CriticalArc Pty Ltd
t: +61 1300 13 53 40
e: contact@criticalarc.com
w: www.criticalarc.com

Job Title: **Information Security Compliance Manager**
Location: **Sutherland, NSW**
Reporting To: **Chief Information Officer**

CriticalArc is a rapidly growing SaaS firm that makes a real difference in the world.

We help keep vulnerable people safe with our SafeZone™ solution - a unified safety, security, and emergency management solution that provides Safety Everywhere™ for an organization's people, wherever they have a duty of care.

SafeZone™ is transforming how leading organizations manage the safety of millions of people every day

We're growing our team in Australia and are looking for someone passionate about compliance, process, risk and security that has diligence and is keen to help us enrich our security posture.

As an **Information Security Compliance Manager**, you will be responsible for working with, supporting, implementing and monitoring our cybersecurity and compliance programs to protect the confidentiality, integrity and availability of data. You will have a passion for pragmatic process, have an eye for detail and exercise patient commitment to ensuring process is followed where required, adapted where necessary and enshrined in policy where prudent.

Responsibilities

1. Information Security Management

- Maintain and ensure continual implementation of information security policies, standards, and procedures.
- Manage information security risk assessments and identify mitigation strategies.
- Conduct internal information security audits and system/vendor privacy audits and ensure ongoing compliance.
- Oversee the upkeep of the Information Security Management System (ISMS).
- Facilitate internal reviews of ISMS artifacts
- Conduct regular Information Security management reviews with senior management

2. Compliance and Regulatory Adherence

- Ensure day-to-day compliance with our current infosec regulations and standards, including ISO27001, SOC-2, CyberEssentials and GDPR
- Work with the CIO to stay updated on regulatory landscape, develop and deliver on a compliance roadmap, including playing a leading role in achieving certification to additional international and jurisdictional standards as the business matures
- Lead or support external audits and security assessments to maintain certifications and accreditations.
- Conduct internal audits on an annual basis, document and follow up on non-conformance

CriticalArc Pty Ltd
t: +61 1300 13 53 40
e: contact@criticalarc.com
w: www.criticalarc.com

3. Privacy and Data Protection

- Take on the role of Data Protection Officer (DPO), ensuring adherence to data privacy laws.
- Manage data privacy practices, including data protection impact assessments, data subject rights, and data retention policies.
- Oversee data breach response and reporting processes in alignment with legal requirements.
- Oversee allocation of business system compliance ownership, and ensure regular access control reviews are carried out

4. Risk Management and Incident Response

- Maintain our risk management program to assess, identify, and address security risks.
- Work with risk owners to ensure regular review of risks and associated controls
- Maintain and evolve incident response plans and lead response efforts for any security incidents.
- Conduct security incident post-mortems and update policies and procedures based on findings.

5. Security Training and Awareness

- Take ownership of the security awareness training programme for staff members.
- Ensure that security best practices and related policies are understood and followed throughout the organization.
- Communicate updates and reinforce a security-first culture across the business.

6. Third-Party Security and Vendor Risk Management

- Assess the security posture of third-party vendors and partners.
- Assist with responses on security-related sections of RFPs and tenders.
- Oversee security requirements in contracts and manage vendor-related security risks.

7. Reporting and Collaboration

- Report regularly on security and compliance status to the leadership team and provide recommendations for improvements
- Assist with preparation of related areas of board reporting where required
- Collaborate with Operations, HR, engineering, legal, and other teams on security initiatives.

Requirements

To be considered for this role you must be an Australian citizen or Permanent Resident, New Zealand citizen with the right to work in Australia. Offers will be subject to a police clearance and background check.

The successful candidate must:

- have the ability to self-motivate, work autonomously, take ownership of initiatives.
- be outcome oriented and think strategically
- show a high level of attention to detail and follow through
- have highly developed oral and written English communication skills.

CriticalArc Pty Ltd
t: +61 1300 13 53 40
e: contact@criticalarc.com
w: www.criticalarc.com

- excellent analytical and problem-solving skills, with the ability to handle and prioritise multiple tasks and projects.

Otherwise, there are no other specific mandatory requirements or experience for this role. However, the following attributes will be highly regarded:

- Relevant qualifications and/or experience in information technology, project management, assurance/audit, governance, compliance, risk, information security management systems or cyber security.
- Knowledge and/or experience of information security frameworks and legislation such as ISO 27001, SOC-2, Essential Eight, FedRamp.
- Experience and skills in effecting incremental change and continuous improvement in an organisation.
- Capable of working effectively with cross-functional teams and explaining complex concepts to non-technical stakeholders.
- Experience in developing, maintaining and applying governance, compliance and risk management frameworks, methodologies and guidelines to ensure robust compliance on a day to day basis.
- Demonstrated skills in the review and continuous improvement of an enterprise management system such as a Quality Management System (QMS) or Information Security Management System (ISMS).

Working Environment

- Role based in Sutherland. Easy train access from eastern suburbs, CBD and south coast without a change and street parking nearby.
- Opportunity to work from home a few days per week
- A competitive remuneration package
- Highly supportive senior leadership and team environment
- A chance to be a part of a fast-growing company that makes a meaningful difference in the world

We are committed to providing a working environment that embraces and values diversity, equity and inclusion. We encourage candidates to speak with a member of our team if you require adjustments to our recruitment process to support you, and the type of working arrangements that would help you thrive.