



Position Description

Technical Account Manager

Business unit:	Cyber Security Operations (CSO) Information Assurance and Cyber Security (IAC) Directorate
Responsible to:	Team Lead, Systems Engineering, Cyber Security Operations
Position purpose:	Technical Account Manager is responsible for the planning, development and implementation of technical IT service management processes to support and enhance our Computer Network Defence (CND) capabilities. Our Technical Account Manager combines their skills, knowledge and passion to manage customer relationships, partnerships and technology products which further enhance our ability to detect, discover, analyse and report sophisticated threats to the security of New Zealand's most significant information assets.
Directorate overview:	The IAC Directorate contributes to the national security of New Zealand by providing technical advice and assistance to Government and organisations with significant national information infrastructures to enable them to protect their information from advanced technology-borne threats. To achieve this, the directorate provides high assurance services; information assurance policy and advice; and high-end cyber security services to detect and respond to such threats.
Remuneration indicator:	Band I
Date Evaluated:	Aug 2015

GCSB vision and values

Our vision

Protecting and Enhancing New Zealand's Security and Wellbeing.

Our values

Respect, Commitment, Integrity, Courage.

Functional relationships

External contacts:	Internal contacts:
<ul style="list-style-type: none">• NZ GOVT central and monitoring agencies• Senior engineers of government agencies, private sector firms, IT service providers and network operators• Senior engineers, technical project managers and liaison officers representing international partner agencies• Providers of technical and project management assurance services	<ul style="list-style-type: none">• Senior GCSB/NZSIS managers particularly Directors and Assistant Directors• Operational GCSB/NZSIS managers• Intelligence Community Shared Services managers and staff in the following areas: Finance, Procurement, Security, HR, Programme/Project Management• GCSB Legal and Compliance teams

Role Specification

Objectives

The position of Technical Account Manager encompasses the following major functions or Objectives:

- Solution Design and Implementation
- Maintenance of Engineered Solutions
- Customer and Partner Engagement

The requirements in the above objectives are broadly identified below:

Jobholder is accountable for:	Jobholder is successful when:
<p><u>Solution design and implementation</u></p> <ul style="list-style-type: none">■ The facilitation of research and development of new, innovative solutions to enable and enhance	<ul style="list-style-type: none">■ Electronic attack threats to monitored entities' infrastructure are identified and understood■ Technical analysis of detected threats

National Cyber Security Centre's (NCSC) discovery and detection of malicious activity.

- Following good industry design practices to ensure that solutions meet highest standards in operations.
- Assisting in the Integration of hardware and software solutions that enable efficient analysis and reporting of threats.
- Development of a service management framework to ensure effectively delivery of capabilities.
- Working with other teams to ensure the successful and efficient implementation of new or enhanced capabilities.

identifies the capability and intention of the malware targeting the victim

- Solutions and enhancements are designed to be inherently secure, resilient and scalable.

Maintain engineered solutions

- Continual review and improvement of engineered solutions and accesses.
- Effective testing and remediation of identified bugs and errors.
- Produce, and make available, documentation on engineered solutions to ensure their longevity
- Pro-active maintenance, monitoring, alerting and support of various systems to ensure maximum performance, stability and uptime.
- Providing support to the users of both Classified and Unclassified CND and other NCSC/IAC Directorate systems as directed
- Adherence to industry standard practices for change and capacity management.

- Existing detection systems remain operational and capable of detecting cyber threats.
- Detection capabilities are routinely reviewed to ensure they are fit for purpose
- NCSC systems are proactively maintained to ensure they are available and responsive for users to fulfil their required functions.
- Usable documentation is produced that clearly articulates the purpose and use of GCSB or partner engineered solution to CND problems
- Documentation is in line with any GCSB engineering standards, policies and guidelines
- Users are enabled to effectively and efficiently use engineered solutions in support of their mission.

Customer and partner engagement

- Interact with Developers, Analysts and Engineers
- Working closely with NCSC customers to maintain expected levels of service
- Actively participate in community and

- The technical capability of individuals within the NCSC is valued across the developer and security community
 - The Systems Engineer maintains awareness of current cyber security issues and technological trends
-

<ul style="list-style-type: none"> industry forums, meetings and conferences ■ Provide engineering or technical assistance to other NCSC and GCSB colleagues to enable the enhancement of business and process ■ Maintain an awareness of information security and general IT industry trends and developments 	<ul style="list-style-type: none"> ■ Productive and enduring relationships are formed with domestic and international partners,
-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------	------------------------------------------------------------------------------------------------------------------------------------------------

Precise performance measures for this position will be developed in discussion between the successful candidate and manager as part of the performance development and review process. It is also expected that you will undertake other duties that can be reasonably be regarded as relevant to the position, your experience and capability.

Person specification

Qualifications

Essential:	Desirable
<ul style="list-style-type: none"> ■ Tertiary degree, or equivalent experience. 	<ul style="list-style-type: none"> ■ Professional computing/networking qualification, e.g. in computer networking, or systems administration. ■ Professional Information Security certifications. ■ DevOps and/or IT Service Management and Governance frameworks qualifications.

Knowledge/experience

Essential:
<ul style="list-style-type: none"> ■ Three years' experience of IT operations models and Service Management processes (such as Change Management, Incident Management, Configuration Management and Systems Development Life Cycle). ■ Experience with Project Management, Service Delivery or Account Management. ■ Experience with DevOps practices and Agile project delivery methodologies. ■ The ability to use or learn about a wide variety of Open Source technologies. ■ Experience with automation, configuration management and monitoring tools. ■ Experience with network or systems engineering or administration. ■ Understanding of system architecture, design and implementation principles. ■ Ability to talk with customers at a technical level.

Personal attributes

- Demonstrates a practical and robust troubleshooting philosophy.
- A commitment to the documentation of process and actions.
- Results oriented with a demonstrable commitment to perform.
- Thinks critically and logically.
- Excellent communication and interpersonal skills.
- The ability to be self-motivated, flexible and a team player.
- An ability and desire to learn new and sometimes complex skills.
- Demonstrate sound judgment, tact and integrity in dealing with sensitive issues.
- Excellent organisational skills and the ability to prioritise and work to deadlines.
- Displays initiative and self-confidence.
- The resilience to operate under pressure and correctly identify and assess risk, and make justifiable operational decisions.

Specialist competencies

The following levels would typically be expected for the 100% fully effective level:

Core competencies

Core competencies are based on and consistent with our values. They describe qualities that are common requirements for all GCSB staff at differing levels in the organisation, irrespective of their specialist skills or the particular requirements of their job. They are complemented by specialist competencies, which (where applicable) are set out in individual performance agreements.

All employees are measured against the following core competencies as part of performance development and review:

- Security
- Teamwork and leadership
- Results focus
- Communication and knowledge sharing
- Professionalism
- Innovation
- Customer focus.

Changes to position description

Positions in the GCSB may change over time as the organisation develops. Therefore we are committed to maintaining a flexible organisation structure that best enables us to meet

changing market and customer needs. Responsibilities for this position may change over time as the job evolves. Such change may be initiated as necessary by the manager of this position. This position description may be reviewed as part of planning for the annual performance cycle.

Health and safety

GCSB is committed to providing a healthy and safe work environment and management practices for all employees. Employees are expected to share this commitment as outlined in current Health and Safety legislation by taking all practicable steps to ensure:

- a. The employee's safety while at work; and
- b. That no action or inaction of the employee while at work causes harm to any other person.

Knowledge management

Employees are responsible for ensuring that all business records created are accessible and stored in the correct manner according to GCSB record keeping policy, standards, and procedures.

Employee: _____

Date: _____

Manager: _____

Date: _____