Microsoft Identity & Access Management Assessment

Active Directory (AD) is the primary identity provider solution for 90 % of Global Fortune 1000. A large number of these organizations rely on on-premises Active Directory systems to synchronize their identities with Azure Active Directory. This integration enables them to establish a single, unified identity solution that streamlines access to applications and services.

Incident response investigations conducted by Mandiant (by Google) and Microsoft have revealed that the main cause of cybersecurity incidents related to Identity and Access Management (IAM) are attributed to misconfigurations within the hybrid identity model.

With our Microsoft Identity & Access Management Assessment you will be able to reap the full benefits and values of your Microsoft Identity Access Management (IAM) suite, uncover the said misconfigurations, and optimize your entire security landscape.

The nature of the Assessment

This Assessment takes into account your unique setting and assists your organization in comprehending and enhancing your Azure Active Directory (Azure AD) environment through an analysis of your existing cloud and/or hybrid Identity & Access Management implementation.

Our objective is to help you pinpoint and evaluate your Azure AD environment, delivering prompt insights and suggestions. The evaluation encompasses these areas:

• Identity Provisioning
• Identity Management
• Access Management
• Security, Governance, and Identity Monitoring

Assessment process

ANALYSIS
We define current state

We analyse your present Microsoft IAM implementation to get a clear understanding of its status and performance in relation to suggested best practices.
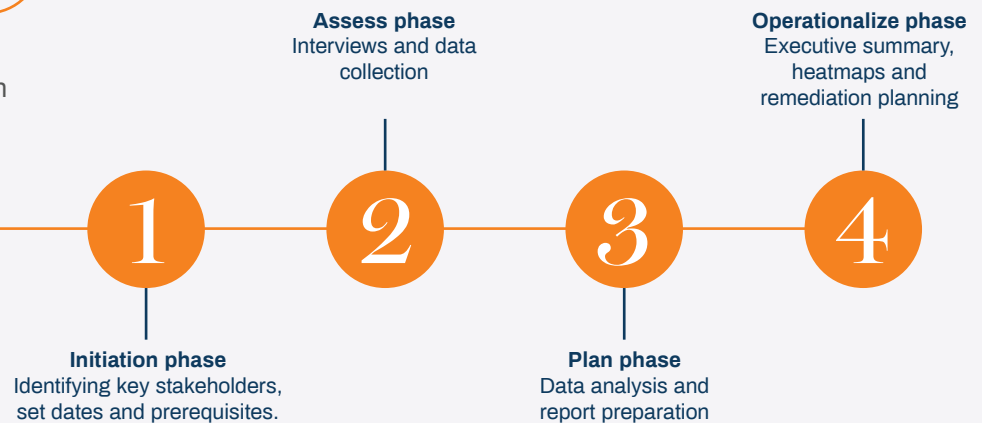
PLAN
We close the gap

We provide you with a detailed action plan, complete with a well-defined roadmap and milestones, to achieve Zero Trust for Identity.

Columbus

Assessment steps

The Assessment will happen in four steps as described on the roadmap.

Assess phase
Interviews and data collection

Operationalize phase
Executive summary, heatmaps and remediation planning

1   **2**   **3**   **4**

Initiation phase
Identifying key stakeholders, set dates and prerequisites.

Plan phase
Data analysis and report preparation

Assessment elements

Interviews and Data Collection may contain, but are not limited to the following Zero Trust and NIS2 areas:

- **Identity Management System**
- **Identity and Access Management** (incl. Identity Lifecycle and Entitlement management)
- **User Provisioning**
- **User Authentication**
- **Strong Authentication**
- **Credentials and Authentication** (incl. Credentials Management)
- **Trust Determination**
- **Access to Resources**
- **Least privilege** (Privileged Accounts, Auditing, Attestation)
- **Secure Administration**
- **Adaptive Access Control**

Recap on the value proposition of the Assessment

Our Microsoft Identity & Access Management Assessment provides you with these benefits:

CLARITY
High level executive presentation of the results and recommendations.

EXPERTISE TRANSFER
Detailed documentation of the findings with technical explanations.Tailored discussions about your current implementation in contrast with best practices

REMEDIATION
Clear plan of remediation accompanied by heatmaps for each area of the IAM implementation.

Remediation plan emphasizing both quick wins and strategic initiatives.

Columbus®

kontakt.dk@columbusglobal.com