Australian Red Cross
THE POWER OF HUMANITY

POSITION DESCRIPTION – MANAGER

Position Title	Information Security Manager	Department	Information Technology
Location	Sydney	Direct/Indirect Reports	0/5
Reports to	Architecture and Planning Manager	Date Revised	January 2015
Budget			

■ Position Level Descriptor

An individual at the Manager level is responsible for some or all of the following: financial, functional, thought or change leadership outcomes. Individuals at a Manager level lead and implement strategies and plans to achieve organizational objectives. The Manager level leads specialist (functional or knowledge areas) or complex, or multi-disciplinary teams. An individual at the Manager level typically reports to an individual at the Executive level.

■ Position Summary

Reporting to the CIO, the Information Security Manager is responsible for assessing and managing all aspects of risk brought to bear on the organisation by IT security and legislative/regulatory compliance issues. The scope of the role includes the management of risks as it manifests in the areas of technology, operations and strategy. Achievement of balance between information security concerns and compliance mandates is a primary objective of this role.

The Information Security Manager will underpin the Business teams, IT Security team and IT Operations teams through a deep knowledge of security practices and the systems the support them. They proactively manage organisational risks through the analysis of internal (systems, process and people) and external environments.
The Information Security Manager will establish an enterprise security stance through policy, architecture, incident management and education processes. The IT security Manager is expected to interface with peers in the Application and Infrastructure departments as well as the leaders of the organisational units to both share the organisational security vision and solicit their involvement in achieving higher levels of enterprise security.

■ Position Responsibilities

Key Responsibilities

- Act a trusted advisor to the organisation on all information security related matters whilst actively educating the organisation.
- Increase the maturity of the organisation when assessed against ISO27001. This to include improvements to vulnerability management etc.
- Complete 3rd Party Security Assessments and ensure that the 3rd party registers are maintained.
- Own, implement and manage the Incident Response process for all Cyber Security incidents.
- Develop business cases to drive the ongoing investment in IT Security.
- Create and maintain the enterprise's security architecture design including defining compliance goals and objectives.
- Establishing guiding principles for flexible, yet holistic security and compliance management.

- Create and maintain security awareness training program working closely with the Information Security business lead for the organisation
- Create and maintain the Red Cross security documents (policies, standards, baselines, guidelines and procedures).
- Creation and maintenance of the IT Risk Register that feeds into the Red Cross Risk Register in order to advise the National Leadership team on critical IT Security risks including communicating strategies for risk mitigation and remediation projects.
- Review proposed projects to identify potential risk and advise of mitigation strategies
- Classify and valuate enterprise data assets
- Maintain up-to-date knowledge of the IT security industry including awareness of new or revised security solutions, improved security processes and the development of new attacks and threat vectors.
- Propose additional security solutions or enhancements to existing security solutions to improve overall enterprise security as per the enterprise's existing procurement processes.
- Assess all IT purchases to ensure they support security and compliance mandates.
- Oversee the deployment, integration and initial configuration of all new security solutions and of any enhancements to existing security solutions in accordance with standard best operating procedures generically and the enterprise's security documents specifically.
- Working with the organisation to define and enforce security and compliance polices and standards
- Conduct all investigations into problematic activity and provide on-going communication with senior management.
- Oversee automation of internal controls and centralise logging and reporting
- Manage securing of all platforms and centralise security event management
- Guide regular security awareness training for all employees to ensure consistently high levels of compliance with enterprise security documents.

■ Position Selection Criteria

Technical Competencies

- Must be a dynamic and self-starting individual who is able to work independently or as part of a team with minimal guidance and direction
- Demonstrated ability to focus IT Security efforts where it will provide the greatest business value.
- A deep knowledge of real world issues that have impacted organisations, understanding why and how they could have been prevented.
- Demonstrated experience in the development of Information Security Businesses cases.
- Development of Incident Response processes and embedding them within the organisation.
- Demonstrated experience in Information Security Management, working with business users, technical teams and 3rd party vendors
- Extensive experience in enterprise security architecture design.
- Extensive experience in enterprise security documentation and policy creation, education and enforcement.
- Experience in designing and delivering employee security awareness training.
- Extensive working knowledge of the following technologies in a windows operating environment;
    - Server and storage platforms
    - Virtualisation
    - Networks and edge devices
    - Messaging environments

- Desktop platforms (Citrix an advantage) and mobile computing environments
- Directory services and access control
- Anti-virus and Malware systems
- Penetration testing tools
- Data Loss Prevention tools.
- Security Information and Event Management.
- Mobile Device Management tools.

- Good working knowledge of ERP, CRM, Web, Enterprise Message Bus, Payment Gateways and other enterprise wide applications:
- Ability to conduct research into IT security issues and products as required.
- Ability to solve problems in a complex environment
- Proven ability to operate effectively in a geographically diverse and multi-faceted environment
- Demonstrated desire to work as part of a high performing team
- Demonstrated vendor relationship management experience
- Highly developed facilitation, negotiation and influencing skills
- Demonstrated ability to apply technology solutions in solving business problems
- Excellent understanding of business complexity and project interdependencies
- Effective communication skills across both technical and non-technical users levels of an organization
- Demonstrates interpersonal skills required to successfully work in a team environment and communicates effectively across a variety of stakeholder groups
- Must be able to continuously learn new skills to keep abreast of industry trends and state of the art technology
- Ability to identify opportunities and transform them into quantifiable and achievable initiatives
- Must demonstrate a commitment to continuous learning and mentoring

Qualifications/Licenses

- Demonstrable experience in IT Security roles.
- Relevant tertiary qualifications, skills and experience in Information Security Management such as:
  - ISACA Certified Information Security Manager
  - ISO/IEC 27001 Certification
  - Qualified Security Assessor
- Current Industry accreditation in COBIT an advantage
- Extensive experience in security analysis, auditing and management frameworks.

Behavioural Capabilities

- **THINK | Investigate, Analyse and Make Decisions | Seeks information and analyses evidence and data to make decisions**

  Regularly monitors and scans the environment for issues which impact the functioning of their department | Creates systems for ensuring the successful cataloguing of information useful to the organisation | Takes calculated risks on the basis of analysis | Applies business rigour to inform situational problem solving and decision making
- **THINK | Organisational Understanding and Compliance | Demonstrates understanding of Red Cross, its broader environment and complies with organisational procedures and guidelines**

Obtains the best result by using knowledge of Red Cross, the sector and the broader environment | Creates and maintains systems for ensuring the successful cataloguing of information for the organisation | Keeps up-to-date with broader sector factors, which may have an impact on the organisation | Understands the viewpoints and activities of other departments within the organisation and relates this work to own department's work | Operates within legal and organisational policy and procedural boundaries

- **ACHIEVE | Change, Adapt and Innovate | Improves processes or programs through demonstrating flexibility and innovation**

  Understands and applies principles of organisational change | Drives processes to facilitate greater engagement with change initiatives | Allocates resources required to implement change | Develops risk mitigation strategies in relation to change initiatives | Ensures the structures and timely implementation of departmental work-plans | Questions traditional assumptions | Ensure availability of critical resources

- **LEAD | Being Strategic | Identifies optimum strategic responses in a changing environment**
  Communicates and provides context for strategies to engage Red Cross stakeholders | Translates Red Cross strategy and Fundamental Principles into operational activity | Demonstrates how the strategy and Fundamental Principles provide a framework to inform decision making and action | Provides opportunities for individuals and groups to understand their contribution to the strategy | Sets standards, goals and expectations for the teams | Ensures staff roles are clear and what's expected of each individual | Recognises positive performance and contributions of team members

- **COLLABORATE | Engage and Influence others | Demonstrates appropriate engaging and influencing skills aligned with Red Cross objectives**

  Builds wide and effective networks of contacts inside and outside the organisation | Partners with other agencies to support Red Cross initiatives | Implements strategy to influence and engage others | Utilises a wide-range of influencing techniques | Identifies and constructively resolves conflict within teams

- **COLLABORATE | Share Information and Communicate Effectively | Shares information consistently and transparently**

  Creates systems to ensure sharing of information | Provides opportunities for others to express their point of view | Takes into account others motivations, issues and concerns when planning communications | Provides mechanisms and opportunities to harvest information from internal and external stakeholders

■ 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 Code of Conduct
- Comply with the Work Health and Safety management system
- Undertake a police check prior to commencement and every 3 years thereafter
- 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