

CASE STUDY · JULY 2025

Remediate before migrating: an infrastructure modernization plan

An anonymized July 2025 project case study of a proposed remediation-first approach to aging virtualization, identity, network, and storage infrastructure.



Conceptual illustration only; not the customer's production environment.

Project snapshot

Detail	Documented scope
Customer	An organization with on-premises infrastructure; customer anonymized
Project date	July 2025
Starting point	Hyper-V infrastructure with aging directory services, host configuration gaps, and network/storage resilience concerns
Decision	Remediate foundational risks first, or migrate workloads while retaining existing dependencies
Status represented	Assessment findings and proposed scope; final selection, delivery, and results are not verified

This project case study is based on the supplied project proposal, not a completion report. Customer identities and identifying environment details have been omitted. The document does not establish a completed Hyper-V-to-VMware migration.

Executive summary

A planned virtualization engagement exposed risks extending beyond the hypervisor. The proposal documented outdated host firmware, incomplete drivers, aging Active Directory services, legacy certificate infrastructure, and limited network and storage redundancy.

Massive IT proposed addressing those dependencies before proceeding with migration. An alternative, faster lift-and-shift path would leave the underlying risks in place. The case illustrates a planning decision: moving virtual machines does not automatically modernize the systems that authenticate users, carry traffic, or provide storage.

The assessment: infrastructure risk below the migration layer

Host readiness

The proposal identified firmware several revisions behind current releases, missing hardware drivers, and hosts configured for legacy BIOS without Secure Boot. It called for firmware and driver updates and a planned operating-system reinstall to transition those hosts to UEFI and Secure Boot.

Directory and hybrid identity

Active Directory included Windows Server 2008 R2 and 2012 R2 domain controllers, an older forest/domain functional level, and an extended-offline controller. Residual Exchange directory objects remained after an on-premises server was removed. RADIUS and an enterprise certificate authority also relied on an aging domain controller, while the Entra Connect deployment lacked a standby arrangement.

Network and storage dependencies

The assessment described core switching without a coordinated redundancy design, broadly permitted inter-VLAN traffic, and iSCSI paths requiring resilience review. Missing cabling and port documentation made safe changes harder to plan. The proposal also noted server activation issues requiring review.

Two paths, different retained risks

Approach	Proposed direction	Important tradeoff
Remediate first	Modernize hosts, directory services, PKI, hybrid identity, network paths, and security baselines before migration	Broader scope and coordination; intended to reduce legacy dependencies
Lift and shift as-is	Proceed with the virtualization work without the foundational remediation	Lower initial scope, but legacy identity, firmware, certificate, and resilience risks remain

The proposal favored remediation first. It did not establish customer approval of either option, completed implementation, or guaranteed vendor support. Supportability would require validation against the final configuration, current vendor requirements, and applicable support agreements.

Massive IT's proposed workstreams

1. Prepare the virtualization hosts

Update management-controller, BIOS, network, and storage firmware; reinstall hosts using UEFI and Secure Boot; and install required hardware drivers. Although the document contains an ambiguous annotation beside this workstream, it is not treated here as evidence of verified completion.

2. Modernize Active Directory and identity

Deploy Windows Server 2022 domain controllers, transfer FSMO roles, retire legacy controllers, and clean up stale directory metadata. The plan proposed raising domain and forest functional levels to 2016 following prerequisite and compatibility review. SYSVOL replication readiness would need separate verification; a functional-level change alone is not evidence that replication migration has been completed.

Review obsolete Exchange objects and attributes before targeted cleanup, rather than removing live mail-routing information indiscriminately. Replace the legacy certificate arrangement with a two-tier SHA-256 PKI, migrate RADIUS policies to a supported server, and establish a staging/failover arrangement for Entra Connect.

3. Strengthen network and storage paths

Document rack and port mappings, label cabling, evaluate switch stacking or clustering, isolate iSCSI traffic, and review storage zoning, multipath I/O, and frame-size consistency. Host teaming and switch configuration would be selected as a compatible design rather than treating LACP and switch-embedded teaming as interchangeable settings.

Inter-VLAN access controls were proposed in coordination with the customer's internal team. Required application traffic would need to be understood before restricting communication.

4. Apply security baselines

Review and implement applicable Microsoft security baselines and Entra hardening. These were proposed configuration workstreams, not proof of compliance certification or elimination of security risk.

What remained to be decided

- An updated network diagram with VLAN, subnet, and port mappings.
- Confirmation of switch capabilities for the intended redundancy design.
- Customer change-control requirements and maintenance windows.
- Approval of the remediation-first or as-is approach.
- Validation of directory, application, host, and storage prerequisites before changes.

Project status and takeaway

The supplied proposal establishes findings, options, and planned work. It does not provide final acceptance, a confirmed destination hypervisor, a completed migration, measured uptime improvements, or verified security outcomes.

The lesson is to assess the infrastructure beneath a migration before moving workloads. A remediation-first plan can make legacy dependencies visible and give stakeholders a clearer decision about scope, sequencing, and retained risk.