

Job Profile

Profile Technical Officer

MITA Career Level 3

Based on SFIA v9

Summary Statement

Administers / supports ICT System components to meet service requirements. Provides telephone support or e-mail support to internal or external clients with technical issues.

Mission

Installs software, configures and upgrades ICT systems. Administers day-to-day operations to satisfy continuity of service, recovery, security and performance needs. To provide user support and troubleshoot ICT problems and issues. The primary objective is to enable users to maximize their productivity through efficient use of ICT equipment or software applications.

Deliverables

Accountable	• Service levels
Responsible	• Solution in operation
	• 1st/2nd line support
Contributor	• Solved incident

Generic Main Tasks – (Applicable to all areas)

- Installing, managing and maintaining operating systems, data management, office automation and utility software across various infrastructure environments.
- Delivering management, technical and administrative services to support and maintain live applications.
- Managing the lifecycle of all problems that have occurred or could occur in delivering a service.
- Coordinating responses to a diverse range of incidents to minimise negative impacts and quickly restore services.
- Coordinating responses to a diverse range of incidents to minimise negative impacts and quickly restore services.
- Agreeing targets for service levels and assessing, monitoring and managing the delivery of services against the targets.
- Ensuring services deliver agreed levels of availability to meet the current and future needs of the business.
- Ensuring service components have the capacity and performance to meet current and planned business needs.
- Provisioning, configuring and optimising on-premises and cloud-based storage solutions, ensuring data availability, security and alignment with business objectives.
- Planning, identifying, controlling, accounting for and auditing of configuration items (CIs) and their interrelationships.
- Managing the release of new and updated services into production, ensuring alignment with business objectives and compliance standards.

- Manages and administers security measures, using tools and intelligence to protect assets, ensuring compliance and operational integrity.
- Assessing risks associated with proposed changes and ensuring changes to products, services or systems are controlled and coordinated.
- Developing, producing and delivering regular and one-off management information to provide insights and aid decision-making.
- Planning, designing and creating content that meets user-centred and organisational needs, encompassing textual information, graphical content and multimedia elements.
- Systematically capturing, developing and leveraging vital knowledge to create value and enhance organisational performance.
- Providing a source of consistent information about available services and products to customers and users.
- Managing the full lifecycle of assets from acquisition, operation, maintenance to disposal.
- Other duties as assigned.

Generic Essential Professional Attributes (Applicable to all areas)		
Code	Description	SFIA Level
SYSP	Systems Software administration	4
ASUP	Application Support	4
PBMG	Problem Management	4
USUP	Incident Management	4
HSIN	Systems Installation and removal	3
SLMO	Service Level Management	3
AVMT	Availability Management	4
CPMG	Capacity Management	4
STMG	Storage Management	3
CFMG	Configuration Management	3
RELM	Release and Deployment	4
SCAD	Security Operations	3
CHMG	Change control	3
BINT	Business Intelligence	3
INCA	Content design and authoring	3
KNOW	Knowledge management	3
SCMG	Service Catalogue Management	3
ASMG	Asset Management	3

SFIA Skills Definition - Generic

SYSP System Software Administration: Level 4 Monitors system software metrics and adjusts configurations for optimum availability and performance. Applies technical expertise to investigate and resolve complex system software issues, requesting action from supplier if required. Analyses system software updates and determines which ones require actions. Develops comprehensive software implementation procedures with robust contingency plans.

ASUP Application Support: Level 4 Maintains application support processes, and checks that all requests for support are dealt with according to agreed procedures. Uses application management software and tools to investigate issues, collect performance statistics and create reports.

PBMG Problem Management: Level 4 Initiates and monitors actions to investigate and resolve problems in systems, processes and services. Determines problem fixes and remedies. Collaborates with others to implement agreed remedies and preventative measures. Supports analysis of patterns and trends to improve problem management processes.

USUP Incident Management: Level 4 Monitors and manages incident queues to ensure incidents are handled according to procedures and service levels. Contributes to developing, testing and improving incident management procedures. Uses analytic tools to track trends. Ensures resolved incidents are properly documented and closed. Supports team members in the correct use of the incident process.

HSIN Systems Installation and Removal: Level 3 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.

SLMO Service Level Management: Level 3 Monitors service delivery performance metrics. Liaises with stakeholders to help them plan for a deterioration in service and/or breaches of service level agreements.

AVMT Availability Management: Level 4 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.

CPMG Capacity Management: Level 4 Monitors service component capacity and initiates actions to resolve any shortfalls according to agreed procedures. Applies techniques to control the demand upon a particular resource or service. Contributes to capacity modelling and planning. Supports the design of service component capacity.

STMG Storage Management: Level 3 Executes routine storage management tasks following established procedures and using standard tools. Implements documented configurations for allocation of storage, installation and maintenance of secure storage systems using the agreed operational procedures. Identifies operational problems, including security-related issues, and contributes to their resolution. Uses standard management and reporting tools to collect and report on storage utilisation, performance and backup statistics.

CFMG Configuration Management: Level 3 Applies tools, techniques and processes to track, log and correct information related to configuration items. Verifies and approves changes ensuring the protection of assets and components from unauthorised change, diversion and inappropriate use. Ensures that users comply with identification standards for object types, environments, processes, life cycles, documentation, versions, formats, baselines, releases and templates. Performs audits to

check the accuracy of the information and undertakes any necessary corrective action under direction.

RELM Release management: Level 4 Plans and schedules releases in line with business requirements and objectives. Coordinates release activities across multiple teams and stakeholders. Manages the release lifecycle, ensuring timely and quality deliverables. Ensures releases meet defined quality, security and compliance standards. Communicates release plans, progress and outcomes to stakeholders. Conducts post-release reviews and identifies areas for improvement.

SCAD Security operations: Level 3 Investigates minor security breaches using established procedures, incorporating analytical tools and techniques. Performs non-standard operational security tasks adapting to evolving technologies and threat landscapes. Addresses and resolves a variety of security events to maintain system integrity and operational continuity.

CHMG Change control: 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.

BINT Business Intelligence: Level 3 Sources and prepares data for analysis and performs standard business intelligence analysis activities. Checks the integrity and validity of data sources. 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.

INCA Content Authoring: Level 3 Produces information artefacts that are accurate, current, relevant and easily understood by the intended audience. Clarifies detailed content requirements with clients and representatives of the intended audience. Designs, creates, controls and evaluates moderately complex subject matter. Makes informed decisions about the best way to present information to an audience. Applies moderation and editing processes to content supplied by others.

KNOW Knowledge management: Level 3 Maintains knowledge management systems and content to meet business needs. Supports others to enable them to complete knowledge management activities and form knowledge management habits. Supports changes to work practices to support capture and use of knowledge. Reports on the progress of knowledge management activities. Configures and develops knowledge management systems and standards.

SCMG Service Catalogue management: Level 3 Collates information needed to populate the service catalogue. Edits and maintains service and product descriptions and keeps the list of available services up to date. Acts as a contact point, receiving and handling routine updates to the service catalogue. Identifies opportunities to improve service catalogue management processes.

ASMG Asset management: Level 3 Applies tools, techniques and processes to create and maintain an accurate asset register. Produces reports and analysis to support asset management activities and aid decision-making.

Essential Basic Attributes	
Autonomy	Works under general direction to complete assigned tasks. Receives guidance and has work reviewed at agreed milestones. When required, delegates routine tasks to others within own team.
Influence	Works with and influences team decisions. Has a transactional level of contact with people outside their team, including internal colleagues and external contacts.
Complexity	Performs a range of work, sometimes complex and non-routine, in varied environments.
Collaboration	Facilitates collaboration between stakeholders who share common objectives. Engages with and contributes to the work of cross-functional teams to ensure that user/customer needs are being met throughout the deliverable/scope of work.
Communication	Communicates with team and stakeholders inside and outside the organisation clearly explaining and presenting information. Contributes to a range of work-related conversations and listens to others to gain an understanding and asks probing questions relevant to their role.
Improvement Mindset	Identifies and implements improvements in own work area. Contributes to team-level process enhancements.
Problem Solving	Applies a methodical approach to investigate and evaluate options to resolve routine and moderately complex issues.
Adaptability	Adapts and is responsive to change and shows initiative in adopting new methods or technologies.
Learning, Development	Absorbs and applies new information effectively with the ability to share learnings with colleagues. Takes the initiative in identifying and negotiating their own appropriate development opportunities.
Decision Making	Uses judgment and substantial discretion in identifying and responding to complex issues and assignments related to projects and team objectives. Escalates when scope is impacted.
Security, Privacy, Ethics	Adapts and applies applicable standards, recognising their importance in achieving team outcomes.

Certification

Name	Relevant Professional Certification
Mandatory	No

Eligibility Criteria

One of the following in an ICT related area:

- i. A qualification in an ICT related area (MQF Level 5 OR higher); OR
- ii. A qualification in an ICT related area (MQF Level 4) AND an additional 1 year experience in an ICT related area; OR
- iii. 2 years' experience in an ICT related area.

Reporting line

Reports to	Head of Department or delegate
Interacts with	Peers
Supervises	N/A

Working Conditions

Normal hours with possibility to provide support in crisis situations after office hours or on weekends. Abnormal support may be required on roster basis.

In case of Control Centre there is a requirement to work on shift-basis in accordance with a pre-defined shift schedule as agreed with Management which may include night shift.

Appendix I – PES and NOC

Main Tasks

- Provisioning, deploying, configuring, operating and optimising technology infrastructure across physical, virtual and cloud-based environments.
- Providing maintenance and support services for communications networks.
- Identifying and classifying security vulnerabilities in networks, systems and applications and mitigating or eliminating their impact.

Essential Professional Attributes Based on SFIA v9 (Appendix I)

Code	Description	SFIA Level
ITOP	IT Infrastructure	4
NTAS	Network Support	2
VUAS	Vulnerability assessment	3

Appendix I - SFIA Skills Definition – PES and NOC

ITOP IT Infrastructure: Level 4 Applies technical expertise to maintain and optimise technology infrastructure, executing updates and employing automation tools. Configures tools and/or creates scripts to automate infrastructure tasks. Maintains operational procedures and checks that they are followed, including adherence to security policies. Uses infrastructure management tools to monitor load, performance, and security metrics. Investigates and enables the resolution of operational and security-related issues. Provides reports and proposals for improvement to stakeholders. Contributes to the planning and implementation of infrastructure maintenance and updates. Implements agreed infrastructure changes and maintenance routines.

VUAS Vulnerability assessment: 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.

NTAS Network Support: Level 2 Assists in the operational configuration of network components and the investigation and resolution of network problems. Assists in the implementation of basic scripting and automation tools to streamline network support tasks. Assists with specified maintenance procedures and follows established safety, security and quality standards. Provides first-line support and guidance to network users, escalating issues as necessary.

Appendix II – NES - ISD

Main Tasks

- Provisioning, deploying, configuring, operating and optimising technology infrastructure across physical, virtual and cloud-based environments.
- Providing maintenance and support services for communications networks.
- Identifying and classifying security vulnerabilities in networks, systems and applications and mitigating or eliminating their impact.

Essential Professional Attributes Based on SFIA v9 (Appendix II)

Code	Description	SFIA Level
ITOP	IT Infrastructure	4
NTAS	Network Support	3
VUAS	Vulnerability assessment	3

Appendix II - SFIA Skills Definition – NES - ISD

ITOP IT Infrastructure: Level 4 Applies technical expertise to maintain and optimise technology infrastructure, executing updates and employing automation tools. Configures tools and/or creates scripts to automate infrastructure tasks. Maintains operational procedures and checks that they are followed, including adherence to security policies. Uses infrastructure management tools to monitor load, performance, and security metrics. Investigates and enables the resolution of operational and security-related issues. Provides reports and proposals for improvement to stakeholders. Contributes to the planning and implementation of infrastructure maintenance and updates. Implements agreed infrastructure changes and maintenance routines.

NTAS Network Support: Level 3 Executes agreed network maintenance tasks and specified operational configuration of network components. Identifies and diagnoses network problems/faults using the required troubleshooting tools and network management software, including addressing security-related issues. Implements and maintains scripts, automation tools and orchestration platforms to optimise network support processes. Collects performance and traffic statistics and collaborates with others to ensure network effectiveness and resolve issues

VUAS Vulnerability assessment: Level 3 Follows standard approaches to perform basic vulnerability assessments for small information systems. Supports creation of catalogues of information and technology assets for vulnerability assessment.

Appendix III – Services - SMD

Main Tasks

- Provisioning, deploying, configuring, operating and optimising technology infrastructure across physical, virtual and cloud-based environments.
- Providing maintenance and support services for communications networks.
- Identifying and classifying security vulnerabilities in networks, systems and applications and mitigating or eliminating their impact.

Essential Professional Attributes Based on SFIA v9 (Appendix III)

Code	Description	SFIA Level
ITOP	IT Infrastructure	3
NTAS	Network Support	2
VUAS	Vulnerability assessment	2

Appendix III - SFIA Skills Definition – Services - SMD

ITOP IT Infrastructure: Level 3 Provisions, deploys and configures infrastructure services and components. Monitors infrastructure for load, performance and security events. Reports metrics and resolves operational issues. Executes standard operational procedures, including backups and restorations. Carries out agreed system software maintenance tasks. Automates routine system administration tasks to specifications using standard tools and basic scripting.

NTAS Network Support: Level 2 Assists in the operational configuration of network components and the investigation and resolution of network problems. Assists in the implementation of basic scripting and automation tools to streamline network support tasks. Assists with specified maintenance procedures and follows established safety, security and quality standards. Provides first-line support and guidance to network users, escalating issues as necessary.

VUAS Vulnerability assessment: 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.