readytech

POSITION DESCRIPTION

Cyber Security GRC Analyst

ReadyTech (ASX:RDY) exists to help communities thrive, and ReadyTechers flourish on making that change happen.

They enjoy taking on challenges that matter to our customers, communities, and the world – and working to solve them with incredible technology that helps navigate complexity, while also delivering meaningful outcomes.

ReadyTechers are enterprising, and hungry to make a difference. But, more than ever, ReadyTechers are *ready for anything.*

POSITION DESCRIPTION

Title	Cyber Security GRC Team Analyst	**Location**	TBC
Report to	Head of Security Operations/Cyber Security GRC Leader	**Direct report(s)**	

The purpose of this role

The Cyber Security GRC Analyst ensures that ReadyTech's information security governance, risk, and compliance (GRC) frameworks are effectively implemented, maintained, and continuously improved to support ongoing compliance with the Australian Government Information Security Manual (ISM), SOC 2, and other relevant frameworks such as ISO 27001, CIS Controls, and NIST.

This role supports the Head of Security Operations/Cyber Security GRC Leader by managing compliance activities, coordinating audits and assessments, and ensuring the organization maintains a strong, risk-aware, and compliant security posture.

The key accountabilities of the role

- Lead the implementation and continuous improvement of ReadyTech's cyber security GRC framework aligned with IRAP, SOC 2, and ISO 27001 standards.
- Coordinate and manage external audits and assessments, ensuring audit readiness, evidence collection, and timely remediation of findings.
- Maintain and oversee the cyber risk register, including risk identification, analysis, treatment, and ongoing monitoring.
- Develop, update, and maintain information security policies, procedures, standards, and guidelines that reflect compliance requirements under IRAP, ISM, SOC 2, and related frameworks.
- Report and communicate cyber performance, compliance status, and risk indicators to executive and governance forums.
- Support the integration of compliance controls into IT and cloud environments to ensure secure-by-design operations.
- Promote a strong security and compliance culture through collaboration, education, and awareness initiatives across the business.

The key responsibilities of the role

Governance & Policy

- Develop, maintain, and align ReadyTech's information security policies and control library with ISM, IRAP, SOC 2, ISO 27001, and NIST frameworks.

- Map control requirements across frameworks to reduce duplication and simplify compliance activities.
- Ensure all policies and standards are reviewed, approved, and communicated to relevant stakeholders.

Risk & Compliance Management

- Manage the cyber risk management process, including assessment, documentation, and reporting of risks.
- Lead compliance activities to maintain certification and attestation under IRAP and SOC 2.
- Support the creation and maintenance of System Security Plans (SSP), Security Plans and Risk Registers, and Plans of Action and Milestones (POA&M) for IRAP.
- Manage vendor and third-party risk assessment programs to ensure compliance with regulatory and contractual obligations.

Audit & Assurance

- Coordinate and facilitate IRAP, ISO assessments and SOC 2 audits, including evidence collection, gap analysis, remediation tracking, and reporting.
- Maintain detailed audit logs and assurance documentation to support external review and internal reporting.
- Conduct internal control testing and assurance reviews to assess compliance effectiveness and identify improvement opportunities.

Awareness & Culture

- Champion a strong security and compliance culture across ReadyTech.
- Deliver targeted training and communication to increase awareness of regulatory and framework requirements.
- Support teams in embedding compliance controls within business processes, development pipelines, and infrastructure management.

The ideal candidate will have these:

1. Skills	- Strong analytical, communication, and presentation skills. - Ability to translate technical risks and controls into business-relevant language. - Exceptional organizational and time management skills with a focus on meeting compliance deadlines. - Demonstrated initiative, accountability, and stakeholder management across technical and non-technical teams.
2. Knowledge	- Deep understanding of security and risk frameworks, including: - IRAP, ASD ISM, and PSPF - SOC 2 Trust Services Criteria - ISO 27001/27002, NIST CSF, and ITIL

	- Familiarity with GRC tools and platforms. - Understanding of cloud and SaaS architectures, especially within Microsoft Azure environments. - Awareness of relevant data privacy and protection regulations
3. Experience	- Minimum 4+ years in information security, with 2+ years in a GRC, compliance, or audit coordination role. - Demonstrated experience coordinating external audits or assessments (IRAP, SOC 2, ISO 27001, or FedRAMP). - Proven experience in managing audit evidence, remediation, and control effectiveness testing. - Background in systems administration or cloud infrastructure preferred, to bridge operational and compliance considerations. - Experience developing and maintaining documentation such as SSPs, POA&Ms, and audit reports.
4. Performance Indicators	- Successful completion and maintenance of IRAP and SOC 2 compliance with minimal findings. - On-time completion of audit and assessment milestones. - Measurable improvement in compliance maturity and risk reduction. - Effective communication of compliance and risk status to executive leadership. - Increased staff awareness and adherence to compliance obligations.