IDENTIFLY PTY LTD
ACN 633065120
ABN 43633065120
53 Byron Place
Adelaide, SA 5000

# Position Description

## Job Title

IAM Engineer | Permanent Full Time

## Location

This role will be primarily located in our Adelaide CBD office. We support hybrid working from office and home. There is an opportunity for remote working arrangements, for the right candidate however our preference is Adelaide based. There will also be occasional onsite client engagement as required.

## Key Purpose

The IAM Engineer is responsible for working with internal stakeholders and external clients to plan, design and deliver identity security solutions. The candidate will have experience with deploying Identity Security solutions in complex IAM environments.

## 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 SA'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

Ideally you come from an Identity or cyber background. You will have excellent customer engagement skills, and a passion for problem solving.

A strong technical acumen is a must, familiarity with the identity security domain is vital. We are looking for experience with IGA, IAM, and PAM systems and principles.

We work heavily with IAM platforms including - Okta, Azure, SailPoint, Saviynt, CyberArk and CrowdStrike and experience in some of these technologies is a must.

IDENTIFLY PTY LTD
ACN 633065120
ABN 43633065120
53 Byron Place
Adelaide, SA 5000

Importantly, the concepts that these platforms support - password management, MFA, SSO, contextual access, risk-based auth, roles, HR as a master, automated provisioning and privileged session management must be well understood and you must have the ability to communicate these concepts.

Experience with Active Directory, AAD, AAD Connect and M365, device management and device authentication would be preferred.

Familiarity with a scripting language will be looked upon favourably.

Identity systems connect with everything, so understanding IAM in a larger digital context is crucial. Experience with any of the following is a nice to have SIEMs, SAP, SuccessFactors, Workday and ServiceNow.

Not all these technologies are necessary to get the job, but a willingness to learn new technologies is what we are after.

You will need to take the initiative, and work comfortably without supervision. You will be expected to 'manage-up' and report back to senior consultants about progress.

Communication is key. You will need to manage expectations of your peers and our customers and the ability to engage with a range of stakeholders and explain complex ideas clearly and effectively. Your written communication skills must be on-point, as a large part of this role will be developing technical design and project as-built, documentation.

We want someone proactive and professional who will also fit culturally with our team.

## Key Responsibilities and Outcomes

The IAM Engineer is responsible for delivering quality solutions to clients as per the project brief provided by Identifly project leads and Directors. This includes the design of solutions, incorporating third party supplier software solutions. The position's key responsibilities include:

1. Proactively engaging with key external stakeholders and Subject Matter Experts (SMEs) to understand their requirements, business direction and technical landscape.
2. Interface with and coordinate tasks with internal and external technical resources. This includes collaborating with Project Managers and technical staff to provide estimates, develop overall implementation solution plans, and taking a lead role in implementations.
3. Generate high quality documents and diagrams including requirements and design documents, architecture diagrams and models, test plans, detailed test cases, as-built, risk assessments, implementations and project plans.
4. Perform system configuration, functional and integration testing, and deploy solutions.
5. Provide technical support to clients and maintenance of deployed technologies.
6. Report on progress, billable hours and deliverables including weekly time writing
7. Other duties as given by the Company Directors.

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

## Working Relationships

This role will work closely with internal and external key stakeholders to understand business and technical needs of our clients, including the deployment and maintenance of technology solutions for our clients.

In particular this role will work closely with clients, Project Managers, Security Managers, IT Managers, Technical SMEs and Security resources to deliver complete solutions for our clients including decisions around appropriate technologies to use.

IDENTIFLY PTY LTD
ACN 633065120
ABN 43633065120
53 Byron Place
Adelaide, SA 5000

# Skills and Experience

## Experience

- 7+ years IT experience
- 4+ in Identity/Security or Infrastructure domains
- Knowledge and experience working with IDaaS solutions (Okta and Entra ID)
- Understanding of and skill working with PAM solutions (CyberArk, Delinea, Silverfort, CrowdStrike)
- Sound knowledge of IAM domains (Access, Authentication, Provisioning, Governance).
- Knowledge of authentication, password management, MFA, SSO and adaptive security.
- Knowledge of Cyber Security Frameworks and Best Practices (NIST, SACSF) (desirable)
- 3+ years of customer facing role, dealing with internal or externals customers regularly
- Must have a proven track record of successfully engaging with stakeholders
- Experience with JIRA and agile delivery frameworks
- Nice to have: SIEM, O365, Ping, Forgerock, SuccessFactors, WorkDay, PeopleSoft, NetIQ, MIM, ServiceNow.
- SkillsProven skill working with Identity Governance and Administration (IGA) platforms (SailPoint, Saviynt)
- Ability to rapdily communicate complex ideas around a technical topic, ideally on the fly on a whiteboard.
- Excellent analytical skills, and ability to engage with a range of stakeholders to understand requirements.
- Excellent written skills with a proven track record of delivering complex and detailed design documents.
- Ability to identify security risks and issues with current or designed deployments.
- Access management hands on technical experience (Okta, Entra ID, Ping, SailPoint).
- Hands on technical experience with Privileged Access Management (CyberArk, Delinea, Silverfort, CrowdStrike)
- Skills or at least an understanding of public cloud management (Azure, AWS, Google)
- Automating solutions and migrations using scripting (PowerShell, Python, Java, JS, SQL etc.)
- System administration skills and understanding of Active Directory, LDAP, RADIUS and ADFS (desirable)
- Integration methods such as API, web-services, database connections, SCIM.
- Professional and effective client liaison.
- Ability to work in a dynamic team environment or autonomously.
- Outstanding attention to detail.

## Skills

- Ability to quickly communicate complex ideas around a technical topic, ideally on the fly on a whiteboard.
- Excellent analytical skills, and ability to engage with a range of stakeholders to understand requirements.
- Excellent written skills with a proven track record of delivering complex and detailed design documents.
- Ability to identify security risks and issues with current or designed deployments.
- Access management hands on technical experience (Okta, Azure, Ping, SailPoint).
- Hands on technical experience with Privileged Access Management (CyberArk, Remediant, Thycotic)
- Hands on technical experience with Identity Governance and Administration (IGA) platforms (SailPoint, Saviynt, ClearSkye)
- Skills or at least an understanding of Public cloud management (Azure, AWS, Google)

IDENTIFLY PTY LTD
ACN 633065120
ABN 43633065120
53 Byron Place
Adelaide, SA 5000

- Automating solutions and migrations using scripting (PowerShell, Python, Java, JS, SQL etc.)
- System administration skills and understanding of Active Directory, LDAP, RADIUS and ADFS (desirable)
- Integration methods such as API, web-services, database connections, SCIM.
- Professional and effective client liaison.
- Excellent verbal and written communication.
- Excellent personal presentation.
- Excellent time management and prioritisation of tasks.
- Ability to work in a dynamic team environment or autonomously.
- Outstanding attention to detail.

## 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
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.