ARMIS

MICROSOFT ENTRA IMPLEMENTATION SERVICES

IDENTITY FOUNDATION

MOVING BUSINESS THROUGH TECHNOLOGY

ENTRA SUITE SERVICES

PROOF OF CONCEPT

Designed to demonstrate the feasibility and potential benefits of Microsoft Entra Suite within a controlled environment.

IMPLEMENTATION SERVICES

Focuses on the full-scale deployment of Microsoft Entra Suite across the organization

IDENTITY FOUNDATION	IDENTITY GOVERNANCE	ADVANCED IDENTITY	IDENTITY GOVERNANCE AND REMOTE ACCESS	PRIVATE ACCESS
› Microsoft Entra ID P2	› Microsoft Entra ID Governane	› Microsoft Entra Suite › MDI	› Microsoft Entra Suite	› Microsoft Entra Private Access

Mod. IT_09-02

ENTRA SUITE SERVICES
IDENTITY FOUNDATION SCOPE

Microsoft Entra emphasizes identity and access management, ensuring that user access and privileges are managed efficiently and securely.

This advanced identity tool focuses on applications, networks, identities, and infrastructures, providing a seamless user authentication experience.

Within the scope of this engagement, we include the activation and configuration of Microsoft Entra, which will achieve the following objectives:

› Provisioning of a central repository with all identities of the client to enable effective access management to the organization's applications, including both cloud and on-premises applications.

› Identity governance that will provide the client with governance policies, such as role-based access management, enforcement of access attestation policies for applications, access segregation, and ensuring that the right people have access to the designated applications.

› Availability of automated workflows for access assignment based on predefined rules.

Mod. IT.09.02

ENTRA SUITE SERVICES

IDENTITY FOUNDATION SCOPE

The proposed services address the following use cases in identity management and access governance, which will be ensured through the execution of the activities identified on the next page, as well as in the overall project plan presented in the Project Approach chapter:

Identity lifecycle management, according to defined rules and process workflows, including:

› Identity provisioning, identity data updates, and identity deprovisioning.

› Implementation of provisioning rules and approval workflows for identity lifecycle management.

Implementation of identity synchronization and consolidation mechanisms:

› Integration with the client's HR repository.

› Synchronization of identities between AD and business applications to Microsoft Entra ID.

Implementation of access governance mechanisms, including entitlement management, access reviews, and self-service access governance.

Implementation of business application lifecycle governance (Up to 4 applications – 2 on premises and 2 cloud):

› Business application registration processes.

› Governance of access to business applications included in the access governance process.

Mod. IT_09.02

IDENTITY FOUNDATION SCOPE

IDENTITY FOUNDATION	ACCESS GOVERNANCE

IDENTITY FOUNDATION

› **HR Integration**:
  › API Inbound HR Integration;
    › Inbound provisioning mapping
    › Implement workflows from HR employees (account generation)
    › Automate HR Synchronization with Entra ID and Active Directory
  › Other Users Types Integration - External Users Provisioning;
  › User Lifecycle Governance- CRUD Policies implementation (internal and external users)

› **Users Attestation**:
  › Conditional Access - Terms of use attestation

› **Identity advanced Security**
  › Privileged identity management (PIM)
  › Create Risk-based Conditional Access policies (sign-in risk, user risk)
  › Create all device and application filters for Conditional Access
  › Identify Risky accounts and vulnerabilities

› **Base Accesses Management**:
  › Users License activation (from base kit of accesses);
  › Base Security groups initial accesses activation.

› **Training and Staging Environment**

› **Production & Go Live**

ACCESS GOVERNANCE

› **Entitlement Management**:
  › Applications Access Manual Profiles definition and creation
  › Administration Roles Profiles definition and creation
  › Catalogues creation and configuration

› **Self Service Access Governance**:
  › Application Delegation Governance;

› **Enterprise App Registration**
  › Application Governance Policies Creation & Applications provisioning;
  › **Non-AD connected applications** - Up to 2 on premises applications integration with automate provisioning and accesses processes;
  › **Non-Entra ID connected applications**: Up to 2 application integration with SCIM integration implementation with automate provisioning policies creation and accesses provisioning.

› **Training and Staging Environment**

› **Integration Tests**

› **Production & Go Live**

Mod. IT 09 02

ARMIS

IDENTITY FOUNDATION ENGAGEMENT APPROACH

Our approach to this engagement follows a phased implementation in three stages, as illustrated in the diagram below.

Each phase has a defined objective and scope, along with a set of deliverables and acceptance criteria.

This phased approach ensures a progressive rollout of functionalities throughout the project, rather than a single final delivery. Below are the objectives of each phase, highlighting key outcomes and associated acceptance criteria.

PHASE	GOAL AND SCOPE	DELIVERABLES	ACCEPTANCE CRITERIA
SOLUTION ANALYSES AND DESIGN	▪ Define project scope, objectives, and stakeholders. Establish governance structure and project plan. ▪ Understand the business requirements, compliance needs, and technical environment. ▪ Design the Identity Governance solution architecture that aligns with business and IT requirements.	▪ Solution design document, architecture diagrams, and integration strategy. ▪ Detailed project plan. ▪ Test plan document	▪ Sign-off on requirements documentation; ▪ Approval of solution design document, architecture diagrams, and integration strategy.
IDENTITY FOUNDATION	▪ Install and configure Microsoft Entra solutions to meet design specifications regarding user Lifecycle Governance, including HR integration; ▪ Configure Base Accesses Management processes;	▪ Successful installation and configuration of Microsoft Entra solutions as per design specifications. ▪ Project documentation, training sessions and materials.	▪ Acceptance tests successfully carried out as per design and technical specifications.
ACCESS GOVERNANCE	▪ Install and configure Microsoft Entra solutions to meet design specifications regarding access governance including Entitlement Management, Access Reviews, Self Service Access Governance and Application integration - Up to 4 applications – 2 on premises and 2 cloud	▪ Successful installation and configuration of Microsoft Entra solutions as per design specifications. ▪ Project documentation, training sessions and materials.	▪ Acceptance tests successfully carried out as per design and technical specifications.

Mod. IT_09-02

ARMISGROUP.COM

PT Porto, Lisbon | **BR** São Paulo, São José dos Campos | **UAE** Dubai | **USA** Miami, New York