MOBIUS APPROACH TO IDENTITY AND ACCESS GOVERNANCE STRATEGY / BUSINESS CASE DEVELOPMENT

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 today. In order to achieve strategic goals such as increasing market share and profitability, businesses 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 one interpretation of policy and all individuals and services are properly authenticated, authorized and audited.

Some of the best practices for IAG include:

• Access rights to IT systems and resources should be granted only in accordance to a person's exact needs as defined by their business job description or their role(s) in the organization.
• Companies should be able to confirm that only authorized users have access to sensitive information and systems.
• Common business process constraints, including such measures as separation of duties, should be enforced.
• Periodic assessments of access rights and privileges should be performed.

The consequences of poor Identity and Access Governance include:

• Poor alignment of authentication and authorization to business and IT goals
• Labour intensive and inefficient manual processes
• Regulatory non-compliance
• Lack of accountability
• Sub-optimal controls
• Incomplete audit trails

One of the most important aspects of the initial phase of implementing IAG within an organisation is the development of a strategy / business case. This strategy / business case should provide an analysis of the potential benefits of an IAG solution within the organisation and ensure that the implementation impacts and risks relevant to the organisation are adequately considered. This strategy / business case can also serve as

the baseline to gauge progress for the IAG project.

The diagram below outlines the key steps to be followed when developing an IAG strategy / business case:

| 1. Establish guiding principles | 2. Determine current state | 3. Determine drivers for change | 4. IAM capability maturity assessment | 5. Determine benefits and impact | 6. Prioritisation and roadmap |

Figure 2: The Mobius Consulting approach to develop an IAG strategy & business case

Step	Description
1. Establish guiding principles	Define the organisation's guiding principles for the scope of IAG as well as principles relating to the people, process and technology aspects.

2. Determine current state	• IAG building blocks – the people, process and technology aspects of the current state of the IAG within an organization should be understood at a high level, including:
	  • Users (e.g. employees, customers, contractors; vendors; partners)
	  • Applications and related technology (e.g. key applications, databases, operating systems, servers, network, etc.)
	  • IAG processes (e.g. administration, identity, access, provisioning)
	  • Monitoring processes and technology (e.g. logging, monitoring, reporting, auditing)
	• Stakeholders - In order to ensure business buy-in it is important to identify who the key stakeholders are and to assess the following key aspects - Why stakeholders may resist; Why stakeholders will cooperate; and how to approach stakeholders in order to avoid resistance and improve cooperation.

3. Determine drivers for change	The following are key points that provide a complete picture when assessing business drivers for implementing IAG: • Enabling business drivers • Regulatory compliance (e.g. Basel II, anti-money laundering, Protection of Private Information, etc.) • Risk management (e.g. security risk and fraud risk) • Process improvement (e.g. business process improvement and administrative process improvement) • Technology improvement
4. IAG capability maturity assessment	Each of the elements (and the components of each) of the Mobius Consulting IAG framework should be assessed for current state capability maturity and the "desired" future state of IAG should be determined. The gap between the current and desired states gives an indication of the changes required.
5. Determine benefits and impact	No business will embark on an initiative unless benefits can be realized in the short and/or long term, it is therefore important to highlight what benefits the business will achieve in implementing IAG within the organization. These business benefits should be linked to the drivers for change identified in step 3. *Note – our approach does not include quantification of the financial benefits by means of creating an IAG financial model in order to explain the cost of avoidance and the Return on Investment (ROI). This can be added if required.* IAG impacts a number of areas within an organization, it is therefore important to ensure that the benefits identified address any shortcomings that the organization may be experiencing, including business facilitation, cost containment, operational efficiency, risk management, user satisfaction and regulatory compliance.
6. Prioritisation and high-level roadmap	The results of the assessment should be analysed to determine the key tasks and projects necessary to achieve the desired state for IAG within the organisation. These tasks and projects should be defined as strategic, tactical or operational and the priority of, and dependencies between, each should be established. This will enable the development of a high-level implementation roadmap for inclusion in the business case.