Azure Active Directory Assessment

Azure AD is an integral part of any Azure tenant setup. The initial setup barrier to use Azure AD is low and AADC helps to setup provisioning accounts to Azure AD quickly. This offer is ideal for customers that want to consolidate grown Identity and Access Management/MFA solutions to reach a best of breed approach for Azure AD infrastructure and Azure AD principles.

But once Azure AD is setup, you might be interested in doing more, to maximize the benefit for your organization:

- You might have existing 3rd party Access Management solutions / Identity Providers in place with probably lots of integrated applications.
- You might have other 3rd party MFA solutions and a VPN solution in place.
- You might have third party user stores in place.
- You might now run 2 worlds in parallel: A fresh AAD-centered Microsoft365 application world with guest processes in addition to a custom web portal based on a 3rd party B2B account solution.

All those topics will have overlapping identity and account management aspects and processes that you might want to further align and consolidate, to maximize business use and avoid unnecessary operation costs.

The service delivered by the offering is available in the languages English and German.

This offering provides you with an assessment, to

- assess your 3rd party IAM environment and processes
- determine the best applicability of the Azure AD features
- provide you with a sorted baseline for cost, timing, dos, and don'ts
- point out where custom implementations are advised or not advised
- successfully consolidate your grown complex IAM infrastructure and processes to a simpler and AAD-aware base
- fully integrate your AAD IAM into your existing landscape
- accelerate the Zero Trust Adaption.

With this, we want to make sure, you can make best use of the Azure AD features, to achieve your goals.

Terms, conditions, and pricing are custom to each engagement.

iC Consult is the world largest IAM expert for workforce and customer IAM with 25 years of experience in enterprise companies. We cover analysis, implementation, and managed service. We support and manage your Azure AD and migrations to Azure AD with our own experts and have extensive experience on Enterprise company level with all market relevant IAM solutions.

Ideally you have prepared in advance

Existing landscape

- What is the state of Azure AD rollout?
- What stakeholders and departments are currently involved?
- What other existing identity silos and interfaces are there that need to be considered in integration/migration scenarios?
- What aspects are there when migrating data from existing identity silos to the new service?
    - usernames
    - redundancy of accounts
    - identity concepts
- What existing portals and applications are there
- What regional and legal aspects regarding accounts need to be considered in your business?
- What authentication and authorization methods are in use in the existing solution?
- What user self-service management functions methods are used in the existing solution?
- What application owner self-service onboarding functions are already in use in the existing solution?

Target picture

- What workforce IAM use cases are there?
- What existing use cases overlap with Azure AD B2B guest accounts?
- What existing B2C/B2B use cases are there in running in parallel with Azure AD B2B processes?
- Which aspects in existing legacy infrastructure need special attention?

Service model expectations

- Which parts do you want to customize or manage inhouse?
- Which parts do you want to manage inhouse?
- Which parts do you want to get managed by a managed service offering?

Overview of the assessment

Align account provisioning and identity lifecycle

- providing a unified integrated IAM management concepts of all your Identities and Accounts in an AAD-conform way
- Unify IAM across AD, AAD and other user stores that you may want to keep
- Aligning AAD SSPR with existing self service solutions

Align auditing aspects

- AAD brings sophisticated password protection features and audit log. It would be a pity to only use that for the AAD silo, ignoring your other account stores.
- Aligning audit logs and 3rd party legacy password solutions to benefit from these AAD features

Align B2B partner management and account concepts

- AAD comes with a sophisticated cross-company guest concept that you should fully embrace and consider in existing B2B partner management processes. It would be sad, to end up having different unaligned partner account management processes.

Align group and application permission lifecycle processes

- Groups in AD, groups in AAD, groups in 3rd party user stores. Get to know, how to best use them in an AAD-aware target picture

Account storage aspects

- Custom extension attribute aspects
- What to store in Azure AD
- How to store custom things that go beyond the data model of Azure AD
- Permission aspects and token claims
- data management and usage aligned over AAD and your 3rd party silos
- Elegantly deal with cross-tenant and multi-tenant scenarios in AAD

Migration or integration of existing 3rd party user stores + MFA solutions

- Merging of regional silo accounts
- Migration aspects of existing MFA credentials and passwords
- Dealing with varying unique identifiers and existing regional account concepts

Migration and integration aspects of existing customer portals and applications

- SSO integrate 3rd party SSO-products that you want to keep as Identity provider or service provider, to maximize the user experience. We are experienced in the migration of very wide range of access management products and can sort it out for you, no matter if its agent-based, OIDC, SAML or WS-Fed.
- Migrating existing account databases and directories
- Dealing with regional account stores

- Handling different kind of login names
- Migrate applications, being aware of SSO-product specific adaptions
- How to smooth-run parallel migration scenarios, to minimize change risks

Embrace modern AAD Zero Trust Features for your AAD world and integrated 3rd party IdPs

- Make use of Azure AD managed devices beyond Azure and Microsoft365 in your enterprise use cases as a modern VPN replacement
- Making best use of Windows Hello for Business as modern password alternative
- CBA as modern authentication as modern password alternative for custom devices
- How to adapt legacy app usage policies to Conditional Access Policies of AAD

Overall IAM and Azure AD recommendations

- Based on your current situation, we can give you best practice recommendation based on our long term practical IAM project and AAD embracement projects.

Addressing open questions, concerns, or issues regarding Azure AD B2C aspects.

On request, iC Consult is able to provide you with further support offers for implementation or managed service of Azure AD and Entra solutions after the assessment phase.