IDENTITY ACCESS MANAGEMENT AND GOVERNANCE SIMPLIFIED

Identity Access Management and Governance (IAMG) is a mouth full.
In fact, just saying it out loud can be daunting, but it really isn't rocket science.

So, what is IAMG all about? Put simply – it is how you manage who has access to what in the organisation, from a physical and system access point of view, based on the individual's role. Sounds straightforward? And, in principle it is, but there are a number of complexities that an organisations needs to have a grip on so that IAMG is implemented and managed correctly.

Firstly, an organisation needs to address the data clean-up process. This begins with understanding the system landscape, existing access processes, legacy system challenges. A large part of this process is also reviewing the system roles, aligning them to the business roles and creating profiles for access.

Knowing the elements for granting, updating and revoking access in the organisation, is imperative for management. Since people are not static, management needs to formalise and communicate the access processes for new employees, movers within the organisation and employees that leave the organisation. This is largely to prevent access cloning and reducing the risk of people keeping their system access and rights when no longer required. If not managed correctly, this can lead to fraudulent activities.

Once the clean-up has been completed the technology solution can become the focus area. During the data clean up and role profiling exercises, management will become embedded in the project and get a much better understanding of the type of technology solution that would best fit the organisations' requirements. This is why it's important to not make a premature decision on the solution early on in the process.

Once the organisation has worked with a technology partner to implement a solution, the business should be equipped and able to manage the processes in the future.