Operational Security Advisor

Technology Services and Solutions (TSS), Organisational Capability and Services Branch (OCS)

The primary purpose of the Operational Security Advisor is to provide leadership, advice and information on operational security across technical delivery within TSS. The Operational Security Advisor ensures that operational ICT security is applied as it relates to business goals and facilitates the safe and effective delivery of business outcomes.

- **Reporting to**: Manager Assurance
- **Location:** Wellington
- **Salary range**: Information Technology I

What we do matters – our purpose

Our purpose is to serve and connect people, communities and government to build a safe, prosperous and respected nation.

In other words, it's all about helping to make New Zealand better for New Zealanders.

How we do things around here – our principles

We make it easy, we make it work
- Customer centred
- Make things even better

We're stronger together
- Work as a team
- Value each other

We take pride in what we do
- Make a positive difference
- Strive for excellence

Working effectively with Māori

Te Aka Taiwhenua – our Māori Strategic Framework – enables us to work effectively with Māori. We accept our privileged role and responsibility of holding and protecting the Treaty of Waitangi / Te Tiriti o Waitangi.

Te Tari Taiwhenua
Internal Affairs

What you will do to contribute	As a result we will see
Operational Security • Set clear, achievable Operational Security Standards for delivery by TSS and vendors • Ensure the appropriate installation, maintenance and monitoring of security controls are in place • Ensure reporting on risk and security profiles is in place both technical and into the business • Continuously improve and enhance DIA's existing ICT Security policies, process and procedures • Work closely with the Security and Risk Team to ensure Security advice is aligned to standards and operational security risks are effectively captured and mitigated • Report regularly on the state of operational security to the Chief Security Officer • Lead operational security practice	• Security risks are appropriately managed and mitigated • ICT Security policies are kept up to date and are accessible on intranet • Operational Security is appropriate and relevant • ICT Standards are kept relevant and reported on • Improved understanding of current ICT security risks across the Department • Plans for improvement that are monitored and reported on
Security awareness • Support and provide training where relevant to managers and staff within TSS • Provide sound security risk management advice to vendors and internal teams in TSS	• Operational Security awareness is raised across TSS • Capability to undertake operational security activity is raised
Stakeholder & Relationship Management • Build and maintain relationships with internal business owners and external vendors to ensure collaborative and effective security services • Work closely with ITMS vendor to report on and improve operational security	• Improved business outcomes
Health and safety (for self) • Work safely and take responsibility for keeping self and colleagues free from harm • Report all incidents and hazards promptly • Know what to do in the event of an emergency • Cooperate in implementing return to work plans	• A safe and healthy workplace for all people using our sites as a place of work. • Health and safety guidelines are followed

Who you will work with to get the job done		Advise	Collaborate with	Influence	Inform	Manage/ lead	Deliver to
Internal	Business Owners	✔	✔	✔	✔		
	Manager, Service Performance and Integration	✔		✔	✔		✔
	Manager Assurance	✔		✔	✔		✔
	Security and Risk team						

Who you will work with to get the job done		Advise	Collaborate with	Influence	Inform	Manage/lead	Deliver to
	Chief Security Officer / Office	✓	✓	✓	✓		✓
	Assurance Advisor		✓	✓	✓		
	Manager Unified Services		✓	✓	✓		✓
External	Vendors	✓	✓	✓	✓	✓	✓

Your delegations

Human Resources and financial delegations	Level Z
Direct reports	None

Your success profile for this role

At DIA, we have a Capability Framework to help guide our people towards the behaviours and skills needed to be successful. The core success profile for this role is Valued Contributor.

Keys to Success:
- Customer Focus
- Continuous improvement
- Teamwork and peer relationships
- Action oriented
- Self-development and learning
- Functional and technical skills

What you will bring specifically

Experience:
- Experience of security management principles, frameworks and controls and experience with conducting or responding to information system audits.
- Some experience training and mentoring people
- Experience in implementing and managing security reporting and advising on security improvement.
- Experience reviewing security designs as part of a project or architecture team is desired but not essential
- Experience in working with vendor/s to deliver shared outcomes

Knowledge:
- Working knowledge of risk management principles, frameworks and processes
- Knowledge of ITIL and other similar Service Management frameworks

Skills:
- Excellent communication skills with the ability to communicate effectively with internal and external stakeholders
- Ability to translate ICT security information into appropriate language for the business
- Ability to evaluate security procedures and measures.
- Relationship Management skills

Your success profile for this role	What you will bring specifically
	Other requirements:
	• Security orientated certification / qualification