Australian Red Cross
THE POWER OF HUMANITY

POSITION DESCRIPTION – TEAM MEMBER

Position Title	Information Security Governance Specialist	Department	Information Technology
Location	Melbourne\ Sydney	Direct/Indirect Reports	Nil
Reports to	Information Security Manager	Date Revised	October 2019
Industrial Instrument	Social Home Care and Disability Services Award		
Job Grade	Job Grade 6	Job Evaluation No:	HRC0009013

■ Position Summary

The Information Security Governance Specialist assists the Information Security Manager assess and evaluate business data/ information risks, relevant data protection and privacy regulations as well as applicable industry standards such as Payment Card Industry Data Security Standards (PCI DSS) and ISO 27001/ ISO27002 leading practices. The Information Security Governance Specialist will assist in formulating, implementing and maintaining data/ information security governance frameworks, policies, processes and practices across the organization. Working closely with the respective business management/ information owners, the Information Security Governance Specialist will coordinate organization-wide data/ information security governance, cybersecurity risk reduction and security uplift activities.

The Information Security Governance Specialist will also assist in identifying and managing third-party related risks, following-up on risk mitigation actions with relevant internal and external stakeholders as well as maintaining up-to-date records of third-party related risks. The Information Security Governance Specialist will also coordinate PCI DSS and ISO27001 implementation and compliance activities across the organization, maintaining up-to-date records and documentation to support compliance.

■ Position Responsibilities

Key Responsibilities

Strategy & Planning

- Establish, build and maintain strong relationships with business unit management
- Work closely with business management to
    - assess data privacy and protection regulations/ requirements applicable to respective business units, operations and activities
    - assess data/ information security governance requirements applicable to third-parties and third-party services
    - perform data/ information security risk assessments covering business units, operations and activities
    - assess data/ information security governance requirements applicable to respective business units, operations and activities
    - formulate data/ information security risk reduction actions plans and coordinate/ follow up, track and report on progress
- Formulate and maintain data/ information security governance frameworks, policies, processes and practices aligned with applicable data protection and data privacy regulations, contractual obligations,

Payment Card Industry Data Security Standard and ISO 27001/ ISO 27002 leading practices.

- Communicate data/ information security governance priorities across the organization and plan, coordinate, monitor, report and advise on the status of key priorities

Acquisition & Deployment

- Coordinate, implement and maintain tools, processes and practices to support the effective implementation, operation and continual improvement of the Information Security Management System (ISMS) across the organization, embedding data protection and data privacy regulations, contractual obligations, Payment Card Industry Data Security Standard and ISO 27001/ ISO 27002 leading practices
- Establish, implement and maintain effective tools, processes and practices to support Incident and Problem management
- Establish, implement and maintain effective tools, processes and practices to enhance data/ information security awareness across the organization
- Maintain up-to-date knowledge of relevant government and state regulation as well as the nature and type of business operations to enable effective assessment of data/ information security risks
- Maintain up-to-date knowledge of latest cybersecurity threats, necessary controls/ countermeasures and security best practices.

Operational Management

- Coordinate and conduct workshops/ discussions to identify data/ information risks and governance requirements and to arrive at business aligned solutions
- Maintain up-to-date business data/ information risk registers (legal/ regulatory requirements, systems/ information ownership, user access matrices, awareness training, suppliers/ third parties, supplier security assessments, PCI DSS compliance, risks/ corrective actions, security exceptions, etc.)
- Formulate and maintain up-to-date information stores, user guides and advisories to assist business managers/ information owners effectively manage data/ information security risks
- Coordinate, facilitate and/ or conduct information security and PCI DSS awareness and training
- Coordinate necessary business legal and regulatory compliance assessments in relation to data/ information governance and security.

■ Position Selection Criteria

Technical Competencies

- Five years' experience covering business analysis, information security and project management
- Excellent communication and interpersonal/ relationship management skills
- Good analytical, problem solving, organization and project management skills
- Experience in assessing and managing business process, supplier, system, IT and project risks
- Experience in ISO27001/ ISO27002 and other information security risk management frameworks
- Experience in facilitating workshops and focussed business meetings to achieve consensuses
- Good understanding of data protection and privacy regulations
- Good understanding of PCI DSS requirements, payment touch-points and related business process
- Good understanding of data/ information security governance leading practices.

Qualifications/Licenses

- Degree qualified or significant experience in Information Security, Business Analysis or Project Management
- Significant experience in managing/ coordinating business focussed data/ information security governance projects

- Experience in conducting data/ information security governance workshops and user awareness sessions
- One or more IT/ information security certifications will be considered an added advantage (PMP – Project Management Professional, CISSP – Certified Information Systems Security Professional, CISM – Certified Information Security Manager, CISA –Certified Information Systems Auditor, ISO27001 Lead Auditor/ Lead Implementer).

Behavioural Capabilities

- **Personal effectiveness | Achieve results |** Demonstrated ability to manage work and achieve the results committed to. Ability to evaluate progress and make adjustments needed to achieve goals. Accept responsibility for mistakes and learn from them.
- **Personal effectiveness | Solving problems |** Demonstrated ability to identify situations or issues, consider options and develop solutions. Ability to communicate any problems, implement solutions and monitor appropriate actions.
- **Team effectiveness | Collaborating |** Demonstrated capability to work with others to reach common goals, sharing information, supporting and building positive and constructive relationships.
- **Organisational effectiveness | Innovating and improving |** Demonstrated ability to identify and raise issues regarding ineffective work processes and take initiative to make improvements.
- **Organisational effectiveness |Managing risk |** Demonstrated ability to work within guidelines, policies and procedures. Awareness of risks involved in an individual's role and works toward minimising their impact.

■ General Conditions

All Red Cross staff and volunteers are required to:

- Adhere to the 7 fundamental principles of Red Cross:

  Humanity | Impartiality | Neutrality | Independence | Voluntary Service | Unity | Universality
- Act at all times in accordance with the Australian Red Cross Ethical Framework and Child Protection Code of Conduct
- Demonstrate skill, knowledge and behaviour to work with Aboriginal and Torres Strait Islander people in a culturally respectful way
- Comply with the Work Health and Safety management system
- Undertake a police check prior to commencement and every 3 years thereafter. Police check renewals may be required earlier than 3 years in order to comply with specific contractual or legislative requirements
- Support a child safe organisation by undertaking screening for suitability to work with children, youth and vulnerable people and to comply with relevant state/territory legislative requirements
- Assist the organisation on occasion, in times of national, state or local emergencies or major disasters