

# Initiatives

# Possible Capabilities

# Core Capabilities

# Stakeholder Goals

# Desired Outcomes

**AuthN & Credential Mgmt**  
 FY16 - External Users  
 FY16 - B2B & B2C  
 FY17 - AAD App Proxy  
 FY17 - Microsoft Passport & Azure MFA

**Applications & Collaboration**  
 FY16 - AAD App Support  
 FY17 - AAD Conditional Access  
 FY17 - Group based License Assignment  
 FY17 - Software Deployment (SCCM)

**Device Mgmt**  
 FY17 - AAD Device Join  
 FY17 - InTune & MDM EDP

**Information Security**  
 FY16 - Azure Rights Mgmt  
 FY17 - AAD Audit API  
 FY17 - Privileged Identity Mgmt  
 FY17 - AAD Rights Based Access Control (RBAC)  
 FY18 - AAD Group Integration Refactor

**Enable Cloud**  
 FY16 - AAD Governance  
 FY17 - AAD Connect  
 FY17 - AAD Cloud App Discovery  
 FY18 - AWS infrastructure  
 FY18 - Azure infrastructure

**Azure AD Security Token Svc**  
**ADFS**  
 Azure AD External Users  
 Windows Domain Trust  
 UW NetID integration  
 Azure AD B2B & B2C  
*Microsoft Passport & Azure MFA*  
*Cloud to On-Premises Token Translation (AAD App Proxy)*

**Directory Svc Integration**  
 App Integration via LDAP/WIA  
 Microsoft Volume License Activation (KMS)  
 Azure AD License Assignment  
 Azure AD Applications  
 Software Deployment (SCCM)

**Delegated OUs & Domain Join**  
 Group Policy for Device Mgmt  
 Windows Domain Migration  
 DDNS & WINS  
 OS Deployment (SCCM + OSD)  
 AAD Device Join & AAD MDM

**Groups Svc Integration**  
 Certificate Services  
 AD Threat reporting  
 Azure AD Security and Auditing  
 Azure RMS  
 Azure AD RBAC  
 Azure AD sourced Groups

**Azure AD Integration**  
 AWS based AD  
 Azure based AD  
 AAD Cloud App Discovery

**Windows Domain Services**  
**Azure AD Services**

**Credential Mgmt**  
 Federated Authentication  
*Multi Factor Authentication*  
*Hybrid Authentication*

**Application Integration**  
 Software Deployment  
 Microsoft License Mgmt  
*Application Mgmt*

**Device Integration**  
 Device Mgmt  
 Device Name Registration & Resolution

**Authorization**  
 Data Protection  
 Auditing

**Cloud Discovery**  
 Cloud based infrastructure

**Authentication & Credential Mgmt**

**Collaboration & Application Mgmt**

**Device Mgmt**

**Information Security**

**Enable Cloud**

A department does not need to run its own AD or Azure AD.

I can share data using Microsoft-based services.

I can provide Microsoft-based services.

UW NetIDs are available for use with Microsoft technology.

UW Groups are available for use with Microsoft technology.

I can easily manage my devices.

I can use cloud based technologies that require Microsoft infrastructure.

Data in Microsoft technologies is secure.

Business Capability Map  
 Updated 04/23/2016  
 Author: Brian Arkills

**Key**  
 ↶ = Plan to retire or divest  
*italics* = no value provided yet

# Microsoft Infrastructure