

Position Description

| | |
|------------------------|---|
| Title | Security Compliance Analyst |
| Business Unit | Information Security Corporate & Finance Services |
| Location | 130 Lonsdale Street, Melbourne |
| Employment type | Full time Ongoing |
| Reports to | Security Manager |

About Uniting

Uniting Vic.Tas is the community services organisation of the Uniting Church. We've been supporting people and families for over 100 years. We work alongside people of all ages in local communities in Victoria and Tasmania. Our services reach to Albury-Wodonga in the north, Mallacoota in East Gippsland, the Wimmera region in the west, and across Tasmania.

We empower children, young people and families to learn and thrive. We're there for people experiencing homelessness, drug and alcohol addiction or mental illness. We support people with disability to live the life they choose. We assist older people to maintain their independence and enjoy life. We provide opportunities to access training and meaningful employment. We're proud to welcome and support asylum seekers to our community. We work to empower people with the information, skills and tools they need to live a healthy, happy life.

As an organisation, we work in solidarity with Aboriginal and Torres Strait Islander people as Australia's First Peoples and as the traditional owners and custodians of this land.

We celebrate diversity and value the lived experience of people of every ethnicity, faith, age, disability, culture, language, gender identity, sex and sexual orientation. We welcome lesbian, gay, bisexual, transgender, gender diverse and non-binary, intersex, and queer (LGBTIQ+) people at our services. We pledge to provide inclusive and non-discriminatory services.

Our purpose: To inspire people, enliven communities and confront injustice

Our values: We are imaginative, respectful, compassionate and bold

1. Position purpose

This position works closely with the Security Manager to ensure the maintenance of the various security standards that Uniting is required to adhere to, maintain various relevant certifications and meet growing external compliance requirements with our key partners in private industry and government. Failure to meet and maintain these standards has a potential direct cost impact in that Uniting could lose funding and/or increase the risk of a breach of privacy or the probability of a serious cyber event.

2. Scope

Budget: nil
People: nil

3. Relationships

Internal

- ICT team/s
- ICT management team
- Business Units delivering services requiring Security compliance certification.

Form: PAC005 Position Description
Date approved: 24 February 2021

Area: People and Culture
Next review date: 1 February 2022

Version: 3.0
Page | 1

Position Description

Security Compliance Analyst

External

- Vendors and partners
- Service providers hosting systems that are subject to external compliance.

4. Key responsibility areas

Security Standards Maintenance

- Coordinate the development, support, and maintenance of Uniting's Security Standards framework as it applies to internal systems within Uniting Vic Tas, sufficient to meet the business, access and security needs of a digital organization.
- Standards to be maintained:
 - ISO 27001 – (2013)
 - Right Fit for Risk – Department of Employment and Workplace Relations (DEWR)
 - Other standards as required.
- Ensure all supporting documentation is up to date and reviewed either once per year or as per required by the Standards and as per Uniting policy.
- Ensure documentation is distributed and acknowledged by the relevant stakeholders within Uniting.
- Co-ordinate and lead any internal or external audit activity within the timeframes required by the relevant standards. Annually this includes at least 1 internal ISO27001 audit, RFFR self-assessment against the current SOA (and ISMS), and annual external ISO27001 audit.
- Review the changes to ACSC ISMS as they are released on a 3 monthly basis and assess the implications to Uniting's compliance with ISO27001 and RFFR.
- Ensure any mandatory or regular security training is updated into stay relevant and that specialized training (i.e. Privileged access management) is completed and recorded.
- Update and maintain supporting processes.

External Compliance responsibility

- Manage the timely response to external requests for evidence of security compliance leveraging information and compliance with relevant security standards.
- Raise annual security compliance questionnaires with external suppliers where Uniting has a contractual right to audit.
- Maintain a register of inbound and outbound compliance requests and responses.
- Where non compliances are identified raise the appropriate non-compliance report and work with impacted party on a remediation plan.
- Where non-compliance cannot be remediated, a risk assessment must be completed and the appropriate risk raised.

Personal accountability

- Compliance with Uniting's values, code of conduct, policies and procedures and relevant government legislation and standards where relevant.
- Cooperate with strategies to actively ensure the safety, protection and well-being of children who come into association with us.
- Ensure appropriate use of resources.
- Work collaboratively with Uniting (Victoria Tasmania) employees and external stakeholders in accordance with Uniting's values and professional standards of behaviour.
- Actively participate in initiatives to maintain, build upon and promote a positive and collaborative workplace.
- Identify opportunities to integrate and work collaboratively across teams.
- Take reasonable care for your own health and safety, and health and safety of others (to the extent required).
- Promote a positive safety culture by contributing to health and safety consultation and communication.
- Promptly respond to and report health and safety hazards, incidents and near misses to line management

Position Description Security Compliance Analyst

- Attend mandatory training sessions (i.e. equal employment opportunity, health, and safety) and mandatory training specific to position.
- Declare anything that you become aware of through the course of your engagement which may impede your suitability to work with children and/or young people.
- Declare any potential or actual conflict of interest that you become aware of through the course of your engagement:
 - Based on a relationship with a current member of Uniting's workforce
 - Based on my ongoing work with another organisation

5. Performance indicators

- These will be developed with the successful candidate based on experience in the role.

6. Person specification

Qualifications

- Graduate level Tertiary qualification in Cyber Security (either undergraduate or master's level)
- Related security certifications (SO -27001 audit – would be an advantage.

Experience

- Strong understanding and education in ISO27001 framework, including leading and maintaining ISO27001 certification.
- Knowledge and understanding of the Department of Workplace Relations (DEWR) Right Fit for Risk (RFFR) framework would be an advantage.
- Strong Understanding of the Australian Cyber Security Centre (ACSC) – Information Security Manual (ISM) and its applicability to ISO27001 and RFFR.
- Understanding of the security management and controls of cloud environments including IaaS, PaaS and SaaS, particularly within Microsoft Azure.
- Understanding of the process of issuing compliance validation questionnaires with external vendors in terms of security compliance

Core selection criteria

- **Values alignment:** ability to demonstrate and authentically promote Uniting's values.
- Demonstrated ability to provide safe environments for children and young people and protect them from abuse and neglect.
- Demonstrated knowledge and skills in the methods, frameworks, practices, standards and governance for the planning, management, and delivery of systems administration services in a complex service environment.
- Strong understanding and education in the development, implementation and management of security controls within a Data Centre processing and storage facilities supporting enterprise-wide services using best practice strategies.
- Demonstrated ability to undertake security controls compliance reviews and security control capacity planning and performance monitoring to ensure continuous improvement based on evidence and reported outcomes.
- Ability to work with vendors and service providers to ensure that the Uniting required outcomes are achieved
- Ability to identify, assess and escalate risks according to the Risk Management framework.
- Proven negotiation skills and the ability to provide and influence a change agenda to a range of stakeholders, including suppliers, staff, and senior management.

Commented [RP1]: Would a Grad be able to do this?

Commented [AS2R1]: Modified scope

Position Description
Security Compliance Analyst



7. We are a child safe organisation

Uniting is a child safe organisation and is committed in everyday practice to ensure the safety and wellbeing of all children, at all times. As a child safe organisation, employment with Uniting is subject to a satisfactory national (and international where relevant) police check and relevant Working With Children Check (and NDIS Worker Screening Check where relevant) to your State prior to commencement of any paid or unpaid work and/or participation in any service or undertaking. It is a condition of employment that all eligible workforce receive the COVID-19 vaccination and supporting evidence may be requested in order to perform duties at any of Uniting's workplaces.

This position description is subject to review and may change in accordance with Uniting's operational, service and consumer requirements.

8. Acknowledgement

I have read, understood, and accepted the above Position Description

Employee

Name:

Signature:

Date: