Cybersecurity Assessor

Position Description

Entity:	Recruiting State
Reports to:	Administratively to Head of IT in recruiting state, Functionally to National Technology Group
Direct reports:	NIL
Location:	Flexible within any of the Society's main metropolitan or regional offices on the eastern seaboard. Possible interstate travels.
Primary position objective:	To provide the Society's management with an assessment of the effectiveness of both the ASD Essential Eight and the NIST cyber security Identify, Protect, Detect, Respond, and Recover processes and activities. The assessment covers sub-processes such as asset management, cyber security awareness training, data security and governance, resource planning, recovery planning and communications.

The St Vincent de Paul Society is an Equal Employment Opportunity Employer

St Vincent de Paul Society

The St Vincent de Paul Society is a member and volunteer-based organisation that has been assisting people experiencing disadvantage for more than 130 years.

The Society was founded by a 20-year-old man named Frederic Ozanam in 1833, who with a group of friends, wanted to make a difference to the poverty and disadvantage that he saw around him in post-Revolution France. Leading by example and with boundless energy, Frederic started what is now a world-wide movement in just 20 short years. The St Vincent de Paul Society has around 61,000 members and volunteers and 3000 staff. Our local member networks, referred to as Conferences, are present in over 1126 communities across Australia.

Our members and volunteers provide assistance to people experiencing disadvantage including food parcels and vouchers, financial assistance, assistance with energy bills and other debt, budget counselling and the provision of other material items such as furniture, clothing and bedding and any other household items. Importantly, our members also provide vital emotional support and referral services as needed.

The St Vincent de Paul Society is a leading provider of community support services and has close to 100 Special Works across the State in the areas of homelessness, mental health, disability, financial counselling, supported accommodation, food provision, refugees and migrants and addiction counselling.

Our Vision

The Society aspires to be recognised as a caring Catholic charity offering 'a hand up' to people in need. We do this by respecting their dignity, sharing our hope and encouraging them to take control of their own destiny.

Our Mission

The St Vincent de Paul Society (the Society) is a lay Catholic organisation that aspires to live the gospel message by serving Christ in the poor with love, respect, justice, hope and joy, and by working to shape a more just and compassionate society.

Our Values

- Commitment: Loyalty in service to our mission, vision and values
- Compassion: Welcoming and serving all with understanding and without judgement
- Respect: Service to all regardless of creed, ethnic or social background, health, gender, or political opinions
- Integrity: Promoting, maintaining and adhering to our mission, vision and values
- Empathy: Establishing relationships based on respect, trust, friendship and perception
- Advocacy: Working to transform the causes of poverty and challenging the causes of human injustice
- Courage: Encouraging spiritual growth, welcoming innovation and giving hope for the future

ROLE OVERVIEW

The role of Cyber Security Assessor will drive the cyber security assessment for all Vinnies states through a range of activities including, but not limited to:

- Plan and conduct NIST and ASD Essential Eight security assessment across all the Society jurisdictions.
- Proactively and productively engage with the members of the National Technology Group to arrange, coordinate and conduct the assessments.
- Travel to each of the Vinnies states to undertake targeted reviews of controls in each state to do the assessment.
- Undertake interviews across Teams and Zoom video conferencing with a sample set of sites in each state to augment physical site visits.
- Verify that application software/network/system security postures are implemented as stated, document deviations, and recommend required actions to correct those deviations.
- Perform security reviews, identify gaps in security architecture and develop a security risk management plan.
- Perform risk analysis (i.e., threat, vulnerability, and probability of occurrence)
- Evaluate IS threats and vulnerabilities to determine whether additional safeguards are required.
- Identify opportunities to improve processes and services of risk management.
- Analyse organisational cyber security issues including gaps in governance, risk, audit and compliance strategies and practices and develop solutions to ensure business, statutory and legislative obligations and standards are met and the organisation is positioned to effectively respond to incidents.
- Provide advice on mitigative controls and relevant technical strategies, policies, standards and practices and the correct application of such advice.

- Document all findings, risk assessments and proposed mitigative controls and initiatives in a report to be reviewed by the National Technology Group and escalated up through the relevant executive groups within the Society.
- Contribute to a safe working environment for members, staff and volunteers by implementing the Society's workplace health and safety practices.

Critical Key Performance Indicators (KPIs)

- Deliver the Security Assessment Report with comprehensive findings and clear recommendations for each jurisdiction within the allocated time.
- Progress and governance reports during assessment.
- High-level problem-solving skills and sound judgment
- Adhere to all relevant employment legislation as dictated by state and federal legislation inclusive of WHS Act 2011 and its regulations.

Key working relationships

- Reports to Members of the National Technology Group (NTG).
- Engage with Various state-based managers and users proposed by the members of the NTG for each state.
- Adapts to changing environments and demands.
- Manages confidential information and demonstrates capacity to maintain confidentiality and professional standards of behavior in difficult and sensitive circumstances
- A proactive, collaborative mindset and demonstrated capacity to work independently and within a team environment.
- Vendors and third parties.

Essential criteria

- Tertiary qualification/s in Information Technology, Computer Science or related field or Bachelor of Cyber Security and Criminology;
- Certified Information Systems Security Professional (CISSP)
- Other relevant certifications / qualifications for example, Security+ and other vendor related security certifications.
- Proven experience in conducting information technology compliance assessments across the NIST Cybersecurity Framework (CSF) v1.1, the ASD Essential Eight and the Essential Eight Maturity Model.
- Good working knowledge of current cyber risks and trends
- In-depth knowledge and experience of next-gen technical architectures, cloud infrastructures, networking infrastructures, evolving business practices, development practices, finding innovative ways to enable secure business practices and strong risk management skills
- Zero-trust architecture and identity management experience required.
- Ability to examine, interpret, document and evaluate security strategies and defences to determine security and business impacts
- Familiarity with Risk Management; with cyber threat hunting and vulnerability management
- Strong organizational, administrative and project coordination skills, ability to effectively

manage multiple priorities, exercise sound judgment, ask questions and be open to the input and decisions of others

- Travel interstate if needed.

Desirable criteria

- Substantial experience implementing Security strategies.
- Experience working on projects with digital, mobile and CRM platforms.
- Experience with penetration testing.
- Substantial experience working on hybrid and Azure Cloud, Microsoft Azure Security, Azure AD, Windows, networking and AD.