VDI Modernization:

Comprehensive Legacy VDI Migration to Cloud-Native Architectures

Executive Summary

This report provides a strategic, evidence-based framework for National Health Service (NHS) Trusts and their leadership to move from the basic possession of Microsoft 365 (M365) licenses, under the national N365 agreement, to deep, transformative, and sustainable adoption.

The analysis demonstrates that the platform, when optimally deployed, is a critical enabler for achieving the NHS's core strategic goals, but that its value is contingent on solving specific challenges related to governance, interoperability, and workforce change management.

1. Executive Summary and Strategic Context

The enterprise computing landscape involves a fundamental architectural transformation, shifting from rigid, capital-intensive on-premises infrastructure to flexible, consumption-based cloud services.

For decades, organizations have relied on legacy Virtual Desktop Infrastructure (VDI) platforms—primarily Citrix Virtual Apps and Desktops and VMware Horizon—to deliver secure, centralized desktops. While these solutions provided necessary control and security, they imposed significant operational overhead, requiring the management of complex control planes, hypervisors, and hardware lifecycles.

The emergence of cloud-native desktop virtualization, spearheaded by Azure Virtual Desktop (AVD) and Windows 365, represents a paradigm shift. This transition is not merely a "lift and shift" of virtual machines; it is a move toward a Desktop-as-a-Service (DaaS) model where the control plane is abstracted as a Platform-as-a-Service (PaaS) offering.

This shift delegates the maintenance of brokering, gateway, and diagnostics services to the cloud provider, allowing internal IT teams to pivot their focus from "keeping the lights on" to optimizing user experience and data security.

This document serves as an exhaustive project framework for migrating legacy VDI environments to Microsoft Azure. It synthesizes architectural analysis, technical migration methodologies, risk management strategies, and financial modeling to provide a roadmap for enterprise architects and program managers.

The objective is to de-risk the migration while maximizing the Return on Investment (ROI) through rigorous planning and the utilization of modern cloud capabilities like multi-session operating systems and elastic scaling.

1.1 The Imperative for Modernization

Organizations clinging to legacy on-premises VDI face mounting technical debt. The "house of cards" architecture of traditional VDI—where a failure in a single component like a SQL database or a licensing server can arrest the entire environment—poses significant business continuity risks. Furthermore, the hardware refresh cycles required to support these environments demand large capital expenditures (CapEx) that are increasingly difficult to justify in an era favoring operating expenditure (OpEx) flexibility.

Modern cloud architectures address these challenges by decoupling the infrastructure from the service. In AVD, the global control plane is managed by Microsoft, ensuring high availability and geographic resilience without customer intervention. This allows organizations to scale globally in minutes, deploying session hosts in regions closest to the user to minimize latency, a feat that would require months of procurement and provisioning in a traditional data center model.

2. Architectural Deep Dive: Legacy vs. Target State

A successful migration is predicated on a granular understanding of the source environment's dependencies and how they map—or fail to map—to the target architecture. This section dissects the technical anatomy of legacy VDI and contrasts it with the cloud-native approach.

2.1 Source Architecture: The Legacy VDI Stack

Legacy VDI environments are characterized by a "component-heavy" architecture. The customer is responsible for the entire stack, from the physical storage arrays and hypervisors up to the delivery controllers and access gateways.

2.1.1 Citrix Virtual Apps and Desktops (CVAD)

The Citrix architecture, typically built on the FlexCast Management Architecture (FMA), relies on a complex web of interdependent services.

- **The Control Layer:** At the heart of a Citrix site is the Delivery Controller, the broker responsible for managing user access and power-managing virtual machines. This component has a critical dependency on Microsoft SQL Server to store site configuration, logging, and monitoring data. If the SQL database becomes unavailable, the site enters connection leasing or Local Host Cache mode, but administrative functions cease. High availability (HA) for Citrix therefore implies HA for SQL (AlwaysOn Availability Groups), adding layers of complexity and licensing cost.

- **The Access Layer:** External access is mediated by Citrix StoreFront and NetScaler (ADC). These components require rigorous certificate management and network configuration. NetScaler, acting as an ICA proxy, is often a single point of failure if not deployed in high-availability pairs.
- **Provisioning Mechanisms:** Citrix environments heavily utilize Machine Creation Services (MCS) or Citrix Provisioning (PVS). PVS, in particular, streams the operating system primarily over the network from a vDisk, placing immense pressure on the network stack and requiring specialized "Write Cache" drives to handle runtime inputs. This creates a dependency on high-performance storage to absorb the IOPS generated during boot storms.
- **Licensing Dependencies:** The environment is strictly gated by the License Server. A failure here triggers a grace period, usually 30 days, after which the entire environment will refuse new connections, creating a potential "kill switch" for business operations if not monitored.

2.1.2 VMware Horizon View

VMware Horizon shares a similar architectural philosophy but uses proprietary components that create different migration challenges.

- **Connection Broker:** The Horizon Connection Server authenticates users via Active Directory and directs them to their desktop. Unlike Citrix, which relies heavily on SQL, the Connection Server uses an AD-LDS (Lightweight Directory Services) instance to replicate data between connection brokers. This replication topology must be healthy for the pod to function.
- **Composer and Instant Clones:** Historical deployments use View Composer for storage efficiency, utilizing "Linked Clones" that depend on a replica disk. Modern deployments use Instant Clones, which leverage "vmFork" technology to rapidly provision desktops from a running parent VM in memory. While efficient, this tight integration with vSphere means that a migration to Azure (which uses a different hypervisor construct) requires a complete rethink of image provisioning strategies.
- **Unified Access Gateway (UAG):** Similar to NetScaler, the UAG secures the Blast Extreme and PCoIP protocols. Migration requires mapping these firewall rules and access policies to Azure network security groups (NSGs) and Azure Firewall.

2.2 Target Architecture: Azure Virtual Desktop (AVD)

Azure Virtual Desktop represents a fundamental inversion of the VDI responsibility model. It moves the complexity of the control plane to the provider.

- **PaaS Control Plane:** Microsoft manages the Web Access, Gateway, Broker, Diagnostics, and REST APIs. These services are globally distributed and load-balanced. The customer does not deploy, patch, or backup these components. This eliminates the need for SQL clusters, Delivery Controllers, and connection brokers, significantly reducing the administrative attack surface.
- **Identity Integration:** AVD relies on Azure Active Directory (Microsoft Entra ID) for authentication. While session hosts can still be joined to a traditional Active Directory Domain Services (AD DS) domain for legacy app compatibility (Kerberos/NTLM), the primary authentication into the service is modern, supporting MFA and Conditional Access natively.
- **Connectivity (Reverse Connect):** A key architectural difference is the "Reverse Connect" transport. Session hosts establish an outbound connection to the AVD control plane using port 443. This eliminates the need for inbound firewall ports (like 3389) on the public internet, drastically improving the security posture compared to traditional RDS deployments.
- **Session Density (Windows 10/11 Multi-session):** Perhaps the most significant differentiator is the Operating System. Legacy VDI forced a choice: use Windows Server (RDS) for high density but poor user experience (no store apps, limited peripheral support), or use Windows 10/11 Client for good experience but low density (1:1 user-to-VM ratio). AVD introduces Windows 10/11 Enterprise Multi-session, which allows multiple concurrent users on a client OS, combining the cost efficiency of server-based computing with the compatibility of a client OS.

2.3 Target Architecture: Windows 365 (Cloud PC)

Windows 365 abstracts the complexity even further, offering a Software-as-a-Service (SaaS) consumption model.

- **Fixed Resource Alignment:** Unlike AVD, where resources are pooled, a Cloud PC is a 1:1 dedicated VM with fixed vCPU and RAM. The cost is predictable and flat, regardless of usage.
- **Management Plane:** Windows 365 is managed almost exclusively via Microsoft Intune (Endpoint Manager). It is treated exactly like a physical laptop; it appears

in the same inventory, receives the same policies, and uses the same update rings. This makes it ideal for organizations that have already matured their modern management practice.

2.4 Architectural Comparison Matrix

Feature Domain	**Legacy VDI (Citrix/VMware)**	**Azure Virtual Desktop (AVD)**	**Windows 365 (Cloud PC)**
Control Plane	Customer Managed (Heavy OpEx)	Microsoft Managed (PaaS)	Microsoft Managed (SaaS)
Infrastructure	On-premises Hypervisors / Hardware	Azure IaaS (Customer Managed)	Microsoft Managed (SaaS)
Protocol	ICA/HDX or Blast/PCoIP	RDP (with UDP Shortpath)	RDP
Image Mgmt	PVS / MCS / Linked Clones	Azure Image Gallery / Nerdio	Intune / Microsoft Managed
Profile Mgmt	Citrix UPM / VMware DEM	FSLogix Profile Containers	Local / FSLogix (Ent)

Cost Model	CapEx (Hardware) + Licensing	Consumption (Pay-as-you-go)	Fixed Monthly Subscription
Networking	MPLS / VPN / SD-WAN	Azure Backbone / ExpressRoute	Microsoft Global Network

Insight: The primary friction point in this architectural transition is the shift from proprietary, highly tuned protocols (HDX) to RDP.

While modern RDP is capable, it does not always match HDX's performance over high-latency or packet-loss networks without specific configurations like **RDP Shortpath** (which forces UDP transport). Migration architects must account for this by rigorously assessing network routes between the user and the Azure region.

3. Pre-Migration Discovery and Assessment

Before a single virtual machine is deployed in Azure, a comprehensive discovery phase is required. The "Lift and Shift" approach often leads to failure in VDI because on-premises resources are frequently over-provisioned, and moving bloated configurations to a consumption-based cloud model results in "bill shock."

3.1 Workload Profiling and Right-Sizing

The goal of profiling is to determine the exact resource consumption of a user session to map it to the correct Azure VM SKU.

- **Data Collection:** Agents (such as Azure Migrate or Lakeside SysTrack) must be deployed to the legacy endpoints. These agents should collect data for a minimum of 30 days to capture business cycles, including month-end processing spikes.

- **Key Metrics:**
  - **CPU:** Average and Peak utilization per user. This informs the "Users per Core" density calculation for multi-session hosts.
  - **RAM:** Memory working set. Browsers (Chrome/Edge) are memory hungry; insufficient RAM leads to paging file usage, which kills storage IOPS performance.
  - **IOPS:** Input/Output Operations Per Second. This is critical. On-prem SANs absorb high write bursts. In Azure, disk performance is throttled by the VM size and Disk SKU. Under-sizing here causes the desktop to freeze.
  - **Network:** Egress bandwidth per user. Since VDI is essentially video streaming, understanding the screen change rate is vital for calculating Azure egress costs.

3.2 Application Rationalization

Migration provides a unique opportunity to clean up the application estate. "Application Sprawl" effectively taxes the migration team.

- **Assessment Strategy:** Applications should be categorized using the "5 R's" framework:
  - **Retain:** Migrate to AVD/W365. These are critical Win32 apps.
  - **Retire:** Legacy apps with zero usage in the last 6-12 months.
  - **Replace:** Replace legacy client-server apps with SaaS alternatives (e.g., move from an on-prem ERP client to the web-based version). This reduces the complexity of the image.
  - **Rehost:** Move the backend database to Azure SQL but keep the frontend on VDI.
  - **Refactor:** Rewrite the app to be cloud-native (rare for VDI projects).
- **Technical Compatibility:** Identify apps with hard dependencies on hardware dongles, MAC addresses (licensing), or jumbo frames, as these often break in Azure virtualization.

3.3 Network Topology Review

Latency is the enemy of VDI. The physical distance between the user and the Azure datacenter dictates the user experience.

- **Latency Thresholds:**
  - **< 50ms:** Excellent Experience (CAD/Video editing feasible).
  - **50ms - 100ms:** Good Experience (Standard Office work).
  - **100ms - 150ms:** Acceptable (Task worker, light typing).
  - **> 150ms:** Poor Experience (Visible typing lag, mouse trailing).
- **Assessment:** Use tools like the Azure Speed Test or Connection Experience Indicator to map user locations to optimal Azure regions. If users are globally distributed, the architecture must support multi-region Host Pools.

4. Technical Migration Runbook

This section details the specific workstreams required to execute the migration. It is structured to serve as a high-level Gantt chart inputs.

4.1 Workstream 1: Foundation (Azure Landing Zone)

The Azure environment must be prepared to receive the workloads. This involves setting up the "plumbing" of the cloud data center.

- **Identity Strategy:**
  - **Entra Connect:** Ensure on-premises Active Directory Domain Services (AD DS) is syncing to Microsoft Entra ID (formerly Azure AD). This is required for user assignment.
  - **Hybrid Join:** Configure Entra Connect to sync the "Computer" objects. AVD Session hosts generally perform best when Hybrid Entra ID Joined, allowing them to accept GPOs from the on-prem domain controllers while benefiting from cloud identity features like Intune management and Conditional Access.
  - **Cloud-Only Identity:** For greenfield or Windows 365 deployments, pure Entra ID Join is preferred to remove the dependency on line-of-sight to domain controllers.
- **Networking Architecture:**
  - **Hub-and-Spoke:** Deploy a "Hub" VNet containing shared services (Azure Firewall, ExpressRoute Gateway, Domain Controllers) and "Spoke" VNets for the Host Pools. This isolates VDI traffic and simplifies security peering.

    - **IP Addressing:** Ensure the Azure VNet address space does not overlap with on-premises networks to allow for VPN/ExpressRoute connectivity.
    - **DNS Resolution:** AVD hosts must be able to resolve on-premises resources (File Servers, Databases). Custom DNS settings on the Azure VNet pointing to IaaS Domain Controllers or DNS Forwarders are mandatory.

4.2 Workstream 2: Image Management and Transformation

The "Golden Image" is the blueprint of the virtual desktop. Legacy images (PVS vDisks/VMDKs) are rarely suitable for direct import due to driver mismatches and legacy agent clutter.

- **Strategy: Build, Don't Migrate:** It is strongly recommended to build new images in Azure rather than converting on-prem images. This ensures a clean registry and prevents issues with "Ghost NICs" or legacy filter drivers from Citrix/VMware.
- **Operating System Selection:**
    - Transition from Windows Server 2016/2019 (common in Citrix XenApp) to **Windows 11 Enterprise Multi-session**. This provides the modern Windows UI and compatibility with Microsoft 365 Apps for Enterprise while maintaining high user density.
- **Optimization:**
    - **VDOT (Virtual Desktop Optimization Tool):** Run this Microsoft script on the image to disable consumer features (Xbox Live, Windows Store auto-update, telemetry) that consume unnecessary CPU cycles.
- **Automation:**
    - Use **Azure Compute Gallery** to manage image versions and replicate them to different regions for disaster recovery.
    - Tools like **Nerdio Manager** can automate the monthly patching process: spin up a VM, apply Windows Updates, run optimization scripts, sysprep, and capture the image without administrator intervention.

4.3 Workstream 3: User Profile Migration (The Shift to FSLogix)

This is often the most complex technical hurdle. Legacy solutions (Citrix UPM, VMware DEM, Roaming Profiles) file-level replication logic. AVD standardizes on **FSLogix Profile Containers**, which encapsulate the entire user profile into a VHDX file that is mounted as a virtual disk at logon.

4.3.1 Storage Architecture

FSLogix requires high-performance, low-latency SMB storage.

- **Azure Files Premium:** The standard recommendation. It offers provisioned IOPS and burst capability.
- **Azure NetApp Files:** Required for large-scale enterprise deployments (>1,000 concurrent users) or extremely IOPS-heavy workloads (developers compiling code). It offers sub-millisecond latency but at a higher cost.
- **Permissions:** Granular NTFS permissions are required on the share. The root folder requires "List Folder" for users, while the subfolders (containers) require "Modify" for the specific user (Creator Owner).

4.3.2 Migration Methodology

Migrating data from a file-based profile (UPM) to a disk-based container (FSLogix) is not a simple copy-paste.

1. **Greenfield Approach (Recommended):** Start users with a fresh profile. Use OneDrive "Known Folder Move" (KFM) to sync Desktop, Documents, and Pictures to the cloud *before* migration. When the user logs into AVD, OneDrive pulls the data down into the new FSLogix profile. This eliminates the risk of carrying over corruption.
2. **Conversion Approach:** If persistence is mandatory (e.g., custom app data in AppData\Roaming), use the FSLogix `frx copy-profile` utility. This command-line tool can convert a local or roaming profile into a VHDX container.
   - *Command:* `frx copy-profile -filename \\share\containers\user.vhdx -username DOMAIN\User -size-mbs 30000`.
   - *Configuration:* Set the `VHDLocations` registry key in `HKLM\SOFTWARE\FSLogix\Profiles` on the session hosts to point to the new Azure Files share.

4.4 Workstream 4: Application Delivery (MSIX App

Attach)

To maintain a clean image, modern architecture favors decoupling applications from the OS.

- **MSIX App Attach:** This technology allows applications to be packaged inside a virtual disk (VHDX/CIM). The OS "reads" the app from the disk without installing it.
  - **Process:**
    1. **Packaging:** Use the MSIX Packaging Tool to capture the application installation.
    2. **Expansion:** Use the `msixmgr` tool to expand the MSIX package into a VHDX image.
    3. **Staging:** Upload the VHDX to the Azure Files share.
    4. **Registration:** Configure the AVD Host Pool to recognize the package.
  - **Certificate Requirement:** All MSIX packages must be signed with a code-signing certificate trusted by the session hosts.
- **Benefits:** This drastically reduces the number of Golden Images required. Instead of a "Finance Image" and an "HR Image," you have one "Corporate Image," and Finance apps are attached dynamically at login.

5. Migration Scenarios and Pathways

Different organizational needs dictate different migration paths. We identify three primary scenarios.

5.1 Scenario A: The "Modernize" Path (Legacy to Native AVD)

- **Profile:** Organization wants to exit the datacenter entirely, remove third-party licensing costs (Citrix/VMware), and simplify management.
- **Target:** Native Azure Virtual Desktop using Windows 11 Multi-session.
- **Architecture:** Control plane is 100% Microsoft. Citrix Delivery Controllers and VMware Connection Servers are decommissioned.
- **Key Challenge:** Loss of granular controls provided by Citrix (e.g., highly detailed

policy engines, Session Recording, specific peripheral redirection support).
- **Outcome:** Maximum cost reduction and simplified "single vendor" stack.

5.2 Scenario B: The "Hybrid" Path (Citrix DaaS on Azure)

- **Profile:** Organization has deep reliance on Citrix HDX features (e.g., specialized medical imaging apps), requires hybrid management (some users on-prem, some in Azure), or has a sunk cost in Citrix licenses.
- **Target:** Citrix DaaS (formerly Citrix Cloud) managing workloads in Azure.
- **Architecture:** The Control Plane moves to Citrix Cloud. "Cloud Connectors" are deployed in the Azure VNet to proxy communication. Workloads run on Azure VMs but are brokered by Citrix.
- **Key Challenge:** Managing the cost of *both* Azure compute and Citrix user licensing. Complexity of maintaining Cloud Connectors.
- **Outcome:** Best-in-class user experience over poor networks (HDX protocol) and retention of familiar management tools.

5.3 Scenario C: The "SaaS" Path (Physical/VDI to Windows 365)

- **Profile:** Organization needs a predictable budget, simple management (Intune), and 1:1 user persistence (e.g., developers needing admin rights).
- **Target:** Windows 365 Enterprise Cloud PCs.
- **Architecture:** No Azure VNet management required (unless using Azure Network Connection). Microsoft manages the NIC and the VM.
- **Key Challenge:** Higher cost per user compared to optimized multi-session AVD. Less flexibility in storage performance tuning.
- **Outcome:** Lowest administrative overhead; "PC in the cloud" experience.

---

6. Financial Modelling: ROI and Cost-Benefit Analysis

The shift from CapEx to OpEx requires a rigorous financial model. In the legacy world, costs were "lumpy" (step-function investments in hardware). In the cloud, costs are linear and consumption-based.

6.1 Cost Drivers in Azure

Unlike the flat cost of a SAN, Azure storage and compute are billed on granular metrics.

Cost Component	Description	Variable Factors
Compute (VMs)	The hourly cost of the Session Hosts.	Instance Size (e.g., D8s_v5), Family (D-series vs E-series), Runtime hours, Region.
Storage (Disks)	The OS disks for the VMs.	Tier (Standard HDD vs Premium SSD), Size (128GB vs 256GB).
Storage (Files)	User Profile storage (FSLogix).	Capacity (GB) and Transactions (Read/Write operations).
Networking	Data leaving Azure (Egress).	**Egress traffic is billable.** VDI is pixel streaming; creating heavy outbound traffic. Ingress is free.
Licensing	Operating System rights.	Win 10/11 Enterprise E3/E5 includes AVD access rights. Server OS requires RDS CALs with SA.

6.2 Cost Optimization Levers

To achieve a positive ROI, the following levers must be pulled:

- **Multi-session Density:** The most critical factor. By stacking 16-24 users on a single D16s_v5 VM, the per-user compute cost drops significantly compared to single-user VDI.
- **Reserved Instances (RI):** Committing to 1 or 3 years of compute capacity for the "base load" (machines running 24/7) can yield savings of up to 72% compared to Pay-As-You-Go rates.
- **Azure Hybrid Benefit (AHB):** Applying existing on-premises Windows Server licenses to Azure VMs can reduce the hourly run rate by removing the OS cost component.
- **Scaling Plans (Autoscale):** Configuring the environment to power off VMs during nights and weekends (e.g., scaling down to 10% capacity) can reduce compute bills by 50-60%. This is impossible in on-prem environments where power savings are negligible.

6.3 ROI Calculation Template

Formula:

$$ROI = \frac{(\text{Total Benefits} - \text{Total Costs})}{\text{Total Costs}} \times 100$$

Total Benefits (Savings):

- **Hardware Avoidance:** Cost of refreshing SAN/Servers (amortized over 3-5 years).
- **Licensing Avoidance:** Elimination of Citrix/VMware renewals + Microsoft RDS CALs (if moving to Win 10/11).
- **Facilities:** Reduction in Datacenter power, cooling, and rack space.
- **Operational Efficiency:** Reduction in FTE hours spent on "keeping the lights on" (patching hypervisors, upgrading firmware).

Total Costs (Investment):

- **Migration Project:** Professional services, labor, and parallel run costs.
- **Azure Consumption:** The monthly Azure bill.
- **Training:** Upskilling staff on Azure/Nerdio/Intune.

6.3.1 Sample TCO Comparison (500 Users / 3 Years)

Cost Category	Legacy On-Premises (3 Years)	Azure Virtual Desktop (3 Years)
Infrastructure (HW)	$450,000 (Servers, SAN, Networking)	$0 (Shifted to Consumption)
Compute Consumption	$30,000 (Power/Cooling)	$280,000 (Azure VMs + Storage)
Licensing	$300,000 (Citrix/VMware + MS RDS)	$0 (Included in M365 E3/E5)
Admin/Ops Labor	$300,000 (Dedicated VDI Admins)	$150,000 (General Cloud Admins)
Network Egress	$0	$25,000
Total TCO	**$1,080,000**	**$455,000**
Cost Per User/Month	**~$60**	**~$25**

Note: This model assumes aggressive use of Auto-scaling and Multi-session. Without these, AVD costs can exceed on-prem.

7. Risk Register and Mitigation

Migration involves moving critical workspaces. Risks must be quantified and managed.

Risk ID	Risk Description	Probability	Impact	Mitigation Strategy
R01	**Latency Sensitivity:** Users in remote regions experience input lag (latency > 150ms).	High	High	Deploy Host Pools in multiple Azure regions closer to users. Implement **RDP Shortpath** to utilize UDP transport for better resilience.
R02	**Legacy App Compatibility:** Critical LOB apps fail on Windows 11 Multi-session.	Medium	High	Test with MSIX App Attach. If incompatible, deploy a separate Host Pool using Windows 10 Single Session or Windows Server 2019.
R03	**Data Egress Costs:** Unanticipated video/data streaming causes billing spikes.	Medium	Medium	Implement Azure Policy to restrict bandwidth-heavy apps. Use RDP properties to cap frame rates or disable media

				redirection features.
R04	**Profile Corruption:** FSLogix containers lock files, preventing login.	Low	High	Configure `VHDLocations` with **Cloud Cache** (local caching of profile) to tolerate storage blips. Use high-availability storage (ZRS).
R05	**Capacity Limits:** Hitting Azure Subscription Quota limits for vCPUs during rollout.	Low	Critical	File Quota Increase Requests with Microsoft Support *weeks* before rollout. Monitor limits via Azure Advisor.