Aurora

Identity Lifecycle Management

For EM&S

Public

Active Directory Challenges

Administration

Native tool limitations and reliance on manual processes create inefficiency

The hybrid AD environment requires separate tools for AD and AAD

Reliance on manual processes facilitate errors causing security gaps and user dissatisfaction

Security

Security suffers as the AD/AAD Admin accounts have unchecked power

It is difficult to universally enforce security as there is no single source of admin control in the hybrid AD environment

No individual accountability for AD/AAD Admin activity elevates risk

IAM

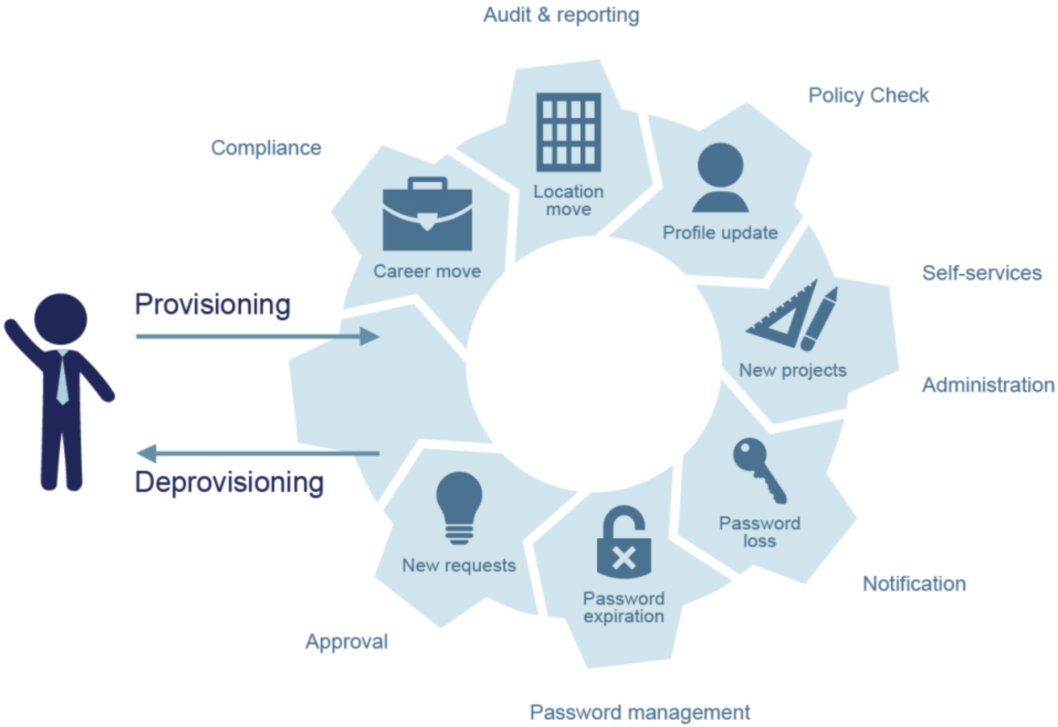
Disjointed and manual user and group management results in inefficiency and heightened risk

Errors present in AD propagate to AAD exacerbating security issues

Narrow scope of Azure-based IAM limits organizations to a Microsoft-only environment

What is Identity Lifecycle Management?

Create, maintain, modify and monitor identities for the duration of a user ’s lifecycle



Public

Why do I need Identity Lifecycle Management?

Identity issues cause problems for both your users and your IT department, ultimately leading to inefficiencies and lost cash for your business

Your users:

- Use the same password for multiple applications and never change them
- Manage passwords in spreadsheets or on sticky notes
- Can still access your data after they no longer work for you
- Forget user names and passwords on a daily basis
- Share and never change passwords for applications like Twitter and LinkedIn
- Want – 1 password for everything
- Want – Self Service for more of their IT, like password resets and changing phone numbers

Your IT department:

- Is burdened with password-related support
- Has zero insight into application usage and security
- Cannot enforce security policies in the cloud
- Lacks proper reporting tools to ensure compliance
- Struggles with integrating your directory infrastructure with the cloud
- Fails to re-harvesting your Office365 licenses
- Fail to disable user accounts when someone leaves

Why Aurora by Core?

Take control of your systems and users, providing quick and easy access to the things they need, but not the things they don’t

Savings

- ☑ Fully managed SaaS or PaaS options
- ☑ Quick time to value, average 3 week implementation
- ☑ Manage AD and Azure AD from 1 web portal
- ☑ Automated user creation from HR systems
- ☑ Policy based user provisioning and de-provisioning
- ☑ Templated workflows ensure consistency
- ☑ Empower users with self-service portals
- ☑ Reduce cost through automation license harvesting
- ☑ Built for Microsoft Enterprise Mobility & Security Suite

Compliance

- ☑ Identity vault for single authoritative identity
- ☑ Role based access control to AD and Azure AD
- ☑ Improved regulatory compliance – GDPR, PCI-DSS
- ☑ Reduced information security risk
- ☑ Audit trail of activities and accounts
- ☑ Maintain directory hygiene
- ☑ SLA backed uptime