BIZMOD

IMPLEMENTING IAMG IN YOUR ORGANISATION

Taking the decision to implement an Identity Access Management and Governance (IAMG) project is the first step in tackling IAMG challenges within the organisation.

Creating a dedicated project team is critical to the success of the project, as internal access management teams rarely have the capacity and expertise to manage this project on their own. That said, the project team must work closely with the access management team and the IT security department to ensure success.

THERE ARE FIVE KEY CONSIDERATIONS FOR ADDRESSING AN IAMG PROJECT:

1. Structure the project around identity, physical and system access:

An IAMG project is complex. An organisation needs to look at physical, identity and system access when assessing its' IAMG requirements. This will include system roles, segregation of duties and revoking of excess access. The COBIT 5 methodology and ISO 9001 standards should form the basis for governance and set the standard for which the IAMG project can be measured against.

The technical side is not the only element of the project, in fact it is the easiest part. A holistic approach needs to be taken, that includes assessing data, processes, technology, and most importantly, employees, as their adoption will ensure success.

2. Implement a data clean-up:

Before implementing a technology solution, a data clean-up is required. Declutter the system roles and prioritise what access is appropriate for the various roles. System roles need to be aligned to the business roles and as a business an understanding and justification for entitlements granted to certain roles.

In addition, legacy systems often create another level of complexity because systems don't talk to each other and access is not always linked to the users' identity, making it difficult to identify and control what other access rights a user may have. Therefore an understanding of the system landscape is vital.

3. Apply a phased approach:

A phased approach is recommended as opposed to a "big bang" outlook. The data needs to be repaired without detrimental effects to the business process. This takes time as there are intricacies involved, which if not understood correctly can harm the day-to-day functioning of the business. Blindly revoking user access could be disastrous.

4. Work with a reputable technology partner:

After completing the data clean up, having an understanding of the system landscape and how access rights are structured the next step is to appoint a technology partner. A reputable partner that will understand the landscape and provide a solution that fits the organisation.

5. Get all stakeholders involved and on board :

It is the people within the organisation that will ensure the project success ultimately. Therefore lastly and most importantly, a solid change management programme is required to ensure that everyone is on board – technical teams and actual users (the managers who grant access). User resistance will impact the project success, so employees need to understand the logic, purpose and systematic approach.