Position description

Position title	Cyber Delivery Specialist (IDAM)
Group / Branch	*Enterprise Transformation & Delivery / Enterprise Delivery*
Reports to (Title)	Head of Delivery- Enterprise Systems
Competency level	*Individual Contributor*

Job Purpose

The Cyber IDAM Specialist provides hands-on identity and access management engineering, governance and delivery capability across South East Water's technology and cyber portfolio. The role designs, configures, integrates, tests and operationalises identity controls across workforce, privileged, service, application and third-party identities.

The role leads practical delivery of identity governance and administration, privileged access management, authentication, multi-factor authentication, single sign-on, role-based access control, access reviews and joiner-mover-leaver processes. It combines strong identity engineering with business process analysis, control design and implementation assurance.

Working across Cyber Security, Enterprise Delivery, Architecture, Technology Services, Human Resources, Operational Technology, Risk and Assurance, Procurement, application owners and delivery partners, the role converts identity risks and regulatory obligations into secure, usable and sustainable outcomes.

Role emphasis: This is a delivery and engineering role. The incumbent must be able to analyse identity processes and controls, configure and integrate IDAM technologies, troubleshoot authentication and provisioning issues, migrate identities safely, and demonstrate that controls operate effectively in production.

Key Accountabilities

1. Identity Architecture, Engineering and Integration

- Design and implement identity solutions across Microsoft Entra ID, Active Directory and hybrid identity environments, including authentication, federation, directory synchronisation, conditional access, MFA and single sign-on.
- Configure and troubleshoot standards-based integrations using SAML 2.0, OAuth 2.0, OpenID Connect, SCIM, LDAP and relevant APIs or connectors.
- Assess application identity patterns, directory dependencies, service accounts, hardcoded credentials, authentication methods and authorisation models; define secure target-state designs and migration requirements.
- Support identity lifecycle integration with authoritative sources and target systems, including data mapping, correlation, reconciliation, provisioning, deprovisioning and exception handling.
- Investigate complex access, token, claims, certificate, connector and synchronisation failures using logs, diagnostics and controlled technical recovery.

2. Identity Governance and Administration

- Design and implement joiner-mover-leaver processes that provide timely access, modification and removal based on authoritative workforce and contractor data.
- Develop role and entitlement models using RBAC and, where appropriate, attribute-based access controls; identify toxic combinations and segregation-of-duties conflicts.
- Implement access request, approval, certification and review workflows, including accountable ownership, escalation, expiry and evidence retention.
- Rationalise groups, roles and entitlements; identify orphaned, dormant, duplicate, excessive or inappropriate access and coordinate remediation with owners.
- Define governance for guest, contractor, supplier, emergency, service and non-human identities, including sponsorship, review, rotation, expiry and removal.

3. Privileged Access and Credential Security

- Deliver privileged access management controls for administrative, application, database, infrastructure, cloud and OT-adjacent privileged accounts.
- Implement credential vaulting, rotation, session control, approval, monitoring and emergency access patterns using platforms such as CyberArk, Beyond Trust or equivalent.
- Apply privileged identity management, just-in-time and time-bound access, named administration, tiered administration and least privilege.
- Discover and remediate unmanaged privileged accounts, embedded credentials, shared administrator access and weak operational practices without disrupting critical services.
- Define break-glass arrangements, monitoring, testing and recovery procedures that balance cyber risk with operational resilience.

4. IDAM Delivery, Migration and Testing

- Lead discovery, requirements, solution design, implementation planning, migration, testing, cutover, rollback and transition activities for IDAM initiatives.
- Create functional, non-functional, data, control and acceptance requirements and maintain traceability through procurement, design, build, testing and handover.
- Develop representative test scenarios covering positive and negative access, lifecycle events, approvals, role assignment, access removal, MFA, SSO, privileged access, failure handling and audit evidence.
- Plan phased onboarding of applications and identity populations, manage dependencies and exceptions, and ensure control effectiveness is verified before go-live.
- Produce operational procedures, support models, runbooks, training, evidence packs and control ownership arrangements for sustainable business-as-usual operation.

5. Cyber Assurance, Monitoring and Risk Management

- Apply least privilege, strong authentication, identity threat detection, logging, monitoring, secure configuration, resilience and recovery across identity services.
- Define identity security metrics and control monitoring for privileged access, stale accounts, failed provisioning, overdue certifications, MFA coverage, exceptions and remediation.
- Support identity-related incident investigation and response, including account compromise, privilege misuse, suspicious authentication and unauthorised access.
- Maintain traceability across risks, control objectives, requirements, designs, test results, exceptions, evidence and residual-risk approvals.

- Assess legacy and operational constraints and develop proportionate treatments that improve security without creating unacceptable service or safety impacts.

6. Regulatory Alignment and Stakeholder Engagement

- Support alignment with the Security of Critical Infrastructure Act and Critical Infrastructure Risk Management Program, Victorian Protective Data Security Standards, ASD Essential Eight and Information Security Manual, NIST Cybersecurity Framework and ISO/IEC 27001.
- Partner with Human Resources, application owners, technology teams and business leaders to establish identity ownership, approval responsibilities and workable access processes.
- Engage vendors and systems integrators on requirements, architecture, integration, configuration, testing, licensing, supportability and assurance evidence.
- Communicate identity risks, control gaps, operational impacts and treatment options clearly to technical, operational and executive stakeholders.

Knowledge, Skills & Experience

- **Relevant delivery experience:** Demonstrated success delivering enterprise IDAM, IGA or PAM initiatives in a complex, regulated or critical-infrastructure environment, with accountability for both technical outcomes and project delivery.
- **Technical expertise:** Strong practical knowledge of Microsoft Entra ID, Active Directory, hybrid identity, modern authentication, identity governance and privileged access, supported by hands-on configuration, integration and troubleshooting experience.
- **Identity standards and platforms:** Working knowledge of relevant identity protocols and integration methods, including SAML 2.0, OAuth 2.0, OpenID Connect, SCIM, LDAP, APIs, certificates, claims and connectors, together with experience using enterprise IGA or PAM platforms.
- **Identity control knowledge:** Sound understanding of identity lifecycle management, RBAC, least privilege, segregation of duties, access certification, MFA, conditional access, privileged access and governance of workforce, third-party and non-human identities.
- **Project management capability:** Proven ability to manage scope, schedules, budgets, resources, dependencies, risks, issues, change, vendors and governance for technically complex initiatives.
- **Analysis and assurance:** Strong requirements, data-analysis and problem-solving skills, with the ability to maintain traceability from risk and control objectives through design, testing, acceptance, audit evidence and operational handover.
- **Stakeholder and communication skills:** Demonstrated ability to work across cyber security, architecture, technology, HR, risk, audit, application and business teams; influence decisions; resolve competing priorities; and communicate clearly with technical and executive audiences.
- **Cyber and regulatory knowledge:** Sound knowledge of Essential Eight, ISO/IEC 27001, Zero Trust principles, the Security of Critical Infrastructure Act, the Critical Infrastructure Risk Management Program and relevant internal security policies.

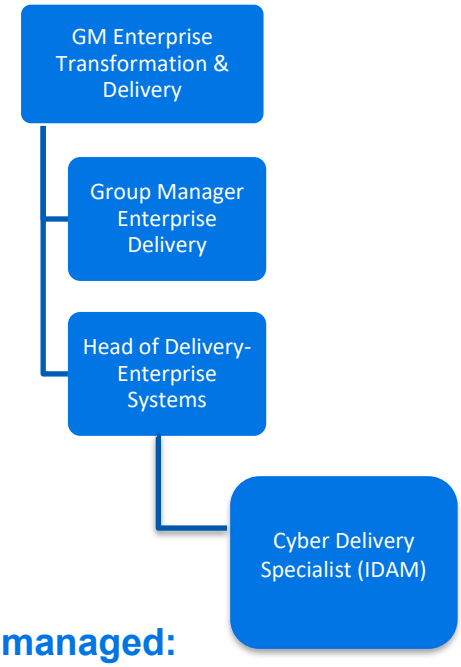
Education and Formal Certifications

- Bachelor’s degree in Cyber Security, Information Technology, Computer Science, Engineering or a related discipline, or equivalent relevant industry experience.
- Relevant Microsoft identity certification, such as Identity and Access Administrator Associate, is highly desirable.

- SailPoint, Saviynt, CyberArk or equivalent IGA and PAM product certification is highly desirable where relevant to the implemented technology stack.
- Professional certifications such as CISSP, CISM, CISA or CRISC are advantageous but do not replace the mandatory requirement for hands-on IDAM engineering and delivery experience.
- Knowledge of ITIL, PRINCE2, Agile delivery or equivalent service and delivery practices is desirable.

Dimensions

Organisational Chart



Number of people managed:

N/A

Size of budget managed:

N/A

Value of Assets managed:

N/A