Australian Government

Position Description

Position Title:	Cyber Security Manager
Reports to:	Executive Manager Information Technology
Division:	Information Technology
Location:	Orange, NSW or remote
Employment Status:	Permanent ongoing
Hours:	Full Time - 36.75 hours/week
Salary Band:	$133,258 to $156,774 per annum
Citizenship:	Right to Work in Australia

About us

RIC (Regional Investment Corporation) is an Australian Government finance provider for farmers and farm-related small businesses. We were established under the *Regional Investment Corporation Act 2018* (RIC Act) to provide low-cost loans to strengthen Australian agriculture and grow thriving regional communities.

RIC farm loans support our customers to prepare, manage through and recover from drought, natural disasters or biosecurity risks causing severe financial disruption. We help accelerate plans for first-generation farmers and next-generation farmers.

Our culture & people

Our people have vision and are empowered to build a leading Australian Government agency known for its contemporary service, expertise, and integrity. They are committed, innovative and their achievements are celebrated. They are as diverse as the work they do. RIC has a vibrant culture which is based on the following Culture Statements:



Be bold, act with purpose



We are down to earth



We embrace difference and act as one

Our customers

We aim to deliver a first-class customer experience by partnering with our customers from the beginning of their journey with us. We respect the time of our customers by being

transparent with them about the loan process, keeping things simple and understanding their needs.

Put simply, our customer experience principles are:



- Respect my time
- Simple and Seamless
- Partner with me
- Understand me

About the job

As the Cyber Security Manager, you will work closely with the Executive Manager Information Technology to shape, prioritise and deliver RIC's cyber security work program. The Executive Manager Information Technology sets RIC's overall cyber direction and risk priorities; you will provide specialist input into that direction, coordinate delivery across the organisation, and provide clear, evidence-based validation that intended security outcomes have been achieved and are being sustained.

Working under broad direction, you will manage and deliver continuous improvement of cyber security controls across RIC's predominantly Microsoft 365 and fully cloud-based operating environment. The role is primarily focused on implementing agreed requirements, coordinating delivery, reviewing evidence and supporting internal teams and service providers to address identified gaps. You may also contribute directly to technical delivery where appropriate.

You will be responsible for:

- Work with the Executive Manager Information Technology to develop, prioritise and maintain RIC's cyber security work program in line with organisational priorities and risk appetite.
- Coordinate delivery of cyber security initiatives across Microsoft 365, Azure, endpoints, identity, cloud services, business applications and supporting technology services.
- Coordinate RIC's system authorisation process and catalogue, ensuring systems have clear ownership, approval status, risk acceptance and current evidence demonstrating compliance with applicable policy and security controls.
- Document and implement requirements for key controls such as authentication, single sign-on, conditional access, logging and monitoring, privileged access, vulnerability and update management, data protection and incident readiness.
- Assess and test the design and operating effectiveness of cyber security controls, maintain appropriate evidence, and validate whether expected outcomes have been achieved.
- Coordinate and track remediation arising from cyber security assessments of systems and applications.

- Prepare analysis, validation findings and supporting material for the Executive Manager Information Technology's reporting and advice to executives, governance committees and the Board on cyber posture, material risks, incidents and improvement priorities.
- Provide specialist advice on the Information Security Manual, Protective Security Policy Framework and other relevant Australian Government cyber security requirements.
- Develop and review cyber security policies, standards, procedures and supporting guidance in consultation with the Executive Manager Information Technology and relevant stakeholders.
- Lead or coordinate cyber security assessments for new and changed systems, cloud services, technology suppliers and projects, including security requirements, control design and residual risk advice.
- Support cyber incident assessment and response, coordinate technical and provider inputs, maintain incident records and supporting evidence, and escalate material matters to the Executive Manager Information Technology.
- Work collaboratively with RIC's managed cyber security service provider, review service reports and security advice, and coordinate follow-up on identified issues and improvement opportunities.
- Build cyber security awareness and capability across RIC and promote practical, risk-based security practices that support business delivery.
- Perform other duties as required.

Job capabilities

To be successful in this role, the candidate is required to have:

- The ability to collaborate with senior leadership to shape strategic priorities and convert them into a practical, achievable program of work.
- Sound judgement and independence in analysing complex cyber security issues, managing risk and escalating material matters.
- Strong cyber security delivery capability, including driving system and application security uplift and embedding secure-by-design practices.
- Clear communication, with the ability to translate technical risk and recommended action into concise advice and supporting material for senior leaders and non-technical stakeholders.
- Strong stakeholder and provider management skills, including the ability to coordinate supplier delivery and validate deliverables against agreed requirements and coordinate delivery across internal teams and external specialists.
- A practical, collaborative approach that balances security, user experience, operational needs and organisational risk.

Knowledge and experience

- Demonstrated experience implementing, assessing and continuously improving organisational cyber security controls, including reviewing the work of technical teams and service providers.
- Strong knowledge of the Essential Eight and the ability to support organisational adoption of the ASD Essentials framework.
- Working knowledge of the Australian Government Information Security Manual and its application in a risk-based control environment.
- Strong experience in a Microsoft 365-based operating environment, including Microsoft Entra ID, Intune, Defender, Purview, Sentinel and Azure security capabilities.
- Demonstrated experience with identity and access management, conditional access, centralised security monitoring, logging, vulnerability management, incident response and cloud security.
- Experience managing system security authorisation, control catalogues, compliance evidence, security assessments, documentation of risk acceptance and remediation tracking.
- Knowledge of emerging cyber security risks and technologies.
- Experience preparing cyber security analysis, risk advice and supporting material for senior executive and governance reporting.

Highly Desirable

- Experience working in, or with, an Australian Government entity is highly desirable, including familiarity with the Protective Security Policy Framework and government assurance expectations.
- Experience working with a managed cyber security service provider, including reviewing service outputs and coordinating incident escalation, follow-up actions and improvements.

Qualifications

- Relevant tertiary qualifications in cyber security, information technology, risk or a related discipline, or equivalent demonstrated professional experience.
- Relevant industry certifications such as CISSP, CISM, CRISC, CCSP, Microsoft security certifications or equivalent are desirable.

Eligibility/Other requirements

- The successful candidate must be an Australian citizen and will be required to undergo pre-employment screening, including a National Police History Check, Anti-Money Laundering and Counter-Terrorism Financing checks, and more.
- The successful candidate must hold, or be able to obtain and maintain, a Baseline Australian Government security clearance.
- Occasional travel to RIC office or other locations may be required.

I acknowledge that I have read and understood the duties, responsibilities and delegations of the position as outlined in the above Position Description.

Name:	**Signature:**	**Date:**
Click or tap here to enter text.		Click or tap to enter a date.