

## Role Name: IT Security Architect

### Role data

|                                  |                                                       |                                    |                             |
|----------------------------------|-------------------------------------------------------|------------------------------------|-----------------------------|
| <b>Position no.</b>              | E13409                                                | <b>Work Area Profile</b>           | Information & Cybersecurity |
| <b>Work Level Classification</b> | Level 9                                               | <b>Directorate / Business Unit</b> | Technology                  |
| <b>Reports to (role)</b>         | National Director, Information & Cybersecurity (CISO) | <b>Location</b>                    | Various                     |
| <b>No. direct reports</b>        | 4                                                     | <b>No. of indirect reports</b>     | 0                           |
| <b>Version date</b>              | September 2026                                        | <b>Tenure</b>                      | 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 is accountable Ahpra's end to end security engineering and architecture function - a major, complex function of Ahpra's core business while ensuring that the user experience for practitioners and internal staff is balanced and supports Ahpra's strategy to prevent harm. The role sets, owns and enforces the enterprise security architecture ensuring Ahpra's platforms and regulatory information holdings are protected, and is the accountable design authority for the security controls designed and implemented across Ahpra's environment. Operating under broad direction and exercising a considerable degree of independence, the role makes security decisions that impact Ahpra, the Technology Directorate, practitioner interactions and user experience, with the potential to affect Ahpra's operations more broadly and its standing with external auditors, assurance partners and government agencies.

Reporting to the National Director, Cyber & Information Security (CISO), the role leads a team of security specialists and security business analysts and is responsible for the achievement of its own and its team's outcomes and KPIs. It owns the multi-year security architecture and engineering roadmap and program of works, the security technology portfolio together with its sourcing and vendor performance, and the design-side assurance that Ahpra's obligations under the Australian Government Information Security Manual, ISO 27001, NIST CSF, PCI DSS and privacy law are built into and evidenced across the environment.

### Key Accountabilities

- Lead the security engineering and architecture function end to end - strategy through design, build, transition and ongoing operation of enterprise security capability - as a major complex function of Ahpra's core business, accountable for its performance across the whole of Ahpra.

- Own, set and enforce the enterprise security architecture for the whole of Ahpra - across all business systems, the national registers, and cloud and on-premise infrastructure - and hold final design authority over the security solutions and capabilities implemented against it.
- 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.
- Define, own and deliver the multi-year security architecture and engineering program of works, including its outcomes, KPIs, milestones and reporting to the CISO, the Technology Directorate leadership team and Ahpra's governance and assurance committees.
- Develop and maintain 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 tokenisation in the organisation, based on relevant data classification criteria and structures.
- Establish a taxonomy of indicators of compromise (IOCs) and communicate it 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, identify gaps in the security architecture, and own the resulting security risk management plan - including the treatment decisions, the remediation program, and the residual risk accepted on Ahpra's behalf within delegation.
- Track developments and changes in the digital business and threat environments to ensure that they are adequately addressed in security strategy plans and architecture artefacts.
- 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.
- Coordinate 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.
- Own the design, testing and validation of Ahpra's internal security controls and the delivery of the resulting remediation, reporting outcomes directly to the CISO, Technology leadership and Ahpra's audit and assurance forums.
- Determine Ahpra's security technology portfolio - selecting, sourcing and approving the tools and services deployed, managing vendor and managed service provider performance against contracted outcomes, and providing budget input and whole-of-life cost advice for the architecture and engineering portfolio.
- Own the design-side assurance of Ahpra's compliance obligations, ensuring that the Australian Government Information Security Manual (ISM), ISO 27001, NIST CSF, PCI DSS and privacy and mandatory notification obligations are designed into the environment and evidenced across it, and directing the corrective action required where they are not.
- 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.
- Recommend the strategic direction for Ahpra's security architecture, taking account of the wider implications for Ahpra's operations, its regulatory standing and the 15 National Boards, and present Ahpra's position on complex security matters to internal and external stakeholders including government agencies, auditors and assurance partners.
- 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.
- Set and enforce the mandatory security design standards and assurance gates that all Ahpra projects and changes must satisfy, and approve or reject solution designs against them.
- Embed a secure-by-design culture across Ahpra by championing the integration of security into organisational training, processes, projects, lifecycle activities and business support functions.
- Create a positive work environment where direct reports are enabled to achieve their potential, in a culture that is values led and focussed on service delivery.
- 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 behaviour
  - Support team member/s health, safety and wellbeing by proactively managing physical, psychosocial and other workplace hazards and risks, and supporting team members in special roles (HSW Committee, Emergency Warden and First Aid Officers)
- Health safety and wellbeing: Ensuring that Ahpra is a healthy and safe working environment with the required level of care and respect for others. This means to:
  - take reasonable care for own and others' health, safety and wellbeing
  - proactively raise any health, safety and wellbeing concerns
  - 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                                                                          | Highly Advanced   |

| Capabilities                            | Proficiency level |
|-----------------------------------------|-------------------|
| Uses information and technology systems | Highly Advanced   |
| Displays personal drive and integrity   | Highly Advanced   |

| Qualifications/Experience | Required                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         |
|---------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Qualifications</b>     | <p>Academic qualification equivalent of a Bachelor, post-graduate or Master's degree or higher in Information Technology (mandatory), or equivalent years of professional experience in a similar position.</p> <p>Security certifications - ISO 27001, CISSP, CISM or equivalent (one or more mandatory).</p> <p>Ability to obtain a Government Security Clearance (desirable).</p> <p>Post-graduate certification / qualification in IT architecture methods (e.g. TOGAF, SABSA) desirable.</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                |
| <b>Experience</b>         | <p>Demonstrated professional experience as a Security Architect across a breadth of industries and / or organisational settings.</p> <p>Highly advanced experience in leading a professional team, with the ability to develop trusted, supportive relationships to drive performance.</p> <p>Exceptional ability to recognise and resolve critical and sensitive issues and to provide high level, authoritative advice for which the role is individually accountable.</p> <p>Demonstrated accountability for a security function end to end, including a program of works, its budget and its reported outcomes.</p> <p>Understanding of, and ideally experience related to, the Australian Government Information Security Manual (ISM), ISO 27001, NIST CSF and other industry standards.</p> <p>Experience of working in a regulatory or compliance-focused environment.</p> <p>Strong experience (including hands on) and knowledge of secure design and implementation of security capabilities, including infrastructure security, Identity and Access Management and Application Security.</p> <p>Direct, hands-on experience or a strong working knowledge of vulnerability management tools.</p> <p>Documented experience and a strong working knowledge of the methodologies to conduct threat-modelling exercises on new applications and services.</p> <p>Full-stack knowledge of IT infrastructure, and direct experience designing IAM technologies and services.</p> <p>Strong working knowledge of IT service management (e.g. ITIL-related disciplines).</p> |

|  |                                                                                                                                                                                                                                                                                                                             |
|--|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|  | <p>Exceptional communication skills with an ability to liaise, negotiate, consult and present to various stakeholder groups.</p> <p>Deep experience in managing relationships with internal business customers, and in architecture development, design and modelling with hands on experience of the supporting tools.</p> |
|--|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|

## 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                                   |                              |