

JOB DESCRIPTION

Specialist Identity and Access Management

ROLE TITLE	Specialist Identity and Access Management
SECTION/DIVISION:	Cyber Security and Identity, Digital Services
REPORTS TO:	Group Leader Enterprise Identity
DIRECT REPORTS (FTE):	Nil
INDIRECT REPORTS (FTE):	Nil
PRIMARY PURPOSE OF THE ROLE:	The Specialist Identity and Access Management (IAM) is responsible for delivering expert-level capability in the design, integration, and operation of identity and access management services across the organisation, ensuring identity platforms, access controls, and authentication services are secure, resilient, scalable, and aligned to contemporary best practice. Operating with a high level of autonomy, the role provides technical expertise across solution design, integration, testing, optimisation, and problem management, ensuring IAM services integrate effectively with enterprise systems and enable seamless, secure user experiences. The role provides specialist advice to digital peers on access models, integration patterns, and the resolution of complex operational issues, proactively identifying improvements and safeguarding the stability and reliability of IAM platforms. Through collaboration with security, infrastructure, and application teams, the IAM Specialist enables secure digital access that supports organisational goals, reduces risk, and delivers a strong user experience.
ACCOUNTABILITIES:	Identity and Access Management, IAMT: level 4 Designs and implements complex identity and access management solutions, focusing on automated access control and role allocation. Oversees the integration of identity and access management services with new technologies. Provides specialised support for complex identity and access management operations and supports implementation of policies and standards. Collaborates with stakeholders to align identity and access management with business objectives and emerging security trends. Specialist advice, TECH: Level 4 Provides detailed and specific advice regarding the application of their specialism to the organisation's planning and operations. Actively maintains knowledge in one or more identifiable specialisms. Recognises and identifies the boundaries of their own specialist knowledge. Where appropriate, collaborates with other specialists to ensure advice given is appropriate to the organisation's needs. Problem management, PBMG: Level 4 Initiates and monitors actions to investigate and resolve problems in systems, processes and services. Determines problem fixes and remedies.

Collaborates with others to implement agreed remedies and preventative measures.

Supports analysis of patterns and trends to improve problem management processes.

Systems integration and build, SINT: Level 4

Provides technical expertise to enable the configuration of system components and equipment for systems testing.

Collaborates with technical teams to develop and agree system integration plans and report on progress. Defines complex/new integration builds. Ensures that integration test environments are correctly configured.

Designs, performs and reports results of tests of the integration build. Identifies and documents system integration components for recording in the configuration management system.

Recommends and implements improvements to processes and tools.

Systems design, DESN: Level 4

Designs system components using appropriate modelling techniques following agreed architectures, design standards, patterns and methodology.

Identifies and evaluates alternative design options and trade-offs. Creates multiple design views to address the concerns of the different stakeholders and to handle functional and non-functional requirements.

Models, simulates or prototypes the behaviour of proposed system components to enable approval by stakeholders.

Produces detailed design specifications to form the basis for the construction of systems. Reviews, verifies and improves own designs against specifications.

IT infrastructure, ITOP: Level 3

Provisions/installs, configures and maintains infrastructure services and components.

Monitors, measures and reports on infrastructure load, performance and security events. Identifies operational issues and contributes to their resolution.

Carries out agreed operational procedures, including backup/restore, using supplied infrastructure tools and scripts.

Carries out agreed system software maintenance tasks. Automates routine system administration tasks to specifications using standard tools and basic scripting.

KEY RELATIONSHIPS:

Internal

Leaders, managers and staff (as clients)
Digital Services Division staff (Technical Peers)
Project sponsors and managers
Enterprise Project Management Office

External

University and industry peers
Vendors, service providers, contractors, consultants, outsourcing organisations

QUALIFICATIONS AND EXPERIENCE:

Essential

Tertiary level qualification in a relevant discipline or recognised qualification(s) appropriate to the role.
Considerable experience delivering Identity and Access Management services in a medium-large or complex organisation.
Experience configuring integration connectors and provisioning/reconciliation workflows between source and target systems
Strong experience with Identity Governance and Administration (IGA) lifecycle processes including provisioning, de-provisioning, role modelling, access governance, and authentication/authorisation patterns.
Proven experience integrating IAM services with enterprise applications, cloud environments, and on-premise systems.

	<u>Preferred</u> Advanced or specialist qualification(s) in IAM, cyber security, cloud architecture, or related domains (e.g., CISSP, CIAM, Microsoft Identity certifications). Demonstrated capability in problem management, incident resolution, and troubleshooting complex identity-related issues. Experience with Privileged Access Management platforms and privileged identity workflows. Proven ability to interpret requirements, develop technical design artefacts, and contribute to IAM architecture and design.
TECHNICAL SKILLS AND KNOWLEDGE:	<u>Essential</u> Strong knowledge of modern IGA and IAM tools and platforms Understanding of authentication and authorisation protocols including SAML, OAuth2.O, OIDC, Kerberos, LDAP. Proficiency with SSO, RBAC, ABAC, Conditional Access, and Zero Trust identity controls. Working knowledge of scripting and automation for identity workflows, provisioning, reporting. Understanding of API-based identity integration and modern identity architectures. <u>Preferred</u> Familiarity with directory modernisation, hybrid identity, and identity transformation initiatives. Understanding of HR and Student Management systems, and the ability to translate business rules into technical onboarding/offboarding/change processes for staff and students within a University context Understanding of secure DevOps practices for identity.
SPECIAL REQUIREMENTS:	After-hours and on call work required on occasion, including short-notice response to unplanned events and scheduled after-hours support. Service and support to University of Otago satellite campuses as required. Some travel may be required. Ministry of Justice check and credit check required as a condition of employment. Staff must comply with the Public Records Act 2005 and the Privacy Act 2020 and are expected to complete training to understand and meet these requirements.
DIRECT BUDGET ACCOUNTABILITY:	Nil
MĀORI STRATEGIC FRAMEWORK:	Act in a manner consistent with the principles and implications, as well as the University's commitment to the Treaty as articulated in the Māori Strategic Framework.
PACIFIC STRATEGIC FRAMEWORK:	Act in a manner consistent with the strategies and goals contained in the University's Pacific Strategic Framework, role-modelling and promoting Pacific values, equity and diversity principles and cultural safety practices.
HEALTH AND SAFETY:	Act and work in a manner compliant with current health and safety at work legislation and University procedures, frameworks and guidelines. Role model safe behaviour and practices, share the responsibility to prevent harm and contribute to a safe campus and work environment, including raising workplace health and safety concerns for self, students, visitors and other staff.
SUSTAINABILITY:	Act in a manner consistent with the University's sustainability commitments; role-modelling sustainable practices, with a particular emphasis on minimising the environmental impact of day-to-day activities.

SKILLS FRAMEWORK FOR THE INFORMATION AGE (SFIA)

Specialist – Identity & Access Management

Role Type: Specialist

SFIA Levels of responsibility

Autonomy	4	Influence	4	Complexity	5	Business Skills	5	Knowledge	4
----------	---	-----------	---	------------	---	-----------------	---	-----------	---

SFIA Skills Profile

Category	Subcategory	Skill	Code	L1	L2	L3	L4	L5	L6	L7
Delivery and operation	Security Services	Identity and Access Management	IAMT							
Strategy and architecture	Advice and guidance	Specialist advice	TECH							
Delivery and operation	Service management	Problem management	PBMG							
Development and integration	Systems development	Systems Integration and build	SINT							
Development and integration	Systems development	Systems Design	DESN							
Delivery and operation	Technology management	Infrastructure Operations	ITOP							

<https://help.sfia.nz/hc/en-nz/sections/4407230514201-Levels-of-responsibility>

<https://sfia-online.org/en/sfia-8/sfia-views/full-framework-view?path=/glance>