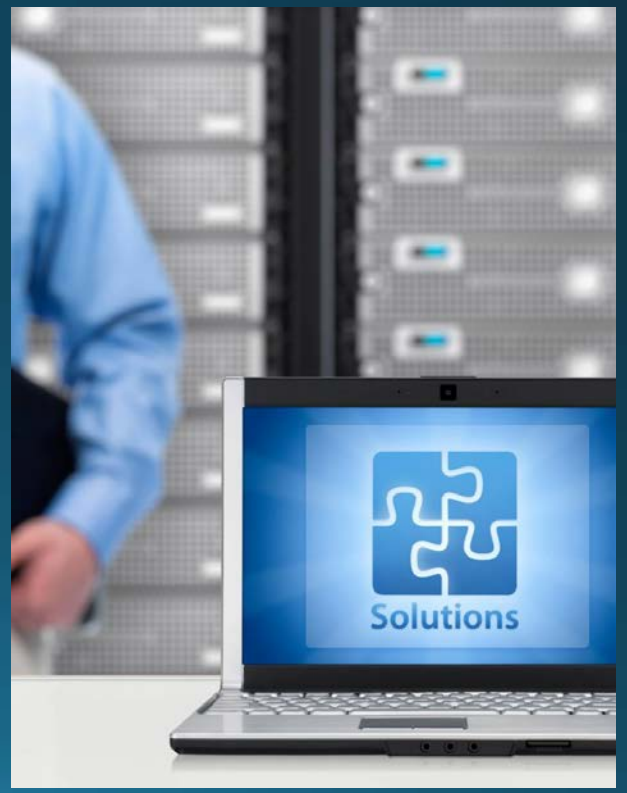
Identity and Access Management

Using Identity Management and Identity Governance to increase Automation and Security.

About Skyline

Established in 2004, Skyline Technology Solutions is an IT solutions provider specializing in delivering end-to-end IT consulting and solutions for the Commercial, State and Local Government and Education sectors. We partner with our customers to address their business needs by fully understanding their challenges and requirements.



Identity Management (IAM, IdM) – defining and managing the roles and access privileges of individual network users, and the circumstances in which those privileges are applied. **The core objective of IdM systems is one identity per individual.**

Identity Governance (IGA, IAG) – Policy-based identity management and access control across multiple systems and applications.

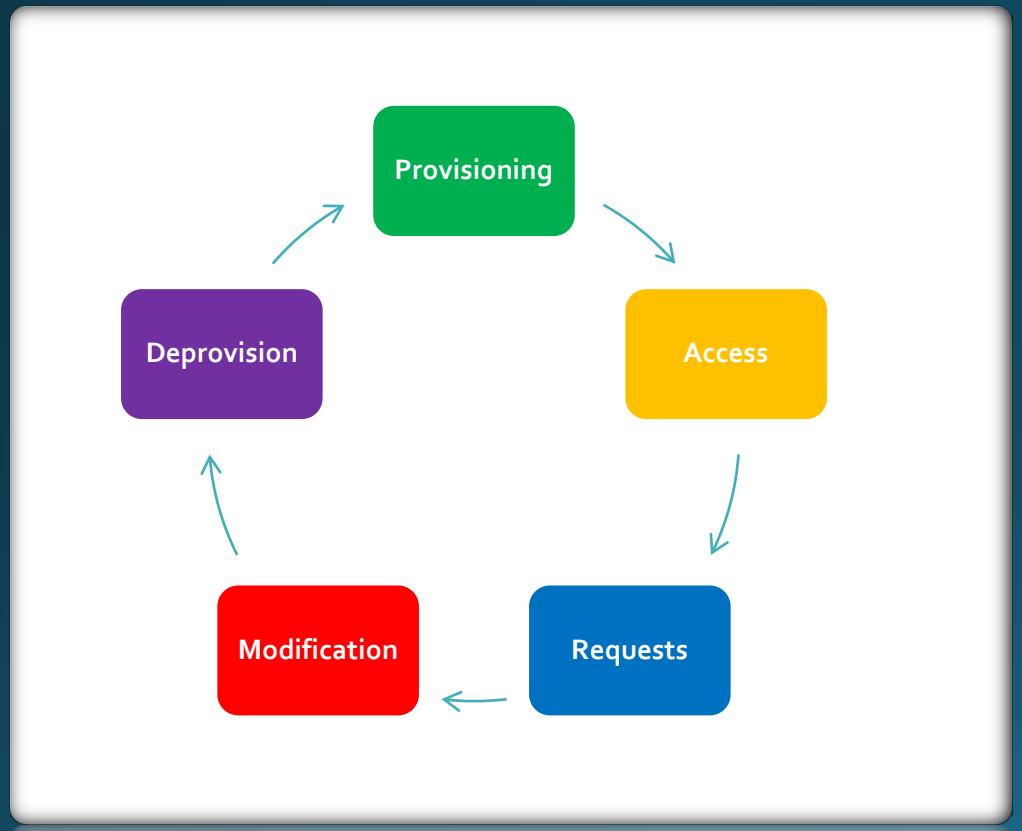
Identity Provider - Provides and asserts identity to external systems and applications

Lifecycle Management – creating, managing, coordinating and restricting the identification, access and governance of identities for access to business tools and information Authentication and Authorization.

Single Sign-on and Multi-Factor Authentication (SSO/MFA) – Often seen together, these two extensions of the IDM ecosystem allow users to access many applications securely signing in once with two or more factor authentication.

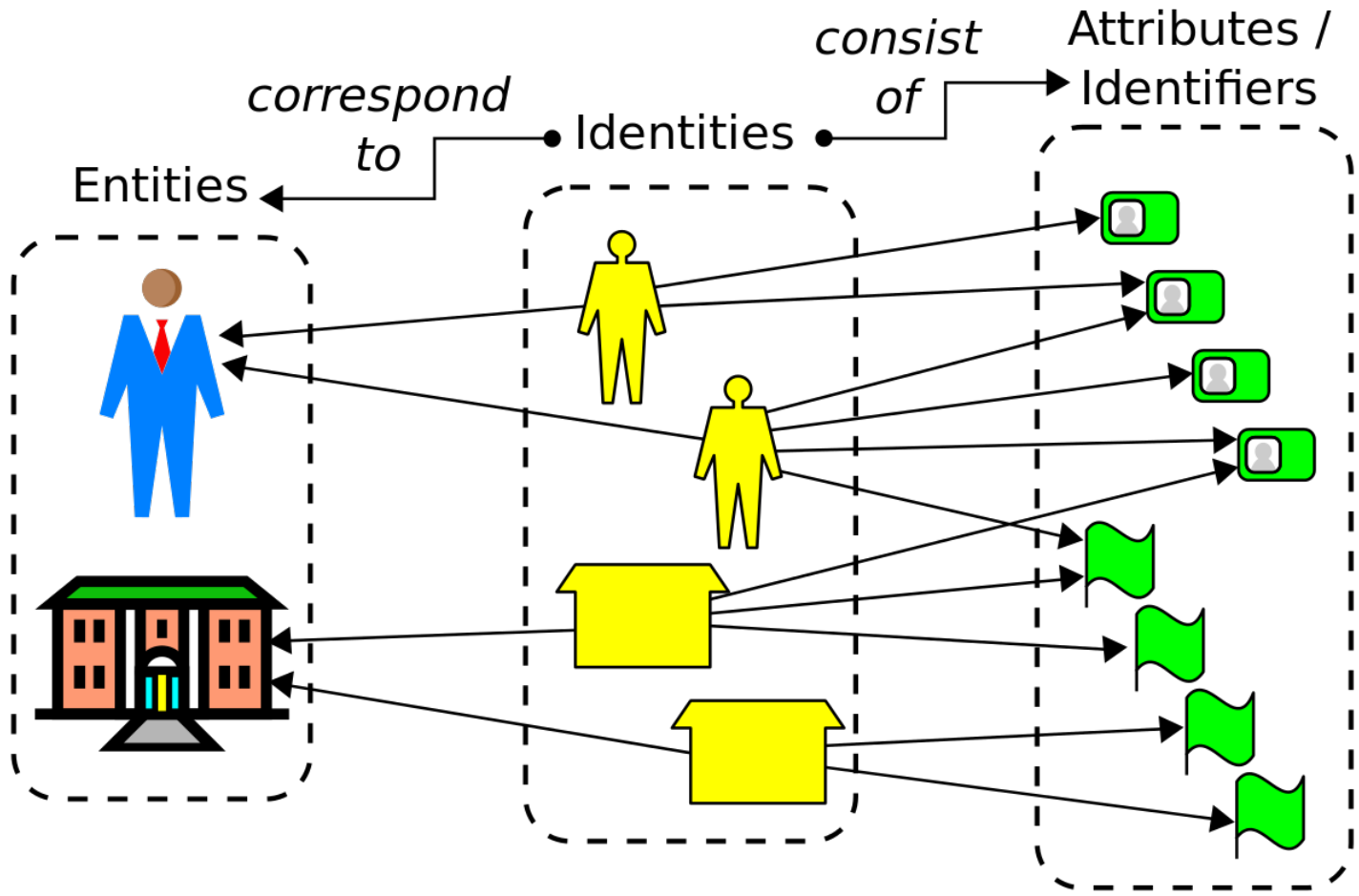
Authorization Standards – SSO typically uses these standards during the authentication process : SAML, OAuth, OpenID, WS-Fed

What Are the Benefits of IAM?



- Lifecycle management greatly simplifies demands on IT and increases user productivity.
- Users can perform self-service password resets.
- Users can be provisioned once and granted access to every application they need.
- Disabling a user in one place will remove access to all applications and reclaim all licenses.
- Customers can provide and limit access for vendors and contractors.
- The helpdesk sees substantially fewer tickets for password resets and access requests.
- Companies are able to deploy new applications faster and with fewer user support issues.
- Security features enable greater regulation compliance and reduced audit time and cost.
- Privileged Access management
- Multiple levels of approval

Identity Management (more) Defined

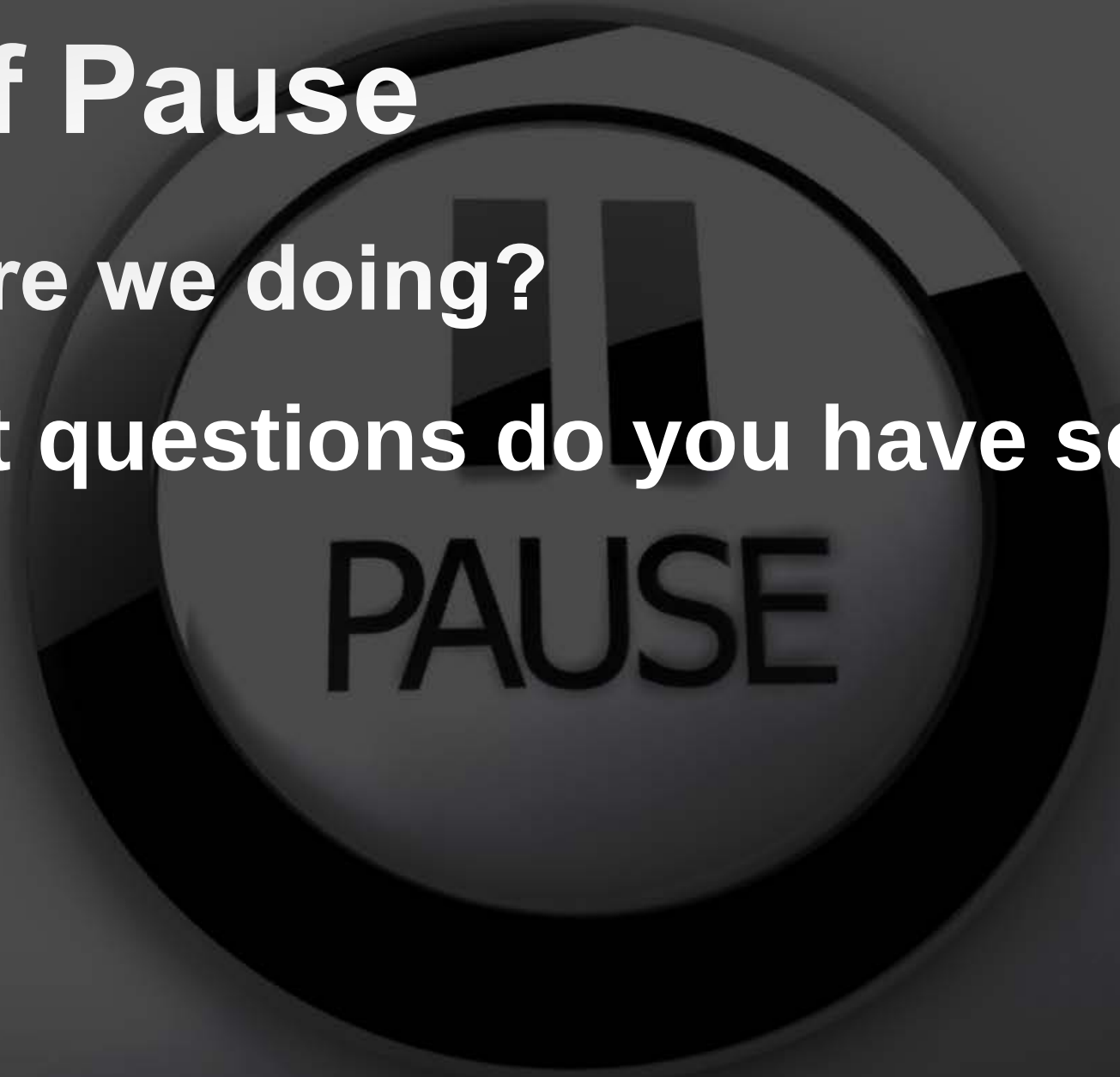


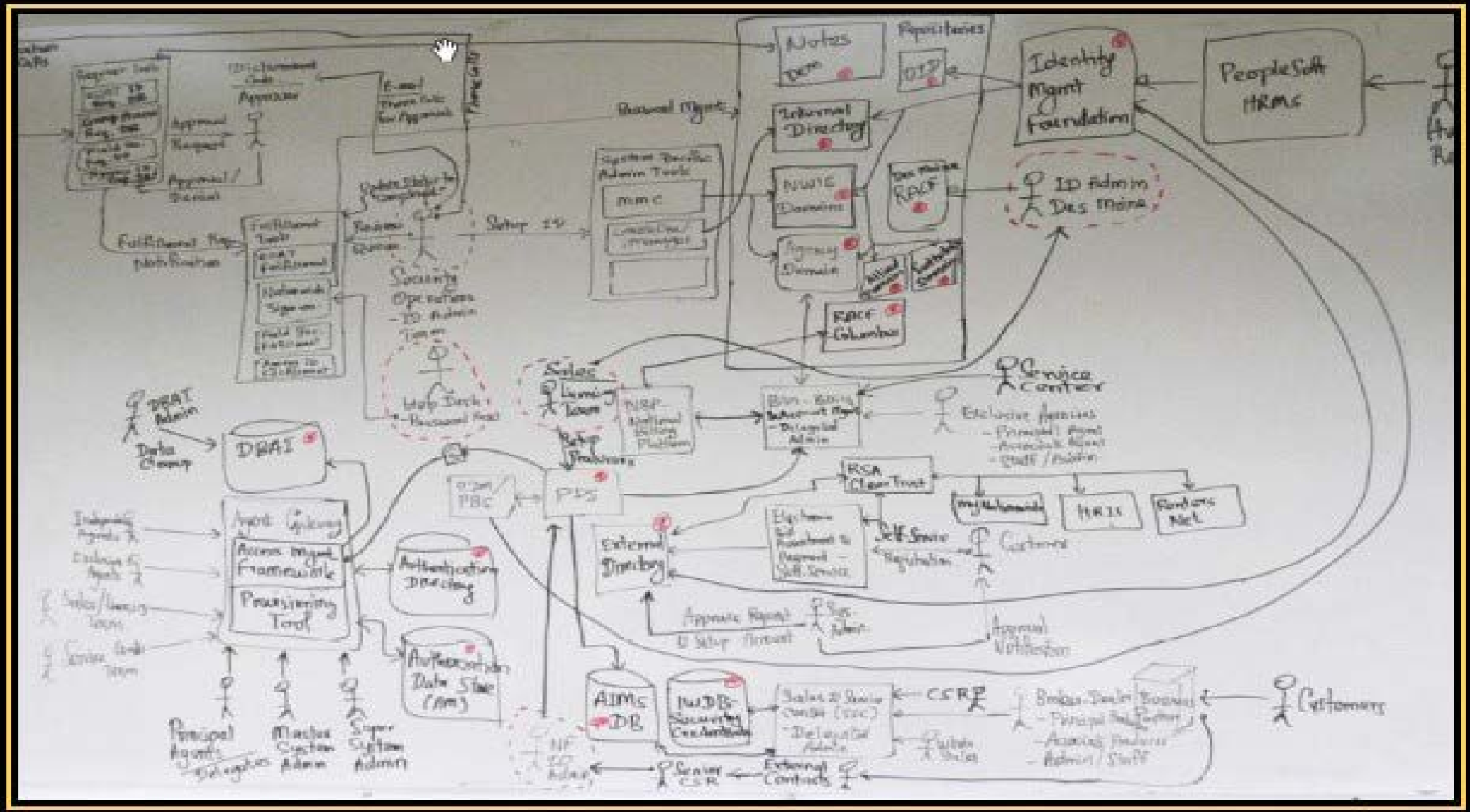
IDM – management of the lifecycle of individual accounts within an organization.

This can encompass anything from a login, workstation, email address, student or teacher application, applying to staff, students, parents which require access to resources provided by the organization.

A Brief Pause

- How are we doing?
  - What questions do you have so far?



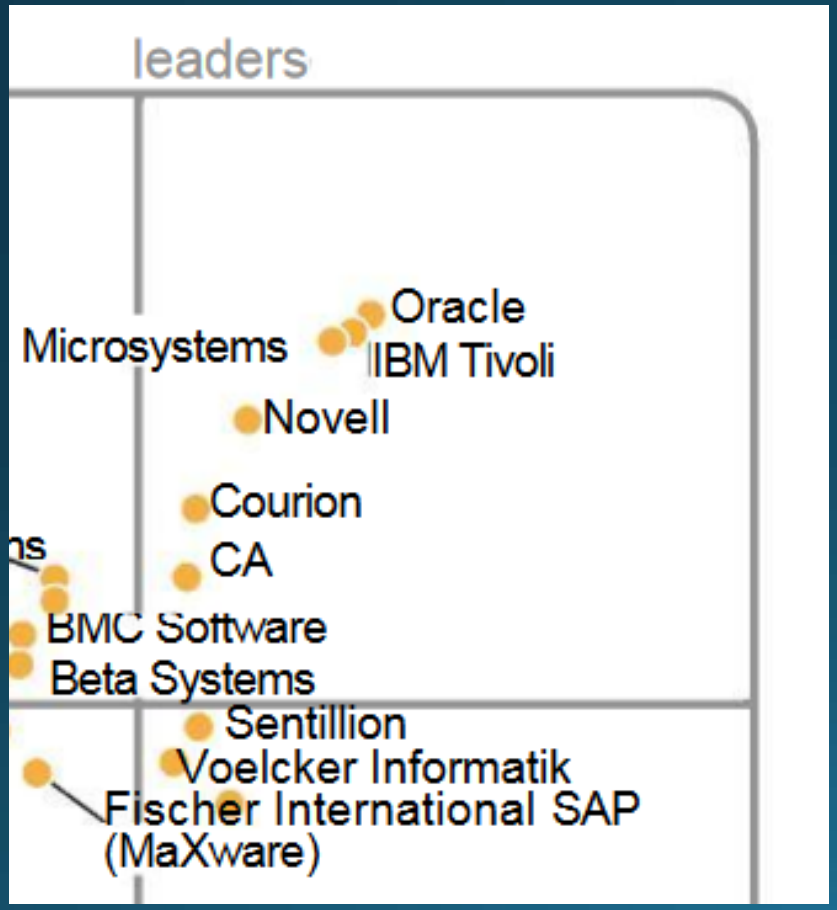


IDENTITY MANAGEMENT

Challenges of Identity Management

- Changing users and user roles
- Users coming from multiple sources
- A BYOD environment and/or users with multiple devices
- Successfully designing and implementing a solution
- Cost!
- Complexity – multiple environments, external users, etc.
- Choosing the right vendor(s) to meet your requirements

Identity Management Vendors August 2008 to June 2017



IGA Vendors


LEADERS
SailPoint
mada
One Identity
Oracle
IBM
(NetIQ)
Saviynt
CA Technologies
Dell Technologies (RSA)

How Does IAM Increase Security?

- Centrally Controlled Access
- Increased Awareness and reporting
- Single Execution point for all access requests for on premise and cloud applications
- Streamlined workflows and approval processes
- Single Action to remove all access

IdM and IGA

What are the differences?

IdM is the set of technical components and policies that enable a single identity per user. Reading information from one or more sources and utilizing business rules to modify or provision accounts in one or more destinations.

IGA is the controls, framework and policies that are utilized to create identities and assign fine grained access to and within applications. As well as correlate, compare and enforce these with compliance requirements.

Q&A

Thank you for attending!