Innovate Dynamics

SOW xx003 for agreement to perform consulting services to Oakwood

DATE	SERVICES PERFORMED BY:	SERVICES PERFORMED FOR:
Sept 19th 2025	DKB Innovate 321 Sycamore Ave. Albany, NY 76543	Innovate Dynamics 123 South Street Manhattan, NY 54321

Index

Engagement Resources

Name	Role	Contact
Zachary Gafford	Solutions Engineer	Xxx-xxxx xxx.xxxx@xxxx.com

Executive Summary

Innovate Dynamics is a growing engineering firm with a "cloudfirst" directive from leadership. They aim to eliminate on-premise physical servers to reduce hardware management and improve accessibility for their remote workforce. This proposal outlines a comprehensive plan to migrate all on-premise server roles and workloads to Microsoft Azure while ensuring seamless user authentication and access.

Current Environment

SRV01	Windows Server 2016 (Domain Controller, DNS, DHCP)
SRV02	Windows Server 2016 (File Server with 2TB of data, custom in-house LOB application)
Connectivity	10/100 Mbps fiber internet
Identity	Users authenticate to the on-premise Active Directory and use Microsoft 365 for email.

Project Goals & Scope

- Migrate all server roles from the on-premise environment to Microsoft Azure.
- Ensure seamless user authentication and access to files and the LOB application.
- Decommission the on-premise physical servers.

Proposed Solution

PS.1 Identity & Directory Services

- Deploy Azure Active Directory (Azure AD) and Azure AD Connect to synchronize existing user identities.

- Transition from the on-premises Domain Controller to Azure AD Domain Services, which provides native DNSfor internal name resolution and integrates with Microsoft 365.
- Configure single sign-on (SSO) for Microsoft 365 and the line-of-business (LOB) application.

Identity Mgmt Deliverables

Service	Description
Azure AD & Azure AD Connect	Azure Active Directory and Azure AD Connect fully deployed to synchronize existing on-premises user identities with the Microsoft 365 cloud environment.
Azure AD Domain Services Transition	Migration from on-premises Domain Controller to Azure AD Domain Services, providing native DNS for internal name resolution and seamless Microsoft 365 integration.
Single Sign-On (SSO) Configuration	SSO enabled and tested for Microsoft 365 and the line-ofbusiness (LOB) application, ensuring seamless, secure access with one set of credentials.

PS.2 File Services & Data Migration

- Migrate file shares from SRV02 to Azure Files or Azure File Sync for cloud-based storage with on-demand access.
- Implement appropriate Azure Storage redundancy (e.g., Geo-Redundant Storage) for business continuity.
- Establish access policies and permissions mirroring the current environment.

Migration Deliverables

Service	Description
File Share Migration	All on-premises file shares from SRV02 migrated to Azure Files or Azure File Sync for secure, cloudbased storage with on-demand access.
Azure Storage Redundancy	Appropriate redundancy (e.g., Geo-Redundant Storage) configured to ensure business continuity and data protection.
Access Policies & Permissions	Access controls and folder permissions established in Azure to mirror the existing on-premises environment, maintaining user roles and security.

PS.3 Application Migration

- Assess the custom LOB application for Azure compatibility.

- Host the application on Azure Virtual Machines or refactor to Azure App Service if feasible.

- Ensure secure connectivity and testing for uninterrupted operations.

PS.4 Networking and Connectivity

- Establish a secure site-to-site VPN or Azure ExpressRoute for reliable connectivity.

- Implement Azure Firewall or Network Security Groups for traffic control and security.

- Configure conditional access and MFA for secure remote logins.

- DNS & DHCP Migration: External DNS will be hosted on Azure DNS, while internal name resolution is handled by Azure AD Domain Services or Azure Private DNS Zones.

- DHCP is provided by Azure Virtual Network services, which automatically assign and manage VM IP addresses. Any remaining on-site devices (e.g., printers) can use the office Meraki firewall or static IPs for basic DHCP if needed.

- On-Site Switching, firewall, & Wi-Fi: Replace the legacy 10/100 Mbps switch with a Cisco Meraki MS225-48-HW managed gigabit switch for high-speed, cloudmanaged networking. Deploy two Cisco Meraki MR46E Wi-Fi 6 access points with PoE for secure, centrally managed wireless coverage, using shielded Cat6a cabling for reliability and future growth.

- Deploy a Cisco Meraki MX75 next-generation firewall and VPN appliance to serve as the secure WAN edge, providing stateful firewalling, DHCP for any on-premises devices, and an encrypted site-to-site VPN connection to Azure.

PS.5 Backup & Disaster Recovery

- Configure Azure Site Recovery for business continuity and disaster recovery.
- Enable Azure Backup for virtual machines, files, and application data.

Implementation Plan

Man-Hours

Phase	Implementation	Details	Time-Frame
Phase1	Assessment & Design	Complete environment discovery, finalize Azure architecture and migration plan, confirm application dependencies, and verify Microsoft Azure and Meraki licensing.	1 week
Phase2	Identity & Network Core	Deploy Azure Active Directory Domain Services and synchronize identities; configure site-to-site VPN; install and configure new Cisco Meraki MX75 firewall, MS225-48-HW switch, and MR46E Wi-Fi 6 access points, including VLANs, DHCP, and secure wireless networks.	1 week
Phase3	Data & Application Migration	Migrate file shares to Azure Files/Azure File Sync and move the line-of-business application to Azure Virtual Machines or App Service. Validate Azure DNS/Private DNS integration and decommission onpremises DNS/DHCP roles.	1 week
Phase4	Cutover, Testing & Decommission	Perform final testing of all workloads, security policies, and failover procedures; decommission the on-premises servers; deliver full system documentation and administrator training.	1 week

Supporting documents and checklist

Document	Scope	Link
Deployment Sheet	Comprehensive guide and checklist for full implementation (installation and configuration steps).	Xxxx
Diagram (Final Site Design)	Visual representation of final network/site design including topology and key connections.	Xxxx
Security Key Guide	Instructions for issuing, registering, and recovering hardware or app-based MFA/security keys.	Xxxx
Supporting Documentation (Azure Runbooks)	Azure runbooks and operational guides for automation, monitoring, and maintenance tasks.	Xxxx

Total estimated project duration: ~4 weeks.

Deliverables and Benefits

Deliverables

Deliverable	Summary
Entra-ID	Fully deployed Azure Active Directory (Entra ID) with synchronized user identities and Azure AD Domain Services providing internal DNS.

Azure Migration	Migration of all file shares and the custom line-of-business (LOB) application to Microsoft Azure, with validated access and performance.
Azure DNS Priv DNS	Retirement of on-premises DNS and DHCP roles, replaced by Azure DNS/ Private DNS for cloud workloads and Meraki-based DHCP for any remaining on-site devices.
Network Update	Installation and configuration of new Cisco Meraki MX75 firewall, MS225-48-HW gigabit managed switch, and MR46E Wi-Fi 6 access points with secure VLANs and shielded Cat6a cabling.
VPN	Secure site-to-site VPN connectivity (or Azure ExpressRoute if selected) linking office devices to Azure services.
Bckup/DR	Implementation of Azure Backup and optional Azure Site Recovery for VM and application data protection.
Site Topology	Complete system documentation, including Azure architecture, network diagrams, DNS/DHCP configuration, and step-by-step migration records.
Training	Administrator training and handover, ensuring the internal IT team can manage Azure resources, Meraki network equipment, and ongoing backups.

Benefits

Benefit	Solution	Problem
Eliminates onpremises servers and their maintenance costs	Migrate workloads, file services, and identity to Azure services (Azure Files, Azure AD, Azure VMs only if needed).	Physical servers require costly maintenance, hardware refresh cycles, and constant patching.
Provides reliable, cloud-native DNS and DHCP services	Implement Azure AD Domain Services with built-in DNS and DHCP integration.	Legacy on-premises DNS/ DHCP servers create single points of failure.
Enhances remote accessibility and on-site performance	Deploy Fortinet FortiSwitch 148FFPOE with gigabit access and 10 Gb uplinks to improve LAN speed and support VPN/remote access.	Existing unmanaged or lowspeed switching creates network bottlenecks and limits performance.
Improves scalability and disaster recovery	Use Azure Backup and Azure Site Recovery for automated off-site protection.	On-premises backup solutions lack elasticity, are vulnerable
Streamlines identity mgmt and auth with Azure AD and SSO	Integrate Microsoft Entra ID (Azure AD) with SSO for Microsoft 365 and business applications.	Multiple local domain controllers and logins complicate identity mgmt and increase security risk.

Assumptions & Exclusions

Custom application code changes are not included unless identified as essential during assessment. (Licensing or code changes for the line-of-business (LOB) application are outside the scope of this project.)

Any building or cabling work needed to install a new gigabit switch is the client's responsibility. (Internet service (1 Gbps fiber) is assumed active prior to installation.)

The client will provide and maintain all required Microsoft 365 user licenses (e.g., Business Premium) and SQL Server licenses beyond those specified.

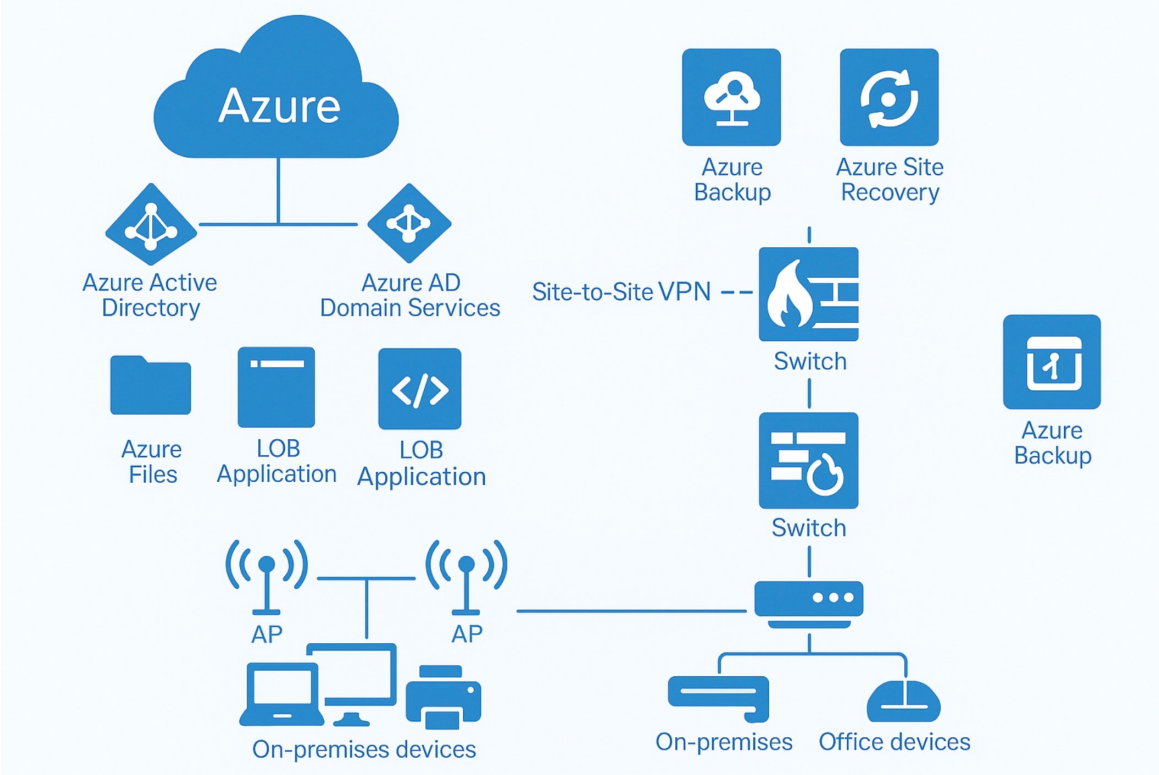
Licensing & Subscriptions

License / Subscription	Notes	Fees & Release Notes
Azure Private DNS Zones (Optional / Recommended)	Internal name resolution inside Azure VNets if needed beyond Azure AD DS built-in DNS.	Recommended if custom internal DNS zones are required.
Azure Backup (Required)	Pay-as-you-go protection for Azure VMs, file shares, and application data.	Provides automated, encrypted cloud backups.
Azure Site Recovery (ASR) (Optional / Recommended)	VM replication and rapid disaster recovery/failover in Azure.	Optional but recommended for improved business continuity.
Microsoft 365 Business Premium (Already in place / Required for users)	Base productivity suite with Azure AD Premium P1 and Intune for identity, MFA, and endpoint compliance.	Foundation license for users; includes key security and management features.
Microsoft Entra ID Premium P2 (Optional)	Advanced Conditional Access, Identity Protection, and Privileged Identity Management (PIM).	Enhances security with just-in-time admin access and risk-based sign-in protection.
Cisco Meraki MS225-48-HW Enterprise License (Required)	Cloud management and firmware support for the Meraki switch.	Required for ongoing operation and updates of the MS225-48 switch.
Cisco Meraki MR46E Enterprise License (two, one per AP) (Required)	Cloud management and firmware support for the wireless access points.	Required for each MR46E access point.
Cisco Meraki MX75 Advanced Security or Enterprise License (Required if MX firewall is deployed)	Enables firewall, SD-WAN, VPN, and security services for the branch gateway.	Required only if the MX75 firewall is part of the deployment.

Decommission and Degassing

Phase	Action	Notes
Assessment & Inventory	Identify all on-premises servers (SRV01, SRV02) and network gear slated for removal or repurposing.	Confirm no production roles remain before decommissioning.
Data Migration Verification	Ensure all files, applications, and DNS/DHCP roles have been successfully migrated to Azure and verified.	Prevent data loss or service interruption during cutover.
Drive Wiping & Degassing	Securely wipe or degauss hard drives removed from servers and network devices.	Document and store certificates of destruction for compliance.
Physical Equipment Removal	Remove old servers and legacy network infrastructure (switches, firewalls, cabling) from the site.	Label and inventory all decommissioned hardware.
Repurpose or Disposal	Recycle, repurpose, or dispose of retired equipment responsibly.	Follow local e-waste regulations and provide disposal/recycling certificates.

Solutions Diagram



Out Of Pocket / Invoice

Client will be invoiced all costs associated with out-of-pocket expenses (including, without limitation, costs and expenses associated with patching, cables termination, local transportation and any other applicable business expenses) listed on the invoice as a separate line item.

Reimbursement for out-of-pocket expenses in connection with performance of this SOW, when authorized and up to the limits set forth in this SOW, shall be in accordance with client's thencurrent published policies governing travel and associated business expenses.

Completion criteria

Contractor shall have fulfilled its obligations when any one of the following first occurs: Contractor accomplishes the contractor activities described within this SOW, including delivery to client of the materials listed in the section entitled "deliverable materials," and client accepts such activities and materials without unreasonable objections. No response from client within 2business days of deliverables being delivered by contractor is deemed acceptance. Contractor and/or client has the right to cancel services or deliverables not yet provided with 20 business days advance written notice to the other party.

Project change control procedure

A project change request (PCR) will be the vehicle for communicating change. The PCR must describe the change, the rationale for the change, and the effect of the change.
The designated project manager of the requesting party (contractor or client) will review the proposed change and determine whether to submit the request to the other party.
Both project managers will review the proposed change and approve it for further investigation or reject it. contractor and client will mutually agree upon any charges for such investigation, if any. If the investigation is authorized, the client project managers will sign the PCR, which will constitute approval for the investigation charges. Contractor will invoice client for any such charges. The investigation will determine the effect that the implementation of the PCR will have on SOW price, schedule and other terms and conditions of the agreement.
Upon completion of the investigation, both parties will review the impact of the proposed change and, if mutually agreed, a change authorization will be executed. A written change authorization and/or PCR must be signed by both parties to authorize implementation of the investigated changes.

Sign Off

Innovative Dynamics	DKB
Name: _____	Name: _____
Signature: _____	Signature: _____
Date: _____	Date: _____