Access Control Analyst (IAM-IGA)

Department: Chief Operating Office

Division: Modernisation and Digital

Reports to: Network and Security Manager

JE Reference: COO1031

Grade: 9   **JE Date:**   26/8/2021

Job purpose

The Access Control Analyst will apply cyber security techniques to support and maintain the various platforms/solutions associated with the Identity and Access Management (IAM) function.

This includes day to day operations and support of the Identity Governance & Administration (IGA), Privilege Access Management (PAM) and Multi-Factor Authentication (MFA) solutions deployed across GoJ. The role will also necessitate the analysis and response to requirements and use cases associated with the on-boarding activities for all IAM relevant solutions.

Within the remit of this role, the analyst will provide effective and accurate technical information, analysis, investigation and support to the organisation and may also involve the provision of security advice as it relates to the effective deployment of IAM solutions.
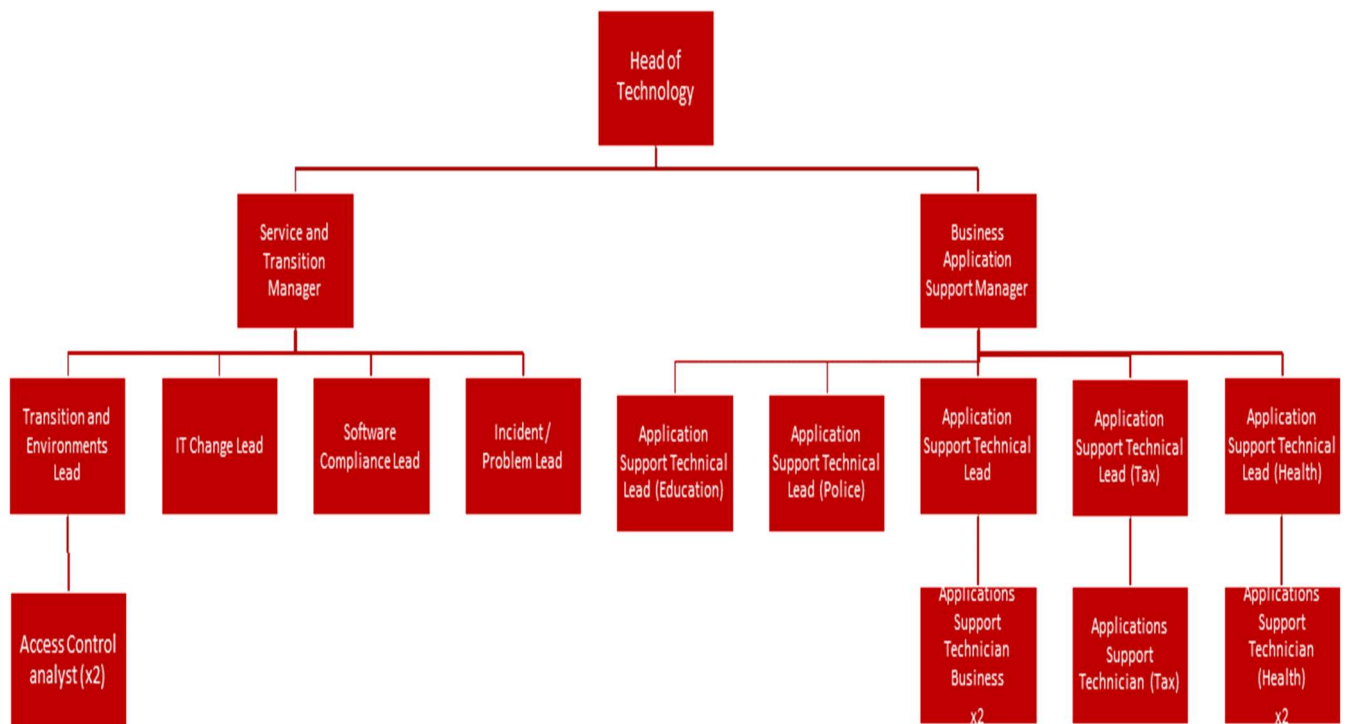
Job specific outcomes

- Manages the day to day operations of IAM solutions deployed across GoJ, providing level 2 and level 3 support to the various platforms as well as providing advice on Joiner, Mover Leaver (JML) functions, Identity Administration/Access Governance and related reviews.

- Overseas and provides IAM engineering guidance/expertise to help on-board systems as required, either through hands-on delivery activities or guiding teams of external staff/engineers to fulfil on-boarding requests to the satisfaction of GoJ standards/blueprints.

- Reviews and analyses the current IAM solution suite performance and function against any compliance, operational or other metrics and reports back on any challenges or key areas of risk that may arise.

- Where required, documents, plans and proposes improvements to the IAM solution suite based upon industry good practice, organisational risk assessments and other related organisational strategies/objectives.

- Communicates risk and makes recommendations to the management team in a technical and non-technical manner to support senior decision makers to ensure the security of information/ data and system assets held by the organisation.

- Oversees activities related to the development, implementation, and maintenance of the organisation's access control policies and procedures, supporting other departmental stakeholders/teams to ensure they are not in conflict with GoJ policies.

Statutory responsibilities

Active engagement, participation and compliance with any other statutory responsibilities applicable to the role, as amended from time to time.

Organisation Chart

Person Specification

ATTRIBUTES	ESSENTIAL	DESIRABLE
Qualifications *Please state the level of education and professional qualifications and / or specific occupational training required.*	Educated to degree level in a related security/ technology subject with a high degree of analytical content, or can demonstrate such a level of equivalent qualifications and experience	
Knowledge *This relates to the level and breadth of practical knowledge **required** to do the job (e.g. the understanding of a defined system, practice, method or procedure).*	Demonstrated knowledge of industry security frameworks and practices, specialising in access control, identity and access management, and identity governance and administration. Good interpersonal skills with a successful track record of helping to align the organisation to key security and risk reduction objectives/drivers. Knowledge of Information Security good practice with a focus on access control, joiner mover and leaver processes, privileged access management and more general IAM governance.	
Technical / Work-based Skills *This relates to the skills specific to the job, e.g. language fluency, vehicle license etc.*	Extensive administrative and engineering experience in a wide range of IAM solutions, including Identity Governance & Administration (IGA), Privileged Access Management (PAM) and Multi-Factor Authentication (MFA). Core business analysis skills to support discreet on-boarding activities associated with the GoJ IAM solution suite. Able to define processes and policies in relation to IAM controls - which include, joiner mover and leaver, access reviews, access request and approvals, role-based access controls, segregation of duties policies. Broad technical knowledge with a good understanding of legacy systems, current and emerging technologies and market trends, with the focus on integrating current and legacy systems such as directories,	

	databases, commercial applications and software as a service applications in relation to IAM controls.	
General Skills/Attributes *This relates to more general characteristics required to do the job effectively, e.g. effective written communication skills, ability to delegate, motivation or commitment etc.*	Strong verbal and written communication skills to influence a wide range of stakeholders. Strong cross-functional team player with ability to manage and coach others Outstanding stakeholder management skills to establish and maintain strong working relationships.	
Experience *This is the proven record of experience and achievement in a field, profession or specialism. This could include a minimum period of experience in a defined area of work if required by an external body (for example a period of post-qualification experience).*	Demonstrable experience across a wide range of Identity and Access Management technologies and services.	Experience of establishing sustainable Identity and Access Management programmes to meet regulatory or contractual requirements.

Core Accountabilities, Attributes and Behaviour Indicators

Appointees to this role will be required to adhere to and perform their duties in line with the standards identified in the States of Jersey tier 5 core accountabilities attributes and behaviour indicators.

The standards relevant to this tier, identified in the Government of Jersey core accountabilities, attributes, and behaviour indicators, are to be attached in a separate document.