MIGRATION CHECKLIST

Citrix PVS → Azure Virtual Desktop

A field-ready, phase-by-phase checklist for architects planning and executing a Citrix XenDesktop/PVS-to-AVD migration.

Prepared by **Chinwike Onyia** — Lead Architect, Endpoint Management & Security

Companion checklist to "From Citrix PVS to Azure Virtual Desktop: A Deep-Dive Migration Blueprint for Architects."

▸ At A Glance: The Seven Phases

Phase	Objective
0 — Assessment & Planning	Inventory the Citrix estate, rationalise apps, map personas, set SLOs
1 — Landing Zone & Hybrid Identity	Stand up Azure networking, RBAC and hybrid identity foundations
2 — Image Conversion & Engineering	Convert PVS vDisk into a cloud-ready, versioned AVD golden image
3 — Host Pools & App Delivery	Configure host pools, load balancing, scaling and app publishing
4 — User Profiles & Data (FSLogix)	Provision profile storage and migrate user profile data
5 — Testing, UAT & Optimisation	Validate performance and experience with representative personas
6 — Cutover & Decommission	Migrate in waves, stabilise, then retire the legacy Citrix estate

How To Use This Checklist

This document turns the migration blueprint into an execution tool. It's organised into the same phases as the underlying methodology — Assessment, Landing Zone, Image Engineering, Host Pools & Delivery, Profiles, Testing, Cutover — plus cross-cutting Networking/Security, Monitoring/DR, and Governance sections that apply throughout.

Suggested use:

- Work top to bottom within a phase, but treat phases as overlapping streams, not a strict waterfall — Landing Zone and Image Engineering can run in parallel, for example.
- Assign an owner and target date to each unchecked item before a phase kicks off; an unowned checklist item is the most common source of slipped cutover dates.
- Use the Pre-Flight Sanity Check near the end as a gate before any wave enters cutover — every item there maps to a real, recurring failure pattern in Citrix-to-AVD migrations.
- The Sign-Off section at the end is designed to be a literal go/no-go gate for each migration wave, not just a formality.

A box left unchecked is not a blocker by default — it's a flag to make a conscious decision (do it, defer it, or explicitly accept the risk) rather than an accidental gap.

PHASE 0 Assessment & Planning

Estate Inventory

- ☐ Document all Delivery Controllers (versions, roles, HA configuration)
- ☐ Document StoreFront servers and store configuration
- ☐ Document License Server (model, edition, expiry)
- ☐ Document PVS servers, farms, sites, and stores
- ☐ Document SQL back-end (instance, version, HA/DR configuration)
- ☐ Inventory all machine catalogues and delivery groups
- ☐ Inventory all vDisks (versions, assigned catalogues, update schedule)
- ☐ Inventory VDA versions in use across the estate

Application Rationalisation

- ☐ Decide RemoteApps vs. full desktops per application/persona
- ☐ Assess each application's multi-session compatibility
- ☐ Plan packaging/installation approach (MSIX, App-V replacement, native install)
- ☐ Flag applications with GPU, COM/ActiveX, or middleware dependencies

Persona Mapping

- ☐ Identify task-worker, knowledge-worker, and engineering/power-user cohorts
- ☐ Establish concurrency assumptions per persona
- ☐ Establish session density assumptions per persona

Profile Strategy

- ☐ Map existing UPM/Roaming profiles to FSLogix Profile Containers
- ☐ Map existing UPM/Roaming profiles to FSLogix Office Containers where applicable
- ☐ Select storage class (Azure Files Premium vs. Azure NetApp Files)

- ☐ Select Azure region/region pair for profile storage

Security Posture Review

- ☐ Review existing Conditional Access policies for applicability to AVD
- ☐ Review MFA enforcement model for end users and admins
- ☐ Review device compliance policy requirements
- ☐ Review target RBAC model for AVD-related roles

Test Plan

- ☐ Define pilot user cohorts
- ☐ Define acceptance criteria for pilot sign-off
- ☐ Define rollback procedure for a failed pilot or wave

Readiness Checks

- ☐ Confirm subscription vCPU, VM family, storage, and network quotas are sufficient
- ☐ Confirm AVD entitlement (licensing) covers the target user base
- ☐ Confirm FSLogix usage rights are in place
- ☐ Establish VPN or ExpressRoute connectivity for hybrid dependencies (AD, DNS, file services, LOB apps)
- ☐ Confirm Azure AD Connect is healthy and synchronising
- ☐ Decide device join model (Hybrid Azure AD join vs. Azure AD join)
- ☐ Complete vDisk snapshots ahead of any destructive changes
- ☐ Export/back up Citrix site configuration
- ☐ Complete SQL back-end backups
- ☐ Complete discovery of print and peripheral requirements
- ☐ Agree SLO targets with stakeholders: logon duration, profile attach time, session density, latency

PHASE 1 Landing Zone & Hybrid Identity

Landing Zone

- ☐ Create Resource Groups per environment (Prod / UAT / Dev) and workload domain
- ☐ Deploy VNet/subnet: AVD Session Hosts (no public inbound; controlled egress)
- ☐ Deploy VNet/subnet: Management (bastion, automation, jump box)
- ☐ Deploy VNet/subnet: Storage-PE (private endpoints for Azure Files/ANF)
- ☐ Apply NSGs with deny-by-default, least-privilege allow rules
- ☐ Deploy Azure Firewall or NVA in the hub for egress control and UDRs
- ☐ Configure content filtering on the firewall/NVA
- ☐ Configure DNS conditional forwarders and hybrid name resolution

Hybrid Identity

- ☐ Validate Azure AD Connect sync health end-to-end
- ☐ Confirm session host join model: Azure AD join or Hybrid Azure AD join
- ☐ Prepare OU / security group structure for policy scoping
- ☐ Define PIM (Privileged Identity Management) assignments for AVD Admins

- ☐ Define PIM/RBAC assignments for Image Admins
- ☐ Define PIM/RBAC assignments for Storage Admins

PHASE 2 Image Conversion & Engineering (PVS → AVD)

Convert the Image

- ☐ Export/convert the PVS vDisk to VHD/VHDX format
- ☐ Remove the PVS Target Device software
- ☐ Remove the Citrix VDA
- ☐ Remove Citrix-specific optimisations, services, and drivers

Install the AVD Stack

- ☐ Install the AVD Agent and Agent Bootloader
- ☐ Install FSLogix
- ☐ Install endpoint protection agent (e.g. Defender)
- ☐ Install monitoring/observability agents

Optimise for Multi-Session

- ☐ Apply Windows multi-session optimisations to scheduled tasks
- ☐ Optimise/disable unnecessary services
- ☐ Optimise the Windows Search indexer
- ☐ Configure Delivery Optimisation settings
- ☐ Add antivirus exclusions for FSLogix VHD(X) paths

Capture & Publish

- ☐ Generalise the image with Sysprep (if required)
- ☐ Upload the VHD to Azure Storage
- ☐ Create a Managed Image from the upload
- ☐ Publish the image to Azure Compute Gallery (Azure Image Gallery) with a version number
  - ☐ Bake in / enforce core FSLogix registry settings via image, GPO, or Intune configuration profile

Governance

- ☐ Tag the image with environment, owner, and version metadata
- ☐ Confirm the Dev → UAT → Production promotion workflow is defined
- ☐ Establish change control for future image updates

PHASE 3 Host Pools, Application Delivery & Autoscaling

Host Pools

- ☐ Decide Pooled vs. Personal host pool per persona/workload
- ☐ Select load-balancing algorithm: breadth-first or depth-first
- ☐ Stand up a validation/staging host pool separate from production

Scaling

- ☐ Define a scaling plan aligned to business hours and concurrency patterns
- ☐ Set minimum and maximum host counts
- ☐ Define ramp-up and ramp-down schedules
- ☐ Configure hibernation or stop/deallocate behaviour for off-hours

Application Delivery

- ☐ Install and validate all applications on the master image
- ☐ Publish RemoteApps to the appropriate user groups
- ☐ Publish full desktops to the appropriate user groups
- ☐ Validate application start-up times
- ☐ Validate application licensing works in the AVD context
- ☐ Validate printer, font, and middleware dependencies
- ☐ Validate COM/ActiveX component dependencies
- ☐ Validate GPU requirements where applicable

PHASE 4 User Profiles & Data (FSLogix)

Storage & Network

- ☐ Provision Azure Files Premium or Azure NetApp Files for profile storage
- ☐ Deploy Private Endpoints for the storage account/ANF volume
- ☐ Confirm AD and DNS integration for the storage layer
- ☐ Enable SMB signing and TLS where applicable

Permissions

- ☐ Set root-level NTFS permissions: EUC Admins and System = Full Control
- ☐ Set Creator Owner permissions on subfolders and files
- ☐ Grant per-user Modify access to each user's own profile folder
- ☐ Configure share-level permissions for EUC Admins and session host computer accounts

Migration

- ☐ Identify all UPM, Roaming, and Local profiles requiring migration
- ☐ Decide whether to pre-create user folders or let FSLogix create them at first logon
- ☐ Seed user data via Robocopy (or equivalent), preserving ACLs
- ☐ Validate pilot profile attach performance
- ☐ Validate OST handling for Outlook
- ☐ Validate Teams and OneDrive cache behaviour
- ☐ Confirm FSLogix exclusions are applied correctly

PHASE 5 Testing, UAT & Optimisation

Pre-Migration Validation

- ☐ Verify session host health and successful image boot
- ☐ Verify AVD agent registration

- ☐ Assess profile container attach performance and storage IOPS headroom
- ☐ Validate name resolution and Active Directory reachability from session hosts
- ☐ Validate line-of-business application connectivity/paths

Pilot

- ☐ Select representative light, medium, and heavy user personas for the pilot
- ☐ Measure logon duration (seconds) against SLO
- ☐ Measure profile attach time (seconds) against SLO
- ☐ Measure session density per VM against plan
- ☐ Measure CPU, RAM, disk queue length, and network latency
- ☐ Triage and remediate: apply Group Policy tweaks as needed
- ☐ Triage and remediate: repackage applications as needed
- ☐ Triage and remediate: adjust storage tier as needed

PHASE 6 Production Cutover & Decommission

Cutover Approach

- ☐ Confirm Citrix and AVD will run side-by-side during the transition window
- ☐ Finalise the wave plan, organised by business unit or persona
- ☐ Confirm monitoring coverage is active for the cutover window
- ☐ Define the stabilisation period required before the next wave proceeds

Decommission (Post-Acceptance Only)

- ☐ Retire Provisioning Services (PVS)
- ☐ Retire Delivery Controllers
- ☐ Retire StoreFront
- ☐ Retire the License Server
- ☐ Decommission Citrix SQL databases after confirming no remaining dependencies
- ☐ Update the CMDB
- ☐ Update network diagrams
- ☐ Update disaster recovery documentation

CROSS-CUTTING Networking & Security Design

Network Topology

- ☐ Confirm hub-and-spoke topology with centralised security in the hub
- ☐ Confirm peering between hub and spokes
- ☐ Confirm VPN or ExpressRoute connectivity to on-premises
- ☐ Apply User Defined Routes (UDRs) through Azure Firewall/NVA where required

Security Guardrails

- ☐ NSGs configured with least-privilege rules and default-deny inbound
- ☐ Azure Firewall/NVA configured with FQDN groups, threat intelligence, IDS/IPS as needed

- ☐ Conditional Access enforced for AVD user access
- ☐ MFA enforced for administrators
- ☐ RBAC scoped correctly; PIM enabled for just-in-time elevation
- ☐ Encryption at rest configured (platform-managed or customer-managed keys)
- ☐ Encryption in transit confirmed (SMB signing / HTTPS)
- ☐ Key Vault deployed for secrets management
- ☐ Managed Identities used for automation (no embedded credentials)
- ☐ Session hosts hardened to CIS/OS baseline standards
- ☐ LAPS/PLAPS configured for local admin account rotation

CROSS-CUTTING Monitoring, Observability & Disaster Recovery

Monitoring & Logging

- ☐ Azure Monitor / Log Analytics collecting AVD service logs
- ☐ Azure Monitor / Log Analytics collecting session host logs
- ☐ Azure Monitor / Log Analytics collecting FSLogix logs
- ☐ Azure Monitor / Log Analytics collecting security logs
- ☐ Dashboards built for logon duration, session density, failed sign-ins, profile attach failures
- ☐ Alerts configured for CPU and RAM thresholds
- ☐ Alerts configured for disk latency
- ☐ Alerts configured for FSLogix mount errors
- ☐ Alerts configured for broker/connection failures

Backup & Disaster Recovery

- ☐ Snapshots/backups configured for Azure Files or ANF profile data
- ☐ Retention periods aligned to agreed RPO/RTO
- ☐ Previous golden image versions retained for rapid rollback
- ☐ Storage mirrored to a region pair for DR
- ☐ Host pool re-provisioning in the secondary region documented

CROSS-CUTTING Governance, Change & Runbooks

- ☐ Change management process defined: image versioning, staged promotion, rollback criteria
- ☐ Resource tagging standard applied: environment, owner, cost centre, image version, OS build
- ☐ Access model defined: AVD Admin, Image Admin, Storage Admin, Security Reader roles
- ☐ Audit trail confirmed via Activity Logs and Log Analytics

Runbooks / SOPs Authored

- ☐ Image update and promotion runbook
- ☐ Drain, patch, and reboot (session hosts) runbook
- ☐ Scaling plan adjustment runbook for peak events
- ☐ Profile corruption restoration runbook

- ☐ Incident response runbook for connection issues and degraded performance

Common Pitfalls — Pre-Flight Sanity Check

Run through this list before any wave enters cutover. Each item reflects a recurring, avoidable failure pattern in Citrix-to-AVD migrations.

Pre-Flight Sanity Check

⚠ Are we treating AVD like Citrix? Re-check any 1:1 Citrix paradigm carried over without re-validating it fits AVD's model.

⚠ Is profile storage sized for real IOPS, not an estimate? Confirm against pilot telemetry, not the original sizing guess.

⚠ Have Private Endpoints actually been deployed for storage, or was this step skipped under time pressure?

⚠ Was UAT run with representative personas (light/medium/heavy), or only an IT smoke test?

⚠ Does a documented, tested rollback runbook exist for this wave — not just a rollback intention?

Migration Wave Sign-Off

Complete once per migration wave before proceeding to cutover. All roles below should approve before the wave is declared go-live.

Role	Name	Approved (Y/N)	Date
Migration Lead			
AVD / Cloud Architect			
Security & Compliance			
Application Owner			
Change / Service Management			
Business Sponsor			

Wave name / scope: _____

Planned cutover date: _____