

## POSITION DESCRIPTION

<b>Position Title</b>	Information Security Analyst
<b>Department / Branch</b>	Digital
<b>Reporting Relationships</b>	Senior Manager Technology Security & Operations
<b>Supervisory responsibilities</b>	Nil
<b>Classification</b>	Package
<b>Effective date</b>	June 2022

### General Responsibilities of Role

#### Objective

Credit Union SA is undertaking an ambitious program of change activity as it transforms into a technology-enabled organisation with digital experience and efficiency at the core of everything we do. To do this, we will continue to embrace leading-edge digital systems and technologies that will require us to challenge traditional practices and strengthen existing technology foundations and frameworks.

The Information Security Analyst will be responsible for the design and implementation of information security and risk systems. This influential role will ensure robust system design and data governance is in place to support operational and change activity. The role will act as an expert on information security, while providing progressive and innovative thinking to ensure the Credit Union's digital transformation objectives can be achieved within a secure environment.

#### Key responsibilities

Reporting to the Senior Manager Technology Security & Operations, you will be required to:

- Provide information security advice and analysis to internal customers and vendors.
- Influence the design of effective and secure technology systems and applications.
- Identify, assess and mitigate information security risks, including control design and implementation.
- Investigate, respond to, resolve and report on information and security incidents and issues.
- Assist with design and implementation of information security assurance and testing activities.
- Develop and enhance information security policies, standards, procedures and guidance.
- Develop, implement and oversee an effective information security management framework.
- Chair the Information Security Committee and act as subject matter expert for information security.
- Liaise with project, operational teams and business leaders to ensure information security is embedded throughout the organisation.
- Assess and advise on appropriate information security practices for key suppliers, vendors and third parties.

- Liaise and work effectively with technology vendors and external audit partners.

The role will operate with a moderate degree of independence and the successful candidate will be expected to plan and implement their own work program under the guidance of the Technology Services Manager. The role will work closely with the internal Risk and Governance team on a day to day basis.

### **Selection Criteria**

The successful candidate will be required to satisfy most of the following criteria:

- Advanced knowledge of contemporary technology, information and security architecture principles and practices.
- Expert understanding of technology and information security constructs, from high level principles through to detailed technical configuration, including network, system and application design and configuration.
- Expert understanding of cyber threat vectors and hacking methodologies.
- Strong knowledge of technology, security, cyber, control and risk frameworks and standards including ITIL, PCIDSS, ISO27001, NIST, OWASP, COBIT and the Australian Privacy Principles.
- Experience with business continuity, disaster recovery planning and incident management.
- Experience working in a complex multi-vendor environment across the whole technology stack.
- Solid understanding of business process and risk analysis.
- Solid understanding of regulatory and compliance requirements applicable to financial services.
- Experience designing and implementing a framework of security controls, including vulnerability assessments and penetration tests.

### **Academic Qualification**

Ideally, tertiary qualifications in a relevant discipline.