Position Details

Technical Services- CSOF6

THE FOLLOWING INFORMATION IS FOR APPLICANTS	
Advertised Job Title	Manager Cyber Security Resilience
Job Reference	100266
Tenure	Indefinite, Full-time
Salary Range	AU$131,113 to AU$153,639 pa + up to 15.4% superannuation
Location(s)	Sydney (Lindfield), Melbourne (Clayton), Canberra (Black Mountain), Brisbane (St Lucia), Hobart (Sandy Bay), Adelaide (Waite)
Applications are open to	Australian Citizens Only
Position reports to the	Chief Information Security Officer
Client Focus – Internal	80%
Client Focus – External	20%
Number of Direct Reports	11
Enquire about this job	Contact Jamie Rossato via email at Jamie.Rossato@csiro.au
How to apply	Apply online at https://jobs.csiro.au/ Internal applicants please apply via **Jobs Central** If you experience difficulties when applying, please email careers.online@csiro.au or call 1300 984 220.

Acknowledgement of Country

CSIRO acknowledges the Traditional Owners of the land, sea and waters, of the areas that we live and work on across Australia. We acknowledge their continuing connection to their culture and pay our respects to their Elders past and present. View our vision towards reconciliation.

Child Safety

CSIRO is committed to the safety and wellbeing of all children and young people involved in our activities and programs. View our Child Safe Policy.

Role Overview

CSIRO is seeking an experienced leader to manage its Cyber Security Resilience team. This team plays a vital role in ensuring that CSIRO's services are secure-by-design and aligned with acceptable risk levels. Working across the entire organisation and a range of strategic projects, the team delivers cyber security engineering and assurance artefacts, identifies risks, and provides recommendations to support informed decision-making.

The successful candidate will be responsible for leading the team's delivery of security resilience activities in line with business impact levels, managing complex workloads and resources, and ensuring high-quality outputs. The role also involves close collaboration with peers in Cyber Operations, and IM&T to embed standard security processes and ensure ongoing assurance of systems and applications throughout their lifecycle, in line with organisational risk appetite and stakeholder expectations.

Duties and Key Result Areas:

- Maintain and establish collaborative and productive relationships with CSIRO operational and research stakeholders to maintain secure delivery of business goals within CSIRO organisational risk appetite.
- Maintain and establish collaborative and productive relationships with project stakeholders to enable secure delivery of business goals within CSIRO organisational risk appetite.
- Manage team and cyber security partner resources/services across multiple programs of work.
- Take ownership of technical assurance capabilities such as vulnerability management, penetration testing with a view to optimise and mature these capabilities.
- Lead CSIRO's supplier cyber risk assurance capabilities to ensure CSIRO suppliers and third-parties risks remain within acceptable levels.
- Take ownership of cyber awareness capabilities of the organisation by developing and implementing a longitudinal, multi-faceted cyber awareness program.
- Be responsible for running and improving CSIRO's cyber architecture capabilities.
- Review and approve cyber security resilience activity artefacts produced by the team prior to release and escalate any significant risks to the Chief Information Security Officer in partnership with key stakeholders.
- Manage cyber security related tickets/requests and reporting, budget planning and forecasting, and delivery of security engineering and assurance activities.
- Facilitate capability development and implementation to support and enhance cyber security resilience team activities.
- Work with the CSIRO teams in embedding cyber security factors into standard development and verification processes applicable to project and ongoing production activities.
- Participate in IMT governance related activities such as the Technical Design Authority (TDA), and Change Management Advisory Board (CMAB).
- Support other cyber security teams as required, especially in the areas of security operations, risk management and privacy.
- Assist IMT and other business unit initiatives with general security guidance, contract & Procurement activities, and business impact assessment support as directed.
- Contribute to knowledge sharing within the team by documenting procedures, issues, risks, lessons learnt, and achievements.
- Communicate effectively and respectfully with all staff, clients and suppliers in the interests of good business practice, collaboration and enhancement of CSIRO's reputation.

- Work collaboratively with colleagues within your team, the business unit and across CSIRO, to reach objectives.
- Establish and lead effective teams, allocate and manage resources and take responsibility for strategic and operational plans for the service and undertake staff performance management and career development.
- Choose appropriate management strategies and communication styles to maintain high levels of motivation and productivity, giving feedback for development purposes and providing support for improvement.
- Adhere to the spirit and practice of CSIRO's Values, Health, Safety and Environment plans and policies, Diversity initiatives and Zero Harm goals.
- Other duties as required.

Selection Criteria

Essential

Under CSIRO policy only those who meet all essential criteria can be appointed.

1. Tertiary and/or industry qualifications in cyber security, IT or equivalent discipline.
2. At least two (2) years managing a cyber security team in an operational or assurance capacity, or at least five (5) years managing an IT team.
3. Demonstrated experience with leading the design, engineering and architecture of cyber security controls and application of cyber security assurance capabilities or resources
4. Demonstrated experience in the application of cyber security and/or information security principles, and best practices.
5. Demonstrated experience in identifying, evaluating, and mitigating risks within an Enterprise environment.
6. Demonstrated experience in managing a technology service/ area or technically leading/designing an enterprise solution.
7. Demonstrated knowledge of enterprise and solution architecture, business analysis and requirements development, vulnerability scanning, penetration testing, threat/risk/gap assessments, compliance audits, and code analysis.
8. Proven track record of effective ticket or request management providing advice to end users and stakeholders as well as issue/problem resolution.
9. Demonstrated ability to communicate, collaborate and work effectively across organisational boundaries and levels with initiative and autonomy.
10. Demonstrated ability to coordinate and manage competing priorities including engagement across multiple IMT strategic projects, day to day operational service delivery, reporting, capacity management, budget management, team management, and project management.
11. Demonstrated ability and willingness to contribute novel ideas and approaches in support of scientific research and keeping the organisation cyber safe.

Desirable

1. Experience in supporting multiple complex projects.
2. Experience with the Protective Security Policy Framework (PSPF).

3. Experience with Australian Cyber Security Centre (ACSC) security guidance, NIST SP guidelines, and Centre of Internet Security (CIS) benchmarks.
4. Good understanding of shared responsibility model in the cloud and/or on-premises.
5. Familiarity with Australian legislation including (but not limited to) the Privacy Act 1988 (Cth) and the Archives Act 1983 (Cth); and
6. Relevant security industry certifications from certification bodies such as ISACA, ISC^2, SANS, PECB, SABSA Institute, The Open Group etc.

Required Competencies

- **Teamwork and Collaboration:** Cooperates with others to achieve organisational objectives and may share team resources in order to do this. Collaborates with other teams as well as industry colleagues.
- **Influence and Communication:** Identifies critical stakeholders and influences them via an influential third party, for example through an established network, to gain support for sometimes contentious, proposals/ideas.
- **Resource Management/Leadership:** Provides leadership that fosters an environment that encourages new ideas and provides support for the development of emerging skills. Creates trust by displaying consistency, understanding, integrity and patience. Plans, seeks, allocates and monitors resources to achieve outcomes.
- **Judgement and Problem Solving:** Anticipates and manages problems in ambiguous situations. Develops and selects an appropriate course of action and provides for contingencies. Evaluates, interprets and integrates complex bodies of information and draws logical conclusions, synthesises proposals and defends options with reasoned arguments.
- **Independence:** Assesses the risk and opportunity of identified strategies, options and actions. Overcomes problems and setbacks in achieving goals. Invariably includes consideration of value-added future impact on bottom line when determining the optimal and efficient use of resources.
- **Adaptability:** Demonstrates flexibility in thinking and adapts to and manages the increasing rate of organisational change by adjusting strategies, goals and priorities.

Special Requirements

Appointment to this role may be subject to conditions including provision of a national police check as well as other security/medical/character clearance requirements.

Security Clearance: NV1 or higher

This is a security assessed position. Applicants must be an Australian citizen, with successful candidate either holding or having the ability to obtain a Negative Vetting 1 Australian Government security clearance.

Note:

- CSIRO utilises the Australian Government Security Vetting Agency to conduct its security clearances. Further information regarding security clearances may be found at https://www1.defence.gov.au/security/clearances

- The Commonwealth requires all Specified Personnel to undergo Work, Health and Safety and Security Awareness training. Training must be undertaken upon commencement and be completed before the commencement of any work. Training is by means of an online courses and questionnaires that can be undertaken at Commonwealth premises.

Referee Requirements

Candidates must provide a minimum of 2 referees. Referee checks will only be performed for candidates shortlisted for interview.

About CSIRO

We solve the greatest challenges through innovative science and technology. Visit CSIRO Online for more information.

CSIRO is a values-based organisation. In your application and at interview you will need to demonstrate behaviours aligned to our values of:

- People First
- Further Together
- Making it Real
- Trusted