National Director, Cyber & Information Security (CISO)

Role data

Position no.	TBC	**Work area profile**	Technology
Work level classification	Executive	**Directorate/Business unit**	Technology
Reports to (role)	Chief Technology Officer	**Location**	Various
No. direct reports	3+	**No. of indirect reports**	10+
Version date	August 2024	**Tenure**	Fixed-term, full-time

The Organisation

The Australian Health Practitioner Regulation Agency (Ahpra) is the national agency responsible for administering the National Registration and Accreditation Scheme (National Scheme) in partnership with 15 National Boards for the regulated health professions.

Ahpra's overall purpose is to protect the public by regulating health practitioners efficiently and effectively in the public interest to facilitate access to safer healthcare for all the community.

With offices in each State / Territory, Ahpra represents National Scheme interests with key community, professional, employer and government stakeholders with local operations governed by the Health Practitioner Regulation National Law Act as in force in each State / Territory.

Role purpose

Reporting to the Chief Technology Officer (CTO) and a member of the Technology Senior Leadership Team, this role is accountable for guidance and leading the delivery and continuous improvement of Ahpra's information and cyber security vision and strategy, by ensuring the continued alignment with business objectives. The National Director – Information and Cyber Security will provide functional leadership of the information and cyber security portfolio to deliver organisational programs and projects which seek to build Ahpra's digital and technology business capabilities and integrate information and cyber security practices within business programs.

This National Director – Information and Cyber Security will lead the establishment and implementation of strategies, programs, and processes to build Ahpra's cyber resilience, to effectively manage threats and associate risks to information security, within evolving and increasingly complex environments. The role will contribute to the development of organisational intelligence by leading external environmental scans and analysis of potential threats, and lead Ahpra's response in strengthening information and cyber security risk controls, to minimise information and cyber security risks for the organisation.

As a senior leader, the National Director – Information and Cyber Security will support a whole of organisation approaches to the delivery of Ahpra's strategic priorities, while highlighting and communicating opportunities for continuous improvement in delivering contemporary, robust, secure, and reliable IT services that support more efficient and commercially sustainable operational delivery. The role will lead the delivery of effective information and cyber security governance and assurance programs and process, and provide regular reporting to Ahpra's governance forums, including National Executive, Finance and Risk Management Committee, and Ahpra Board.

Key accountabilities

- Provide subject matter expertise in the leadership, development, and execution of a renewed Technology vision and strategy, that meets the strategic objectives and operational requirements of the organisation.
- Lead the establishment, implementation, and communication of strategies, programs, and processes to build Ahpra's cyber resilience and strategic direction, to effectively manage threats and associate risks to information security.
- Lead the cyber security standing committee, comprising of key cyber security and business executives, meeting formally on a monthly basis to provide risk based governance across cyber security in Aphra.
- Communicate Ahpra's cyber security vision and strategy to organisational stakeholders, cyber supply chains, and key external stakeholders, to provide visibility and awareness of organisational accountabilities, and promote broad security cultural change across the organisation.
- Develop partnerships with the business to develop clarity of business objectives and deliverables, and the proactive and continued alignment of information and cyber security practices and application of security controls as part of business planning and risk management.
- Assure that the organisation's processes are compliant with cybersecurity policy, standards, regulations, and legislation.
- Develop and maintain procedures to assess and manage information and cyber security risks within organisational supply chains, by collaborating with organisational teams responsible for contractor and vendor management procedures, e.g., procurement, legal, etc.
- Oversee the organisational response to cyber security incidents, through mobilising and engaging resources and teams necessary to contribute to the organisational response, and effectively communicate with internal and external stakeholders to bring clarity to the situation, following up with detailed reporting.
- Contribute to the development, implementation, and maintenance of Ahpra's business continuity and disaster require plans, to support improved business resilience and ensure the continued operation of critical business processes.
- Develop a culture of strong information security attitudes and practises throughout the organisation with awareness training, to facilitate broad security cultural change, and 'security by design' mindsets in the delivery of business-led technology programs.
- Implement cyber security measurement metrics and key performance indicators and provide regular reporting on strategic and operational risks, program status reporting, and environmental considerations to the CTO and Ahpra's governance forums, ensuring that complex technical terms and 'jargon' are translated into audience-specific communications.
- Effectively manage delivery of the information and cyber security portfolio in line with agreed budgets.
- Develop sound business cases to influence further organisational investment and access to funding to support further cyber security uplift activities and organisational response to security incidents.
- Create a positive work environment that encourages teamwork, collaboration, and cooperation between and among teams.
- Drive change management initiatives and foster a culture of continuous improvement with the cyber and information security function.

- People Management: Achieving organisational goals by effectively managing the team's and team members' workplace performance. This means to:
    - Enhance and encourage direct reports' potential through development and coaching activities
    - Take actions to close identified performance gaps in a timely and effective manner
    - Comply with Ahpra performance objectives setting, review and development processes
    - Motivate direct reports' behaviour by providing clear direction and recognition of achievements as well as personally modelling Ahpra standards of behavior.

- Commit to eliminating or reducing physical and / or psychosocial risks to the health, safety and wellbeing of all workers so far as reasonably practicable, by effectively discharging all responsibilities as defined by Ahpra's policies and procedures and health and safety legislation.

- Ensure the workplace provides a safe working environment with the required level of care and respect for its participants. This means to:

  – take reasonable care for own and others' health, safety and wellbeing
  – adhere to Ahpra's workplace health, safety and wellbeing policies and procedures.

Capabilities for the role

The Ahpra Capability framework applies to all Ahpra employees. Below is the complete list of capabilities and proficiency level required for this position.

Capabilities	Proficiency level
Commits to customer service	Advanced
Displays leadership	Highly Advanced
Generates and delivers the strategic vision	Highly Advanced
Demonstrates an awareness of the National Registration and Accreditation Scheme (the National Scheme) and the National Law	Advanced
Builds constructive working relationships	Highly Advanced
Communicates effectively	Highly Advanced
Demonstrates accountability in delivering results	Highly Advanced
Uses information and technology systems	Highly Advanced
Displays personal drive and integrity	Highly Advanced

Qualifications and experience

Qualifications/Experience	Required
Qualifications	Minimum Bachelor's degree in Information Technology is highly desirable, or equivalent years of professional experience in a similar position.
Experience	Demonstrated leadership and delivery of significant technology programs linked to business outcomes at a senior level. Demonstrated ability to recognise and resolve critical and sensitive issues and provide executive level advice to Executives, Committees and Boards. Exceptional communication skills with an ability to liaise, negotiate, consult and manage change at the senior level. Demonstrated ability to develop business cases and make sound recommendations based on organisational maturity, budget and change readiness. Experience with regulatory compliance and Australian government security frameworks - Protective Security Policy Framework and the Information Security Manual. Experience managing a team of IT professionals with a focus on building capability, developing talent, and creating a culture of collaboration and support, whilst maintaining clear ownership of accountabilities and responsibilities. Strong business and commercial acumen in managing high risk projects in a politically sensitive environment on time and within budget. Strong consulting skills and an ability to discuss IT requirements with the business in non-technical terms when required

Key relationships

Internal relationships	External relationships
Chief Executive Officer	Technology vendors
National Executive	Industry bodies
Ahpra Board and its sub-committees	Government agencies, statutory authorities, and peak bodies
Ahpra Senior Leaders (National Directors)	Australian Signals Directorate and Australian Cyber Security Centre
National Boards	Internal & External Auditors
Technology directorate team members	
Direct reports and team	