



OAKWOOD

SOW xx001 for agreement to perform

MANUFACTURING

consulting services to

Oakwood

DATE	SERVICES PERFORMED BY:	SERVICES PERFORMED FOR:
Sept 19th 2025	DKB Innovate 321 Frisco Ave. Frisco, TX 76543	OakWood Manufacturing 123 South Street Manhattan, NY 54321

Index

- [Engagement Resources](#)
- [Executive Summary](#)
- [Current Environment](#)
- [Project Goals & Scope](#)
- [Proposed Solution](#)
 - [PS.1 Server Platform](#)
 - [PS.2 Network Modernization](#)
 - [PS.3 Backup & Disaster Recovery](#)
 - [PS.4 Management & Security](#)
- [Implementation Plan](#)
- [Deliverables and Benefits](#)
- [Assumptions & Exclusions](#)
- [Licensing & Subscriptions](#)
- [Decommission and Degassing](#)
- [Solutions Diagram](#)
- [Out Of Pocket / Invoice](#)
- [Completion criteria](#)
- [Project change control procedure](#)
- [Sign Off](#)

Engagement Resources

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





Executive Summary

Oakwood Manufacturing's existing technology environment is approaching EOL and no longer provides the performance, reliability, or protection the business requires. Key business applications experience lag and current backup practices expose risk.

This proposal recommends a comprehensive modernization of on-premises infrastructure by upgrading servers, networking, and security while integrating Microsoft Azure as a dedicated platform for disaster recovery and off-site backups. The result will be a resilient and scalable foundation that supports daily operations and makes room for growth in the years ahead.

Current Environment

Server	Dell PowerEdge R720 (2012)
Server Roles	Domain Controller, DNS/DHCP, File Server, SQL Server 2014 (LOB database).
Networking	Mixed unmanaged 10/100 Mbps switches; single consumergrade firewall/router; multiple mismatched consumer Wi-Fi access points.
Backup	External USB drives swapped weekly and taken off-site.

Project Goals & Scope

- Replace the aging server with current-generation hardware and a supported operating system.
- Overhaul core network infrastructure: enterprise-grade firewall, managed switches, and centrally managed Wi-Fi.





- Implement backup and disaster recovery to meet RTO/RPO targets while keeping production on-prem.
- Deliver a scalable, secure solution with a 5-7 year life cycle.

Proposed Solution

PS.1 Server Platform

Hardware: Dell PowerEdge R7625 rack server equipped with dual AMD EPYC 4th Generation 9004-series CPUs. Each CPU can have up to 96 cores / 192 threads (depending on model), for up to ~192 cores total in a 2-CPU configuration.

Memory: Supports up to 24 DDR5 RDIMM slots, with a maximum of 6 TB of RAM, running at speeds up to 4800 MT/s. Registered ECC memory only.

Primary Storage (OS / VMs): Eight 3.84 TB enterprise NVMe solid-state drives in a native NVMe backplane, configured in RAID 10 with a dedicated hot spare — delivering ~15 TB usable, high-IOPS, low-latency storage.

Local Backup Storage: Dedicated backup array of three 4 TB enterprise SSDs in RAID 5, giving ~8 TB usable for staging MABS image backups and fast local restores. The RAID controller supports hot-swappable, no-downtime expansion as needed.

Virtualization: Microsoft Hyper-V for VM management.

Operating Systems: Windows Server 2022 for core infrastructure (Domain Services, File Services, SQL Server 2022).

High Availability & Expansion: RAID 10 for primary storage with hot spare for resilience. Supports online capacity expansion for backup SSD array.

Server Hardware Deliverables

Device	Make/Model	QTY	Spec
Server	Dell PowerEdge R7625	1	Server Specs
Memory	32GB RDIMM, 5600MT/s, Dual Rank	8	Module Specs
CPU	AMD EPYC 9224 2.50GHz, 24C/48T, 64M Cache	2	Compute Specs
Primary Storage	3.84 TB enterprise NVMe solid-state	8	Storage Specs
Local Storage	4 TB enterprise SSDs	3	Storage Specs





Virtualization	Hyper-V	3	VM specs
Operating Sys	Windows Server 2022	1	OS Specs
Raid Controller	PERC H965i	1	Perc specs
Rack	22u Rack on caster wheel.	1	Rack Specs
PSU	Hot-plug Redundant PS (1+1) 1100W, -48vDC	2	PSU Specs

PS.2 Network Modernization

Firewall / Security: Fortinet FortiGate 70G next-generation firewall, with full IPS, VPN (site-to-site & client), and advanced threat protection from FortiGuard services.

Switching: Cisco Meraki MS355-24X2-HW (24-port multigigabit + PoE) managed Layer-3 switch, including VLAN segmentation and stacking as needed. Use shielded Cat6a cabling for reliability and speed.

Wireless: Two Cisco Meraki MR56 WiFi-6 (802.11ax) access points, cloud-managed. They support multigigabit Ethernet uplinks and high client density, suitable for both corporate and guest networks. Use shielded Cat6a cabling for AP connections

Network Hardware Deliverables

Device	Make/Model	QTY	Spec Sheet
Firewall	Fortinet FortiGate 70G	1	FW Specs
Switch	Cisco Meraki MS355-24X2-HW	1	Switch Specs
Access Point	Cisco Meraki MR56	2	AP Specs
CAT6a	Shielded CAT6a Bundle 1000ft	1	Cable Specs

PS.3 Backup & Disaster Recovery

Microsoft Azure Backup Server (MABS) is installed directly on the Hyper-V host to create a full, bare-metal system image of the physical Dell PowerEdge R7625. This captures the host operating system, Hyper-V configuration, and all drivers, enabling complete bare-metal recovery if the server hardware or disks must be rebuilt.

For performance and rapid local restores, three 4 TB enterprise SSDs are configured in RAID 5, providing approximately 8 TB of fault-tolerant local storage as the MABS backup volume. This volume stages backups and serves as a fast on-site recovery cache before data is transferred to Azure. The Dell PERC RAID controller also supports online capacity expansion, allowing additional SSDs to be added to this RAID-5 array in a hot-swappable, no-downtime manner as storage needs grow.





In parallel, Azure Backup protects each Hyper-V virtual machine individually, taking application- and crash-consistent snapshots with daily incremental backups. This allows single-VM or even single-file restores without re-imaging the host server.

To ensure seamless business continuity during a major outage, Azure Site Recovery (ASR) is also enabled for all critical VMs. ASR continuously replicates each VM to Azure and can automatically fail over to Azure in the event of a host or site failure, starting the replicated VMs with preconfigured virtual networking so users can continue working with minimal disruption.

Recovery Process: In a disaster, new hardware can be booted from an Azure-generated recovery ISO to connect securely to the Recovery Services vault and stream the full host image back to the server. Individual VMs can also be restored or spun up instantly in Azure via ASR, providing flexible options ranging from single-file recovery to full, automated failover.

PS.4 Management & Security

Centralized Patching & Monitoring:

Microsoft Intune and Azure Arc, integrated with Windows Admin Center, provide full RMM-style management. This combination delivers automated patch deployment, configuration management, and real-time health and performance monitoring for the Hyper-V host, all virtual machines, and network equipment from a single cloud-based console.

Out-of-Band Management:

The Dell PowerEdge R7625 includes iDRAC9 Enterprise, providing secure, browser-based remote console and power control even when the host OS is offline. This enables full remote management, firmware updates, and recovery in the event of an operating system failure or network outage.

Role-Based Access Control (RBAC) & Multi-Factor Authentication (MFA):

Enforce least-privilege principles through Azure Active Directory roles and conditional access, ensuring users and administrators have only the permissions required for their duties. MFA is mandatory for all privileged operations.

Advanced Threat Protection:

Enable Microsoft Defender for Endpoint on all servers and endpoints, integrated with Microsoft 365 Defender and Fortinet FortiGate threat intelligence feeds for coordinated detection and response to malware, phishing, and zero-day exploits.

Encrypted Data at Rest and In Transit:

Use BitLocker (or equivalent) on all server and backup volumes, TLS/SSL for all network traffic, and VPN/IPsec tunnels for site-to-site or remote access.

Immutable and Geo-Redundant Backups:

Backups stored in Azure Recovery Services vaults are immutable and geographically redundant, ensuring protection against ransomware and accidental deletion.

Comprehensive Logging & Auditing:



*Statement Of Work*

Centralize Windows Event Logs, Azure AD sign-in logs and Fortinet firewall logs into Microsoft Sentinel or a SIEM of choice for long-term retention, alerting, and compliance reporting.

Security Awareness & Training:

Conduct periodic security training and phishing simulations to keep users alert to evolving threats.

Documented Incident Response Plan:

Provide detailed runbooks and escalation paths for responding to security events, including ransomware, data breaches, and insider threats.

VLAN Isolation:

Segment on-site networks into dedicated, secure VLANs to contain traffic and reduce risk.

Implementation Plan

Man-Hours

Phase	Implementation	Details	Time-Frame
Phase1	Assessment & Design	Finalize detailed design, order and stage hardware, and configure Azure services	1.5 week
Phase2	Deployment	Install servers, configure virtualization, and migrate data and roles	1 week
Phase3	Network Upgrade	Replace firewall and switches, deploy enterprise Wi-Fi. Network configuration.	.5 week
Phase4	Backup & DR	Configure Azure Backup and perform disaster recovery failover testing	.5 week
Phase5	Validation & Handover	Conduct user acceptance testing, provide training, and deliver final documentation	1 week

Supporting documents and checklist

Document	Scope	Link
Deployment Checklist	Confirms shipping. Inventory. Room/U-space, Nics, Switchports, Completes warrant, BIOS/Firmware updates	Xxxx
Migration Guide	Guide for the physical and virtual migration of services from old equipment to new. Physical server/Switch/fw migration and cloud migration services setup and handover.	Xxxx
Post Install Checklist	Checklist for server post installation (update inventory, customer facing/internal documentation, set ILO and assign IP, domain, and hostname etc..)	Xxxx





DR Runbook	Complete guide for disaster recovery on-prem and public cloud	<u>Xxxx</u>
Site Guide	Find all customer facing data: -Network (Vlans, IP assignments) -Server names and Roles -Backup Runbook -DR Runbook -Services -Cloud and local credentials -Past tickets and checklist -Bios/FW versions -OS/SW license and details	<u>Xxxx</u>
Training	security, RMM procedures, & administrator Training for IT staff	<u>Xxxx</u>

Total estimated project duration: ~4.5 weeks.

Deliverables and Benefits

Deliverables

Deliverable	Summary
New Production Server Platform	High-performance server fully installed and migrated.
Modernized Network Infrastructure	Enterprise firewall, managed switch, and Wi-Fi 6 with structured cabling.
Comprehensive Backup & Disaster Recovery	Automated backups and tested failover to maintain business continuity.
Centralized Management & Security	Unified monitoring, patching, and access control with strong security.
Complete Documentation & Training	System diagrams, runbooks, and administrator training sessions.
Validation & Testing	Full failover and restore testing to confirm RTO and RPO requirements.

Benefits

Benefit	Solution	Problem
Performance	Cutting edge, Fast, reliable system response for applications and file access.	Old equipment was slow and no longer supported.
Resilience	Built-in backup and recovery keep services running during outages. Cloud services ensure fast recovery of Virtual Machines and Virtual Services.	Manual USB backups risked loss and slow recovery.





Statement Of Work

Stronger Security	Current-generation Windows Server, next-gen firewalling, multifactor authentication, and encrypted, immutable backups greatly reduce exposure to ransomware and unauthorized access	Outdated firewall and weak authentication left systems exposed.
Simplified Management	Cloud-based monitoring and patching through Intune and Azure Arc, combined with iDRAC for out-of-band control, streamline admin and speed up maintenance or recovery tasks.	Maintenance was manual and inconsistent.
Growth	Hot-swappable storage, expandable capacity, and cloud elasticity give the infrastructure flexibility beyond the next five to seven years.	Old hardware limited future expansion.
Operating Cost	Clear documentation and automation reduce time and expense.	Frequent manual fixes increased workload and costs.

Assumptions & Exclusions

- *All production workloads will remain on-premises except for disaster-recovery and backup replicas hosted in Azure.*
- *Licensing or code changes for the line-of-business (LOB) application are outside the scope of this project.*
- *The client will provide and maintain all required Microsoft 365 user licenses (e.g., Business Premium) and SQL Server licenses beyond those specified.*
- *Internet service (1 Gbps fiber) will be provisioned and active prior to installation.*
- *Any construction, electrical, or HVAC modifications needed to meet power or cooling requirements are the responsibility of the client or building contractor.*





- *User endpoint devices (laptops, desktops, mobile devices) and their individual software licensing are not included, except for Intune enrollment and baseline security policy.*
- *Ongoing Azure consumption charges for Backup, Site Recovery, and monitoring are billed directly to the client's Azure subscription and are not part of the implementation fee.*
- *Future expansion of hardware or Azure services beyond what is explicitly quoted will require a separate scope and estimate.*

Licensing & Subscriptions

License / Subscription	Notes
Windows Server 2022 Datacenter (corebased)	Operating system license for core infrastructure.
SQL Server 2022 (per core or Server + CAL, if required by the LOB application)	Database license for the line-of-business application.
Azure Backup (per VM + storage)	Cloud backup service for virtual machines.
Azure Site Recovery (per VM)	Disaster-recovery replication and failover for VMs.
Microsoft Azure Backup Server	No license fee
Fortinet FortiGate 70G	FortiCare + FortiGuard subscription
Cisco Meraki MS355-24X2-HW	Enterprise license
Cisco Meraki MR56	Enterprise license (two, one per AP)
Microsoft 365 Business Premium	Existing; includes Azure AD P1
Azure AD Premium P2	(Optional) if advanced identity governance is needed
Windows Server CALs	(Optional) if using Standard edition
RMM Azure Arc and Intune	Included in O365 subscription

Decommission and Degassing

Phase	Action	Notes
-------	--------	-------





MOCKUP

Page 10 of 12

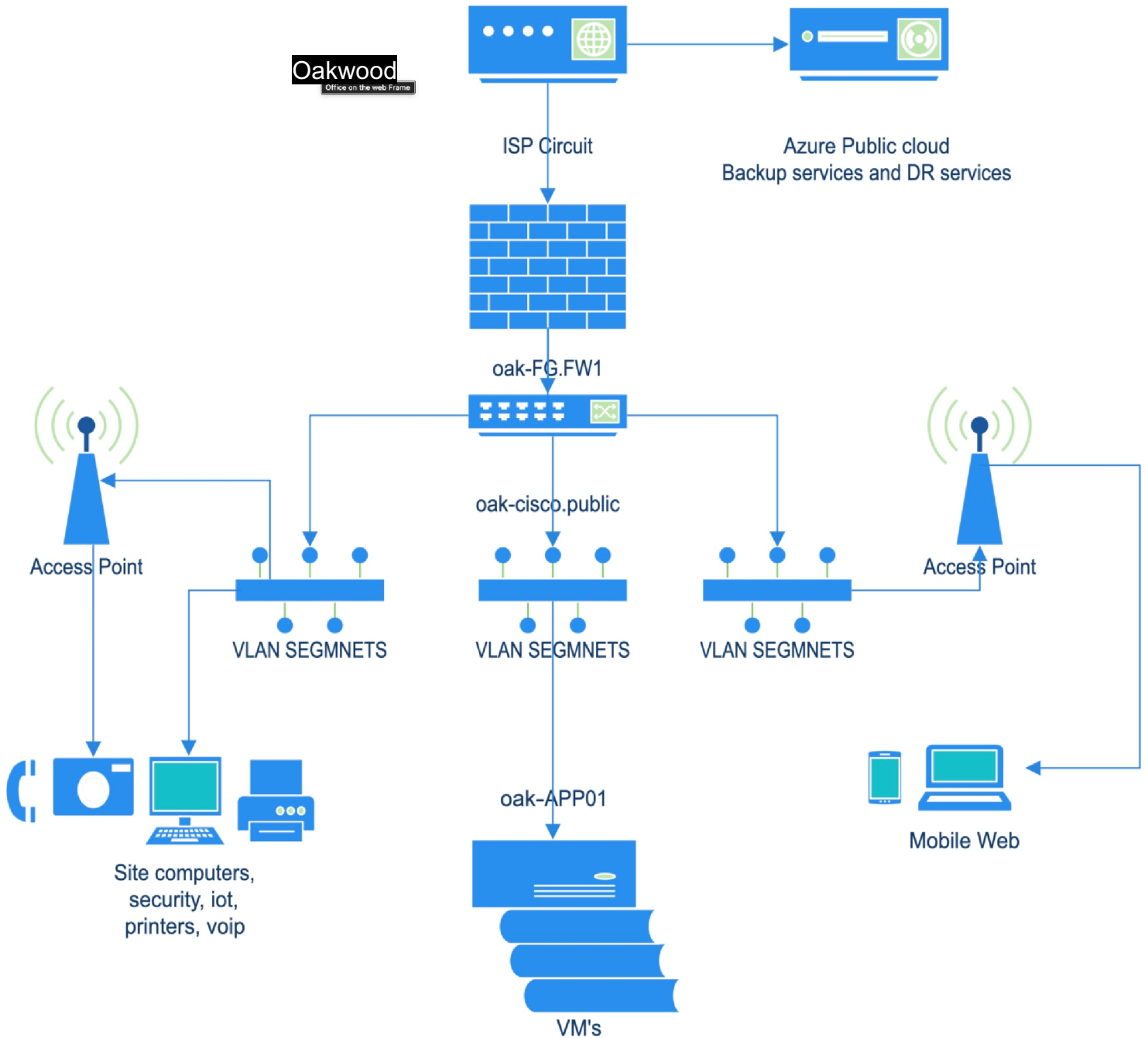
Statement Of Work

Preparation	Schedule cutover window and notify users.	Confirm backups are complete and migration plan is approved.
Server Cutover	Migrate all roles and data to the new server.	Verify successful migration before powering down old server.
Network Cutover	Replace legacy firewall, switches, and access points with new equipment.	Ensure all network services are stable before decommissioning old gear.
Drive Degassing	Securely wipe and degauss all drives removed from old server and network devices.	Document the data-destruction process for compliance and provide certificates.
Hardware Removal	Physically remove decommissioned server and network hardware.	Tag and inventory all removed components for final audit.
Disposal / Recycling	Recycle or dispose of retired equipment in an environmentally responsible manner.	Provide disposal or recycling certificates as needed.





Solutions Diagram





Statement Of Work

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

OAKWOOD

DKB

Name: _____

Name: _____

Signature: _____

Signature: _____

Date: _____

Date: _____

