SFIA and CompTIA

Mappings

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

Generic levels of responsibility

SFIA first defines seven generic levels of responsibility, with 5 characteristics (Autonomy, Influence, Complexity, Knowledge and Business Skills) 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 characteristics, SFIA also provides definitions for 102 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 definition, supported by differential definitions 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 definition and the differential definition 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+	
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 definition	The operation and control of the IT infrastructure (comprising physical or virtual hardware, software, network services and data storage) either on-premises or provisioned as cloud services) that is required to deliver and support the information systems needs of a business. Includes preparation for new or changed services, operation of the change process, the maintenance of regulatory, legal and professional standards, the building and management of systems and components in virtualised and cloud computing environments and the monitoring of performance of systems and services in relation to their contribution to business performance, their security and their sustainability. The application of infrastructure management tools to automate the provisioning, testing, deployment and monitoring of infrastructure components.
	Level 1	Contributes, under supervision, to infrastructure operation.
	Level 2	Carries out agreed operational procedures of a routine nature. Contributes to maintenance, installation and problem resolution.
DBAD	**Database administration** Overall definition	The installation, configuration, upgrade, administration, monitoring and maintenance of databases. Providing support for operational databases in production use and for internal or interim purposes such as iterative developments and testing. Improving the performance of databases and the tools and processes for database administration (including automation).
	Level 2	Assists in database support activities.
PROG	**Programming / software development** Overall definition	The planning, designing, creation, amending, verification, testing and documentation of new and amended software components in order to deliver agreed value to stakeholders. The identification, creation and application of agreed software development and security standards and processes. Adopting and adapting software development lifecycle models based on the context of the work and selecting appropriately from predictive (plan-driven) approaches or adaptive (iterative/agile) approaches.
	Level 2	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	**Systems installation/ decommissioning** Overall definition	The installation, testing, implementation or decommissioning and removal of cabling, wiring, equipment, hardware and associated software, following plans and instructions and in accordance with agreed standards. The testing of hardware and software components, resolution of malfunctions, and recording of results. The reporting of details of hardware and software installed so that configuration management records can be updated.
	Level 1	Following agreed procedures, performs simple installations, replaces consumable items, checks correct working of installations, and documents and reports on work done.
	Level 2	Installs or removes hardware and/or software, and associated connections, using supplied installation instructions and tools. Conducts tests and corrects malfunctions. Documents results in accordance with agreed procedures. Assists with the evaluation of change requests. Contributes, as required, to investigations of problems and faults concerning the installation of hardware and/or software and confirms the correct working of installations.
NTAS	**Network support** Overall definition	The provision of network maintenance and support services. Support may be provided both to users of the systems and to service delivery functions. Support typically takes the form of investigating and resolving problems and providing information about the systems. It may also include monitoring their performance. Problems may be resolved by providing advice or training to users about the network's functionality, correct operation or constraints, by devising work-arounds, correcting faults, or making general or site-specific modifications.
	Level 2	Assists in investigation and resolution of network problems. Assists with specified maintenance procedures.

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

Code/level	Skill name	Overall description, and Description at the specified level(s)
SCAD	**Security administration** Overall definition	The provision of operational security management and administrative services. Typically includes the authorisation and monitoring of access to IT facilities or infrastructure, the investigation of unauthorised access and compliance with relevant legislation.
	Level 1	Performs simple security administration tasks. Maintains relevant records and documentation.
	Level 2	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.
USUP	**Incident management** Overall definition	The processing and coordination of appropriate and timely responses to incident reports, including channelling requests for help to appropriate functions for resolution, monitoring resolution activity, and keeping clients appraised of progress towards service restoration.
	Level 2	Following agreed procedures, identifies, registers and categorises incidents. Gathers information to enable incident resolution and promptly allocates incidents as appropriate.
PBMG	**Problem management** Overall definition	The resolution (both reactive and proactive) of problems throughout the information system lifecycle, including classification, prioritisation and initiation of action, documentation of root causes and implementation of remedies to prevent future incidents.
	Level 3	Investigates problems in systems, processes and services. Assists with the implementation of agreed remedies and preventative measures.

A+ Core Series (220-1001 & 220-1002)

Code/level	Skill name	Overall description, and Description at the specified level
ITOP	**IT Infrastructure** Overall definition	The operation and control of the IT infrastructure (comprising physical or virtual hardware, software, network services and data storage) either on-premises or provisioned as cloud services) that is required to deliver and support the information systems needs of a business. Includes preparation for new or changed services, operation of the change process, the maintenance of regulatory, legal and professional standards, the building and management of systems and components in virtualised and cloud computing environments and the monitoring of performance of systems and services in relation to their contribution to business performance, their security and their sustainability. The application of infrastructure management tools to automate the provisioning, testing, deployment and monitoring of infrastructure components.
	Level 3	Carries out agreed operational procedures, including infrastructure configuration, installation and maintenance. Uses infrastructure management tools to collect and report on load and performance statistics and to automate the provisioning, testing and deployment of new and changed infrastructure. Contributes to the implementation of maintenance and installation work. Uses standard procedures and tools to carry out defined system backups, restoring data where necessary. Identifies operational problems and contributes to their resolution.
HSIN	**Systems installation/ decommissioning** Overall definition	The installation, testing, implementation or decommissioning and removal of cabling, wiring, equipment, hardware and associated software, following plans and instructions and in accordance with agreed standards. The testing of hardware and software components, resolution of malfunctions, and recording of results. The reporting of details of hardware and software installed so that configuration management records can be updated.
	Level 2	Installs or removes hardware and/or software, and associated connections, using supplied installation instructions and tools. Conducts tests and corrects malfunctions. Documents results in accordance with agreed procedures. Assists with the evaluation of change requests. Contributes, as required, to investigations of problems and faults concerning the installation of hardware and/or software and confirms the correct working of installations.

A+ Core Series (220-1001 & 220-1002) – continued

Code/level	Skill name	Overall description, and Description at the specified level
NTAS	**Network support** Overall definition	The provision of network maintenance and support services. Support may be provided both to users of the systems and to service delivery functions. Support typically takes the form of investigating and resolving problems and providing information about the systems. It may also include monitoring their performance. Problems may be resolved by providing advice or training to users about the network's functionality, correct operation or constraints, by devising work-arounds, correcting faults, or making general or site-specific modifications.
	Level 2	Assists in investigation and resolution of network problems. Assists with specified maintenance procedures.
PBMG	**Problem management** Overall definition	The resolution (both reactive and proactive) of problems throughout the information system lifecycle, including classification, prioritisation and initiation of action, documentation of root causes and implementation of remedies to prevent future incidents.
	Level 3	Investigates problems in systems, processes and services. Assists with the implementation of agreed remedies and preventative measures.
SCAD	**Security administration** Overall definition	The provision of operational security management and administrative services. Typically includes the authorisation and monitoring of access to IT facilities or infrastructure, the investigation of unauthorised access and compliance with relevant legislation.
	Level 2	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.
USUP	**Incident management** Overall definition	The processing and coordination of appropriate and timely responses to incident reports, including channelling requests for help to appropriate functions for resolution, monitoring resolution activity, and keeping clients appraised of progress towards service restoration.
	Level 2	Following agreed procedures, identifies, registers and categorises incidents. Gathers information to enable incident resolution and promptly allocates incidents as appropriate.

Network+ (N10-007)

Code/level	Skill name	Overall description, and Description at the specified level
ITOP	**IT Infrastructure** Overall definition	The operation and control of the IT infrastructure (comprising physical or virtual hardware, software, network services and data storage) either on-premises or provisioned as cloud services) that is required to deliver and support the information systems needs of a business. Includes preparation for new or changed services, operation of the change process, the maintenance of regulatory, legal and professional standards, the building and management of systems and components in virtualised and cloud computing environments and the monitoring of performance of systems and services in relation to their contribution to business performance, their security and their sustainability. The application of infrastructure management tools to automate the provisioning, testing, deployment and monitoring of infrastructure components.
	Level 3	Carries out agreed operational procedures, including infrastructure configuration, installation and maintenance. Uses infrastructure management tools to collect and report on load and performance statistics and to automate the provisioning, testing and deployment of new and changed infrastructure. Contributes to the implementation of maintenance and installation work. Uses standard procedures and tools to carry out defined system backups, restoring data where necessary. Identifies operational problems and contributes to their resolution.
NTAS	**Network support** Overall definition	The provision of network maintenance and support services. Support may be provided both to users of the systems and to service delivery functions. Support typically takes the form of investigating and resolving problems and providing information about the systems. It may also include monitoring their performance. Problems may be resolved by providing advice or training to users about the network's functionality, correct operation or constraints, by devising work-arounds, correcting faults, or making general or site-specific modifications.
	Level 3	Identifies and resolves network problems following agreed procedures. Uses network management software and tools to collect agreed performance statistics. Carries out agreed network maintenance tasks.

Network+ (N10-007) – continued

Code/level	Skill name	Overall description, and Description at the specified level
SCAD	**Security administration** Overall definition Level 3	The provision of operational security management and administrative services. Typically includes the authorisation and monitoring of access to IT facilities or infrastructure, the investigation of unauthorised access and compliance with relevant legislation. Investigates minor security breaches in accordance with established procedures. Assists users in defining their access rights and privileges. Performs non-standard security administration tasks and resolves security administration issues.
USUP	**Incident management** Overall definition Level 3	The processing and coordination of appropriate and timely responses to incident reports, including channelling requests for help to appropriate functions for resolution, monitoring resolution activity, and keeping clients appraised of progress towards service restoration. Following agreed procedures, identifies, registers and categorises incidents. Gathers information to enable incident resolution and promptly allocates incidents as appropriate. Maintains records and advises relevant persons of actions taken.
RFEN	**Radio frequency engineering** Overall definition Level 2	The deployment, integration, calibration, tuning and maintenance of radio frequency (RF) and analogue elements of IT systems. Assists with setting up, tuning and functional checks of radio frequency/analogue elements. Resolves faults down to line replaceable unit (LRU) level or escalates according to given procedures. Carries out user confidence checks and escalates faults according to given procedures.

Security+ (SY0-501)

Code/level	Skill name	Overall description, and Description at the specified level
SCTY	**Information security** Overall definition	The selection, design, justification, implementation and operation of controls and management strategies to maintain the security, confidentiality, integrity, availability, accountability and relevant compliance of information systems with legislation, regulation and relevant standards.
	Level 3	Communicates information security risks and issues to business managers and others. Performs basic risk assessments for small information systems. Contributes to vulnerability assessments. Applies and maintains specific security controls as required by organisational policy and local risk assessments. Investigates suspected attacks. Responds to security breaches in line with security policy and records the incidents and action taken.
SCAD	**Security administration** Overall definition	The provision of operational security management and administrative services. Typically includes the authorisation and monitoring of access to IT facilities or infrastructure, the investigation of unauthorised access and compliance with relevant legislation.
	Level 3	Investigates minor security breaches in accordance with established procedures. Assists users in defining their access rights and privileges. Performs non-standard security administration tasks and resolves security administration issues.
CORE	**Conformance review** Overall definition	The independent assessment of the conformity of any activity, process, deliverable, product or service to the criteria of specified standards, best practice, or other documented requirements. May relate to, for example, asset management, network security tools, firewalls and internet security, sustainability, real-time systems, application design and specific certifications.
	Level 3	Collects and collates evidence as part of a formally conducted and planned review of activities, processes, products or services. Examines records as part of specified testing strategies for evidence of compliance with management directives, or the identification of abnormal occurrences.

Security+ (SY0-501) – continued

Code/level	Skill name	Overall description, and Description at the specified level
NTAS	**Network support** Overall definition	The provision of network maintenance and support services. Support may be provided both to users of the systems and to service delivery functions. Support typically takes the form of investigating and resolving problems and providing information about the systems. It may also include monitoring their performance. Problems may be resolved by providing advice or training to users about the network's functionality, correct operation or constraints, by devising work-arounds, correcting faults, or making general or site-specific modifications.
	Level 3	Identifies and resolves network problems following agreed procedures. Uses network management software and tools to collect agreed performance statistics. Carries out agreed network maintenance tasks.
DGFS	**Digital forensics** Overall definition	The collection, processing, preserving, analysis, and presentation of forensic evidence based on the totality of findings including computer-related evidence in support of security vulnerability mitigation and/or criminal, fraud, counterintelligence, or law enforcement investigations.
	Level 4	Contributes to digital forensic investigations. Processes and analyses evidence in line with policy, standards and guidelines and supports production of forensics findings and reports.
USUP	**Incident management** Overall definition	The processing and coordination of appropriate and timely responses to incident reports, including channelling requests for help to appropriate functions for resolution, monitoring resolution activity, and keeping clients appraised of progress towards service restoration.
	Level 3	Following agreed procedures, identifies, registers and categorises incidents. Gathers information to enable incident resolution and promptly allocates incidents as appropriate. Maintains records and advises relevant persons of actions taken.

Cloud+ (CV0-002)

Code/level	Skill name	Overall description, and Description at the specified level
ITOP	**IT Infrastructure** Overall definition	The operation and control of the IT infrastructure (comprising physical or virtual hardware, software, network services and data storage) either on-premises or provisioned as cloud services) that is required to deliver and support the information systems needs of a business. Includes preparation for new or changed services, operation of the change process, the maintenance of regulatory, legal and professional standards, the building and management of systems and components in virtualised and cloud computing environments and the monitoring of performance of systems and services in relation to their contribution to business performance, their security and their sustainability. The application of infrastructure management tools to automate the provisioning, testing, deployment and monitoring of infrastructure components.
	Level 3	Carries out agreed operational procedures, including infrastructure configuration, installation and maintenance. Uses infrastructure management tools to collect and report on load and performance statistics and to automate the provisioning, testing and deployment of new and changed infrastructure. Contributes to the implementation of maintenance and installation work. Uses standard procedures and tools to carry out defined system backups, restoring data where necessary. Identifies operational problems and contributes to their resolution.
STMG	**Storage management** Overall definition	The planning, implementation, configuration and tuning of storage hardware and software covering online, offline, remote and offsite data storage (backup, archiving and recovery) and ensuring compliance with regulatory and security requirements.
	Level 3	Performs regular high-performance, scalable backups and restores on a schedule and tracks offsite storage. Carries out documented configuration for allocation of storage, installation and maintenance of secure storage systems as per the agreed operational procedure. 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.

Cloud+ (CV0-002) – continued

Code/level	Skill name	Overall description, and Description at the specified level
AVMT	**Availability management**	The definition, analysis, planning, measurement, maintenance and improvement of all aspects of the availability of services, including the availability of power. The overall control and management of service availability to ensure that the level of service delivered in all services is matched to or exceeds the current and future agreed needs of the business, in a cost effective manner.
	Level 4	Contributes to the availability management process and its operation and performs defined availability management tasks. Analyses service and component availability, reliability, maintainability and serviceability. 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.
HSIN	**Systems installation/ decommissioning** Overall definition	The installation, testing, implementation or decommissioning and removal of cabling, wiring, equipment, hardware and associated software, following plans and instructions and in accordance with agreed standards. The testing of hardware and software components, resolution of malfunctions, and recording of results. The reporting of details of hardware and software installed so that configuration management records can be updated.
	Level 3	Installs or removes hardware and/or software, using supplied installation instructions and tools including, where appropriate, handover to the client. Conducts tests, corrects malfunctions, and documents results in accordance with agreed procedures. Reports details of all hardware/software items that have been installed and removed so that configuration management records can be updated. Provides assistance to users in a professional manner following agreed procedures for further help or escalation. Reviews change requests. Maintains accurate records of user requests, contact details and outcomes. Contributes to the development of installation procedures and standards.

Cloud+ (CV0-002) – continued

Code/level	Skill name	Overall description, and Description at the specified level
SCAD	**Security administration** Overall definition Level 2	The provision of operational security management and administrative services. Typically includes the authorisation and monitoring of access to IT facilities or infrastructure, the investigation of unauthorised access and compliance with relevant legislation. 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.
NTAS	**Network support** Overall definition Level 3	The provision of network maintenance and support services. Support may be provided both to users of the systems and to service delivery functions. Support typically takes the form of investigating and resolving problems and providing information about the systems. It may also include monitoring their performance. Problems may be resolved by providing advice or training to users about the network's functionality, correct operation or constraints, by devising work-arounds, correcting faults, or making general or site-specific modifications. Identifies and resolves network problems following agreed procedures. Uses network management software and tools to collect agreed performance statistics. Carries out agreed network maintenance tasks.

Linux+ (XK0-004)

Code/level	Skill name	Overall description, and Description at the specified level
SYSP	**System software** Overall definition	The provision of specialist expertise to facilitate and execute the installation and maintenance of system software such as operating systems, data management products, office automation products and other utility software.
	Level 4	Reviews system software updates and identifies those that merit action. Tailors system software to maximise hardware functionality. Installs and tests new versions of system software. Investigates and coordinates the resolution of potential and actual service problems. Prepares and maintains operational documentation for system software. Advises on the correct and effective use of system software.
HSIN	**Systems installation/ decommissioning** Overall definition	The installation, testing, implementation or decommissioning and removal of cabling, wiring, equipment, hardware and associated software, following plans and instructions and in accordance with agreed standards. The testing of hardware and software components, resolution of malfunctions, and recording of results. The reporting of details of hardware and software installed so that configuration management records can be updated.
	Level 3	Installs or removes hardware and/or software, using supplied installation instructions and tools including, where appropriate, handover to the client. Conducts tests, corrects malfunctions, and documents results in accordance with agreed procedures. Reports details of all hardware/software items that have been installed and removed so that configuration management records can be updated. Provides assistance to users in a professional manner following agreed procedures for further help or escalation. Reviews change requests. Maintains accurate records of user requests, contact details and outcomes. Contributes to the development of installation procedures and standards.

Linux+ (XK0-004) – continued

Code/level	Skill name	Overall description, and Description at the specified level
ITOP	**IT Infrastructure** Overall definition	The operation and control of the IT infrastructure (comprising physical or virtual hardware, software, network services and data storage) either on-premises or provisioned as cloud services) that is required to deliver and support the information systems needs of a business. Includes preparation for new or changed services, operation of the change process, the maintenance of regulatory, legal and professional standards, the building and management of systems and components in virtualised and cloud computing environments and the monitoring of performance of systems and services in relation to their contribution to business performance, their security and their sustainability. The application of infrastructure management tools to automate the provisioning, testing, deployment and monitoring of infrastructure components.
	Level 3	Carries out agreed operational procedures, including infrastructure configuration, installation and maintenance. Uses infrastructure management tools to collect and report on load and performance statistics and to automate the provisioning, testing and deployment of new and changed infrastructure. Contributes to the implementation of maintenance and installation work. Uses standard procedures and tools to carry out defined system backups, restoring data where necessary. Identifies operational problems and contributes to their resolution.
SCAD	**Security administration** Overall definition	The provision of operational security management and administrative services. Typically includes the authorisation and monitoring of access to IT facilities or infrastructure, the investigation of unauthorised access and compliance with relevant legislation.
	Level 2	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.

Linux+ (XK0-004) – continued

Code/level	Skill name	Overall description, and Description at the specified level
PROG	**Programming/software development** Overall definition	The planning, designing, creation, amending, verification, testing and documentation of new and amended software components in order to deliver agreed value to stakeholders. The identification, creation and application of agreed software development and security standards and processes. Adopting and adapting software development lifecycle models based on the context of the work and selecting appropriately from predictive (plan-driven) approaches or adaptive (iterative/agile) approaches.
	Level 2	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+ (SK0-004)

Code/level	Skill name	Overall description, and Description at the specified level
HSIN	**Systems installation/ decommissioning** Overall definition	The installation, testing, implementation or decommissioning and removal of cabling, wiring, equipment, hardware and associated software, following plans and instructions and in accordance with agreed standards. The testing of hardware and software components, resolution of malfunctions, and recording of results. The reporting of details of hardware and software installed so that configuration management records can be updated.
	Level 3	Installs or removes hardware and/or software, using supplied installation instructions and tools including, where appropriate, handover to the client. Conducts tests, corrects malfunctions, and documents results in accordance with agreed procedures. Reports details of all hardware/software items that have been installed and removed so that configuration management records can be updated. Provides assistance to users in a professional manner following agreed procedures for further help or escalation. Reviews change requests. Maintains accurate records of user requests, contact details and outcomes. Contributes to the development of installation procedures and standards.
AVMT	**Availability management** Overall definition	The definition, analysis, planning, measurement, maintenance and improvement of all aspects of the availability of services, including the availability of power. The overall control and management of service availability to ensure that the level of service delivered in all services is matched to or exceeds the current and future agreed needs of the business, in a cost effective manner.
	Level 4	Contributes to the availability management process and its operation and performs defined availability management tasks. Analyses service and component availability, reliability, maintainability and serviceability. 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.

Server+ (SK0-004) – continued

Code/level	Skill name	Overall description, and Description at the specified level
STMG	**Storage management** Overall definition Level 3	The planning, implementation, configuration and tuning of storage hardware and software covering online, offline, remote and offsite data storage (backup, archiving and recovery) and ensuring compliance with regulatory and security requirements. Performs regular high-performance, scalable backups and restores on a schedule and tracks offsite storage. Carries out documented configuration for allocation of storage, installation and maintenance of secure storage systems as per the agreed operational procedure. 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.
SYSP	**System software** Overall definition Level 4	The provision of specialist expertise to facilitate and execute the installation and maintenance of system software such as operating systems, data management products, office automation products and other utility software. Reviews system software updates and identifies those that merit action. Tailors system software to maximise hardware functionality. Installs and tests new versions of system software. Investigates and coordinates the resolution of potential and actual service problems. Prepares and maintains operational documentation for system software. Advises on the correct and effective use of system software.
SCAD	**Security administration** Overall definition Level 3	The provision of operational security management and administrative services. Typically includes the authorisation and monitoring of access to IT facilities or infrastructure, the investigation of unauthorised access and compliance with relevant legislation. Investigates minor security breaches in accordance with established procedures. Assists users in defining their access rights and privileges. Performs non-standard security administration tasks and resolves security administration issues.

Server+ (SK0-004) – continued

Code/level	Skill name	Overall description, and Description at the specified level
ITOP	**IT Infrastructure** Overall definition	The operation and control of the IT infrastructure (comprising physical or virtual hardware, software, network services and data storage) either on-premises or provisioned as cloud services) that is required to deliver and support the information systems needs of a business. Includes preparation for new or changed services, operation of the change process, the maintenance of regulatory, legal and professional standards, the building and management of systems and components in virtualised and cloud computing environments and the monitoring of performance of systems and services in relation to their contribution to business performance, their security and their sustainability. The application of infrastructure management tools to automate the provisioning, testing, deployment and monitoring of infrastructure components.
	Level 3	Carries out agreed operational procedures, including infrastructure configuration, installation and maintenance. Uses infrastructure management tools to collect and report on load and performance statistics and to automate the provisioning, testing and deployment of new and changed infrastructure. Contributes to the implementation of maintenance and installation work. Uses standard procedures and tools to carry out defined system backups, restoring data where necessary. Identifies operational problems and contributes to their resolution.
PBMG	**Problem management** Overall definition	The resolution (both reactive and proactive) of problems throughout the information system lifecycle, including classification, prioritisation and initiation of action, documentation of root causes and implementation of remedies to prevent future incidents.
	Level 4	Initiates and monitors actions to investigate and resolve problems in systems, processes and services. Determines problem fixes/remedies. Assists with the implementation of agreed remedies and preventative measures.

CySA+ Cybersecurity Analyst (CS0-001 or CS0-002)

Code/level	Skill name	Overall description, and Description at the specified level
SCTY	**Information security** Overall definition	The selection, design, justification, implementation and operation of controls and management strategies to maintain the security, confidentiality, integrity, availability, accountability and relevant compliance of information systems with legislation, regulation and relevant standards.
	Level 3	Communicates information security risks and issues to business managers and others. Performs basic risk assessments for small information systems. Contributes to vulnerability assessments. Applies and maintains specific security controls as required by organisational policy and local risk assessments. Investigates suspected attacks. Responds to security breaches in line with security policy and records the incidents and action taken.
	Level4	Explains the purpose of and provides advice and guidance on the application and operation of elementary physical, procedural and technical security controls. Performs security risk, vulnerability assessments, and business impact analysis for medium complexity information systems. Investigates suspected attacks and manages security incidents. Uses forensics where appropriate.
INAN	**Analytics** Overall definition	The application of mathematics, statistics, predictive modeling and machine-learning techniques to discover meaningful patterns and knowledge in recorded data. Analysis of data with high volumes, velocities and variety (numbers, symbols, text, sound and image). Development of forward-looking, predictive, real-time, model-based insights to create value and drive effective decision-making. The identification, validation and exploitation of internal and external data sets generated from a diverse range of processes.
	Level 3	Undertakes analytical activities and delivers analysis outputs, in accordance with customer needs and conforming to agreed standards.

CySA+ Cybersecurity Analyst (CS0-001 or CS0-002) – continued

Code/level	Skill name	Overall description, and Description at the specified level
TECH	**Specialist advice** Overall definition	The development and exploitation of expertise in any specific area of information or communications technology, digital working, specific techniques, methodologies, products or application areas, for the purposes of providing specialist advice.
	Level4	Actively maintains knowledge in one or more identifiable specialisms. Provides detailed and specific advice regarding the application of their specialism(s) to the organisation's planning and operations. Recognises and identifies the boundaries of their own specialist knowledge. Collaborates with other specialists, where appropriate, to ensure advice given is appropriate to the needs of the organisation.
SCAD	**Security administration** Overall definition	The provision of operational security management and administrative services. Typically includes the authorisation and monitoring of access to IT facilities or infrastructure, the investigation of unauthorised access and compliance with relevant legislation.
	Level 3	Investigates minor security breaches in accordance with established procedures. Assists users in defining their access rights and privileges. Performs non-standard security administration tasks and resolves security administration issues.
	Level 4	Maintains security administration processes and checks that all requests for support are dealt with according to agreed procedures. Provides guidance in defining access rights and privileges. Investigates security breaches in accordance with established procedures and recommends required actions and supports / follows up to ensure these are implemented.

CySA+ Cybersecurity Analyst (CS0-001 or CS0-002) – continued

Code/level	Skill name	Overall description, and Description at the specified level
USUP	**Incident management** Overall definition	The processing and coordination of appropriate and timely responses to incident reports, including channelling requests for help to appropriate functions for resolution, monitoring resolution activity, and keeping clients appraised of progress towards service restoration.
	Level4	Prioritises and diagnoses incidents according to agreed procedures. Investigates causes of incidents and seeks resolution. Escalates unresolved incidents. Facilitates recovery, following resolution of incidents. Documents and closes resolved incidents according to agreed procedures.
CORE	**Conformance review** Overall definition	The independent assessment of the conformity of any activity, process, deliverable, product or service to the criteria of specified standards, best practice, or other documented requirements. May relate to, for example, asset management, network security tools, firewalls and internet security, sustainability, real-time systems, application design and specific certifications.
	Level 3	Collects and collates evidence as part of a formally conducted and planned review of activities, processes, products or services. Examines records as part of specified testing strategies for evidence of compliance with management directives, or the identification of abnormal occurrences.
	Level 4	Conducts formal reviews of activities, processes, products or services. Collects, collates and examines records as part of specified testing strategies for evidence of compliance with management directives, or the identification of abnormal occurrences. Analyses evidence collated and drafts part or all of formal reports commenting on the conformance found to exist in the reviewed part of an information systems environment.
DGFS	**Digital forensics** Overall definition	The collection, processing, preserving, analysis, and presentation of forensic evidence based on the totality of findings including computer-related evidence in support of security vulnerability mitigation and/or criminal, fraud, counterintelligence, or law enforcement investigations.
	Level4	Contributes to digital forensic investigations. Processes and analyses evidence in line with policy, standards and guidelines and supports production of forensics findings and reports.

PenTest+ (PT0-001)

Code/level	Skill name	Overall description, and Description at the specified level
PENT	**Penetration testing** Overall definition	The assessment of organisational vulnerabilities through the design and execution of penetration tests that demonstrate how an adversary can either subvert the organisation's security goals or achieve specific adversarial objectives. Penetration testing may be a stand-alone activity or an aspect of acceptance testing prior to an approval to operate. The identification of deeper insights into the business risks of various vulnerabilities.
	Level 4	Maintains current knowledge of malware attacks, and other cyber security threats. Creates test cases using in-depth technical analysis of risks and typical vulnerabilities. Produces test scripts, materials and test packs to test new and existing software or services. Specifies requirements for environment, data, resources and tools. Interprets, executes and documents complex test scripts using agreed methods and standards. Records and analyses actions and results. Reviews test results and modifies tests if necessary. Provides reports on progress, anomalies, risks and issues associated with the overall project. Reports on system quality and collects metrics on test cases. Provides specialist advice to support others.
	Level 5	Coordinates and manages planning of penetration tests, within a defined area of business activity. Delivers objective insights into the existence of vulnerabilities, the effectiveness of defences and mitigating controls - both those already in place and those planned for future implementation. Takes responsibility for integrity of testing activities and coordinates the execution of these activities. Provides authoritative advice and guidance on the planning and execution of vulnerability tests. Defines and communicates the test strategy. Manages all test processes, and contributes to corporate security testing standards.
TECH	**Specialist advice** Overall definition	The development and exploitation of expertise in any specific area of information or communications technology, digital working, specific techniques, methodologies, products or application areas, for the purposes of providing specialist advice.
	Level4	Actively maintains knowledge in one or more identifiable specialisms. Provides detailed and specific advice regarding the application of their specialism(s) to the organisation's planning and operations. Recognises and identifies the boundaries of their own specialist knowledge. Collaborates with other specialists, where appropriate, to ensure advice given is appropriate to the needs of the organisation.

PenTest+ (PT0-001) – continued

Code/level	Skill name	Overall description, and Description at the specified level
CORE	**Conformance review** Overall definition	The independent assessment of the conformity of any activity, process, deliverable, product or service to the criteria of specified standards, best practice, or other documented requirements. May relate to, for example, asset management, network security tools, firewalls and internet security, sustainability, real-time systems, application design and specific certifications.
	Level 3	Collects and collates evidence as part of a formally conducted and planned review of activities, processes, products or services. Examines records as part of specified testing strategies for evidence of compliance with management directives, or the identification of abnormal occurrences.
	Level 4	Conducts formal reviews of activities, processes, products or services. Collects, collates and examines records as part of specified testing strategies for evidence of compliance with management directives, or the identification of abnormal occurrences. Analyses evidence collated and drafts part or all of formal reports commenting on the conformance found to exist in the reviewed part of an information systems environment.
INAN	**Analytics** Overall definition	The application of mathematics, statistics, predictive modeling and machine-learning techniques to discover meaningful patterns and knowledge in recorded data. Analysis of data with high volumes, velocities and variety (numbers, symbols, text, sound and image). Development of forward-looking, predictive, real-time, model-based insights to create value and drive effective decision-making. The identification, validation and exploitation of internal and external data sets generated from a diverse range of processes.
	Level 3	Undertakes analytical activities and delivers analysis outputs, in accordance with customer needs and conforming to agreed standards.

CASP+ CompTIA Advanced Security Practitioner (CAS-003)

Code/level	Skill name	Overall description, and Description at the specified level
SCTY	**Information security** Overall definition Level 4	The selection, design, justification, implementation and operation of controls and management strategies to maintain the security, confidentiality, integrity, availability, accountability and relevant compliance of information systems with legislation, regulation and relevant standards. Explains the purpose of and provides advice and guidance on the application and operation of elementary physical, procedural and technical security controls. Performs security risk, vulnerability assessments, and business impact analysis for medium complexity information systems. Investigates suspected attacks and manages security incidents. Uses forensics where appropriate.
SCAD	**Security administration** Overall definition Level 4	The provision of operational security management and administrative services. Typically includes the authorisation and monitoring of access to IT facilities or infrastructure, the investigation of unauthorised access and compliance with relevant legislation. Maintains security administration processes and checks that all requests for support are dealt with according to agreed procedures. Provides guidance in defining access rights and privileges. Investigates security breaches in accordance with established procedures and recommends required actions and supports / follows up to ensure these are implemented.
CORE	**Conformance review** Overall definition Level 4	The independent assessment of the conformity of any activity, process, deliverable, product or service to the criteria of specified standards, best practice, or other documented requirements. May relate to, for example, asset management, network security tools, firewalls and internet security, sustainability, real-time systems, application design and specific certifications. Conducts formal reviews of activities, processes, products or services. Collects, collates and examines records as part of specified testing strategies for evidence of compliance with management directives, or the identification of abnormal occurrences. Analyses evidence collated and drafts part or all of formal reports commenting on the conformance found to exist in the reviewed part of an information systems environment.

CASP+ CompTIA Advanced Security Practitioner (CAS-003) – continued

Code/level	Skill name	Overall description, and Description at the specified level
DGFS	**Digital forensics** Overall definition Level 5	The collection, processing, preserving, analysis, and presentation of forensic evidence based on the totality of findings including computer-related evidence in support of security vulnerability mitigation and/or criminal, fraud, counterintelligence, or law enforcement investigations. Conducts investigations to correctly gather, analyse and present the totality of findings including digital evidence to both business and legal audiences. Collates conclusions and recommendations and presents forensics findings to stakeholders. Contributes to the development of policies, standards and guidelines.
USUP	**Incident management** Overall definition Level 4	The processing and coordination of appropriate and timely responses to incident reports, including channelling requests for help to appropriate functions for resolution, monitoring resolution activity, and keeping clients appraised of progress towards service restoration. Prioritises and diagnoses incidents according to agreed procedures. Investigates causes of incidents and seeks resolution. Escalates unresolved incidents. Facilitates recovery, following resolution of incidents. Documents and closes resolved incidents according to agreed procedures.
BURM	**Business risk management** Overall definition Level 5	The planning and implementation of organisation-wide processes and procedures for the management of risk to the success or integrity of the business, especially those arising from the use of information technology, reduction or non-availability of energy supply or inappropriate disposal of materials, hardware or data. Carries out risk assessment within a defined functional or technical area of business. Uses consistent processes for identifying potential risk events, quantifying and documenting the probability of occurrence and the impact on the business. Refers to domain experts for guidance on specialised areas of risk, such as architecture and environment. Co-ordinates the development of countermeasures and contingency plans.

CASP+ CompTIA Advanced Security Practitioner (CAS-003) – continued

Code/level	Skill name	Overall description, and Description at the specified level
NTDS	**Network design** Overall definition	The production of network designs and design policies, strategies, architectures and documentation, covering voice, data, text, e-mail, facsimile and image, to support strategy and business requirements for connectivity, capacity, interfacing, security, resilience, recovery, access and remote access. This may incorporate all aspects of the communications infrastructure, internal and external, mobile, public and private, Internet, Intranet and call centres.
	Level 5	Produces outline system designs and specifications, and overall architectures, topologies, configuration databases and design documentation of networks and networking technology within the organisation. Specifies user/system interfaces, including validation and error correction procedures, processing rules, access, security and audit controls. Assesses associated risks, and specifies recovery routines and contingency procedures. Translates logical designs into physical designs.
AVMT	**Availability management**	The definition, analysis, planning, measurement, maintenance and improvement of all aspects of the availability of services, including the availability of power. The overall control and management of service availability to ensure that the level of service delivered in all services is matched to or exceeds the current and future agreed needs of the business, in a cost effective manner.
	Level 5	Provides advice, assistance and leadership associated with the planning, design and improvement of service and component availability, including the investigation of all breaches of availability targets and service non-availability, with the instigation of remedial activities. Plans arrangements for disaster recovery together with supporting processes and manages the testing of such plans.

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	**Learning assessment and evaluation** Overall definition	The assessment of knowledge, skills and behaviours by any means whether formal or informal against frameworks such as SFIA. The evaluation, selection, adoption and adaptation of assessment methods, tools, and techniques based on the context of the assessment and how the results of the assessment are to be used. The evaluation of learning or educational activities against defined skills/competency development outcomes.
	Level 4	Performs routine and non-routine skill/competency assessments of knowledge, skills and behaviour using specified methods and according to specified standards aligned with ethical, legal and regulatory requirements. Uses the outcomes of assessments and other data to analyse and evaluate the effectiveness of learning/educational activities.
TMCR	**Learning design and development** Overall definition	The specification, design, creation, packaging and maintenance of materials and resources for use in learning and development in the workplace or in compulsory, further or higher education. Typically involves the assimilation of information from existing sources, selection and re-presentation in a form suitable to the intended purpose and audience. Includes instructional design, content development, configuration and testing of learning environments, and use of appropriate current technologies such as audio, video, simulation and assessment. May include third party accreditation.
	Level 4	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, including creation of simulated data, and replication of external systems, interfaces, and assessment systems. Secures external accreditations as appropriate.

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	**Learning delivery** Overall definition	The transfer of business and/or technical skills and knowledge and the promotion of professional attitudes in order to facilitate learning and development. Uses a range of techniques, resources and media (which might include eLearning, on-line virtual environments, self-assessment, peer-assisted learning, simulation, and other current methods).
	Level 4	Prepares or customises and delivers learning activities and the learning environment for a variety of audiences. Teaches, instructs, trains students/learners in order to develop knowledge, techniques and skills using appropriate methods, tools, online environments, equipment and materials. Oversees students/learners in performing practical activities and work, advising and assisting where necessary, and ensuring that maximum learning benefit is gained from the practical experience. Provides detailed instruction as necessary and responds to wide-ranging and detailed questioning in own area(s) of specialisation. Assesses objectively, against pre-set criteria, the ability levels of students and reports as appropriate. Develops examples and case study material for use in pre-defined courses. Adapts simple course material to meet the needs of students.
TEAC	**Teaching and subject formation** Overall definition	The specification, design, development, delivery and assessment of curricula for computing and for information technology (including electronic communication), at any level of the education system from primary through to tertiary (all age ranges) and in the workplace. The topics addressed are those of the fundamental and more advanced areas of computing and the common skills needed to make productive use of computers and IT systems for both computing and IT professionals and competent users of IT based systems including the ideas of computational thinking and the application of computational concepts to everyday and professional life. Special attention is paid to the methods, techniques and pedagogy (the study of being a teacher, tutor or lecturer, and the process of teaching) of computing & IT education.
	Level 5	Delivers computing and IT curricula either in a formal educational context from primary through to tertiary level or in the workplace. Specialises in delivering Computing and IT education at the relevant educational level. Is aware of the techniques and methods used to evaluate and critique research in computing and IT education and applies good practice in learning content design, development and delivery.

Cloud Essentials+ (CLO-002)

Code/level	Skill name	Overall description, and Description at the specified level
BUAN	**Business analysis** Overall definition	The methodical investigation, analysis, review and documentation of all or part of a business in terms of business goals, objectives, functions and processes, the information used and the data on which the information is based. The definition of requirements for improving processes and systems, reducing their costs, enhancing their sustainability, and the quantification of potential business benefits. The collaborative creation and iteration of viable specifications and acceptance criteria in preparation for the deployment of information and communication systems. The adoption and adaptation of business analysis approaches based on the context of the work and selecting appropriately from predictive (plan-driven) approaches or adaptive (iterative/agile) approaches.
	Level 3	Investigates operational needs and problems, and opportunities, contributing to the recommendation of improvements in automated and non-automated components of new or changed processes and organisation. Assists in defining acceptance tests for these recommendations.
SORC	**Sourcing** Overall definition	The provision of policy, internal standards and advice on the procurement or commissioning of externally supplied and internally developed products and services. The provision of commercial governance, conformance to legislation and assurance of information security. The implementation of compliant procurement processes, taking full account of the issues and imperatives of both the commissioning and supplier sides. The identification and management of suppliers to ensure successful delivery of products and services required by the business.
	Level 2	Assists in 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 evaluation of tenders.

Project+ (PK0-004)

Code/level	Skill name	Overall description, and Description at the specified level
PRMG	**Project management** Overall definition	The management of projects, typically (but not exclusively) involving the development and implementation of business processes to meet identified business needs, acquiring and utilising the necessary resources and skills, within agreed parameters of cost, timescales, and quality. The adoption and adaptation of project management methodologies based on the context of the project and selecting appropriately from predictive (plan-driven) approaches or adaptive (iterative/agile) approaches.
	Level 4	Defines, documents and carries out small projects or sub-projects (typically less than six months, with limited budget, limited interdependency with other projects, and no significant strategic impact), alone or with a small team, actively participating in all phases. Identifies, assesses and manages risks to the success of the project. Applies appropriate project management methods and tools whether predictive (plan-driven) approaches or adaptive (iterative/agile) approaches. Agrees project approach with stakeholders, and prepares realistic plans (including quality, risk and communications plans) and tracks activities against the project schedule, managing stakeholder involvement as appropriate. Monitors costs, timescales and resources used, and takes action where these deviate from agreed tolerances. Ensures that own projects are formally closed and, where appropriate, subsequently reviewed, and that lessons learned are recorded.
PROF	**Portfolio, programme and project support** Overall definition	The provision of support and guidance on portfolio, programme and project management processes, procedures, tools and techniques. Support includes definition of portfolios, programmes, and projects; advice on the development, production and maintenance of business cases; time, resource, cost and exception plans, and the use of related software tools. Tracking and reporting of programme/project progress and performance are also covered, as is the capability to facilitate all aspects of portfolio/ programme/ project meetings, workshops and documentation.
	Level 3	Uses recommended portfolio, programme and project control solutions for planning, scheduling and tracking. Sets up project files, compiles and distributes reports. Provides administrative services to project boards, project assurance teams and quality review meetings. Provides guidance on project management software, procedures, processes, tools and techniques.