Position Description

Job Title

IAM Architect | Permanent Full Time

Location

This role supports flexible working arrangements, including remote work for interstate candidates. For those based in Adelaide, we offer a hybrid model with the option to work from both the office and home. Candidates from **Queensland** are especially encouraged to apply.

Key Purpose

The IAM Architect is responsible for defining, designing, and leading the delivery of complex Identity and Access Management (IAM) solutions across client environments. This role provides technical and architectural leadership in shaping secure, scalable, and modern IAM ecosystems aligned with business objectives and regulatory requirements.

The IAM Architect acts as a trusted advisor and technical expert, ensuring that identity strategies are well-designed, secure, and integrated effectively with enterprise applications, cloud platforms, and infrastructure. The role requires strong experience in architectural frameworks, governance, and solution design across IAM, IGA, and PAM domains.

About Us

We are a leading implementation partner specialising in Identity and Access Management, Privileged Access Management, and Identity Governance. We are a forward-thinking team of cybersecurity professionals driven by the desire to secure all apps and users.

We help businesses secure their environments by using modern tools, expert knowledge and a pragmatic approach.

We are rapidly becoming Australia's best-known IAM provider and are a trusted partner to our clients in Adelaide and across the country. Our reputation is built on being knowledgeable, highly experienced, effective and reliable.

Our team is everything. Hand-picked, high performing, driven and as smart as they come.

- We have grown since rapidly since 2019 and we will continue to attract the A-grade talent we need to grow and be the best.
- We have customised training plans to meet our people's needs whilst enhancing the capability of our business.
- We have fun and get the job done.
- We mentor and vet our staff to grow them into autonomous stars.

We are always looking for awesome, talented people to join our A-grade team.

About You

You are an experienced IAM professional with a strong architectural background and deep technical expertise in Identity Governance and Administration (IGA), Access Management (AM), and Privileged Access Management (PAM) technologies.

You are comfortable translating business requirements into secure and scalable identity architectures and guiding delivery teams through design, implementation, and optimisation. You take ownership, communicate clearly, and can lead conversations with senior stakeholders, project managers, and technical specialists.

We're looking for:

- Proven ability to design and implement enterprise IAM solutions leveraging technologies such as Saviynt, SailPoint, Okta, Entra ID, and CyberArk.
- Deep understanding of IAM concepts including SSO, MFA, RBAC, ABAC, lifecycle management, and zero trust principles.
- Experience developing architecture artefacts including high-level and low-level designs, roadmaps, and governance frameworks.
- ßßStrong knowledge of integration patterns across cloud, SaaS, and hybrid environments (APIs, SCIM, OIDC, SAML, REST).
- A consultative approach with the ability to influence business and technical outcomes.

You will:

- Provide architectural guidance and assurance for IAM project delivery.
- Drive alignment with security and compliance standards (NIST, ISO27001, Essential Eight).
- Mentor engineers and consultants to uplift IAM delivery capability.
- Communicate complex ideas clearly and effectively to diverse stakeholders.

Working Relationships

The IAM Architect works closely with Identify project teams, clients, and partners to design and deliver secure, scalable identity solutions. Key relationships include:

- Clients and executive stakeholders to define IAM strategies and target-state architectures.
- Project Managers and Senior Consultants to ensure successful delivery.
- Security Managers, Solution Architects, and Technical SMEs to integrate IAM solutions within enterprise environments.
- Vendor and partner contacts to stay abreast of platform capabilities and product enhancements.

Key Responsibilities and Outcomes

- Define IAM architectures and solution designs, ensuring alignment with business objectives and security policies.
- Lead discovery workshops and document requirements, translating them into actionable architecture artefacts.
- Develop and maintain IAM roadmaps, reference architectures, and integration frameworks.

- Provide governance and oversight during project delivery phases, ensuring alignment with design and quality standards.
- Collaborate with delivery teams to ensure technical feasibility and integration alignment across IAM, IGA, and PAM solutions.
- Conduct architectural reviews, risk assessments, and design validations.
- Contribute to pre-sales and proposal activities by shaping IAM solutions and providing technical estimates.
- Stay current with emerging IAM trends, technologies, and compliance frameworks.
- Provide mentoring and thought leadership across the Identifly IAM practice.
- Report on architectural progress, risks, and outcomes to Directors and client stakeholders.

Responsibilities may be varied by Identifly in order to allow Identifly to respond to operational or client needs or requirements.

Experience & Skills

Experience

- 10+ years total IT experience with at least 5+ years in Identity & Access Management or Security Architecture.
- Proven hands-on experience delivering enterprise IAM solutions using Saviynt, SailPoint, Okta, Entra ID, and/or CyberArk.
- Strong understanding of Identity Governance, Authentication, Access Provisioning, and Federation protocols.
- Demonstrated experience in architectural governance, documentation, and design reviews.
- Experience across multiple domains: Cloud (Azure, AWS, GCP), DevOps, API integration, and application security.
- Knowledge of Cyber Security Frameworks (NIST, ISO 27001, Essential Eight).
- Client-facing consulting experience, demonstrating influence and credibility at senior levels.

Skills

- Ability to develop and communicate IAM architectural strategies and roadmaps.
- Expertise in design and configuration of Saviynt, SailPoint, Okta, and Entra ID.
- Strong knowledge of identity standards (SCIM, SAML, OAuth, OIDC, FIDO2, LDAP).
- Hands-on experience with PAM technologies such as CyberArk or Delinea.
- Excellent analytical and problem-solving abilities.
- Strong written and verbal communication skills, capable of producing design documents, proposals, and presentations.
- Scripting and automation capabilities (PowerShell, Python, Java, SQL).
- Ability to manage multiple projects and priorities in a fast-paced environment.
- Collaborative mindset and willingness to mentor junior staff.

Candidate Responses

1. Provide cover letter responding to the following:
   a. Summary of how you meet criteria of the role
   b. Clearly stipulate if you have proven technical experience as per the specification
2. Provide your CV:
   a. Outline your technical skills
   b. Outline your client interaction experiences
   c. Provide us any additional information that you think will contribute to your success
   d. Clearly state your location.

Selection Process

1. Short list applications based on candidate responses and suitability for role
2. Identifly will contact you if you have been shortlisted and arrange a F2F/virtual interview
3. F2F interview conducted at Identifly Office, Adelaide CBD – If, in South Australia
4. For your interview:
   a. Prepare questions about the role (if any)
   b. Be prepared to answer questions about your experience
   c. Be prepared to discuss salary
5. The right candidate: We know when we meet the right person, and we will act quickly to onboard them. Be prepared to be made an offer and provide details of potential start date.