network problems/faults using the required troubleshooting methodology and tools. Uses network management software and tools to collect agreed performance and traffic statistics.</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>

Cloud+ (CV0-003) – continued

Code/level	Skill name	Overall description, and Description at the specified level
PEDP	<p>Personal data protection Overall description</p> <p>Level 5</p>	<p>Implementing and operating a framework of controls and management strategies to promote compliance with personal data legislation.</p> <p>Contributes to the development of policy, standards and guidelines related to personal data legislation. Provides expert advice and guidance on implementing personal data legislation controls in products, services and systems. Investigates major data breaches and recommends appropriate control improvements. Creates and maintains an inventory of data that are subject to personal data legislation. Conducts risk assessments, business impact analysis for complex information systems and specifies any required changes. Ensures that formal requests and complaints are dealt with according to approved procedures. Prepares and submits reports and registrations to relevant authorities.</p>
CHMG	<p>Change control Overall description</p> <p>Level 2</p> <p>Level 3</p> <p>Level 4</p>	<p>Assessing risks associated with proposed changes and ensuring changes to products, services or systems are controlled and coordinated.</p> <p>Applies tools, techniques and processes to administer, track, log, report on change requests. Applies change control procedures for standard, low-risk changes.</p> <p>Develops, documents and implements changes based on requests for change. Applies change control procedures. Applies tools, techniques and processes to manage and report on change requests.</p> <p>Assesses, analyses, develops, documents and implements changes based on requests for change. Ensures that operational processes are in place for effective change control. Develops, configures and maintains tools to manage and report on the lifecycle of change requests. Identifies problems and issues and recommend corrective actions.</p>

Cloud+ (CV0-003) – continued

Code/level	Skill name	Overall description, and Description at the specified level
CIPM	Organisational change management Overall description Level 3	Planning, designing and implementing activities to transition the organisation and people to the required future state. Follows standard techniques to investigate and analyse the size, nature and impact of changes to operational activities. Contributes to the recommendations for change management plans and actions. Supports implementation and engages with stakeholders under direction.

Linux+ (XK0-005)

Code/level	Skill name	Overall description, and Description at the specified level
SYSP	<p>System software Overall description</p> <p>Level 3</p> <p>Level 4</p>	<p>Installing, managing, controlling, deploying and maintaining infrastructure systems software, to meet operational needs and service levels.</p> <p>Monitors operational systems for resource usage and failure rates, to inform and facilitate system software tuning. Applies system software parameters to maximise throughput and efficiency. Installs and tests new versions of system software. Contributes to preparation of software implementation procedures with fall back contingency plans.</p> <p>Monitors system software metrics and adjusts configurations for optimum availability and performance. Reviews system software updates and identifies those that merit action. Configures system software for required functionality and performance. Investigates and resolves system software problems, requesting action from supplier if required.</p>
HSIN	<p>Systems installation and removal Overall description</p> <p>Level 2</p> <p>Level 3</p>	<p>Installing and testing, or decommissioning and removing, systems or system components.</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>

Linux+ (XK0-005) – continued

Code/level	Skill name	Overall description, and Description at the specified level
ITOP	<p>IT Infrastructure Overall description</p> <p>Level 2</p> <p>Level 3</p>	<p>Deploying, configuring and operating IT Infrastructure.</p> <p>Carries out routine operational procedures, including the execution of specified automation tools/scripts. Amends existing automation tasks under supervision to gain a basic understanding of the scripting language/automation tools. Contributes to maintenance and installation. Monitors and reports on infrastructure performance to enable service delivery. Resolves issues or refers to others for assistance.</p> <p>Provisions/installs, configures and maintains infrastructure services and components. Monitors, measures and reports on infrastructure load, performance and security events. Identifies operational issues and contributes to their resolution. Carries out agreed operational procedures, including backup/restore, using supplied infrastructure tools and scripts. Carries out agreed system software maintenance tasks. Automates routine system administration tasks to specifications using standard tools and basic scripting.</p>
SCAD	<p>Security operations Overall description</p> <p>Level 1</p> <p>Level 2</p>	<p>Delivering management, technical and administrative services to implement security controls and security management strategies.</p> <p>Performs simple security administration tasks. Maintains relevant records and documentation.</p> <p>Receives and responds to routine requests for security support. Maintains records and advises relevant persons of actions taken. Assists in the investigation and resolution of issues relating to access controls and security systems. Documents incident and event information and produces incident, exception, and management reports.</p>

Linux+ (XK0-005) – continued

Code/level	Skill name	Overall description, and Description at the specified level
PROG	Programming/software development Overall description Level 2	Developing software components to deliver value to stakeholders. Designs, codes, verifies, tests, documents, amends and refactors simple programs/scripts. Applies agreed standards and tools to achieve a well-engineered result. Reviews own work.

Server+ (SK0-005)

Code/level	Skill name	Overall description, and Description at the specified level
HSIN	<p>Systems installation and removal Overall description</p> <p>Level 3</p>	<p>Installing and testing, or decommissioning and removing, systems or system components.</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>
AVMT	<p>Availability management Overall description</p> <p>Level 4</p>	<p>Ensuring that services deliver agreed levels of availability to meet the current and future needs of the business.</p> <p>Analyses service and component availability, reliability, maintainability and serviceability. Contributes to the availability management process and its operation. Performs defined availability management tasks. Ensures that services and components meet and continue to meet all of their agreed performance targets and service levels. Implements arrangements for disaster recovery and documents recovery procedures. Conducts testing of recovery procedures.</p>
SCAD	<p>Security operations Overall description</p> <p>Level 3</p>	<p>Delivering management, technical and administrative services to implement security controls and security management strategies.</p> <p>Investigates minor security breaches in accordance with established procedures. Assists users in defining their access rights and privileges. Performs non-standard operational security tasks. Resolves security events and operational security issues.</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 3</p>	<p>Planning, implementing and optimising the technologies and processes used for data storage.</p> <p>Performs regular high-performance, scalable backups and restores on a schedule and tracks offsite storage. Implements documented configurations for allocation of storage, installation and maintenance of secure storage systems using the agreed operational procedures. Identifies operational problems and contributes to their resolution. Uses standard management and reporting tools to collect and report on storage utilisation, performance and backup statistics.</p>
SYSP	<p>System software Overall description</p> <p>Level 3</p> <p>Level 4</p>	<p>Installing, managing, controlling, deploying and maintaining infrastructure systems software, to meet operational needs and service levels.</p> <p>Monitors operational systems for resource usage and failure rates, to inform and facilitate system software tuning. Applies system software parameters to maximise throughput and efficiency. Installs and tests new versions of system software. Contributes to preparation of software implementation procedures with fall back contingency plans.</p> <p>Monitors system software metrics and adjusts configurations for optimum availability and performance. Reviews system software updates and identifies those that merit action. Configures system software for required functionality and performance. Investigates and resolves system software problems, requesting action from supplier if required.</p>

Server+ (SK0-005) – continued

Code/level	Skill name	Overall description, and Description at the specified level
ITOP	IT infrastructure Overall description Level 3	Deploying, configuring and operating IT Infrastructure. Provisions/installs, configures and maintains infrastructure services and components. Monitors, measures and reports on infrastructure load, performance and security events. Identifies operational issues and contributes to their resolution. Carries out agreed operational procedures, including backup/restore, using supplied infrastructure tools and scripts. Carries out agreed system software maintenance tasks. Automates routine system administration tasks to specifications using standard tools and basic scripting.
PBMG	Problem management Overall description Level 4	Managing the life cycle of all problems that have occurred or could occur in delivering a service. Initiates and monitors actions to investigate and resolve problems in systems, processes and services. Determines problem fixes and remedies. Collaborates with others to implemented agreed remedies and preventative measures. Supports analysis of patterns and trends to improve problem management processes.
COPL	Continuity management Overall description Level 2 Level 3	Developing, implementing and testing a business continuity framework. Maintains records of all related testing and training and ensures the availability of all documentation. Records the actions taken and the consequences following an incident or live testing of a continuity plan for a lessons-learned report. 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.

Server+ (SK0-005) – continued

Code/level	Skill name	Overall description, and Description at the specified level
PEDP	<p>Personal data protection Overall description</p> <p>Level 5</p>	<p>Implementing and operating a framework of controls and management strategies to promote compliance with personal data legislation.</p> <p>Contributes to the development of policy, standards and guidelines related to personal data legislation. Provides expert advice and guidance on implementing personal data legislation controls in products, services and systems. Investigates major data breaches and recommends appropriate control improvements. Creates and maintains an inventory of data that are subject to personal data legislation. Conducts risk assessments, business impact analysis for complex information systems and specifies any required changes. Ensures that formal requests and complaints are dealt with according to approved procedures. Prepares and submits reports and registrations to relevant authorities.</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>Applies tools, techniques and processes to administer, track, log, report on change requests. Applies change control procedures for standard, low-risk changes.</p> <p>Develops, documents and implements changes based on requests for change. Applies change control procedures. Applies tools, techniques and processes to manage and report on change requests.</p>

Server+ (SK0-005) – continued

Code/level	Skill name	Overall description, and Description at the specified level
BURM	<p>Risk management Overall description</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>Undertakes basic risk management activities. Maintains documentation of risks, threats, vulnerabilities and mitigation actions.</p>
CIPM	<p>Organisational change management Overall description</p> <p>Level 3</p>	<p>Planning, designing and implementing activities to transition the organisation and people to the required future state.</p> <p>Follows standard techniques to investigate and analyse the size, nature and impact of changes to operational activities. Contributes to the recommendations for change management plans and actions. Supports implementation and engages with stakeholders under direction.</p>

CySA+ Cybersecurity Analyst (CS0-002)

Code/level	Skill name	Overall description, and Description at the specified level
SCTY	Information security Overall description	Defining and operating a framework of security controls and security management strategies.
	Level 3	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.
	Level4	Provides guidance on the application and operation of elementary physical, procedural and technical security controls. Explains the purpose of security controls and performs security risk and business impact analysis for medium complexity information systems. Identifies risks that arise from potential technical solution architectures. Designs alternate solutions or countermeasures and ensures they mitigate identified risks. Investigates suspected attacks and supports security incident management.
THIN	Threat intelligence Overall description	Developing and sharing actionable insights on current and potential security threats to the success or integrity of an organisation.
	Level 2	Contributes to routine threat intelligence gathering tasks. Monitors and detects potential security threats and escalates in accordance with relevant procedures and standards.
	Level 3	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.
	Level 4	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 sources of threat intelligence sources.

CySA+ Cybersecurity Analyst (CS0-002) – continued

Code/level	Skill name	Overall description, and Description at the specified level
VURE	<p>Vulnerability research Overall description</p> <p>Level 3</p> <p>Level 4</p> <p>Level 5</p>	<p>Conducting applied research to discover, evaluate and mitigate new or unknown security vulnerabilities and weaknesses.</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> <p>Designs and executes complex vulnerability research activities. Specifies requirements for environment, data, resources and tools to perform assessments. Reviews test results and modifies tests if necessary. Creates reports to communicate methodology, findings and conclusions. Advises on deception methods by exploiting identified patterns. Makes an active contribution to research communities.</p> <p>Plans and manages vulnerability research activities. Maintains a strong external network in the area of vulnerability research. Gathers information on new and emerging threats and vulnerabilities. Assesses and documents the impacts and threats to the organisation. Creates reports and shares knowledge and insights with stakeholders. Providing expert advice and guidance to support the adoption of tools and techniques for vulnerability research. Contributes to the development of organisational policies, standards, and guidelines for vulnerability research and assessment.</p>

CySA+ Cybersecurity Analyst (CS0-002) – continued

Code/level	Skill name	Overall description, and Description at the specified level
TECH	<p>Specialist advice Overall description</p> <p>Level4</p>	<p>Providing authoritative advice and direction in a specialist area.</p> <p>Provides detailed and specific advice regarding the application of their specialism to the organisation's planning and operations. Actively maintains 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 appropriate to the organisation's needs.</p>
SCAD	<p>Security operations Overall description</p> <p>Level 3</p> <p>Level 4</p>	<p>Delivering management, technical and administrative services to implement security controls and security management strategies.</p> <p>Investigates minor security breaches in accordance with established procedures. Assists users in defining their access rights and privileges. Performs non-standard operational security tasks. Resolves security events and operational security issues.</p> <p>Maintains operational security processes and checks that all requests for support are dealt with according to agreed procedures. Provides advice on defining access rights and the application and operation of elementary physical, procedural and technical security controls. Investigates security breaches in accordance with established procedures and recommends required actions. Provides support and checks that corrective actions are implemented.</p>

CySA+ Cybersecurity Analyst (CS0-002) – continued

Code/level	Skill name	Overall description, and Description at the specified level
USUP	<p>Incident management Overall description</p> <p>Level 4</p>	<p>Coordinating responses to incident reports, minimising negative impacts and restoring service as quickly as possible.</p> <p>Ensures that incidents are handled according to agreed procedures. Prioritises and diagnoses incidents. Investigates causes of incidents and seeks resolution. Escalates unresolved incidents. Facilitates recovery, following resolution of incidents. Documents and closes resolved incidents. Contributes to testing and improving incident management procedures.</p>
AUDT	<p>Audit Overall description</p> <p>Level 3</p> <p>Level 4</p>	<p>Delivering independent, risk-based assessments of the effectiveness of processes, the controls, and the compliance environment of an organisation.</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> <p>Contributes to planning and executing of risk-based audit of existing and planned processes, products, systems and services. Identifies and documents risks in detail. Identifies the root cause of issues during an audit, and communicates these effectively as risk insights. Collates evidence regarding the interpretation and implementation of control measures. Prepares and communicates reports to stakeholders, providing a factual basis for findings.</p>
DGFS	<p>Digital forensics Overall description</p> <p>Level 4</p>	<p>Recovering and investigating material found in digital devices.</p> <p>Designs and executes complex digital forensic investigations on devices. Specifies requirements for resources and tools to perform investigations. Processes and analyses evidence in line with policy, standards and guidelines and supports the production of forensics findings and reports.</p>

CySA+ Cybersecurity Analyst (CS0-002) – continued

Code/level	Skill name	Overall description, and Description at the specified level
BURM	<p>Risk management Overall description</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>Undertakes basic risk management activities. Maintains documentation of risks, threats, vulnerabilities and mitigation actions.</p>
DATS	<p>Data science Overall description</p> <p>Level 2</p> <p>Level 3</p>	<p>Applying mathematics, statistics, data mining and predictive modelling techniques to gain insights, predict behaviours and generate value from data.</p> <p>Under guidance, applies given data science techniques to data. Analyses and reports findings and remediates simple issues, using algorithms implemented in standard software frameworks and tools.</p> <p>Applies existing data science techniques to new problems and datasets using specialised programming techniques. Selects from existing 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 conforming to agreed standards.</p>

CySA+ Cybersecurity Analyst (CS0-002) – continued

Code/level	Skill name	Overall description, and Description at the specified level
ITOP	<p>IT infrastructure Overall description</p> <p>Level 1</p> <p>Level 2</p> <p>Level 3</p> <p>Level 4</p>	<p>Deploying, configuring and operating IT Infrastructure.</p> <p>Contributes, under supervision, to routine infrastructure operation. Gains understanding of infrastructure components and services by following the activities of experienced colleagues.</p> <p>Carries out routine operational procedures, including the execution of specified automation tools/scripts. Amends existing automation tasks under supervision to gain a basic understanding of the scripting language/automation tools. Contributes to maintenance and installation. Monitors and reports on infrastructure performance to enable service delivery. Resolves issues or refers to others for assistance.</p> <p>Provisions/installs, configures and maintains infrastructure services and components. Monitors, measures and reports on infrastructure load, performance and security events. Identifies operational issues and contributes to their resolution. Carries out agreed operational procedures, including backup/restore, using supplied infrastructure tools and scripts. Carries out agreed system software maintenance tasks. Automates routine system administration tasks to specifications using standard tools and basic scripting.</p> <p>Provides technical expertise to enable the correct application of operational procedures. Contributes to the planning and implementation of infrastructure maintenance and updates. Implements agreed infrastructure changes and maintenance routines. Uses infrastructure management tools to determine load and performance statistics. Configures tools and/or creates scripts to automate the provisioning, testing and deployment of new and changed infrastructure. Maintains operational procedures and checks that they are executed following agreed standards. Investigates and enables the resolution of operational issues. Provides reports and proposals for improvement, to specialists, users and managers.</p>

CySA+ Cybersecurity Analyst (CS0-002) – 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 performs 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>Personal data protection Overall description</p> <p>Level 5</p>	<p>Implementing and operating a framework of controls and management strategies to promote compliance with personal data legislation.</p> <p>Contributes to the development of policy, standards and guidelines related to personal data legislation. Provides expert advice and guidance on implementing personal data legislation controls in products, services and systems. Investigates major data breaches and recommends appropriate control improvements. Creates and maintains an inventory of data that are subject to personal data legislation. Conducts risk assessments, business impact analysis for complex information systems and specifies any required changes. Ensures that formal requests and complaints are dealt with according to approved procedures. Prepares and submits reports and registrations to relevant authorities.</p>

CySA+ Cybersecurity Analyst (CS0-002) – continued

Code/level	Skill name	Overall description, and Description at the specified level
SLEN	<p>Systems and software life cycle engineering Overall description</p> <p>Level 4</p>	<p>Establishing and deploying an environment for developing, continually improving, and securely operating software and systems products and services.</p> <p>Elicits requirements for systems and software life cycle working practices and automation. Prepares design options for the working environment of methods, procedures, techniques, tools, and people. Selects systems and software life cycle working practices for software components and micro-services. Deploys automation to achieve well-engineered and secure outcomes.</p>
CIPM	<p>Organisational change management Overall description</p> <p>Level 3</p>	<p>Planning, designing and implementing activities to transition the organisation and people to the required future state.</p> <p>Follows standard techniques to investigate and analyse the size, nature and impact of changes to operational activities. Contributes to the recommendations for change management plans and actions. Supports implementation and engages with stakeholders under direction.</p>

CySA+ Cybersecurity Analyst (CS0-002) – continued

Code/level	Skill name	Overall description, and Description at the specified level
BPTS	Acceptance testing Overall description Level 2 Level 3	<p>Validating systems, products, business processes or services to determine whether the acceptance criteria have been satisfied.</p> <p>Assists in planning, preparing and executing acceptance tests for systems, products, business processes or services. Assists in collecting feedback from acceptance testing.</p> <p>Follows agreed standards and techniques to devise and execute test cases and scenarios based on pre-defined acceptance criteria. Analyses and reports on test activities, results, issues and risks.</p>
CHMG	Change control Overall description Level 2 Level 3	<p>Assessing risks associated with proposed changes and ensuring changes to products, services or systems are controlled and coordinated.</p> <p>Applies tools, techniques and processes to administer, track, log, report on change requests. Applies change control procedures for standard, low-risk changes.</p> <p>Develops, documents and implements changes based on requests for change. Applies change control procedures. Applies tools, techniques and processes to manage and report on change requests.</p>

PenTest+ (PT0-002)

Code/level	Skill name	Overall description, and Description at the specified level
PENT	<p>Penetration testing Overall description</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>Follows standard approaches to design and execute penetration testing activities. Researches and investigates attack techniques and recommend ways to defend against them. Analyses and reports on penetration testing activities, results, issues and risks.</p> <p>Selects appropriate testing approach 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>
TECH	<p>Specialist advice Overall description</p> <p>Level4</p>	<p>Providing authoritative advice and direction in a specialist area.</p> <p>Provides detailed and specific advice regarding the application of their specialism to the organisation's planning and operations. Actively maintains 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 appropriate to the organisation's needs.</p>

PenTest+ (PT0-002) – continued

Code/level	Skill name	Overall description, and Description at the specified level
AUDT	Audit Overall description Level 3 Level 4	<p>Delivering independent, risk-based assessments of the effectiveness of processes, the controls, and the compliance environment of an organisation.</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> <p>Contributes to planning and executing of risk-based audit of existing and planned processes, products, systems and services. Identifies and documents risks in detail. Identifies the root cause of issues during an audit, and communicates these effectively as risk insights. Collates evidence regarding the interpretation and implementation of control measures. Prepares and communicates reports to stakeholders, providing a factual basis for findings.</p>
DATS	Data science Overall description Level 2 Level 3	<p>Applying mathematics, statistics, data mining and predictive modelling techniques to gain insights, predict behaviours and generate value from data.</p> <p>Under guidance, applies given data science techniques to data. Analyses and reports findings and remediates simple issues, using algorithms implemented in standard software frameworks and tools.</p> <p>Applies existing data science techniques to new problems and datasets using specialised programming techniques. Selects from existing 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 conforming to agreed standards.</p>

PenTest+ (PT0-002) – continued

Code/level	Skill name	Overall description, and Description at the specified level
SCTY	<p>Information security Overall description</p> <p>Level 3</p>	<p>Defining and operating a framework of security controls and security management strategies.</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>
VURE	<p>Vulnerability research Overall description</p> <p>Level 3</p> <p>Level 4</p> <p>Level 5</p>	<p>Conducting applied research to discover, evaluate and mitigate new or unknown security vulnerabilities and weaknesses.</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> <p>Designs and executes complex vulnerability research activities. Specifies requirements for environment, data, resources and tools to perform assessments. Reviews test results and modifies tests if necessary. Creates reports to communicate methodology, findings and conclusions. Advises on deception methods by exploiting identified patterns. Makes an active contribution to research communities.</p> <p>Plans and manages vulnerability research activities. Maintains a strong external network in the area of vulnerability research. Gathers information on new and emerging threats and vulnerabilities. Assesses and documents the impacts and threats to the organisation. Creates reports and shares knowledge and insights with stakeholders. Providing expert advice and guidance to support the adoption of tools and techniques for vulnerability research. Contributes to the development of organisational policies, standards, and guidelines for vulnerability research and assessment.</p>

PenTest+ (PT0-002) – continued

Code/level	Skill name	Overall description, and Description at the specified level
VUAS	Vulnerability assessment Overall description	Identifying and classifying security vulnerabilities in networks, systems and applications and mitigating or eliminating their impact.
	Level 2	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.
	Level 3	Follows standard approaches to performs basic vulnerability assessments for small information systems. Supports creation of catalogues of information and technology assets for vulnerability assessment.
	Level 4	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.
	Level 5	Plans and manages vulnerability assessment activities within the organisation. Evaluates and selects, reviews vulnerability assessment tools and techniques. Provides expert advice and guidance to support the adoption of agreed approaches. Obtains and acts on vulnerability information and conducts security risk assessments, business impact analysis and accreditation on complex information systems.
BURM	Risk management Overall description	Planning and implementing organisation-wide processes and procedures for the management of risk to the success or integrity of the enterprise.
	Level 3	Undertakes basic risk management activities. Maintains documentation of risks, threats, vulnerabilities and mitigation actions.

CASP+ CompTIA Advanced Security Practitioner (CAS-004)

Code/level	Skill name	Overall description, and Description at the specified level
SCTY	<p>Information security Overall description</p> <p>Level 4</p>	<p>Defining and operating a framework of security controls and security management strategies.</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 mitigate identified risks. Investigates suspected attacks and supports security incident management.</p>
SCAD	<p>Security operations Overall description</p> <p>Level 4</p>	<p>Delivering management, technical and administrative services to implement security controls and security management strategies.</p> <p>Maintains operational security processes and checks that all requests for support are dealt with according to agreed procedures. Provides advice on defining access rights and the application and operation of elementary physical, procedural and technical security controls. Investigates security breaches in accordance with established procedures and recommends required actions. Provides support and checks that corrective actions are implemented.</p>
AUDT	<p>Audit Overall description</p> <p>Level 4</p>	<p>Delivering independent, risk-based assessments of the effectiveness of processes, the controls, and the compliance environment of an organisation.</p> <p>Contributes to planning and executing of risk-based audit of existing and planned processes, products, systems and services. Identifies and documents risks in detail. Identifies the root cause of issues during an audit, and communicates these effectively as risk insights. Collates evidence regarding the interpretation and implementation of control measures. Prepares and communicates reports to stakeholders, providing a factual basis for findings.</p>

CASP+ CompTIA Advanced Security Practitioner (CAS-004) – continued

Code/level	Skill name	Overall description, and Description at the specified level
DGFS	<p>Digital forensics Overall description</p> <p>Level 5</p>	<p>Recovering and investigating material found in digital devices.</p> <p>Conducts investigations to correctly gather, analyse and present findings, including digital evidence, to both business and legal audiences. Collates conclusions and recommendations and presents forensics findings to stakeholders. Plans and manages digital forensics activities within the organisation. Provides expert advice on digital forensics. Contributes to the development of digital forensics policies, standards and guidelines. Evaluates and selects digital forensics tools and techniques.</p>
USUP	<p>Incident management Overall description</p> <p>Level 4</p>	<p>Coordinating responses to incident reports, minimising negative impacts and restoring service as quickly as possible.</p> <p>Ensures that incidents are handled according to agreed procedures. Prioritises and diagnoses incidents. Investigates causes of incidents and seeks resolution. Escalates unresolved incidents. Facilitates recovery, following resolution of incidents. Documents and closes resolved incidents. Contributes to testing and improving incident management procedures.</p>
BURM	<p>Business risk management Overall description</p> <p>Level 5</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>Plans and implements complex and substantial risk management activities within a specific function, technical area, project or programme. Implements consistent and reliable risk management processes and reporting to key stakeholders. Engages specialists and domain experts as necessary. Advises on the organisation's approach to risk management.</p>

CASP+ CompTIA Advanced Security Practitioner (CAS-004) – continued

Code/level	Skill name	Overall description, and Description at the specified level
NTDS	<p>Network design Overall description</p> <p>Level 3</p> <p>Level 4</p> <p>Level 5</p>	<p>Designing communication networks to support strategic and operational requirements and producing network strategies, architectures, policies and related documentation.</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 and standards.</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>
AVMT	<p>Availability management Overall description</p> <p>Level 5</p>	<p>Ensuring that services deliver agreed levels of availability to meet the current and future needs of the business.</p> <p>Provides advice and guidance on the planning, design and improvement of service and component availability. Investigates all breaches of availability targets and service non-availability and initiates remedial activities. Develops plans for disaster recovery together with supporting processes. Manages the testing of disaster recovery plans.</p>

CASP+ CompTIA Advanced Security Practitioner (CAS-004) – continued

Code/level	Skill name	Overall description, and Description at the specified level
VURE	Vulnerability research Overall description	Conducting applied research to discover, evaluate and mitigate new or unknown security vulnerabilities and weaknesses.
	Level 3	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.
	Level 4	Designs and executes complex vulnerability research activities. Specifies requirements for environment, data, resources and tools to perform assessments. Reviews test results and modifies tests if necessary. Creates reports to communicate methodology, findings and conclusions. Advises on deception methods by exploiting identified patterns. Makes an active contribution to research communities.
	Level 5	Plans and manages vulnerability research activities. Maintains a strong external network in the area of vulnerability research. Gathers information on new and emerging threats and vulnerabilities. Assesses and documents the impacts and threats to the organisation. Creates reports and shares knowledge and insights with stakeholders. Providing expert advice and guidance to support the adoption of tools and techniques for vulnerability research. Contributes to the development of organisational policies, standards, and guidelines for vulnerability research and assessment.

CASP+ CompTIA Advanced Security Practitioner (CAS-004) – continued

Code/level	Skill name	Overall description, and Description at the specified level
VUAS	Vulnerability assessment Overall description	Identifying and classifying security vulnerabilities in networks, systems and applications and mitigating or eliminating their impact.
	Level 2	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.
	Level 3	Follows standard approaches to performs basic vulnerability assessments for small information systems. Supports creation of catalogues of information and technology assets for vulnerability assessment.
	Level 4	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.
	Level 5	Plans and manages vulnerability assessment activities within the organisation. Evaluates and selects, reviews vulnerability assessment tools and techniques. Provides expert advice and guidance to support the adoption of agreed approaches. Obtains and acts on vulnerability information and conducts security risk assessments, business impact analysis and accreditation on complex information systems.
PORT	Software configuration Overall description	Designing and deploying software product configurations into software environments or platforms.
	Level 3	Assists in designing, verifying, documenting, amending and refactoring moderately complex software configurations for deployment. Applies agreed standards and tools, to achieve a well-engineered result. Collaborates in reviews of work with others as appropriate.

CASP+ CompTIA Advanced Security Practitioner (CAS-004) – 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 sources of threat intelligence sources.</p>
PEDP	<p>Personal data protection Overall description</p> <p>Level 5</p>	<p>Implementing and operating a framework of controls and management strategies to promote compliance with personal data legislation.</p> <p>Contributes to the development of policy, standards and guidelines related to personal data legislation. Provides expert advice and guidance on implementing personal data legislation controls in products, services and systems. Investigates major data breaches and recommends appropriate control improvements. Creates and maintains an inventory of data that are subject to personal data legislation. Conducts risk assessments, business impact analysis for complex information systems and specifies any required changes. Ensures that formal requests and complaints are dealt with according to approved procedures. Prepares and submits reports and registrations to relevant authorities.</p>

CASP+ CompTIA Advanced Security Practitioner (CAS-004) – continued

Code/level	Skill name	Overall description, and Description at the specified level
CHMG	Change control Overall description	Assessing risks associated with proposed changes and ensuring changes to products, services or systems are controlled and coordinated.
	Level 2	Applies tools, techniques and processes to administer, track, log, report on change requests. Applies change control procedures for standard, low-risk changes.
	Level 3	Develops, documents and implements changes based on requests for change. Applies change control procedures. Applies tools, techniques and processes to manage and report on change requests.
	Level 4	Assesses, analyses, develops, documents and implements changes based on requests for change. Ensures that operational processes are in place for effective change control. Develops, configures and maintains tools to manage and report on the lifecycle of change requests. Identifies problems and issues and recommend corrective actions.
IRMG	Information management Overall description	Planning, implementing and controlling the full life cycle management of digitally organised information and records.
	Level 4	Supports the implementation of information and records management policies and standard practice. Monitors the implementation of effective controls for internal delegation, audit and control relating to information and records management. Reports on the consolidated status of information controls to inform effective decision-making. Identifies risks around the use of information. Recommends remediation actions as required.

CASP+ CompTIA Advanced Security Practitioner (CAS-004) – continued

Code/level	Skill name	Overall description, and Description at the specified level
GOVN Level 6	Governance Overall description	Defining and operating a framework for making decisions, managing stakeholder relationships, and identifying legitimate authority. Implements the governance framework to enable governance activity to be conducted. Within a defined area of accountability, determines the requirements for appropriate governance reflecting the organisation's values, ethics and wider governance frameworks. Communicates delegated authority, benefits, opportunities, costs, and risks. Leads reviews of governance practices with appropriate and sufficient independence from management activity. Acts as the organisation's contact for relevant regulatory authorities and ensures proper relationships between the organisation and external stakeholders.
ITMG Level 5	Technology service management Overall description	Managing the provision of technology-based services to meet defined organisational needs. Takes responsibility for managing the design, procurement, installation, upgrading, operation, control, maintenance and effective use of specific technology services. Leads the delivery of services, ensuring that agreed service levels, security requirements and other quality standards are met. Ensures adherence to relevant policies and procedures. Ensures that processes and practices are aligned across teams and providers to operate effectively and efficiently. Monitors the performance of technology services. Provides appropriate status and other reports to managers and senior users.
CIPM Level 3	Organisational change management Overall description	Planning, designing and implementing activities to transition the organisation and people to the required future state. Follows standard techniques to investigate and analyse the size, nature and impact of changes to operational activities. Contributes to the recommendations for change management plans and actions. Supports implementation and engages with stakeholders under direction.

Data+ (DA0-001)

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>Designs and implements 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>
STPL	<p>Enterprise and business architecture Overall description</p> <p>Level 5</p>	<p>Aligning an organisation's technology strategy with its business mission, strategy, and processes and documenting this using architectural models.</p> <p>Develops models and plans to drive the execution of the business strategy, taking advantage of opportunities to improve business performance. Contributes to creating and reviewing a systems capability strategy which meets the business's strategic requirements. Determines requirements and specifies effective business processes, through improvements in technology, information or data practices, organisation, roles, procedures and equipment.</p>

Data+ (DA0-001) – continued

Code/level	Skill name	Overall description, and Description at the specified level
DATS	Data science Overall description	Applying mathematics, statistics, data mining and predictive modelling techniques to gain insights, predict behaviours and generate value from data.
	Level 2	Under guidance, applies given data science techniques to data. Analyses and reports findings and remediates simple issues, using algorithms implemented in standard software frameworks and tools.
	Level 3	Applies existing data science techniques to new problems and datasets using specialised programming techniques. Selects from existing 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 conforming to agreed standards.
	Level 4	Investigates the described problem and dataset to assess the usefulness of data science and analytics solutions. Applies a range of data science techniques and uses specialised programming languages. Understands and applies rules and guidelines specific to the industry, and anticipates risks and other implications of modelling. Selects, acquires and integrates data for analysis. Develops data hypotheses and methods and evaluates analytics models. Advises on the effectiveness of specific techniques based on project findings and comprehensive research. Contributes to the development, evaluation, monitoring and deployment of data science solutions.
NUAN	Numerical analysis Overall description	Creating, analysing, implementing, testing and improving algorithms for numerically solving mathematical problems.
	Level 4	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.

Data+ (DA0-001) – continued

Code/level	Skill name	Overall description, and Description at the specified level
INAS	<p>Information assurance Overall description</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>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>
PEDP	<p>Personal data protection Overall description</p> <p>Level 5</p>	<p>Implementing and operating a framework of controls and management strategies to promote compliance with personal data legislation.</p> <p>Contributes to the development of policy, standards and guidelines related to personal data legislation. Provides expert advice and guidance on implementing personal data legislation controls in products, services and systems. Investigates major data breaches and recommends appropriate control improvements. Creates and maintains an inventory of data that are subject to personal data legislation. Conducts risk assessments, business impact analysis for complex information systems and specifies any required changes. Ensures that formal requests and complaints are dealt with according to approved procedures. Prepares and submits reports and registrations to relevant authorities.</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 4</p>	<p>Developing and implementing plans, policies, and practices that control, protect and optimise the value of data assets.</p> <p>Devises and implements master data management processes for specific subsets of data. Assesses the integrity of data from multiple sources. Provides advice on the transformation of data from one format/medium to another. Maintains and implements information handling procedures. Enables the availability, integrity and searchability of information through the application of formal data and metadata structures and protection measures.</p>
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 and communicate 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 requirements. Establishes, modifies and maintains data structures and associated components. Communicates the details of data structures and associated components to others using the data structures and associated components.</p> <p>Investigates enterprise data requirements where there is some complexity and ambiguity. Plans own data modelling and design activities, selecting appropriate techniques and the correct level of detail for meeting assigned objectives. Provides advice and guidance to others using the data structures and associated components.</p>

Data+ (DA0-001) – continued

Code/level	Skill name	Overall description, and Description at the specified level
BINT	<p>Business intelligence Overall description</p> <p>Level 2</p> <p>Level 3</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> <p>Sources and prepares data for analysis and performs standard business intelligence analysis activities. Creates and delivers standard reports in accordance with stakeholder needs and conforming to agreed standards. Investigates the need for new or revised business intelligence analysis. Contributes to the recommendation of improvements. Engages with stakeholders under direction.</p>
VISL	<p>Data visualisation Overall description</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>Uses a visualisation product, 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.</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. Contributes to exploration and experimentation in data visualisation.</p>

CTT+ Certified Technical Trainer (TK0-201 and TK0-202 or TK0-203)

Code/level	Skill name	Overall description, and Description at the specified level
LEDA	Competency assessment Overall description Level 3 Level 4	<p>Assessing knowledge, skills, competency and behaviours by any means, whether formal or informal, against frameworks such as SFIA.</p> <p>Performs routine assessments of knowledge, skill, competency or behaviour using specified methods.</p> <p>Performs routine and non-routine assessments of knowledge, skill, competency or behaviour using specified methods. Provides advice and guidance to support the adoption of assessment methods and tools. Moderates assessments conducted by other assessors. Reviews and improves usage and application of assessment methods and tools.</p>
TMCR	Learning design and development Overall description Level 3 Level 4	<p>Designing and developing resources to transfer knowledge, develop skills and change behaviours.</p> <p>Designs, creates, customises and maintains learning materials and resources to deliver agreed outcomes, and meet accreditation requirements when appropriate. Contributes to the design, configuration and testing of learning environments.</p> <p>Specifies the content and structure of learning and development materials. Takes responsibility for design, creation, packaging and maintenance and manages development to deliver agreed outcomes. Where required, designs, configures and tests learning environments. Secures external accreditations as appropriate.</p>

CTT+ Certified Technical Trainer (TK0-201 and TK0-202 or TK0-203) – continued

Code/level	Skill name	Overall description, and Description at the specified level
ETDL	<p>Learning delivery Overall description</p> <p>Level 2</p> <p>Level 3</p> <p>Level 4</p>	<p>Transferring knowledge, developing skills and changing behaviours using a range of techniques, resources and media.</p> <p>Performs a range of learning activities under direction to support the delivery of learning objectives. Assists in the preparation of learning environments. Observes learners performing practical activities and work, providing assistance within routine enquiries and escalating where needed.</p> <p>Delivers learning activities to a variety of audiences using prepared materials to meet established learning objectives. Uses established guidelines for the preparation of the environment. Assists with the development and maintenance of examples and case study materials. Appropriately uses a range of learning delivery techniques to enable learners to develop skills, capability, techniques and required knowledge. Observes learners performing practical activities and work. Advises and assists where necessary. Provides detailed instruction where necessary and responds to questions, seeking advice in exceptional conditions beyond own experience.</p> <p>Prepares and delivers learning activities for a variety of audiences to meet learning objectives. Contributes to the design and selection of appropriate environments. Effectively uses a broad range of learning delivery techniques to enable learners to develop skills, capability, techniques and required knowledge. Develops and updates examples and case study materials. Observes and evaluates learners performing practical activities and work. Advises and assists learners to enable the delivery of learning objectives. Tailors the approach to learning delivery to enhance the experience of learners. Provides detailed instruction as necessary and responds to detailed questions in own area of specialisation. Adapts materials to meet the needs of learners.</p>

CTT+ Certified Technical Trainer (TK0-201 and TK0-202 or TK0-203) – continued

Code/level	Skill name	Overall description, and Description at the specified level
TEAC	<p>Teaching Overall description</p> <p>Level 2</p> <p>Level 3</p> <p>Level 4</p> <p>Level 5</p>	<p>Delivering and assessing curricula in a structured and systematic education environment.</p> <p>Contributes to the delivery of aspects of computing and IT curricula in a formal educational context. Applies good practice in learning content design, development and delivery. Assesses student performance in aspects of a curriculum area, providing support to enhance student understanding as needed.</p> <p>Delivers the majority of a curriculum. Applies good practice in learning content design, development and delivery. Maintains awareness of relevant pedagogical and domain research. Assesses student performance across a curriculum. Provides feedback and support to help students improve their understanding.</p> <p>Delivers a curriculum. Applies good practice supported by pedagogical research to learning content design, development and delivery. Assesses student performance and reviews cohort performance. Advises and assists students to enable the achievement of learning objectives.</p> <p>Leads the teaching and assessment of a curriculum or learning pathway. Implements enhancement strategies for teaching and assessment. Reviews pedagogical research and practices relevant to topics in the curricula. Applies good teaching practices in learning content design, development and delivery. Contributes to the development and implementation of specialist teaching practices needed by the curriculum. Evaluates and monitors student achievements and the effectiveness of teaching activities across the curriculum. Advises on the use of appropriate pedagogies and assessment approaches.</p>

CTT+ Certified Technical Trainer (TK0-201 and TK0-202 or TK0-203) – continued

Code/level	Skill name	Overall description, and Description at the specified level
OFCL	Organisational facilitation Overall description Level 4	Supporting workgroups to implement principles and practices for effective teamwork across organisational boundaries and professional specialisms. Facilitates a series of group activities or workshops in situations of complexity and ambiguity and competing stakeholder needs. Designs a structured sequence of meetings, events or workshops to solve complex problems. Understands required outcomes and outputs from teams and facilitates the team to deliver these. Helps to improve team processes and performance in workshops or meetings, events or workshops.
SUBF	Subject formation Overall description Level 4	Specifying, designing and developing curricula within a structured and systematic education environment. Contributes to curriculum development by selecting or specifying curriculum content or assessment approaches for one or more specialist areas.

Cloud Essentials+ (CLO-002)

Code/level	Skill name	Overall description, and Description at the specified level
BUSA	Business situation analysis Overall description Level 3	Investigating business situations to define recommendations for improvement action. 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.
SORC	Sourcing Overall description Level 2	Managing, or providing advice on, the procurement or commissioning of products and services. 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.
BURM	Risk management Overall description Level 3	Planning and implementing organisation-wide processes and procedures for the management of risk to the success or integrity of the enterprise. Undertakes basic risk management activities. Maintains documentation of risks, threats, vulnerabilities and mitigation actions.

Cloud Essentials+ (CLO-002) – continued

Code/level	Skill name	Overall description, and Description at the specified level
FEAS Level 3	Feasibility assessment Overall description	Defining, evaluating and describing business change options for financial, technical and business feasibility, and strategic alignment. 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.
DESN Level 3	Systems design Overall description	Designing systems to meet specified requirements and agreed systems architectures. 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.
CHMG Level 2 Level 3	Change control Overall description	Assessing risks associated with proposed changes and ensuring changes to products, services or systems are controlled and coordinated. Applies tools, techniques and processes to administer, track, log, report on change requests. Applies change control procedures for standard, low-risk changes. Develops, documents and implements changes based on requests for change. Applies change control procedures. Applies tools, techniques and processes to manage and report on change requests.

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 portfolio, programme and project management reports. Maintains programme and project files from supplied actual and forecast data.</p> <p>Provides administrative services to project boards, project assurance teams and quality review meetings. Uses recommended portfolio, programme and project control solutions for planning, scheduling and tracking. Sets up project files, compiles and distributes reports. Provides guidance on project management software, procedures, processes, tools and techniques.</p>
BUSA	<p>Business situation analysis Overall description</p> <p>Level 3</p>	<p>Investigating business situations to define recommendations for improvement action.</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	<p>Stakeholder relationship management Overall description</p> <p>Level 4</p>	<p>Influencing stakeholder attitudes, decisions, and actions for mutual benefit.</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 plan. 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	<p>Organisational change management Overall description</p> <p>Level 3</p>	<p>Planning, designing and implementing activities to transition the organisation and people to the required future state.</p> <p>Follows standard techniques to investigate and analyse the size, nature and impact of changes to operational activities. Contributes to the recommendations for change management plans and actions. Supports implementation and engages with stakeholders under direction.</p>