# Position Description

## POSITION DETAILS

| | |
|---|---|
| **Title of Position:** | Cyber Security Risk Analyst |
| **Reports to:** | Manager Cyber Security |
| **Division:** | People and Safety |
| **Function:** | Cyber Security |
| **Number of Direct Reports:** | Nil |
| **Grade:** | 6 |

## HEALTH, SAFETY & WELLBEING

ElectraNet is committed to a Safety-First culture and a work environment promoting the health, safety and wellbeing of all workers. To sustain this culture, all leaders are required to implement and maintain the areas of ElectraNet's safety management system under their control, where the health, safety and wellbeing of all workers comes first while ensuring full compliance with all legislative and policy requirements.

All employees are required to contribute to the Safety First culture by exercising their duty of care to themselves and one another, by working safely, by adhering to all reasonable safety instructions, by using all equipment provided in accordance with safe work methods and by promptly reporting any unsafe working practices or hazardous working conditions.

## POSITION OVERVIEW

The Cyber Security Risk Analyst is responsible for the planning, identification, implementation, control, review, audit and assurance of technology and operational risks. The Cyber Security Risk Analyst will identify, prioritise and mitigate these risks while ensuring compliance with best practices in design and delivery of technology solutions.

The Cyber Security Risk Analyst provides ElectraNet with the capability to design, build and operate the respective security technologies and processes. Furthermore, they provide technical advice and leadership, staff mentoring, security event validation, triage, and incident response.

Success in this role is characterised by working closely with internal stakeholders to develop a shared understanding of their Cyber Security needs whilst developing and nurturing collaboration and effective communication to maximise improvement opportunities in meeting ElectraNet's control objectives.

## KEY RESPONSIBILITIES

### OPERATIONAL & TECHNICAL

Capable of working for extended periods under general supervision, you will be accountable in contributing to technical advice and operational support in:

- Managing and analysing incoming Cyber Security and technology risks through risk identification and classification, control selection and testing.
- Preparing risk reports and ensuring actions are documented and delivered.
- Tracking and monitoring risk activities, notifying action owners, and escalating where required.
- Ensuring risks and remediation plans are regularly addressed and compliance for Cyber Security across all in-scope assets and environments.
- Conducting quality assurance on all risk assessments.
- Ensuring system security controls, changes and operations are compliant against policy, standards, and processes.
- Building understanding and awareness of Cyber Security risks throughout the organisation.
- Improving the Cyber Security processes, solutions, and professional practices of the team.
- Using judgement to make risk-based recommendations and decisions within parameters.

- Providing technical expertise in protecting the confidentiality, integrity and availability of assets, information, and operations technology.
- Acting as a Subject Matter Expert to provide input and advice on projects whilst leading and championing a “Secure by Design” approach.
- Monitoring, and contributing to, the day-to-day operations and administration of security systems and controls, including for example:
    - Identity and Access Management
    - Threat Management
    - Vulnerability assessments and remediation
    - Third Party Assessments
    - Incident Identification and Response
    - Security Analytics
    - Security configuration hardening
- Performing and supporting internal audits for security compliance on policy, processes, and standards
- Contributing to the implementation of roadmaps for the Cyber Security team and Organisational Resilience Program.
- Contributing to the review and continuous improvement of guidelines, processes, and systems; and
- You may be directed to undertake other duties commensurate with your skills and classification level.

**BEHAVIOURAL**

- Build and maintain strong working relationships with and between internal and external stakeholders, delivering a high level of customer service.
- Create and develop a respectful workplace environment that values cultural diversity, innovation, open discussion and cross functional collaboration to help drive high performance.
- Lead by example; role model desired behaviour and priorities, demonstrate personal accountability for self-development and for achieving quality and timely result.
- Carry out the role in a professional and ethical manner and in accordance with ElectraNet’s values, Code of Conduct and other policies.

## SIGNIFICANT WORKING RELATIONSHIPS

- External suppliers and service providers
- Internal stakeholders

## SELECTION CRITERIA

**KNOWLEDGE, SKILLS & EXPERIENCE:**

**Essential**

- Minimum 3-5years’ experience, in a Cyber Security risk related role
- Ability to apply theoretical and practical knowledge to solve commonly encountered problems.
- Understanding and working knowledge of industry specific frameworks e.g., ISO 31000, AESCSF , NIST CSF, NIST RMF, ES-C2M2,.
- Demonstrated knowledge of risk management methods and tools
- Strong understanding of Privacy legislation and requirements in Australia, such as AESCSF.
- Demonstrated capability in implementing and growing a function
- Experience in developing documentation and procedures relating to all aspects of all Cyber Security and risk services
- Experience in securing and monitoring of Microsoft Azure and O365.
- Understanding of infrastructure and application architecture, log analysis, security forensics and incident response.

# Position Description

- Demonstrated experience in vulnerability/threat assessment, identification, and risk reduction.
- Proven experience in securing critical real-time systems.
- Experience working with 3rd party suppliers to deliver assurance services.
- A continuous improvement focus with the proven ability to constructively challenge the status quo.
- Demonstrated ability to effectively partner build and maintain collaborative relationships with key internal and external stakeholders.
- A customer and outcome focussed approach with sound verbal and written communication skills.
- Demonstrated initiative, accountability, and the ability to adapt of changing priorities.
- Well-developed commercial acumen and influencing skills with the ability to work autonomously.
- Proven ability to translate technical information into simple concepts/meanings for internal and external stakeholders.
- Well-developed analytical, investigation and problem-solving skills.
- Demonstrable, advanced written and verbal communication skills; good interpersonal skills.
- Demonstrable ability to work as a team member and actively promote office harmony.
- Willingness to undergo requisite security, background, or Police check; and
- Flexible approach to working hours and after-hours commitments.
- Experience with a security information and event management system (SIEM) for audit.

**Desirable**

- Electricity Industry or critical infrastructure background an advantage

**QUALIFICATIONS:**

- Tertiary qualifications in Cyber Security – or equivalent experience (essential)
- Valid Drivers Licence (essential)
- Certifications in ISACA CRISC, ISACA CISA, ITILv3, iso 31000, Cisco CCIE Security, CompTIA Security+, CompTIA CySA+, GSEC: SANS GIAC Security Essentials, CEH: Certified Ethical Hacker or equivalent (desirable)

NOTE: Copies of the above listed qualifications/licences/certificates are required as evidence on appointment.