ideiio

2020 | Whitepaper | v1.0

Identity Governance and Administration Maturity Model.

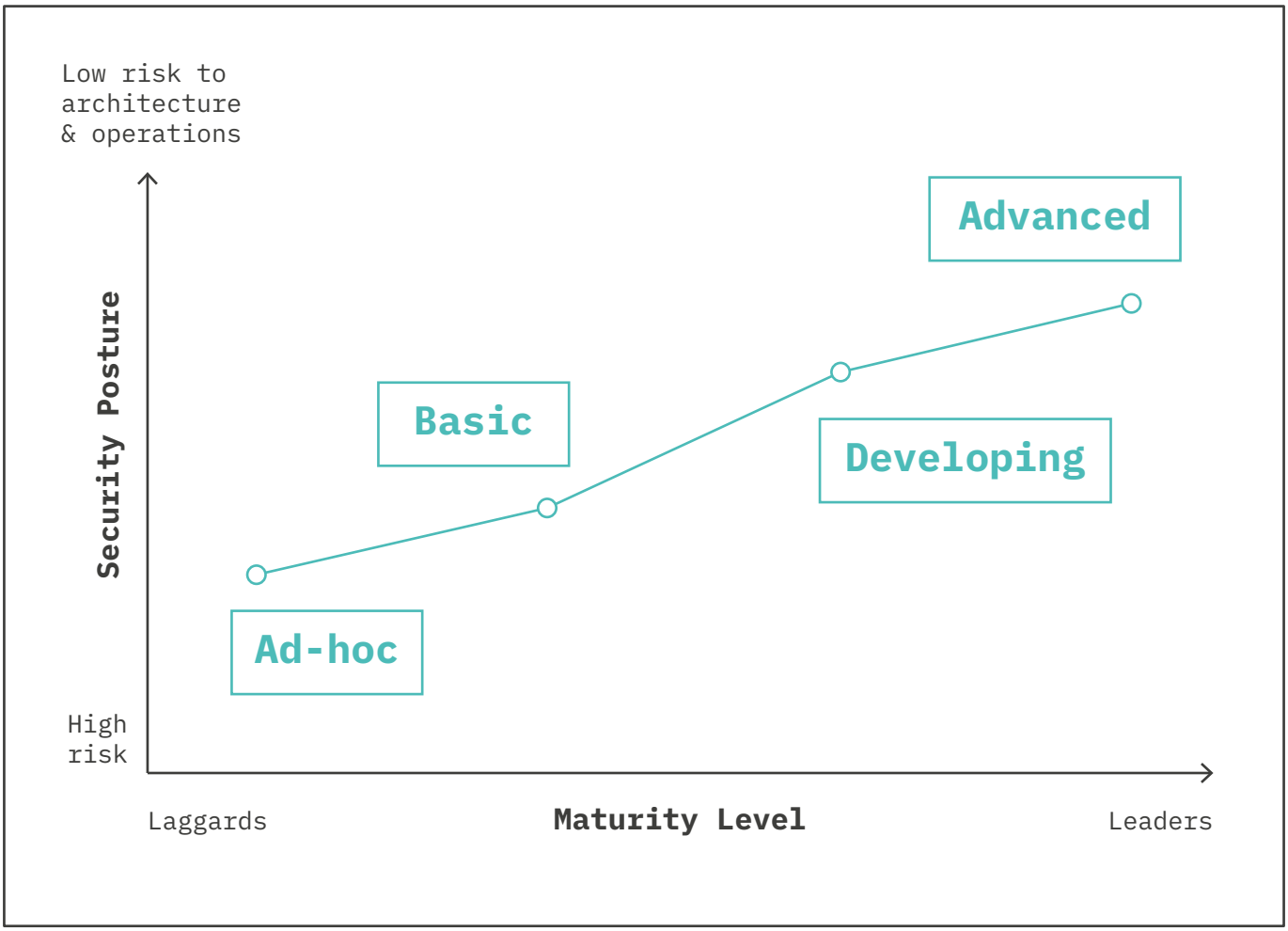
The IGA Maturity Model.

The ideiio Identity Governance and Administration (IGA) maturity model presents a roadmap for your identity management journey.

The four phases show the evolving maturity levels organisations go through on their way to reaching the advanced level.

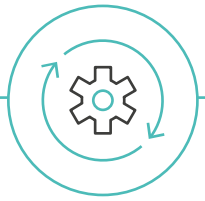
Identity Governance Administration (IGA) provides the foundation for identity management, allowing organisations to ensure that processes are in place to validate and certify user access levels and requests, so users are only granted the minimum access they need to carry out their role. Without having IGA in place, organisations face a real security risk that users may gain blanket access to all applications which is accumulated over their tenure.

Our maturity model provides an insight to where you are in your IGA journey and highlights the steps you need to take to grow, allowing you to evaluate risks and determine priorities.



Ad-hoc

- Not driven by authoritative data
- No automation of provisioning to connected applications
- No defined Role Based Access Control (RBAC) model
- Driven by spreadsheets and/or helpdesk tickets
- No governance (approval workflows or certification)
- No automated disablement of accounts



Basic

- Driven by authoritative data, but not synchronised
- Semi-automated provisioning via IT Service Management (ITSM) workflow for core applications
- Limited role and access rules
- Certification via spreadsheets or other paper-based system
- Semi-automated disabling of access via ITSM workflow

Developing

- Identity lifecycle driven by authoritative data
- Automatic sync of identity data from the authoritative source
- Automated provisioning to core applications
- Semi-automated provisioning via ITSM for all non-core applications
- Defined RBAC model
- Approvals workflows for core applications
- Automated disablement of access for core applications

Advanced

- Automated provisioning to all applications
- Full coverage across cloud and legacy, on-premise applications
- Self-service capabilities for end-users
- Approvals workflows for on-demand access requests
- Certification campaigns
- Micro-certification for external users
- Forensic audit trail
- Support for multiple lifecycles and user types
- Access and governance reporting and analytics

Ad-hoc

Organisations that are in the Ad-hoc phase of IGA maturity have a high degree of risk. Processes are primarily manual with no authoritative data source or defined RBAC model. Managed by spreadsheets and helpdesk tickets, tasks are burdensome, often lengthy and at risk of human error or abuse with further risks when users leave the organisation and their access needs to be revoked.

Basic

When organisations progress to the basic stage of IGA maturity, they are driven by authoritative data and have semi-automated provisioning via ITSM workflows for core applications. These organisations have limited role and access rules in place and carry out certification via spreadsheets or other paper based, manual systems. Disabling user access is semi-automated via ITSM workflows.

Developing

As organisations move into the developing phase of IGA maturity, identity lifecycles are driven by authoritative data, with automatic sync of the data identity from the authoritative source. This in turn automates provisioning to core applications, with semi-automated provisioning to non-core applications via ITSM. These organisations have a defined RBAC model and approvals workflow for their core applications with automated disablement or access to these applications when a user is no longer in need of or authorised to access them.

Advanced

Organisations that achieve the advanced stage of IGA maturity have automated provisioning across all applications, whether cloud, legacy or on-premise. Their users have self service capability to review their identity, request access and reset passwords. Access requests follow an approval workflow to meet with on-demand requests. Access can be reviewed through certification campaigns or micro-certification campaigns for external users. With this level of governance organisations have a forensic audit trail of who has access to what, at what level and who granted that access and why. Advanced organisations are able to support multiple lifecycles and user types across their estate regardless of being employee, affiliate or external.

Case Studies.

For a global car rental company with multiple franchises across 174 countries, managing identities for staff and affiliates was a mammoth task. In a franchise outlet staff turnover is fluid making a central management system even more of a challenge, with multiple authoritative sources. User provisioning could take a number of weeks, by which time the individual in question could have left or changed role, creating even more work to provision further access or deprovision altogether. Governance and certification had been carried out primarily through spreadsheets. The company was at a basic level of identity governance.

Following the implementation of ideiio, user lifecycle management was automated across franchise outlets, which with delegated administration means that individual business unit owners could manage the identities within their franchise, approving and revoking access governed by central access policies and workflow. With self service capabilities, individuals are now able to take responsibility for their own identities and access requests. The company's ability to provide full identity governance and administration at a global level has been transformed, and they are now operating at the advanced level of identity governance and administration.

A US credit union with multiple financial regulations to adhere to had been managing identity lifecycles and governance through a number of methods including spreadsheets, with some automation for provisioning. This was a basic level of identity governance.

By implementing ideiio they were able to fully automate provisioning and deprovisioning of users into on-premise and cloud applications based on their roles and fine-grained entitlements. Department and application managers are able to run campaigns to review access and extend or remediate as needed, reducing security risks such as accumulated access throughout the identity lifecycle. All governance and compliance audits can be run, managed and exported into user readable formats with ease, allowing the credit union to prove to its auditors satisfaction that it was operating at an advanced level of identity governance and administration.

ideiio
intuitive identity

About ideiio

We are industry experts who have come together with the bright idea of making identity lifecycle management simpler for our customers.

For more information:

hello@ideiio.com
ideiio.com

EMEA & APAC

8 Exchange Quay
Manchester M5 3EQ, UK

t. +44 (0)161 204 7788

North & Latin America

1755 Teslar Drive, Suite 206,
Colorado Springs CO 80920, US

t. +1 719 453 1067