New Zealand Intelligence Community
Te Rōpū Pārongo Tārehu o Aotearoa
nzic.govt.nz

Position Description

IT Security Certification Assessor

Directorate:	Protective Security
Position purpose:	The purpose of this position is to assess systems against government standards to ensure compliance and operability. This position will also be seen as the certification subject matter expert offering advice and guidance to a range of individuals / teams.
Directorate overview:	The Protective Security (PS) Directorate delivers a full range of protective security functions to the NZIC and for New Zealand. The PS Directorate leads the implementation of the Protective Security Requirements (PSR) programme, which aims to substantially improve the security culture of the public service and, potentially, the private sector. The PS Directorate is also responsible for protecting the integrity of the public service and NZIC through effective security clearance management, vetting services and counter intelligence functions. Led by the PS Directorate, the NZIC will be an exemplar of physical, IT and personnel security best practice.
Direct Reports:	Nil
Financial authorities:	Nil
Remuneration indicator:	Band H
Date evaluated:	12 September 2017

NZSIS mission and values

Our mission

Keeping New Zealand and New Zealanders safe and secure

Our values

Collaborative, Courageous, Positive, Driven, Self-aware

Functional relationships

External contacts:	Internal contacts:
• GCSB system owners • GCSB Accreditation team members • Counterparts within the wider New Zealand Intelligence Community and central government agencies • Other partner intelligence agencies and law enforcement organisations • Other relevant public or private sector organisations as required	• Directorate staff and contractors • NZSIS system owners and their representatives/associates (system administrators, system engineers, testers etc) • NZIC Certification Authorities • IT Security Advisors • NZIC Chief Information Security Officers • NZIC Chief Security Officers • NZIC IT Security Managers • NZIC Communication Security Officers

Objectives

The position of IT Security Certification Assessor encompasses the following major functions or objectives:

- Assess IT systems for certification
- Promote certification practice in the NZIC
- Provide expert advice pre and post system certification
- Health, Safety and Wellbeing
- Risk management

The requirements in the above objectives are broadly identified below:

Jobholder is accountable for:	Jobholder is successful when:
Assess IT systems for certification	
• Assess compliance of systems for system security	• Systems are thoroughly assessed for compliance in accordance with standards, legislation and regulations.

• Assess test plans and test results for system security	• System owners furnish fulsome test methodologies including the process for testing systems to ensure they are secure and results attest to this outcome.
• Complete inspection of systems	• System inspections are completed via a paper based review of certification artefacts and/or a hands-on interaction with the system functionality provided by a Subject Matter Expert.
• Production of a final report comprising findings of the assessment and recommendations to the Certification Authority	• Recommendations to the Certification Authority are to the expected standard and meet requirements. Reviews and recommendations are made in a timely manner as agreed with management / stakeholders.
• Maintain records on the management and status of system certifications	• All records on the management and status of system certifications are complete, correct and easily accessible.
Promotes the certification practice in the NZIC	• Is recognised as the subject matter expert in system certification • Ensures certification artefacts (templates) are up to date and accurately reflect standards (such as the PSR and ISM) • Provides accurate and timely certification advice and guidance to IT Security Advisors as they work collaboratively with system owners/project teams • Provides timely and relevant education on certification requirements, including delivery of training and educational materials
Health, Safety and Wellbeing	• Health and safety (of self) is practiced by: o Working safely and take responsibility for keeping self and colleagues free from harm. o Reporting all incidents and hazards promptly. o Knowing what to do in the event of an emergency. o Cooperating in implementing return to work plans.

Risk management	• All activities take account of security, operational and organisation reputational risk and these risks are managed to approved standards and escalated to management where appropriate. • All activities are consistent with NZSIS legally mandated role and functions. • Any residual risks in systems are identified and highlighted

Precise performance measures for this position will be developed in discussion between the jobholder 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

This section is designed to capture the expertise required for the role at the 100% fully effective level. (This does not necessarily reflect what expertise the current jobholder has.) This may be a combination of knowledge, experience, key skills, attributes, job specific competencies, qualifications or equivalent level of learning.

Qualifications

Essential:	Desirable:

• Information Systems or Computer Science degree, or
• Information Assurance and Security (Level 7) Graduate Diploma
• ISACA Certified Information Systems Auditor or Security Manager (CISA/CISM) or GIAC Security Essentials (GSEC), or equivalent experience
	• IT security qualification such as System Security Certified Practitioner (SSCP)
	• Other industry recognised certification such as:
	  ○ Information Technology Infrastructure Library (ITIL)
	  ○ The Open Group Architecture Framework (TOGAF)

Knowledge/experience

Essential:	Desirable:
• At least five years experience in large scale and complex IT systems design, implementation and maintenance. • Experience in conducting IT security assessments, audits and applying security risk management practices. • Proven knowledge and application of: ○ AS/NZS ISO 31000:2009 Risk Management principles and guidelines.	• Proven understanding of protective security principles and practices, including familiarity with Protective Security Requirements and the New Zealand Information Security Manual. • Holistic understanding and exposure to certification and accreditation frameworks in an Intelligence Community context.

  - ISO/IEC 27006:2011 Information Technology – Security Techniques – Requirements for bodies providing audit and certification of information security management systems.
  - ISO/IEC 27007:2011 Information Technology – Security Techniques Guidelines for information security management systems auditing
- Well developed interpersonal skills with the ability to engage with a diverse range of people at all levels of the organisation.

Personal attributes

- Ability to work independently using sound judgement and initiative.
- Proven ability to work as a member of a successful team at all levels of the organisation.
- A high level of accuracy and attention to detail.
- Professional customer focus with a strong commitment to providing a high standard of customer service.
- Strong analytical skills with the ability to work methodically and display an aptitude for problem solving.
- Excellent written and oral communication skills, with an ability to convey technical information in a manner that is understood by the audience.
- Self motivated with excellent planning and organisational skills, and the ability to prioritise tasks to meet deadlines and effectively manage changing priorities.
- Proven coaching and mentoring skills and ability.
- Demonstrated high levels of integrity and an ability to maintain a TSS security clearance.

Changes to position description

Positions in the NZSIS 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

NZSIS 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 the 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 NZSIS record keeping policy, standards, and procedures.

Employee: _____ Date: _____

Manager: _____ Date: _____