Role name: IT Security Architect

Role data

Position no.	TBC	**Work Area Profile**	Cyber and Information Security
Work Level Classification	Level 9	**Directorate / Business Unit**	Technology
Reports to (role)	National Director, Information & Cybersecurity (CISO)	**Location**	Various
No. direct reports	6	**No. of indirect reports**	0
Version date	August 2024	**Tenure**	Permanent

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

The IT Security Architect plays an integral role in defining and assessing the Ahpra's security strategy, architecture and practices, through the effective design and implementation of secure solutions that meet the growing needs of the organisation. Working closely with the Lead – Enterprise Architect, Project teams, IT SMEs, vendors, managed service providers, and business stakeholders, the IT Security Architect consults, advises, and oversees the secure design of both strategic and day to day initiatives to ensure alignment with enterprise security architecture.

Reporting to the National Director, Information & Cybersecurity, the role contributes to the secure design and implemenation of Ahpra's Cybersecurity Strategy and transformation initiatives, through effectively translating business objectives and risk management strategies into specific security processes enabled by security technologies and services. Leading a team of security specialists and security business analysts, , the IT Security Architect, provides expert advice, technical leadership, and serves as the custodian for Ahpra's cyber security architectural practice.

Key Accountabilities

- Develop and maintain an enterprise security architecture that enables the Ahpra to develop and implement security solutions and capabilities that are clearly aligned with business, technology and threat drivers.

- Determine security requirements by evaluating Ahpra's Business and Technology strategies and leading threat risk assessment activities; research information security standards; conduct system security and vulnerability analyses and risk assessments.

- Develop security strategy plans and roadmaps based on sound enterprise architecture practices for all environments including cloud and on-premise infrastructure.
- Develop and maintains security architecture artefacts (e.g., models, templates, standards and procedures) that can be used to leverage security capabilities in projects and operations.
- Determine baseline security configuration standards for operating systems (e.g., OS hardening), network segmentation and identity and access management (IAM)
- Develop standards and practices for data encryption and tokenization in the organization, based on relevant data classification criteria and structures.
- Establishes a taxonomy of indicators of compromise (IOCs) and communicate across Technology functions and project teams,
- Document and address information security, cybersecurity architecture, and systems security engineering requirements throughout the acquisition life cycle.
- Perform security reviews, identifies gaps in security architecture, and develops a security risk management plan.
- Track developments and changes in the digital business and threat environments to ensure that they're adequately addressed in security strategy plans and architecture artifacts.
- Validate enterprise and other reference architectures for security best practices and recommend changes to enhance security and reduce risks, where applicable.
- Validate security configurations and access to enterprise tools which are deployed across Ahpra.
- Facilitate threat modelling of services and applications that tie to the risk and data associated with the service or application.
- Coordinates with DevOps teams to advocate secure coding practices.
- Review and document data flows of sensitive information within and across the organisation and recommend controls to ensure that this data is adequately secured.
- Support the testing and validation of internal security controls, as directed by the National Director – Information and Cybersecurity (CISO) or Ahpra's internal audit team.
- Review security technologies, tools, and services, and makes recommendations to the broader security team for their use, based on security, financial and operational metrics.
- Define and document how the implementation of new systems or new interfaces between systems impacts the security posture of the current environment.
- Develop and enhance strategic relationships with key business stakeholders, actively manage their expectations and monitor satisfaction levels.
- Address business demand by capturing high level technology requirements, perform scoping, impact analysis, and provide inputs to the strategic prioritisation forums and processes.
- Define, document, and maintain the security domain architecture(s) including associated roadmaps and frameworks to deliver the desired outcomes aligned with Business and Digital Strategies.
- Analyse wider industry trends and best practice to identify best-in-class technology and enterprise security architecture.
- Provide technical expertise, advice and support to project teams during the design phase.

- 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.
- Health Safety and Wellbeing: Ensuring the workplace provides a safe working environment with the required level of care and respect for its participants meaning 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	Highly Advanced
Displays leadership	Advanced
Generates and delivers the strategic vision	Advanced
Demonstrates an awareness of the National Registration and Accreditation Scheme (the National Scheme) and the National Law	Intermediate
Builds constructive working relationships	Advanced
Communicates effectively	Highly Advanced
Demonstrates accountability in delivering results	Advanced
Uses information and technology systems	Highly Advanced
Displays personal drive and integrity	Advanced

Qualifications/Experience	Required
Qualifications	Minimum Bachelor's Degree in Information Technology: Computer Science, Information Science, cybersecurity or related field. Post-graduate certification/qualification in IT architecture methods (e.g. TOGAF, SABSAa) desirable

Experience	Demonstrated professional experience as Security Architect, across a breadth of industries and / or organisational settings. Strong leadership experience and skills in managing security artefacts. Strong experience (including hands on) and knowledge of secure design and implementation of security capabilities (including but not limited to infrastructure security, Identity and Access Management, Application Security). Direct, hands-on experience or a strong working knowledge of vulnerability management tools. Documented experience and a strong working knowledge of the methodologies to conduct threat-modelling exercises on new applications and services. Full-stack knowledge of IT infrastructure. Direct experience designing IAM technologies and services. Strong working knowledge of IT service management (e.g., ITIL-related disciplines): Exceptional communications skills with an ability to liaise, negotiate, consult and present to various stakeholder groups. Prioritisation skills and experience Deep experience in managing relationships with internal business customers. A clear understanding of business architecture standards/policies Strong understanding of the business domains Deep experience in architecture development, design, modelling, and hands on experience with tools Knowledge on IT tools and process automation Good understanding of development and project management processes and methodologies with applied project management experience

Key relationships

Internal Relationships	**External Relationships**
CTO	Technology vendors
Ahpra National Executive and their respective leadership teams	Managed service providers
IT Project Managers	Government agencies
Lead – Enterprise Architect	Internal & External auditors
Technology directorate peers	