Formula5

HIPAA

NIST National Institute of Standards and Technology

Entra ID Governance

The Way to Enhance Security on the Enterprise Level

Vision

The strategic partner for business acceleration powered by advanced technology and exceptionally talented people

Mission

The people-first company that builds strong relationships, provides expert guidance, breaks through technology boundaries, and challenges the limits so that our clients and our people can achieve beyond what is believed possible

- ✓ Experts in AI, Data, Identity and Security
- ✓ Azure MVPs and Certified Specialists
- ✓ 4 Partner Solution Designations and Advanced Specialization
- ✓ Eligible for Azure Innovate and AMM
- ✓ CPOR ready
- ✓ ECIF ready

More at: formula5.com/advanced-microsoft-partner/

Microsoft
Solutions Partner

Key Challenges with Identity Governance

PERMANENTLY ASSIGNED ROLES

MISSING CONDITIONAL ACCESS SETUP / POOR SETUP

ACCESS TO PROJECTS / GROUPS

ONBOARDING / MOVING / LEAVING PROCESS

YEARLY WHEEL OF REVIEWS

MANUAL WORK

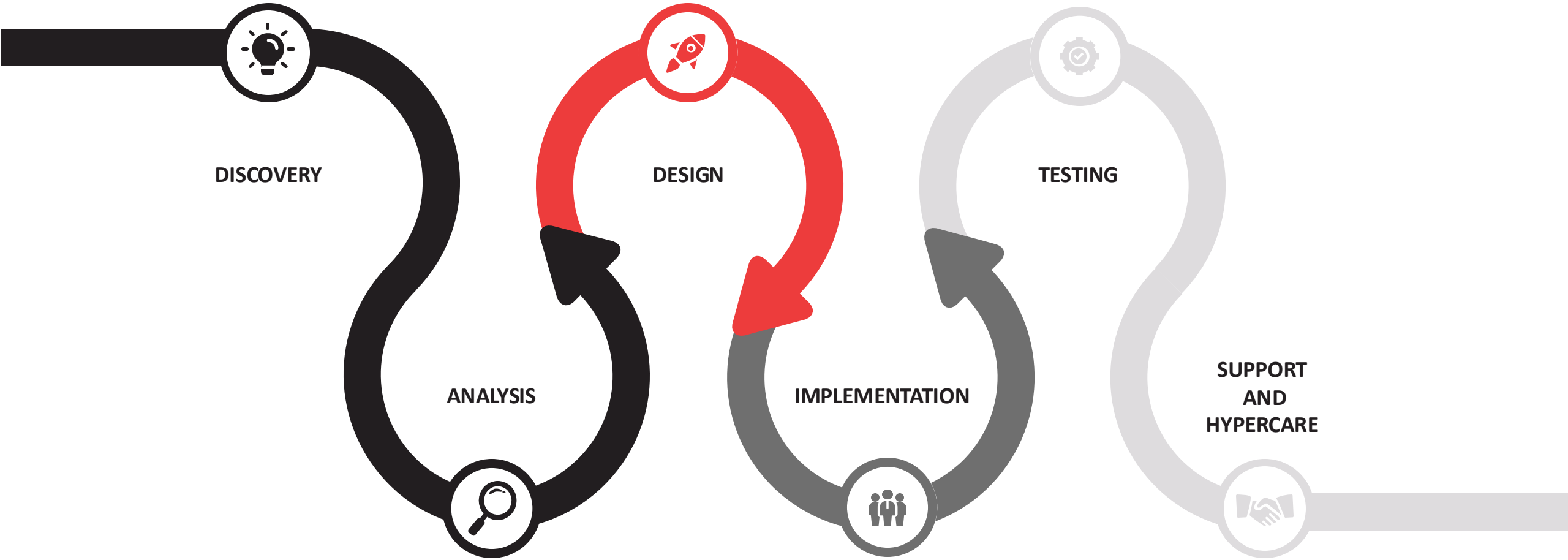
Our Aproach

Implementation using scripts and templates

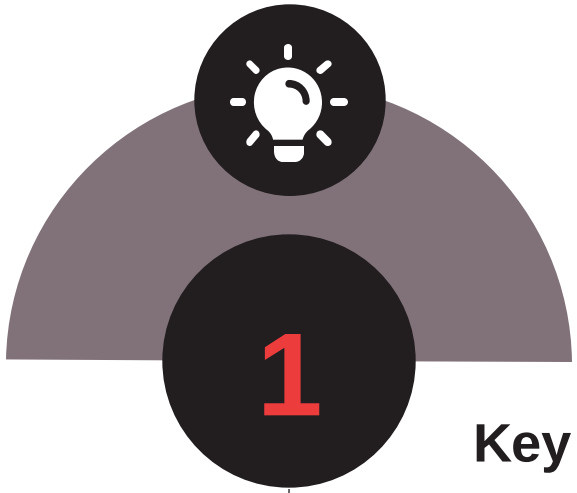
Automation using Azure DevOps

Modularized Governance configuration

Identity Governance Implementation Phases



Discovery



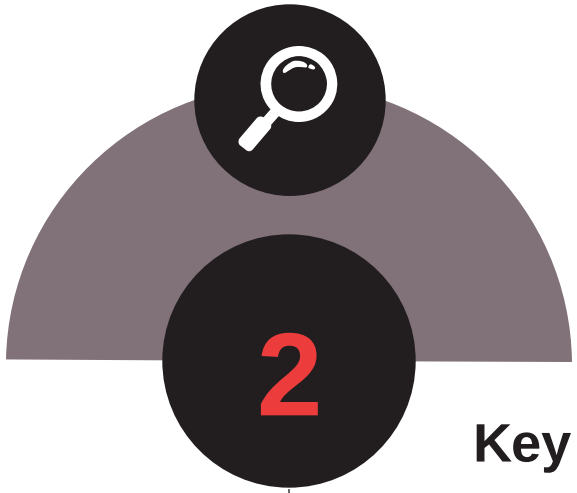
Key actions in this phase

- Conduct workshops to identify internal and external access requirements.
- Audit current Entra ID configurations according to **Zero Trust Framework**
- Identify governance needs, catalog requirements, and compliance expectations.
- Identify existing identity management solutions, access policies, and governance frameworks.
- Document user roles, groups, and permissions across systems.
- Gather stakeholder input to understand governance objectives

Key Deliverables

- Discovery report including access and governance needs.
- Requirements matrix for catalogs, access packages, reviews, and terms of use.

Analysis



Key actions in this phase

- Conduct workshops to identify internal and external access requirements.
- Audit current Entra ID configurations, user roles, and policies.
- Identify governance needs, catalog requirements, and compliance expectations.
- Compare current access controls with best practices in Entra ID Governance.
- Identify risks related to over-permissioned users, orphaned accounts, or lack of audit trails.
- Prioritize governance features such as access reviews, entitlement management, and separation of duties.
- Define key milestones and success metrics for the implementation phase.

Key Deliverables

- Examination of materials from the discovery phase
- Catalog of governance requirements
- Gaps identification and risks, such as over-permissioned users and orphaned accounts
- Milestones setup for Entra ID Governance implementation

Design

Key actions in this phase

- Define catalogs for internal and external users.
- Design access packages for role-based access.
- Plan access reviews for compliance and periodic access validation.
- Design a 3-tier PIM model for managing elevated permissions.
- Design conditional access policies with **Zero Trust Framework** to protect Tier 0 cloud accounts
- Implement workflows for Joiner, Mover, and Leaver processes to automate identity lifecycle management (including optional custom workflow leveraging Azure Logic App).
- Draft terms of use for internal and external users.

Key Deliverables

- Governance architecture design document.
- Access package and review structure.
- Workflow diagrams for Joiner, Mover, Leaver processes.
- Draft terms of use document.

Implementation

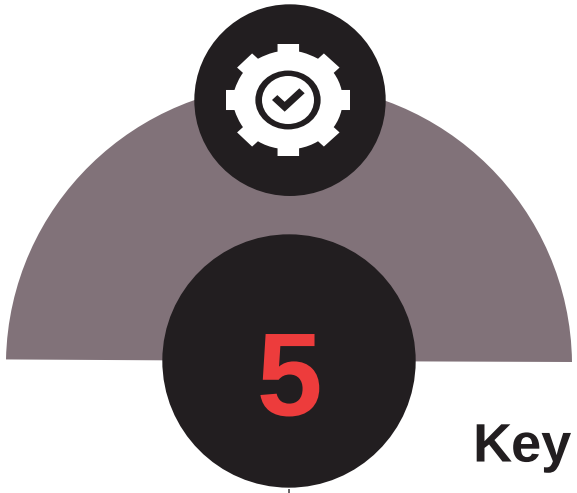
Key actions in this phase

- Create up to 2 catalogs (1 for internal users, 1 for external users).
- Establish up to 5 access packages per catalog with role-based access policies and up to 5 access reviews per catalog for continuous compliance.
- Implement a 3-tier Privileged Identity Management (PIM) model for role assignments, eligibility, and activation.
- Implement up to 2 conditional access policies protection Tier 0 accounts.
- Configure company-specific terms of use for internal and external users.
- Implement Joiner, Mover, Leaver (JML) workflows
- Conduct comprehensive testing and validation to ensure configurations are functional and compatible.

Key Deliverables

- Fully configured catalogs, access packages, access reviews, PIM, and terms of use.
- Implementation report summarizing configurations.

Testing



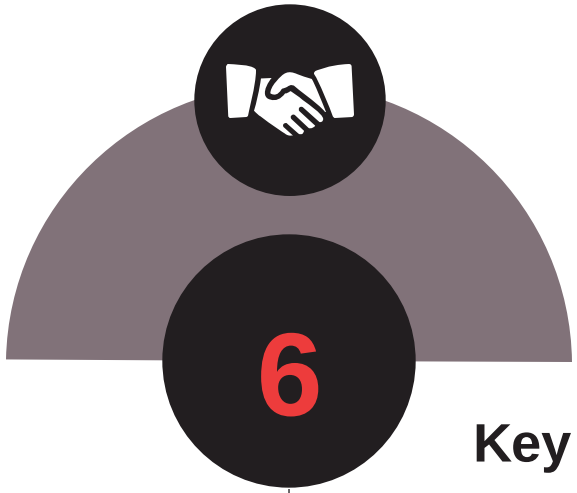
Key actions in this phase

- Validate access packages for proper permissions and workflows.
- Test access reviews for automated reminders and periodic compliance checks.
- Verify PIM configurations for elevated role management.
- Simulate acceptance of terms of use for different user types.

Key Deliverables

- Test results report.
- Issue resolution log.

Support and Hypercare



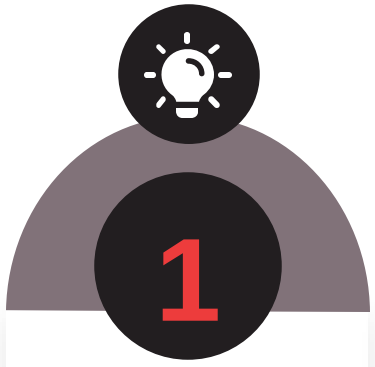
Key actions in this phase

- Monitor configurations for anomalies or compliance concerns.
- Conduct knowledge transfer sessions for IT teams.
- Provide hypercare support for up to 4 weeks.

Key Deliverables

- Final operational guide and troubleshooting documentation.
- Post-implementation summary report.

Summary of Deliverables for Each Phase



DISCOVERY

- Discovery report
- Governance requirements matrix

ANALYSIS

- Examination of materials from the discovery phase
- Gaps identification

DESIGN

Architecture document covering:

- Access package design
- Access review design
- PIM design
- Terms of use design

IMPLEMENTATION

Configuration of the following items:

- Catalogs
- Access packages
- Access reviews
- PIM
- Terms of use

TESTING

- Testing results report
- Resolved issues log

SUPPORT AND HYPERCARE

- Operational guide and troubleshooting documentation
- Final project report with recommenda-tions

Estimated Implementation Time

Phase	Hours
Discovery	20
Design	40
Implementation	80
Testing	20
Support and Hypercare	20
Total	**180**

Formula5

HIPAA

NIST National Institute of Standards and Technology

Contact us!

+1 949.413.1313

info@formula5.com