Job Profile

Profile	Analyst
MITA Career Level *Based on SFIA v9*	3

Summary Statement

Identify, analyse and react to situations/data depending on area of work, using a reliable set of processes, tools and/or technology solutions.

Mission

Provide support, including analysis, identification, protection, detection, response and/or recovery from events and situations. Performs real-time monitoring, analysis in relation to business, data, security events or threats. Work collaboratively, to develop sufficient understanding of all roles within the team to provide assistance to other functions as required.

Deliverables

Accountable	• Business, or detection and monitoring of threats
Responsible	• Business area or 1st/2nd line security support
Contributor	• Business, or resolution of incidents

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

Reporting line

Reports to	Line Manager
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.

For the Cyber Security areas, may need to work in accordance with a pre-defined shift schedule as agreed with Management which may include night shift.

Appendix I - SOC

Main Tasks

- Manages and administers security measures, using tools and intelligence to protect assets, ensuring compliance and operational integrity.
- Defining and operating a framework of security controls and security management strategies.
- Identifying and classifying security vulnerabilities in networks, systems and applications and mitigating or eliminating their impact.
- Recovering and investigating material found in digital devices.
- Developing and sharing actionable insights on current and potential security threats to the success or integrity of an organisation.
- Coordinating responses to a diverse range of incidents to minimise negative impacts and quickly restore services.
- Developing software components to deliver value to stakeholders.
- Conducting applied research to discover, evaluate and mitigate new or unknown security vulnerabilities and weaknesses.

Essential Professional Attributes Based on SFIA v9 (Appendix I)

Code	Description	SFIA Level
SCAD	Security Operations	4
SCTY	Information Security	3
VUAS	Vulnerability Assessment	3
DGFS	Digital Forensics	3
THIN	Threat Intelligence	3
USUP	Incident Management	4
PROG	Software Development	2
VURE	Vulnerability Research	3

SFIA Skills Definition - SOC

SCAD Security operations: Level 4 Maintains and optimises operational security processes. Checks that all requests for support are dealt with according to established protocols, including for cloud-based and automated systems. Provides advice on implementing and managing physical, procedural and technical security encompassing both physical and digital assets. Investigates security breaches in accordance with established procedures using advanced tools and techniques and recommends necessary corrective actions. Enables effective implementation of recommended security measures and monitors their performance.

SCTY Information security: 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.

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.

DGFS Digital Forensics: Level 3 Applies standard forensic tools and techniques to examine digital devices. Recovers and analyses damaged, deleted or hidden data from various digital sources and devices. Maintains the integrity of digital evidence and ensures its collection adheres to legal admissibility standards.

THIN Threat intelligence: 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.

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 analytics tools to track trends. Ensures resolved incidents are properly documented and closed. Supports team members in the correct use of the incident process.

PROG Programming/software development: Level 2 Designs, codes, verifies, tests, documents, amends and refactors simple programs/scripts. Applies agreed standards, tools and basic security practices to achieve a well-engineered result. Reviews own work.

VURE Vulnerability research: 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.

Appendix II – Security Governance

Main Tasks

- Carry out governance activities related to departmental business continuity.
- Planning and implementing processes for managing risk across the enterprise, aligned with organisational strategy and governance frameworks.
- Defining and operating a framework of security controls and security management strategies.
- Manages and administers security measures, using tools and intelligence to protect assets, ensuring compliance and operational integrity.
- Identifying and classifying security vulnerabilities in networks, systems and applications and mitigating or eliminating their impact.
- Delivering independent, risk-based assessments of the effectiveness of processes, the controls and the compliance environment of an organisation.
- Implementing and promoting compliance with information and data management legislation.
- Protecting against and managing risks related to the use, storage and transmission of data and information systems.

Essential Professional Attributes Based on SFIA v9 (Appendix II)

Code	Description	SFIA Level
COPL	Continuity Management	3
BURM	Risk Management	3
SCTY	Information security	4
SCAD	Security Operations	2
VUAS	Vulnerability Assessment	3
AUDT	Audit	3
PEDP	Information Data Compliance	4
INAS	Information Assurance	3

SFIA Skills Definition – Security Governance

COPL Continuity Management: Level 3 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.

BURM Risk Management: Level 3 Undertakes basic risk management activities. Maintains documentation of risks, threats, vulnerabilities and mitigation actions.

SCTY Information security: Level 4 Provides guidance on the application and operation of elementary physical, procedural and technical security controls. Explains the purpose of security controls and performs security risk and business impact analysis for medium complexity information systems. Identifies risks that arise from potential technical solution architectures. Designs alternate solutions or countermeasures and ensures they manage identified risks. Investigates suspected attacks and supports security incident management.

SCAD Security Operations: Level 2 Receives and responds to routine requests for security support. Maintains records and effectively communicates actions taken. Assists in the investigation and resolution of issues relating to security systems using basic diagnostic tools and techniques. Documents incident and event information and generates reports on exceptions and security events. Contributes to management reporting processes.

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.

AUDT Audit: Level 3 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.

PEDP Information and data compliance: Level 4 Supports the implementation of policy, standards and guidelines related to information and data legislation and compliance requirements. Monitors the implementation of effective controls for internal delegation, audit and control relating to information management. Reports on the consolidated status of information controls to inform effective decision-making. Identifies risks around the use of information and data that is subject to specific legislation. Recommends remediation actions as required.

INAS Information Assurance: Level 3 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.

Appendix III – Threat Intelligence

Main Tasks

- Developing and sharing actionable insights on current and potential security threats to the success or integrity of an organisation.
- Manages and administers security measures, using tools and intelligence to protect assets, ensuring compliance and operational integrity.
- Defining and operating a framework of security controls and security management strategies.
- Identifying and classifying security vulnerabilities in networks, systems and applications and mitigating or eliminating their impact.
- Conducting applied research to discover, evaluate and mitigate new or unknown security vulnerabilities and weaknesses.
- Enabling data-driven decision making by extracting, analysing and communicating insights from structured and unstructured data.
- Facilitating understanding of data by displaying concepts, ideas and facts using graphical representations.
- Developing software components to deliver value to stakeholders.

Essential Professional Attributes Based on SFIA v9 (Appendix IV)

Code	Description	SFIA Level
THIN	Threat Intelligence	4
SCAD	Security Operations	2
SCTY	Information Security	3
VUAS	Vulnerability Assessment	4
VURE	Vulnerability Research	4
DAAN	Data Analytics	2
VISL	Data Visualisation	3
PROG	Software Development	2

SFIA Skills Definition – Threat Intelligence

THIN Threat Intelligence: 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 threat intelligence sources.

SCAD Security Operations: Level 2 Receives and responds to routine requests for security support. Maintains records and effectively communicates actions taken. Assists in the investigation and resolution of issues relating to security systems using basic diagnostic tools and techniques. Documents incident and event information and generates reports on exceptions and security events. Contributes to management reporting processes.

SCTY Information Security: 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.

VUAS 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.

VURE Vulnerability Research: 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.

DAAN Data Analytics: Level 2 Assists in data preparation and analysis activities under direction. Processes and validates data to support analytics. Generates standard reports and insights using established tools and methods.

VISL Data Visualisation: Level 3 Uses visualisation products, as guided, to design and create data visuals. Selects appropriate visualisation techniques from the options available. Engages with the target user to prototype and refine specified visualisations. Assists in developing narratives around data sets to support understanding and decision-making.

PROG Software Development: Level 2 Designs, codes, verifies, tests, documents, amends and refactors simple programs/scripts. Applies agreed standards, tools and basic security practices to achieve a well-engineered result. Reviews own work.

Appendix IV – Cyber Defense

Main Tasks

- Manages and administers security measures, using tools and intelligence to protect assets, ensuring compliance and operational integrity.
- Defining and operating a framework of security controls and security management strategies.
- Identifying and classifying security vulnerabilities in networks, systems and applications and mitigating or eliminating their impact.
- Testing the effectiveness of security controls by emulating the tools and techniques of likely attackers.
- Developing and sharing actionable insights on current and potential security threats to the success or integrity of an organisation.
- Leads the adoption, management and optimisation of methods and tools, ensuring effective use and alignment with organisational objectives.
- Plans, executes and manages offensive cybersecurity operations, including target selection, electronic target folders and post-operation analysis.

Essential Professional Attributes Based on SFIA v9 (Appendix V)

Code	Description	SFIA Level
SCAD	Security Operations	3
SCTY	Information Security	3
VUAS	Vulnerability Assessment	4
PENT	Penetration Testing	4
DGFS	Digital Forensics	2
THIN	Threat Intelligence	3
METL	Methods and Tools	3
PROG	Software Development	2
OCOP	Offensive Cyber Operations	3

SFIA Skills Definition – Cyber Defense

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.

SCTY Information Security: 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.

VUAS 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.

PEN Penetration Testing: Level 4 Selects appropriate testing approaches using in-depth technical analysis of risks and typical vulnerabilities. Produces test scripts, materials and test packs and tests new and existing networks, systems or applications. Provides advice on penetration testing to support others. Records and analyses actions and results and modifies tests if necessary. Provides reports on progress, anomalies, risks and issues associated with the overall project.

DGFS Digital Forensics: Level 2 Assists with digital forensic investigations under routine supervision. Supports the recovery of damaged, deleted or hidden data from digital devices. Helps collect and preserve digital information and evidence according to established protocols.

THIN Threat Intelligence: 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.

METL Methods and Tools: Level 3 Provides support on the use of existing methods and tools. Configures and maintains methods and tools within a known context. Creates and updates the documentation of methods and tools. Identifies and resolves basic issues related to tool usage.

PROG SOFTWARE DEVELOPER: Level 2 Designs, codes, verifies, tests, documents, amends and refactors simple programs/scripts. Applies agreed standards, tools and basic security practices to achieve a well-engineered result. Reviews own work.

OCOP Offensive Cyber Operations: Level 3 Carries out specific tasks within offensive cyber operations, aligning operational tasks with broader objectives. Supports the creation and maintenance of electronic target folders, gathering and verifying target information. Assists in the execution of operations, maintaining operational security. Prepares detailed reports and participates in post-operation analysis.

Appendix V – NCC

Main Tasks

- Creating new and potentially disruptive approaches to performing business activities.
- Managing preparation and submission of bids and proposals for contracts, grants, projects, or services.
- Forecasting, planning and monitoring the emergence and effective realisation of anticipated benefits from projects and programmes.
- Providing support and guidance on portfolio, programme and project management processes, procedures, tools and techniques.
- Conducting in-depth analysis of financial data to derive insights and support decision-making.
- Systematically capturing, developing and leveraging vital knowledge to create value and enhance organisational performance.
- Gathering, analysing and interpreting data about markets, customers and competitors to inform business decisions and strategies.

Essential Professional Attributes Based on SFIA v9 (Appendix VI)

Code	Description	SFIA Level
BPRE	Business Process Improvement	4
BIDM	Bid/Proposal Management	4
BENM	Benefits Management	3
PROF	Portfolio, programme and project support	3
FIAN	Financial Analyses	3
KNOW	Knowledge Management	3
MRCH	Market Research	4

SFIA Skills Definition - NCC

BPRE Business Process Improvement: Level 4 Analyses and designs business processes to identify alternative solutions to improve efficiency, effectiveness and exploit new technologies and automation. Develops graphical models of business processes to facilitate understanding and decision-making. Recommends implementation approaches for process improvement initiatives.

BIDM Bid/proposal management: Level 4 Leads the creation of small to medium proposals, integrating technical analysis and broader context. Coordinates team efforts, shapes the proposal structure and addresses financial aspects including budgeting and pricing strategies. Identifies and manages proposal risks, ensuring timely compliance with stakeholder expectations. Engages with stakeholders and shapes proposal structure and content based on in-depth discussions and feedback.

BENM Benefits Management: Level 3 Supports the identification and tracking of benefits for projects and programmes. Collects data to measure benefits realisation.

PROF Portfolio, programme and project support: Level 3 Provides foundational support for projects, programmes, or portfolios. Assists with planning, scheduling, tracking and reporting using established tools and processes. Follows recommended solutions to ensure accurate documentation and communication of project progress. Collaborates closely with project teams and stakeholders, gathering updates and information to maintain project records and ensure alignment with project objectives. Participates in project boards, assurance teams and quality review meetings when necessary.

FIAN Financial analysis: Level 3 Applies established financial analysis techniques and processes to carry out specific tasks such as detailed data analysis, report generation and interpretation of financial metrics. Contributes to the development of actionable insights for decision-making. Communicates financial analysis findings to relevant stakeholders.

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 enable capture and use of knowledge. Reports on the progress of knowledge management activities. Configures and develops knowledge management systems and standards.

MRCH Market research: Level 4 Designs and conducts market research studies independently. Analyses market data to identify trends, opportunities and challenges. Segments markets and identifies target customers based on research findings. Prepares research reports and presentations to communicate findings and recommendations.

Appendix VI - Business

Main Tasks

- Investigating business situations to define recommendations for improvement action.
- Managing requirements through the entire delivery and operational lifecycle.
- Creating abstract or distilled models of business scenarios, representing processes, data and roles to support decision-making and analysis.
- Developing, producing and delivering regular and one-off management information to provide insights and aid decision-making.
- Developing models and diagrams to represent, communicate and manage data requirements and data assets.
- Managing and developing products or services throughout their full lifecycle, from inception through growth, maturity, and decline, to retirement.

Essential Professional Attributes Based on SFIA v9 (Appendix III)

Code	Description	SFIA Level
BUSA	Business situation analysis	4
REQM	Requirements definition and management	3
BSMO	Business modelling	3
BINT	Business intelligence	3
DTAN	Data modelling and design	3
PROD	Product Management	3
BIDM	Bid/Proposal Management	4
FIAN	Financial Analyses	3
KNOW	Knowledge Management	3

SFIA Skills Definition – Business

BUSA Business situation analysis: Level 4 Investigates business situations where there is some complexity and ambiguity. Adopts holistic view to identify and analyse problems and opportunities. Contributes to the selection of the approach and techniques to be used for business situation analysis. Conducts root cause analysis and identifies recommendations for improvements. Engages and collaborates with operational stakeholders.

REQM Requirements definition and management: Level 3 Defines and manages scoping, requirements definition and prioritisation activities for small-scale changes and assists with more complex change initiatives. Follows agreed standards and applies appropriate techniques to elicit and document detailed requirements. Provides constructive challenge to stakeholders as required. Reviews requirements for errors and omissions. Prioritises requirements and documents traceability to source. Provides input to the requirements baseline/backlog. Investigates, manages and applies requests for changes to requirements, in line with change management policy.

BSMO Business modelling: Level 3 Produces models for straightforward business scenarios with clear boundaries, selecting suitable techniques to meet assigned objectives. Engages with subject matter experts to ensure models are accurate and meet business requirements. Applies established techniques to meet objectives, modelling business processes, roles and data. Collaborates with stakeholders to address issues and ensure models provide clarity and insight. Tests models and makes improvements as needed, ensuring accuracy and relevance to the business context.

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.

DTAN Data modelling and design: Level 3 Applies standard data modelling and design techniques based upon a detailed understanding of organisational requirements. Establishes, modifies and maintains data structures and associated components. Communicates and explain the details of data structures and components to others.

PROD Product management: Level 3 Creates and curates various content to support the adoption and usage of products or services. Monitors results and feedback from product campaigns. Applies standard techniques and tools to carry out analysis and performance monitoring activities for specified products. Supports problem resolution, resolves issues and acts on feedback for products in use.

BIDM Bid/Proposal Management: Level 4 Leads the creation of small to medium proposals, integrating technical analysis and broader context. Coordinates team efforts, shapes the proposal structure and addresses financial aspects including budgeting and pricing strategies. Identifies and manages proposal risks, ensuring timely compliance with stakeholder expectations. Engages with stakeholders and shapes proposal structure and content based on in-depth discussions and feedback.

FIAN Financial Analyses: Level 3 Applies established financial analysis techniques and processes to carry out specific tasks such as detailed data analysis, report generation and interpretation of financial metrics. Contributes to the development of actionable insights for decision-making. Communicates financial analysis findings to relevant stakeholders.

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 enable capture and use of knowledge. Reports on the progress of knowledge management activities. Configures and develops knowledge management systems and standards.