# MOBIUS IDENTITY AND ACCESS GOVERNANCE FRAMEWORK

Controlling access to information in order to grant the right person the right level of access to information at the right time has become one of the most important initiatives within organisations are extending their operations and user base and must ensure efficient management of user identities and access. In addition, audit and regulatory requirements continue to expand and penalties for non-compliance are substantial.

The common term associated with the management of user profiles and related system access is Identity and Access Governance (IAG). IAG can be defined as a framework for business processes and technology that facilitates the management of electronic identities to enable the initiation, capturing, recording and management of user identities and their related access permissions in an controlled and auditable manner. This ensures that access privileges are granted according to a single interpretation of policy and all individuals and services are properly authenticated, authorised and audited.

The Mobius Consulting approach to IAG is focused on helping clients reduce the costs of their operations and improve efficiency, risk management and security and is closely aligned to global best practices such as COBIT and ITIL. The Mobius Consulting IAG framework recognises that IAG occurs at a strategic / design level which is driven from a top-down approach (these governance and compliance elements are reflected as the orange base in the diagram alongside) as well as on a day to- day basis within the IT and Business Operations themselves (these management and operational processes are reflected as the grey wedges in the diagram alongside).

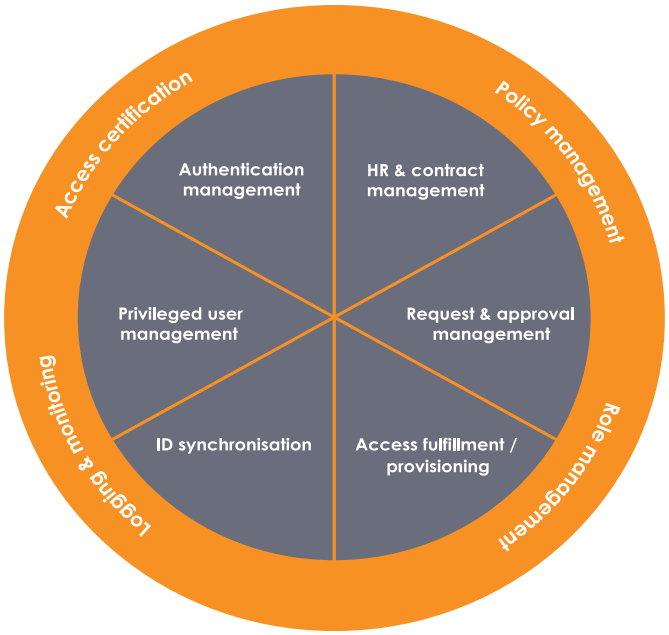


*Figure 1: The Mobius Consulting IAG framework*

THE TABLE TO FOLLOW PROVIDES A BRIEF DESCRIPTION FOR EACH OF THE IAG CAPABILITIES OUTLINED ABOVE.

For more information, contact Mobius Consulting on +27 21 20 111 20 or +27 10 590 6111
email info@mobiusconsulting.co.za or visit our website www.mobiusconsulting.co.za

| | |
|---|---|
| **Governance and compliance** | |
| Policy management | The process of documenting, approving, reviewing and communicating policies relating to Identity and Access Governance. |
| Role management | The process of managing system roles from designing and configuring the roles to maintaining and certifying (reviewing) the roles on an on-going basis. System roles should be designed in line with enterprise job roles and should be based on minimum access principles. To ensure appropriate segregation of duties, no user should have access to perform a process from end-to-end. |
| Access certification | The process of reviewing users and their roles and/or access rights on a regular basis to ensure that they remain appropriate. |
| Logging and monitoring | The process of logging and reviewing security events on a regular basis to ensure that suspicious events are detected and remediated in a timely manner. |
| **Identity management and provisioning** | |
| Human Resource and contract management | The process of on boarding and off boarding an individual (employee / contractor / third party) through an approved process. This includes the creation of an individual's digital identity, modification of an individual's status upon transfer, promotion or demotion as well as the termination of an individual's digital identity upon leaving the organisation. |
| Request and approval management | The process of requesting and approving user access to a system resource. Requesting access can occur via a number of mediums / channels. The function of approving access should be restricted to business owners. |
| Access fulfilment / provisioning | The process of creating a user account on a target system, assigning access rights or removing / disabling access rights or a user account. |
| ID synchronisation | The process of disseminating identity and access related data between authoritative sources and target systems. |
| Privileged user management | The process of managing privileged user accounts (accounts that have full access and authorisations or elevated privileges) across IT systems, applications and infrastructure. |
| **Access management** | |
| Authentication management | The process of verifying a digital identity that is attempting to access a system resource using a set of credentials. |