DESIGN Document

Journey to Modern Workplace

Peter Cashen & Nic Fuller

July 2025

# Table of Contents

Table of Contents 1

1. Executive Summary 3

2. Current State Overview 3

3. Target State Vision (PC) 19

4. Key Prerequisites (NF) 20

5. Critical Decisions & Planning Considerations (NF) 25

6. Modern Management Foundations to Implement (PC) 32

7. Application Modernisation 33

8. Windows Update for Business 33

9. User Data and Enterprise State Roaming 33

10. Security and Endpoint Protection 33

11. Device Lifecycle Management 33

12. Reporting, Monitoring & Ongoing Support 34

13. Change Management & User Communication 34

14. Pilot & Rollout Strategy 34

15. Known Challenges and Mitigations 34

16. Implementation Checklist 35

## Purpose

This document is to provide a guide for planning for moving customers to a Modern Cloud managed Windows 11 workplace managed via Microsoft Intune.

## Abbreviations

Several abbreviations are used throughout this document. The below table has been created to help clarify the meaning of each abbreviation:

|  |  |
| --- | --- |
| Abbreviation | Definition |
| Example | Example |

## Document Approvals

|  |  |  |
| --- | --- | --- |
| Name | Job Title | Email |
| Dan Lewis | Managing Lead Architect | dan.lewis@oneadvanced.com |
|  |  |  |

## Version Control

|  |  |  |  |
| --- | --- | --- | --- |
| Date | Version | Issued by | Changes |
|  |  |  |  |

1. Executive Summary

Overview of the transition

Benefits of moving to modern management

Scope and intended audience.

Presales – considerations, business requirement

1. Current State Overview

Before embarking on the transition to a cloud-managed Modern Desktop environment, it is crucial to perform a thorough assessment of your organisation’s current desktop management setup. This Current State Overview section provides a structured approach to document all key aspects of the existing environment. By capturing details on devices, infrastructure, policies, and operations, IT planners can identify gaps and plan a smooth migration from an on-premises SCCM (ConfigMgr) managed model to Intune (Microsoft Endpoint Manager) cloud management. Below, we break down the major domains to assess and the types of data to collect in each area, using clear subheadings and bullet points for readability.

* 1. Device Inventory

Begin by cataloguing all endpoint devices in scope. A comprehensive device inventory helps gauge the scale of the migration and spot any legacy endpoints that may need upgrades or special handling. Key data points to document include:

Device Count and Types: Total number of client devices and their form factors (desktops, laptops, mobile devices, tablets, etc.). Include both corporate-owned and any BYOD/personal devices that access corporate resources.

Hardware Details: For each device model, record specifications such as make/model, CPU, RAM, storage, and age or purchase date. Identify any aging hardware that may not meet Windows 10/11 requirements or might be due for refresh.

Operating System Versions: List the OS platform and version on each device (e.g., Windows 10 22H2, Windows 11, macOS, etc.). Highlight devices running outdated or unsupported OS versions, for example, any remaining Windows 7/8 systems should be flagged for upgrade or replacement. Modern cloud management via Intune requires Windows 10 or later for full support.

Enrolment/Join Status: Note each device’s identity state: domain-joined to on-prem AD, Azure AD-joined, Hybrid Azure AD-joined, or Azure AD registered. This will indicate readiness for Intune enrolment (since Intune primarily manages Azure AD-joined or hybrid-joined devices). If devices are not yet Azure AD-aware, plan for steps to integrate them into Azure AD.

Usage and Locations: If available, include information on where devices are used (office, remote, specific regions) and usage patterns. This can help in planning content distribution and support (for example, a large population of remote laptops might necessitate different enrolment strategies).

Suggested tools: Leverage your existing SCCM database or asset management reports to export hardware and software inventory. SCCM’s hardware inventory can provide lists of devices with their OS and specs. Many organisations also run PowerShell scripts or use IT asset management tools to gather detailed inventories. Ensure the inventory encompasses all devices that will need management under Intune, including any that may not currently be in SCCM (e.g. remote users’ PCs not regularly connecting). This device inventory forms the foundation of your migration planning.

* 1. Configuration Manager (SCCM) Infrastructure

Document the current SCCM/MECM infrastructure and configuration that supports your legacy desktop management. This includes the architectural components, sites, and system roles that are in place on-premises. Key areas to assess and record:

Site Topology and Roles: Diagram or list your Configuration Manager hierarchy. Include the primary site (or central administration site if applicable) and any secondary sites. Enumerate all site system roles, e.g., management points, distribution points (DPs), software update points (SUP/WSUS), reporting services points, etc along with the servers hosting them and their locations. For each site server and role, capture the server OS version and hardware specs to understand the current hosting environment.

SCCM Version and Health: Note the current SCCM build (version and build number) and the SQL Server version for the site database. Verify you are on a supported version and have applied recent updates. It’s also wise to check the health status of key components (site status, component status) and any known issues. For example, confirm that distribution points are healthy and content replication is working.

Content Distribution Methods: Review how software and updates are distributed across your network today. Document the number and placement of DPs, any use of branch caching or peer-to-peer distribution, and whether cloud distribution (Cloud Distribution Point or Delivery Optimization) is in use. Identify network boundary groups and throttling settings used to control bandwidth. This information will help plan for content delivery in Intune (which relies more on internet distribution and Delivery Optimization).

Client Details: Record the SCCM client agent deployment status across devices (what percentage of endpoints have the client installed and healthy). Also note client settings in effect (e.g., polling intervals, cache size, etc.) that might be relevant when transitioning to Intune policies.

AD Integration and Schema Extensions: Verify if Active Directory schema was extended for SCCM and document any AD dependencies (like System Management container permissions). Also note the discovery methods in use (AD discovery for users/devices) and any forests being scanned. This indicates how tightly SCCM is woven into AD, which will shift as Intune uses Azure AD.

Current Workloads and Integrations: List which endpoint management workloads SCCM is handling (software distribution, patching, OS imaging, compliance, etc.), and whether any of these are already offloaded or integrated with cloud services. For instance, note if Cloud Management Gateway (CMG) is deployed to manage internet-based clients, if Tenant Attach or co-management with Intune is already enabled for any devices, or if Desktop Analytics (now deprecated) was used for update planning. Also mention any integration with third-party tools (for software packaging, endpoint security, ITSM, etc.) that tie into SCCM. Each integration point may need reconfiguration or an Intune-compatible replacement in the new model.

By compiling a detailed picture of the SCCM infrastructure, you can plan which components will be retired, which might remain in co-management (if any), and ensure nothing critical is overlooked. (For example, documenting “Boundary Groups X and Y cover remote offices using on-prem DPs” will highlight that those offices might require additional internet bandwidth or use of Delivery Optimization when moved to cloud.)

* 1. Identity and Directory Services

Assess and document your current identity model for both users and devices, as this underpins authentication and access in a modern cloud-managed environment. Intune and other modern management tools are tightly integrated with Azure AD (Entra ID) for identity-driven control, so understanding your present directory setup is vital:

Active Directory (On-Premises): Describe your Active Directory environment, number of domains, forests, and the organisational unit (OU) structure used for computers and users. Note how devices are joined: most mid-large organisations have computers joined to AD domains. If multiple AD domains or forests exist, document trust relationships and how SCCM is interacting with each (SCCM discovery settings can reveal which domains/OU it manages).

Azure AD (Entra ID): Indicate whether an Azure AD tenant is in place and if Azure AD Connect is syncing on-premises identities to Azure AD (most Office 365 or Microsoft 365 enterprises will have this). Confirm the identity synchronization status and if Hybrid Azure AD Join is enabled for Windows devices. Knowing the percentage of devices that are already Hybrid AAD joined versus purely on-prem AD joined will influence your Intune enrolment approach. If devices are only AD-joined currently, plan for enabling Hybrid join or moving to cloud join during the migration.

User Identity and Authentication: Document how users currently authenticate to resources. For example, do you use AD FS or federation services for enabling cloud logon (which might be the case if using Office 365)? Are users leveraging multi-factor authentication today for any services? In a modern desktop scenario, Azure AD-based Conditional Access and MFA are common, so understanding current practices helps in planning equivalent or improved controls with Intune/Entra ID.

Groups and Role Structure: Inventory the AD security groups or distribution groups that are used for managing devices or users (e.g. groups used for software deployments, GPO filtering, or SCCM collections). Analyse your user and device group’s structure, this is important because Intune will use Azure AD groups (synced from AD or cloud-only) for targeting apps and policies. Note any dynamic grouping logic or complex nesting that might need to be recreated in Azure AD. Also, list any administrative roles or service accounts in AD that relate to device management (for example, any service accounts SCCM uses, or any delegation of AD permissions for managing computers).

Identity Security Posture: Include any current identity-related security measures. For instance, if password policies or lockout policies are enforced via GPO, if smart card or certificate-based authentication is used for logon, or if there are naming conventions and tagging of device objects in AD. These details could affect how you design Azure AD join and Intune compliance policies. Additionally, note if any identities (user or device) are purely cloud (Azure AD only) as they will have no on-prem GPO/SCCM footprint but will need Intune policies.

Ensuring that your Azure AD tenant is prepared is a key pre-migration step, Intune’s cloud management relies on it. In summary, capture the current state of AD/Azure AD integration so you can plan to transition policies and enrolment flows accordingly. For example, if many devices are not yet Hybrid Azure AD joined, you might include a phase to enable that for existing AD-joined machines to smooth their Intune enrolment.

(Intune uses Azure AD for device registration and user targeting, so any gaps in syncing or Azure AD setup must be addressed before migration. The planning should also consider identity cleanup e.g. removing stale computer accounts, so the new environment has accurate device records.)

* 1. Group Policy and Configuration Settings

Most large organisations maintain numerous Group Policy Objects (GPOs) and configuration scripts to enforce settings on Windows PCs. As part of the current state assessment, inventory all GPOs and related configuration baselines that apply to your endpoints. This domain often requires careful analysis, since Intune’s MDM policies will eventually replace or replicate many of these settings. Key steps and data to collect:

GPO Inventory: Export a list of all GPOs in your Active Directory, especially those linked to the OUs containing client computers and those applied to users. Document the purpose of each GPO and major settings it enforces (e.g., security options, firewall rules, Internet Explorer settings, Office ADMX policies, etc.). Pay attention to GPOs critical for security (like password policies, BitLocker settings, Windows Update settings) and those configuring the user environment. This list will serve as a checklist for what needs to be mapped to Intune configuration profiles or compliance policies.

Group Policy Analytics: Take advantage of tools to analyse GPOs for cloud compatibility. Microsoft provides Group Policy Analytics in Intune to evaluate which GPO settings are supported by MDM providers. By importing your GPOs into this tool, you can generate a report showing which settings have equivalent Intune policies, which might conflict, or which are not supported in modern management. The report will categorize GPOs or settings as “supported/ready for migration” vs. “not supported” (or deprecated), helping prioritize which policies can be moved to Intune and which will require an alternative solution. Make note of any GPOs that cannot be translated directly, for example, complex logon scripts or printer deployment policies, as these will need special consideration (such as replacing with Intune PowerShell scripts or new cloud-managed approaches).

Security Baselines and Compliance Settings: If you use SCCM Configuration Baselines or scripts to enforce configuration (outside of GPO), list those as well. Some organisations implement CIS or STIG security baseline settings via GPO or SCCM baselines, ensure those settings are captured in your inventory. Intune offers Security Baselines templates and custom CSP policies, but you need to know which settings are currently in effect on your PCs to configure Intune accordingly.

Local Policies & Scripts: Document any local machine policies or startup/login scripts (for example, logon scripts that map drives or deploy apps). These may be implemented via GPO (User logon scripts) or via SCCM (e.g., as scheduled tasks or package installs). Identify what those scripts do, as Intune might require a different method (such as Intune PowerShell scripts or use of Azure AD login scripts) to achieve the same outcomes.

Administrative Templates in Intune: Be aware that many ADMX-backed settings can be configured through Intune’s Administrative Templates or Settings Catalogue if supported. As part of the GPO analysis, mark which settings are MDM-compatible. The goal is to create a mapping of current GPO settings to future Intune policies. Microsoft’s analytics tool can even automate migrating multiple GPOs to Intune configuration profiles (with a “best effort” migration), but it’s important to review the output carefully.

Exceptions and Hard-to-Migrate Settings: Highlight any configuration that might not have a cloud-friendly equivalent. For example, GPOs that require the device to be on-prem (like certain software deployment GPOs or folder redirection policies) or settings that rely on on-prem infrastructure. These will need separate planning, e.g., replacing folder redirection with OneDrive Known Folder Move, replacing GPO software installs with Intune app push, etc. By listing these now, you can include them in the project plan for remediation or alternative solutions.

In summary, create a GPO-to-Intune matrix: for each major policy or setting, determine if it will be migrated, replaced, or retired. This ensures that moving to Intune won’t leave any important configuration unmanaged. It’s often useful to prioritize core security and compliance GPOs first, e.g., policies enforcing BitLocker, firewall, Windows UUpdate,since Intune will need to enforce those via device configuration profiles or compliance policies. Using Intune’s Group Policy analytics is highly recommended to speed up this assessment. The output will show which GPO settings can be directly migrated to MDM profiles and flag any unsupported ones (for instance, certain legacy settings with no MDM counterpart).

(Remember to involve your domain GPO administrators in this process. They often have insight into which policies are truly necessary versus old artifacts. This is a good opportunity to clean up redundant or outdated GPOs so they are not blindly replicated in the new environment.

* 1. Application Landscape

A detailed application inventory is another critical component of the current state documentation. Applications are the lifeblood of user productivity, and moving to Intune will require packaging and deploying apps in new ways. To prepare, list all the applications installed or managed in the current environment, along with relevant attributes and data points:

Application Catalog: Compile a list of all software titles deployed to users or computers. Microsoft’s planning guidance suggests starting with “a list of the apps your users regularly use.” These are the apps you’ll need on their devices in the new environment. Include in the inventory: business productivity suites (e.g., Microsoft 365 apps), line-of-business (LOB) applications, custom in-house apps, developer tools, legacy apps, web applications (especially if any rely on legacy browsers or IE mode), and even small utilities that are widely installed.

Deployment Method & Format: For each application, note how it is currently delivered and managed. Are they packaged in SCCM as “Applications” or “Packages” or deployed via GPO or scripts? Identify the installer type, MSI, EXE, Script, App-V, Microsoft Store app, etc. This will indicate how you might package it for Intune (Intune supports Win32 .intunewin packages for Win32 apps, MSIX, Store apps, etc.). For example, an MSI deployed via SCCM can likely be wrapped into an Intune Win32 package with minimal changes, whereas a complex task sequence or script-based install might require conversion to a PowerShell script deployment or a Win32 app model in Intune.

Application Owner and Criticality: Document the business owner or department for each app and its importance (critical, optional, retired). This helps prioritize testing and migration, mission-critical apps (ERP systems, security agents, etc.) must be ready for Intune deployment early. Also note if any app has licensing constraints or device-specific licensing that might be affected by reinstallation or re-enrollment.

Version and Update Info: Record the current version of each application in use and how updates are applied. Some apps may auto-update (e.g., Chrome, Zoom), some are updated via SCCM or manual processes. Knowing this helps plan whether Intune will simply deploy the latest version or if you need an update strategy (Intune can push updates for Microsoft 365 Apps and some Store apps, but third-party apps might need packaging of new versions or use of tools like Windows Package Manager).

Compatibility Considerations: Identify any known compatibility issues with newer OS or MDM management. For instance, legacy 32-bit apps or apps that require outdated frameworks (like old Java or .NET versions) should be flagged. Also, if an application currently requires a device to be domain-joined or connected to the LAN (for license servers or database access), note that dependency, it might influence whether the app can run on an Azure AD joined device off-network or if adjustments (e.g., VPN or Azure AD application proxy) are needed.

Packaging and Source Files: Ensure you have the source installation files or package definitions for each app. As part of this assessment, verify you have the latest installers or a method to repackage each app in Intune. If you have internally developed apps, check that you can obtain their installer or deployable package.

Usage Data: If possible, include metrics on application usage. SCCM’s software metering or other analytics might show which apps are actively used vs. installed but rarely used. This can feed into an app rationalization exercise, you may decide not to migrate certain rarely used or redundant applications, reducing the support burden in the new environment. Focus on the core set of applications that truly need to be managed and deployed to users going forward.

By collecting this information, you can plan the application migration in detail. Intune supports many app types (Win32, Microsoft 365, LOB MSI, store apps, etc.), but each app will need to be prepared. For example: MSI apps can be added directly or repackaged; EXE installers likely need to be wrapped into .intunewin format using Microsoft’s Win32 Content Prep Tool; apps delivered via scripts or task sequences may need new scripting in Intune or different deployment approaches. Knowing the current state ensures you don’t miss any critical software during the move.

(As a best practice, engage application owners early, let them validate if the latest versions are being used and if any upcoming upgrades should coincide with the Intune migration. Also consider using this phase to eliminate obsolete software and consolidate titles, which will simplify your modern desktop environment.)

* 1. Compliance and Device Posture

Assess the current compliance posture of your endpoints and the policies or tools used to evaluate compliance. In a legacy environment, “compliance” might be enforced through a combination of GPO security settings, SCCM compliance settings (configuration baselines), antivirus status, and manual audits. Intune will introduce device compliance policies to continuously assess if a device meets requirements (for example, requiring encryption, password, OS version, etc.). To prepare, gather information on:

Corporate Compliance Requirements: Document the security and configuration standards that all devices are expected to meet in your organisation. These could include encryption mandates (e.g., all laptops must have BitLocker enabled), password/PIN policies (e.g., require complex passwords or screen lock after X minutes), antivirus/endpoint protection requirements, minimum OS levels or patch levels, and any regulatory standards (PCI, HIPAA, GDPR, etc.) that dictate device controls. Essentially, list out what “compliant” means in your environment today.

Current Compliance Enforcement: Describe how these requirements are currently enforced or measured. For instance, are you using SCCM Configuration Baselines to check settings or configurations (like verifying BitLocker or firewall status)? Do you rely on Active Directory GPOs to enforce many of these and assume compliance if GPOs applied? Is there a separate endpoint security or vulnerability management tool that reports on compliance (for example, a tool that scans for missing patches or insecure configurations)? Compile reports if available: e.g. What percentage of devices are fully encrypted, have up-to-date AV signatures, have installed the latest Windows updates, etc.

Deviation and Risk Areas: Identify where compliance might be lacking. If, for example, your last SCCM compliance report or security audit found 10% of devices are not encrypted or 15% are behind on patching, note these as current state issues. They represent technical debt that might be addressed during the migration (since moving to Intune is an opportunity to improve compliance via stricter cloud policies and maybe Conditional Access that blocks non-compliant devices).

Policies and Baselines: Gather the details of any compliance-related policies. This overlaps with the GPO and security baseline inventory, e.g., if you have a “Windows Firewall must be ON” policy or “Device must lock after 15 minutes idle” policy, capture those details. If SCCM’s Endpoint Protection or Device Compliance feature was in use (for instance, the SCCM antimalware policy or configuration items to check settings), list those policies and what they check. Also, note if any compliance reports are regularly produced for management (like monthly security posture reports), this will indicate which metrics you need to continue tracking in the new system (Intune and Defender for Endpoint can report on similar metrics).

Certificates and Network Access: If compliance in your context extends to things like valid device certificates (for Wi-Fi/VPN) or posture checks for network access control, document how that’s done currently. For example, some organisations use Network Access Protection (NAP) (old tech) or NAC solutions that require certain health attestation. Note any such systems or requirements, as they will need integration with or replacement by Intune/Conditional Access in the future.

Exceptions Handling: Note if there are devices that are out of compliance but have exceptions (e.g., a group of kiosk PCs with no BitLocker due to lack of TPM, or developers with local admin rights as an exception to policy). Recording these will help create plans to either grandfather those in or eliminate the exceptions moving forward.

In short, the goal is to have a snapshot of how secure and compliant your devices are today, and by what means that is achieved. Intune will offer compliance policies that mirror many of these checks (for example, enforcing encryption, requiring antivirus, requiring a minimum OS version, etc.), and Conditional Access can tie compliance to resource access. Your current state analysis should set the baseline so you can measure improvement and ensure no requirement is overlooked.

(Keep in mind that moving to modern management often improves compliance visibility, for instance, Intune can provide real-time compliance status and integrate with Defender for Endpoint to assess risk. As you document the current posture, you might already identify policies to implement in Intune’s compliance center. Microsoft recommends establishing a baseline of compliance policies early in the Intune rollout.)

* 1. Security Tools and Policies

It is important to map out all security tools, agents, and configurations currently in use on endpoints, as these will influence your Intune migration strategy. Modern Desktop management will likely consolidate or replace some of these with cloud-driven solutions (for example, using Microsoft Defender and Intune’s built-in controls). In this section, document:

Endpoint Protection (Anti-Virus/Anti-Malware): Identify the primary anti-malware solution on your Windows endpoints. Many organisations use Microsoft Defender Antivirus (managed via SCCM or Group Policy), while others use third-party AV like Symantec, McAfee, CrowdStrike, etc. Note which product is installed on clients and how it’s managed. If SCCM’s Endpoint Protection policies are used to manage Defender, list those policy settings (exclusions, scan schedules). If a third-party AV is in place, how is it administered and will it remain, or are you planning to move to Defender for an integrated solution? This will determine if you need to deploy a new AV or turn off old agents during the transition.

Endpoint Detection and Response (EDR) / Advanced Threat Protection: Document any advanced security agents on endpoints (e.g., Microsoft Defender for Endpoint, CrowdStrike Falcon, Carbon Black, etc.). If you have Defender for Endpoint (MDE), note how it’s deployed (SCCM can onboard devices to MDE, or via script). Intune has native integration with MDE for reporting device risk, so knowing current deployment helps plan switching the onboarding mechanism. If another EDR is present, plan how it will co-exist or whether it will be replaced.

Disk Encryption and Key Management: Check how BitLocker (or other full-disk encryption) is managed presently. Many SCCM environments use MBAM (Microsoft BitLocker Administration and Monitoring) integrated with SCCM or stand-alone, or they simply use AD to backup BitLocker keys. Document the percentage of devices encrypted and where the recovery keys live (AD, MBAM database, etc.). If MBAM is in use, note its version and integration. Intune can manage BitLocker keys and enforce encryption compliance, so you’ll likely replace MBAM with Intune’s BitLocker management or a similar service. It’s crucial to ensure no devices slip through without their keys backed up during the transition.

Firewalls and Device Control: List how Windows Firewall is managed (GPO? SCCM policy? Third-party firewall?). If via GPO/SCCM, include the main rules or any non-default settings, as these will need to be configured in Intune’s Endpoint Security policies or CSPs. Similarly, if you use device control features (like blocking USB storage via Group Policy or an endpoint DLP/device control agent), capture that. Intune can manage some of these via policies (e.g., removable drive restrictions via configuration profiles or Defender settings).

Other Endpoint Agents: Inventory any other security or management agents running on endpoints. Common ones: VPN clients, Wi-Fi profiles, MDM agents (if any coexist, perhaps not in a pure SCCM environment), data loss prevention (DLP) agents, client certificates for network access, local admin management tools (such as Microsoft LAPS for rotating admin passwords via GPO). Each of these has a cloud analog (Intune can push VPN and Wi-Fi profiles with certificates, and Azure AD now has an integrated LAPS feature, etc.), but you need to know what’s there now. For instance, if users currently authenticate to Wi-Fi via a certificate deployed by GPO, you’ll need Intune’s certificate deployment in the new setup.

Security Monitoring and Logs: Note how security events or logs are collected. Do you have any integrations like sending Windows Defender ATP alerts to a SIEM, or using SCCM’s alerts for malware detection? If SCCM’s reporting is used for compliance or threat events, mark that down. Intune, combined with cloud tools, will have different monitoring, so ensure equivalent coverage is planned (e.g., via Defender for Endpoint and Microsoft 365 security center for unified logging).

Conditional Access and Access Policies: Although more of an identity piece, include any existing Conditional Access policies or other access control in place (via Azure AD or other solutions) that pertain to device state. For example, some organisations might already have a Conditional Access policy requiring domain-joined or compliant PCs for certain apps. Document these because after migration, you will likely adjust them to require Intune compliance. Also note if any on-prem Network Access Control (NAC) systems are used for VPN or Wi-Fi that check device posture, these might need integration with Intune’s compliance (some NACs can consume Intune compliance data via API).

Physical Security & Miscellaneous: If relevant, mention any other endpoint security measures like BIOS password management, use of security keys (YubiKeys, etc.), or application control solutions (AppLocker or Windows Defender Application Control policies currently in place). These might need to be carried over (Intune can deploy AppLocker/WDAC policies too).

By auditing the security tools and configurations in the current state, you ensure that the migration to Intune does not inadvertently weaken security. Instead, you can plan to either migrate these controls into Intune’s toolset or integrate third-party tools with Intune where possible. For example, if MBAM is currently used for BitLocker, you’d plan to use Intune’s BitLocker policy and key escrow going forward, but you must note to migrate recovery keys or escrow new ones properly. If Defender AV is currently managed by SCCM, you’ll switch to Intune Endpoint Protection policies, but make sure to capture the exclusions and settings you have now, so they can be reconfigured in Intune.

In many cases, moving to modern management with Intune is a chance to simplify the endpoint security stack, possibly consolidating to Microsoft’s integrated security if you choose. However, ensure any removal or replacement of security software is done methodically, to avoid leaving gaps. Your current state documentation of these tools is the reference to check off that each control is accounted for in the target state.

* 1. Software Updates and Patch Management

Understanding how software updates are currently managed will guide how you transition to cloud-based update methods like Windows Update for Business. Document the existing patch management process and infrastructure in detail:

WSUS/SCCM Infrastructure: Note whether you use SCCM’s Software Update Point (SUP) with WSUS to deploy Windows Updates, and any details of that setup. Include the WSUS server locations, how they sync (categories/products), and if there are multiple WSUS for different regions. If SCCM is orchestrating updates, record the maintenance windows and deployment rings (e.g., maybe an “IT pilot group” gets patches first, then a week later broad deployment, capture that policy).

Update Cadence and Compliance: Describe the current patch cycle. Are Windows patches deployed monthly on Patch Tuesday with a certain schedule? What about out-of-band patches? Also, how quickly are updates applied and what is the current compliance rate (e.g., “90% of PCs install updates within 2 weeks of release” or any SLA)? This will be useful to set targets for Intune’s update rings and measure improvement or changes. If you have recent compliance reports from SCCM or WSUS (e.g., percent of devices missing critical updates), include that data in your notes.

Feature Updates (OS Upgrades): Document how you handle major Windows 10/11 feature updates. Are these done via SCCM task sequences, servicing plans, or not done regularly? If many devices are still on older builds, that’s a consideration (Intune can manage feature updates via Windows Update for Business). List the Windows 10/11 builds in use from your device inventory to see if there’s consistency or a need to catch up older builds as part of migration.

Office and Application Updates: Include how Microsoft 365 Apps (Office) are updated if applicable, via SCCM, via Office CDN (internet), or not standardized? Similarly, note if third-party applications are patched using any mechanism (SCCM with SCUP or third-party catalogues, or manual installs). Some orgs use tools (or even SCCM packages) to update common apps like browsers, Java, Adobe, etc. Capture any such process, as you may need an Intune strategy (Intune doesn’t natively auto-update third-party apps except via Winget or store integration, so you might plan to leverage Winget/Store apps or a third-party service in the new model).

Update Policies and GPOs: Check for any Group Policies related to Windows Update (for example, policies that control automatic update settings on clients, or defer upgrades). Typically, SCCM environments have GPO set to make the computer get updates from WSUS/SCCM and not auto-reboot on its own. List those because they will need to be replaced or removed when shifting to WUfB. Intune’s update rings will take over the job, but conflicting GPOs must be addressed.

Reboot and Compliance Settings: Document how reboots for updates are handled currently (e.g., SCCM may have user experience settings to suppress reboots during work hours). Also, if using SCCM maintenance windows, note those schedules (like servers or special groups might have designated patch times). Even though Intune doesn’t have maintenance windows in the same way, knowing this helps communicate changes to users/teams.

Reporting and Monitoring: Identify what reports or dashboards are used to track update deployment. SCCM has built-in reports for compliance; if those are provided to management, note that so you can later configure Intune Update Compliance reports or Endpoint Analytics to deliver similar insights. Microsoft also provides Update Compliance via Azure (Log Analytics) if you use that, mention if in use.

Collecting this information ensures you plan an update strategy in Intune that meets or exceeds what you have now. For example, if currently you patch monthly with 2 deferral rings, you might use Intune’s Update Rings and feature update deployments to mirror that. Or if you find many devices are behind on updates, you might tighten compliance in the new environment. Be prepared to address any gaps; for instance, Intune’s Windows Update for Business will require devices to get updates from Microsoft cloud services, so check that network egress is allowed (see Networking section) and that clients don’t have policies locking them to on-prem WSUS.

(One side benefit to highlight: moving to cloud update management can reduce the load on your network from having on-prem update servers. However, it shifts load to internet bandwidth, so plan accordingly. Also, Intune’s tenant attach or co-management can allow piloting WUfB on some devices while others still use SCCM during transition, your current state data will help identify such pilot groups, e.g., “IT department laptops on Windows 11” could test Intune update rings first.)

* 1. Network and Connectivity

The network context in which your devices operate is a key part of the current state. Transitioning to Intune (cloud management) will impact network traffic patterns and require certain connectivity. Assess the following aspects of networking and document their current state:

• Corporate Network Topology: Provide an overview of your network layout relevant to client devices. List major office locations, datacenters, and remote connectivity setup. For each site, note the connectivity type (LAN, Wi-Fi) and whether users predominantly work on-network or remotely. If you have many remote users or branch offices, identify them because after moving to Intune, those clients will get updates/apps over the internet rather than via local SCCM distribution points.

• VPN and Remote Access: Document how remote users connect today. Do they use a VPN to access corporate resources? If so, is it always-on or user-initiated, and do clients need to be on VPN to receive updates/software from SCCM? Many organisations found during increased remote work that they needed solutions like Cloud Management Gateway or split-tunnel VPN to allow direct internet update traffic. If not already noted, mention if a Cloud Management Gateway (CMG) or similar is in place to manage internet-based clients. This shows how well your current setup already accommodates cloud management. If you rely heavily on VPN for management, plan for adjusting that (Intune-managed devices generally don’t require VPN for management, but they do need internet access).

• Internet Bandwidth and Proxies: Since Intune and cloud updates will fetch content from the internet (Microsoft’s CDN, Office CDN, etc.), assess your internet egress capacity. Document current bandwidth at major sites and current internet usage. For example, if patches and software come from an internal SCCM DP today, note that Intune will instead have clients download from internet endpoints. Identify if your network uses proxy servers or firewall filtering for outbound traffic. If yes, list any proxy authentication requirements or limits, because you may need to configure proxy bypasses for Intune and Azure service URLs. Ensure you have or will have firewall rules to allow Intune device communication (to Azure AD, Intune, Office 365, Windows Update URLs, etc.).

• Network Constraints: Note any locations with limited connectivity or high latency. For instance, if you have field sites with very slow links that currently rely on a local SCCM DP for content, those will need special consideration (perhaps using Delivery Optimization peer caching or adding a Connected Cache server). Mark down if Delivery Optimization is already configured via GPO or SCCM client settings for peer-to-peer content sharing. If not, plan to utilize it with Intune to reduce internet load.

• Name Resolution and Services: If devices today depend on internal DNS or other network services (like on-prem authentication), mention those. Azure AD joined devices using Intune might not always be on internal DNS, etc., so if any critical corporate apps require internal network access, you might need always-on VPN or application proxy solutions. Identifying these needs now (e.g., an app that only works on the intranet) will inform whether you need to deploy Intune-managed VPN profiles or reconsider certain app architectures.

• Content Distribution Mechanisms: Overlaps with SCCM infrastructure, but from a network lens, note how content is optimized. Do you use BranchCache or any caching appliances for SCCM content? Do remote sites pull over WAN or have local cache? Intune relies heavily on internet distribution; however, Microsoft’s Delivery Optimization (DO) can enable devices in the same LAN to share downloaded bits. If not using DO yet, highlight that as a new mechanism to configure. Also, if any users are in countries/regions with limited Azure datacenter presence or slow internet, that should be flagged.

• Network Security Controls: Consider if there are any NAC solutions or firewall rules that differentiate managed vs unmanaged devices. For example, some networks block unmanaged devices from certain resources. When devices transition to Intune/Azure AD join, ensure the network will still recognize them appropriately (possibly via Certificate or Intune NAC integration). Document any such controls now, e.g., “802.1x network access requires domain machine certificate””,because after migration that might be replaced with an Intune-delivered certificate for Azure AD joined devices.

In essence, the current state network assessment ensures that moving management to the cloud will not be hindered by infrastructure. It also helps predict bandwidth impact. Often, it’s useful to involve your networking team to get data on current SCCM traffic vs internet traffic. The aim is to prepare the network (open required URLs, maybe upgrade bandwidth or implement peer caching) so that software distribution and updates via Intune will be efficient.

(Real-world tip: Many organisations set up a pilot where they shift patching of a subset of clients to Windows Update for Business and monitor the WAN impact. Use the inventory of remote vs on-site devices to design such pilots. If you have network monitoring data, establish a baseline of how much data SCCM content distribution uses; you can then anticipate cloud content usage. Intune and cloud updates can actually reduce complexity, but you must be sure your internet pipes and policies are ready.)

* 1. Support and Operations

Finally, evaluate the IT support structure and operational processes for managing desktops currently. Migrating to a modern desktop model will affect how IT supports devices, so capturing the current state of operations allows you to plan training and process updates. Focus on how devices are provisioned, maintained, and serviced today:

Provisioning and Imaging: Document the process for setting up new or rebuilt PCs. Do you use SCCM OSD (Operating System Deployment) with imaging and task sequences? If so, note details: e.g., PXE boot, custom images, Task Sequence steps (especially if they install software or join domain, etc.). If imaging is done outside SCCM (like using MDT or manual cloning), record that. This is critical because in a Modern Desktop world, you may shift to Windows Autopilot for provisioning new devices, instead of traditional imaging. Knowing the current imaging process (how long it takes, what it configures, what drivers or apps are injected) helps in replicating those outcomes via Autopilot and Intune policies. Also, identify if different departments have unique images or if any offline domain join or specific provisioning steps are used.

Software Deployment Requests: Describe how IT handles requests for new software or updates. For example, do end-users go through a self-service portal (like SCCM’s Software Center or a ticketing system) to get applications? Are there automated deployments or is it mostly helpdesk-driven? If using Software Center, note that Intune’s equivalent is the Company Portal app for self-service. If users are accustomed to one method, you’ll need to manage the change. Document any internal SLAs for software deployment or any approval workflows.

Incident and Problem Management: High-level, summarize how support tickets related to desktops are handled. Which teams are involved (e.g., Service Desk Level 1, Desktop Support Level 2, SCCM admins Level 3)? This matters because post-migration, roles might shift, for instance, Tier 1 might handle resetting a device via Intune instead of reimaging via SCCM. Note any common incidents (like VPN issues, BitLocker lockouts, etc.) as those processes might change with Intune (e.g., Intune can help with BitLocker recovery key retrieval via Azure).

Remote Support Tools: List the tools used for remote assistance or control. SCCM offers Remote Control and many use tools like TeamViewer, Remote Desktop, or Microsoft Quick Assist. If your helpdesk relies on the SCCM Remote Control tool to connect to user machines on the LAN, note that. Intune has a Remote Help (if licensed) or integrates with TeamViewer for similar functionality. Ensure you have a plan to replace the remote-control method. If any special tools are used for macOS or mobile device support, list them as well.

Update and Maintenance Processes: Beyond automated patching, how are emergency updates or out-of-band fixes handled? For example, do support teams manually push updates via SCCM or scripts when needed? Also, document how often machines are reprovisioned or swapped, if the practice has been to reimage a PC for any major issue, that might change with Intune/Autopilot where a reset or refresh can be triggered. Outline any regular maintenance tasks (like SCCM client health checks, monthly reboots, disk encryption checks by support, etc.).

Documentation and Knowledge Base: Gather any existing runbooks or support docs for managing the current environment. This might include SCCM admin guides, troubleshooting steps for client issues, etc. These documents indicate what the support staff currently checks or fixes (for instance, an SCCM client repair script). Each of those steps will need a counterpart in Intune (e.g., troubleshooting Intune enrollment or configuration sync). Identifying them now helps ensure support teams are retrained appropriately.

End-User Support and Training: Note how users are supported in terms of IT guidance. Is there a portal or FAQ for common tasks (e.g., how to get software from Software Center)? Do users call the helpdesk for things like joining Wi-Fi, or is it automated? This is relevant because moving to Intune might introduce new user-facing elements (like Company Portal, or different UI for updates). Recognize any user experience differences and plan to update documentation for end-users accordingly.

Operational Metrics: If available, review metrics like number of monthly support tickets for desktop issues, average time to resolve, etc. While not directly technical, if (for example) your helpdesk gets many tickets about software installation failures or BitLocker recovery, those are areas to focus improvements in the new design (e.g., Intune can empower users to install apps or view BitLocker keys via the portal, potentially reducing tickets). Mark any pain points in current operations that the modern desktop approach should try to address.

* 1. In Summary

As part of this assessment, consider using structured frameworks or assessment templates. Many organisations employ checklists or questionnaires during a current-state review, for instance, Microsoft’s Cloud Adoption Framework or enterprise architecture templates, to ensure all operational aspects are covered. While you may not name specific third-party tools, you can use generic scripts and reports (for example, a PowerShell script to gather SCCM client health across all devices, or an inventory of GPOs and applications) to collect needed data. The goal is a holistic view of “Day 0” operations, so that you can design the future “Day 1 and beyond” operations with Intune with minimal disruption.

In summary, understanding how IT supports the environment today will help you align your support model with the modern desktop approach.

You might identify training needs (e.g., cloud portal administration), shifts in responsibility (less imaging work, more policy management), and process changes (using Intune for wipes, using new remote assist tools, etc.). Documenting the current processes ensures that during migration, the IT support teams and end-users are prepared and that no critical support function is lost.

By thoroughly covering each of the domains above, Device Inventory, SCCM Infrastructure, Identity, GPOs, Applications, Compliance, Security, Updates, Networking, and Operations, you create a comprehensive Current State Overview. This serves as the baseline for your migration project. It not only helps in planning technical steps (like what policies to recreate in Intune, what apps to package, what network changes to implement) but also in stakeholder communication. Stakeholders can see clearly what is in place today and thus appreciate what will change when moving to a modern Intune-managed desktop environment.

Ensuring all this information is documented (often in spreadsheets, diagrams, and narrative form as we’ve outlined) will greatly support the success of your Modern Desktop migration blueprint. Each item you’ve assessed will tie into later phases of your project plan, whether it’s design decisions (based on current gaps or capabilities) or migration task sequences. A well-executed current state assessment, as detailed here, lays the groundwork for a smooth and informed transition.

1. Target State Vision

Establishing a clear vision for the modern desktop target state is critical to aligning technical decisions, stakeholder expectations, and migration efforts across the programme. This section defines what “good” looks like in a cloud-managed endpoint environment, focusing on user experience, architectural design, and operational outcomes.

The target state represents the end goal: a simplified, secure, and agile endpoint environment underpinned by Microsoft Intune, Entra ID (Azure AD), and Windows Autopilot, supporting Zero Trust principles and hybrid work scenarios. The vision described here can be adapted for varying organisational needs but should serve as a consistent reference point throughout delivery.

* 1. Modern Desktop Characteristics

The target modern desktop environment should exhibit the following characteristics:

* **Cloud-native and agile:** Devices are managed entirely via cloud-based services (Intune, Entra ID), eliminating dependencies on traditional domain-joined infrastructure.
* **User-first experience:** Fast out-of-box setup using Autopilot, seamless application access via Company Portal, and minimal IT touch during provisioning or break/fix scenarios.
* **Zero Trust security model:** Conditional Access enforces compliance and risk-based decisions at login and application access. Data is protected via encryption, MFA, and strong identity controls.
* **Scalable and consistent operations:** Configuration, updates, and security policies are enforced through cloud policies and dynamic groups, providing consistency across geographies and departments.
* **Data and identity-centric:** Users can work securely across devices, with data stored in OneDrive and access governed by their identity rather than the network they are on.
* **Telemetry-driven management:** Real-time health and compliance insights are captured via Endpoint Analytics and Microsoft Defender integrations, driving proactive remediation.
  1. Technology Architecture

A standard modern desktop implementation will be based on the following architectural pillars:

|  |  |
| --- | --- |
| Component | Role in Target State |
| Microsoft Intune | Core MDM and MAM platform for Windows, macOS, iOS, Android |
| Entra ID | Device identity, group management, Conditional Access, role-based access control |
| Windows Autopilot | Enables zero-touch provisioning and out-of-box setup for new and re-provisioned PCs |
| Microsoft 365 Apps | Cloud productivity suite, deployed and updated via Intune |
| Defender for Endpoint | Advanced threat protection, EDR and compliance signals |
| Windows Hello for Business | Passwordless authentication and improved sign-in security |
| OneDrive for Business | Profile and document redirection (KFM), enabling enterprise state roaming |

* 1. End User Experience

The modern desktop experience for end users should be:

* **Fast and secure out-of-box:** New devices arrive pre-registered and pre-assigned via Autopilot. Users sign in with cloud credentials and receive apps, policies, and security settings automatically.
* **Self-service enabled:** Apps are available via the Company Portal. Password resets, BitLocker key recovery, and device wipe are handled via self-service portals or helpdesk with minimal disruption.
* **Mobile and consistent:** Whether in-office or remote, users experience the same performance, security, and access controls.
* **Minimal downtime:** Issues are resolved via reset, autopilot re-provisioning, or remote assistance, avoiding re-imaging or manual interventions.
  1. Alignment to Business Strategy

The modern desktop target state enables the following business objectives:

* **Hybrid workforce enablement:** Secure access from anywhere without reliance on VPN or LAN-only systems.
* **Operational cost reduction:** Eliminates on-prem infrastructure (e.g. SCCM servers, imaging infrastructure), reduces manual IT effort.
* **Faster time to value:** New starters are productive on day one with fully provisioned, policy-compliant devices.
* **Security assurance:** Compliance, encryption, and access controls enforced through a unified cloud stack.
* **Future-proofing:** Aligns with Microsoft’s roadmap and ecosystem strategy, reducing the need for disruptive architectural change in future.
  1. Summary

The target state defines a fully cloud-managed, secure, and user-centric Modern Desktop environment built on **Microsoft Intune**, **Entra ID**, and **Windows Autopilot**. Devices are managed without reliance on traditional on-prem infrastructure, enabling agile provisioning, Zero Trust security, and consistent user experiences regardless of location.

This future state empowers organisations to:

* Streamline device onboarding through **Autopilot and out-of-box provisioning**
* Enforce strong identity and compliance via **Conditional Access and Entra ID**
* Simplify operations through **policy-driven configuration** and **centralised management**
* Reduce infrastructure overhead and improve end-user satisfaction
* Align with Microsoft’s roadmap and leading standards for **hybrid work and endpoint security**

The vision balances technical excellence with user experience, enabling scalable, secure, and future-ready desktop operations.

1. Key Prerequisites
   1. Key Prerequisites: Tenant Configuration Readiness

Before initiating the technical deployment of a Modern Desktop environment, it is essential to ensure that the foundational cloud tenant configuration is in a mature and operationally ready state. Many challenges encountered during endpoint onboarding, policy deployment, and identity management can be traced back to incomplete or inconsistent tenant setup. This section outlines the critical prerequisites required for tenant readiness, with a specific focus on Entra ID (formerly Azure AD) configuration, cloud-only versus hybrid identity decisions, and licensing alignment.

* + 1. Purpose of Tenant Readiness Assessment

The cloud tenant underpins all Modern Desktop capabilities from device identity and compliance to policy enforcement and reporting. A tenant readiness assessment enables the project team to:

* Confirm that core cloud identity and device services are operational and aligned with architectural requirements.
* Identify misconfigurations or gaps that could block device onboarding or degrade user experience.
* Ensure licensing models and feature access align with the planned deployment approach.
* Establish a consistent and supportable baseline across production, pilot, and test environments.
* Entra ID hybrid or cloud-only decisions
  1. Entra ID Configuration and Identity Model

A clear understanding of the organisation’s identity approach is foundational to Modern Desktop success. Key considerations include:

* + 1. Identity Source Strategy
* **Cloud-Only Identity**  
  Suitable for greenfield deployments, remote-first workforces, or where legacy domain join is being deprecated. Simplifies provisioning and reduces dependency on legacy infrastructure but may require rethinking existing access policies and automation processes.
* **Hybrid Identity (Synchronized with On-Prem AD)**  
  Retains integration with existing Active Directory environments via directory synchronisation. Often used where legacy applications, group policies, or domain-based access are still in use.
  + - 1. Recommendation

Clearly document the chosen model and ensure it aligns with broader enterprise identity and application strategy. Avoid partial implementations that lead to inconsistent user experiences or device states.

* + 1. Directory Synchronisation and Federation Readiness (if applicable)
* Validate that directory synchronisation services are healthy, up to date, and scoped appropriately for device objects and relevant user attributes.
* Review any identity federation configurations (e.g. SSO, token lifetimes, MFA integration) for compatibility with Intune, compliance policies, and conditional access scenarios.
  + 1. Device Identity and Join Method
* Decide whether devices will be **Entra ID joined**, **hybrid joined**, or **registered only** (for BYOD or mobile).
* Ensure all required prerequisites (e.g. Autopilot profile assignments, enrolment restrictions, naming conventions) are tested and confirmed for the chosen model.
  1. Conditional Access and Security Dependencies

Modern Desktop deployment typically involves enforcement of security baselines via Conditional Access policies. These are dependent on a well-structured identity and compliance posture.

* Validate baseline Conditional Access policies do not block device enrolment or initial provisioning.
* Define and test onboarding policies that allow temporary, scoped relaxation of controls for provisioning or testing.
* Confirm integration with compliance signals (e.g. Intune compliance policies, Defender risk levels) to support adaptive access decisions.
  1. Tenant Environment Hygiene and Governance

Establishing good tenant hygiene reduces risk and improves predictability during rollout:

* Clean up stale user, device, and group objects.
* Review and document tenant-wide policies (e.g. device restrictions, naming conventions, enrolment limits).
* Establish environment segmentation (e.g. test vs production) with appropriate RBAC roles and change control mechanisms.
* Ensure audit logging and alerting is enabled and tested for key identity and device events.

Licensing: Intune, Entra, Autopilot

* 1. Licensing Considerations

Licensing affects both technical capability and compliance. Organisations must ensure that all required features for Modern Desktop are covered by assigned licences across users and devices.

* + 1. Core Licence Features to Validate

Licences should entitle users/devices to:

* Mobile Device Management (MDM) capabilities via Intune
* Entra ID Premium features (for Conditional Access, dynamic groups, etc.)
* Microsoft Defender or equivalent endpoint protection and compliance integrations (if in scope)
* Windows Enterprise OS entitlements (where upgrading from Pro)
* Autopilot and provisioning-related services

**Tip**: Maintain a matrix of required capabilities versus current licensing tiers. Identify any gaps and budget for uplift or consolidation where necessary.

* + 1. Licence Assignment Strategy
* Ensure consistent licence assignment across pilot and production environments to avoid configuration drift.
* Consider group-based licence assignment to reduce operational overhead and support scaling.
* Include frontline workers, VIPs, and service accounts in the licensing review to avoid unintentional exclusions.
  1. Overcoming Network Challenges in the Legacy On-Prem Environment

Before transitioning to a Modern Desktop model, it is essential to understand and mitigate the inherent limitations posed by a legacy, on-premises network architecture. These limitations can significantly impede deployment velocity, user experience, and the effectiveness of cloud-based management platforms such as Intune. This section outlines common network-related challenges within SCCM-managed environments and provides strategic guidance for overcoming them to ensure a successful migration to a cloud-managed model.

* + 1. Hurdles in Traditional On-Prem Network Architectures

Legacy desktop environments typically operate within tightly controlled, perimeter-based networks. While this model provided robustness in an era of static devices and centralised offices, it now presents several barriers to modern, flexible endpoint management:

* Dependency on Internal Infrastructure  
  Devices often require direct network line-of-sight to internal distribution points, management points, or domain controllers for patching, policy application, and software deployment.
* Latency and Congestion on VPNs  
  Remote endpoints connecting via VPN may experience high latency or throttling, resulting in degraded performance for software distribution, updates, and compliance checks.
* Limited Support for Roaming or Hybrid Workstyles  
  Rigid networking boundaries can restrict access for mobile or hybrid users, leading to inconsistent policy enforcement and security gaps outside the corporate LAN.
* Bottlenecks in Content Delivery  
  Traditional peer caching and file share delivery models may not scale effectively across multiple branch locations or large geographic regions.
* Firewall and Proxy Constraints  
  Outbound network restrictions or legacy proxy configurations may block cloud service endpoints required by Modern Desktop management platforms.
  + 1. Strategic Considerations for Network Readiness

To enable a scalable and performant Modern Desktop model, organisations must proactively re-architect parts of their networking and connectivity posture. The following recommendations outline practical approaches to addressing common network issues:

Decouple Endpoint Management from the Corporate LAN

* Shift from internal management point reliance to cloud-based service endpoints for device registration, compliance, and configuration.
* Encourage the use of internet-facing management paths wherever possible to eliminate VPN dependency.
* Validate and implement published ports and protocols for cloud services (e.g. Intune, update delivery, authentication) are allowed via perimeter firewalls and proxies.
  + 1. Optimise Content Delivery Mechanisms
* Leverage cloud-native content delivery approaches such as distributed cache or peer-based delivery optimised for cloud environments.
* Assess and rationalise existing on-prem content distribution infrastructure; decommission or repurpose where appropriate.
* Ensure bandwidth policies are in place to prevent contention during peak delivery windows.
  + 1. Modernise Remote Access Approaches
* Replace or augment traditional VPN with more adaptive connectivity methods such as split tunnelling or zero trust network access (ZTNA).
* Ensure that policy enforcement, patching, and telemetry collection do not require always-on VPN connectivity.
  + 1. Conduct a Cloud Connectivity Readiness Assessment
* Inventory all outbound dependencies required by cloud-managed devices (e.g., device management, update services, identity providers).
* Audit firewall and proxy rulesets to ensure whitelisting of necessary cloud service endpoints and URLs.
* Validate device connectivity scenarios both inside and outside the corporate network using representative pilot devices.
  + 1. Ensure Resilience Across Distributed Locations
* Where local internet breakout is in use, confirm that cloud endpoint access is consistent across all sites.
* Establish a monitoring strategy to identify degraded performance or service disruptions at remote offices or branch sites.
  + 1. Implementation Tactics and Transitional Guidance

For most enterprises, addressing network challenges is not a one-time exercise but a phased realignment that must run in parallel with desktop modernisation efforts. Key recommendations include:

* Begin with a network readiness assessment as part of discovery, feeding into the broader migration plan.
* Pilot a small set of cloud-managed devices in varied network locations to surface real-world connectivity gaps early.
* Incorporate network remediation milestones into your project roadmap to ensure changes align with broader deployment waves.
* Engage security and network teams early to gain alignment on proxy configurations, firewall policies, and trusted cloud endpoints.
* Implement vendor published guidelines on URL and IP Whitelisting. Failure to do this will cause issues at some point.

1. Critical Decisions & Planning Considerations

When establishing your Modern Desktop programme, the core technical pillars must be fully understood, planned and interwoven into your overall roadmap. The sections that follow provide richer context, decision-criteria, and planning guidance for each foundational area.

* 1. Entra ID Device identity model (Entra ID Join, moving away from OnPrem)

Selecting the appropriate device-join model is a foundational decision for your Modern Desktop programme. Below is a deep dive into the two primary options, with expanded implementation guidance, prerequisites, and decision criteria.

* + 1. Cloud-Only Join

Devices are directly joined to Entra ID, removing on-premises domain dependencies and leveraging cloud-native management capabilities.

* + - 1. Overview & Prerequisites

##### Device Requirements

* UEFI firmware with Secure Boot and TPM 2.0 enabled
* Modern OS image prepared for cloud-based enrolment (e.g. provisioning package or Autopilot profile)
* Hardware inventory reports to confirm device compatibility

##### Network & Identity Pathways

* Ensure outbound connectivity to Entra ID, Intune and other cloud endpoints (e.g. identity, update, certificate services)
* Configure conditional access jump-start policies to allow first-time device registration without blocking on compliance checks

##### Implementation Steps

* Create and assign a cloud-join provisioning profile.
* Distribute devices via drop-ship or zero-touch model, ensuring they receive internet access before first logon.
* Monitor device registration health via automation scripts or telemetry dashboards.
* Post-enrolment, apply policy and application assignments dynamically using device attributes.
  + - 1. Pros

Infrastructure Simplification

* Eliminates on-premises domain controllers, management points and synchronisation services for join operations.

Accelerated Provisioning

* Devices enrol out of the box, reducing technician touchpoints and build-room dependency.

Unified Policy Enforcement

* All devices governed in a single cloud directory, streamlining compliance and reporting.
  + - 1. Cons & Mitigations

Legacy App Access

* On-premises applications must be published via application proxy or accessed over VPN; requires redesign of access topology.

Internet Dependency

* First-boot experience relies on internet connectivity; mitigate via local breakout or temporary network-on-ramp solutions.

User Authentication Flow

* Users authenticate with cloud credentials only; ensure identity federation or password write-back is configured if required.
  + 1. Hybrid Join (Transition Phase)

Devices remain joined to the on-premises Active Directory and are synchronised into Entra ID, supporting a phased move toward full cloud identity.

* + - 1. Overview & Prerequisites

##### Directory Synchronisation

* + Health-checked sync service configured to include computer objects and required attributes.

##### Certificate Provisioning

* + On-premises certificate services (if using certificate-based hybrid trust) or token-based federation enabled.

##### Co-Management Readiness

* + Intune-bit of co-management enabled via management authority and workload splits.
    1. Implementation Steps
* Enable directory synchronisation for device objects, ensuring filters exclude test or out-of-scope OUs.
* Configure hybrid join settings in the tenant: specify service connection points or federation endpoints.
* Pilot hybrid-joined devices alongside cloud-only cohorts to validate GPO application, certificate issuance, and Intune policy delivery.
* Collect telemetry on policy conflicts, join-related errors, and user sign-in latency.
  + - 1. Pros

Preserves Existing Controls

* Continues to apply legacy group policies and on-prem authentication flows for applications not yet migrated.

Gradual Transition Path

* Enables IT teams to migrate workloads incrementally, reducing risk for critical systems.
  + - 1. Cons & Mitigations

Increased Complexity

* Devices exist in two identity realms; requires reconciliation of policy order and conflict resolution.
* Mitigate by documenting policy precedence and using automation scripts to detect drift.

Dependency on Legacy Infrastructure

* Continued reliance on on-prem domain controllers and certificate services; schedule sunset milestones to avoid indefinite dual-state.

User Experience Variability

* Some users may see different login or policy behaviours. Manage via clear communication and support playbooks.
  1. Scope and Timeline

A well-defined scope and an achievable timeline are essential to maintain momentum, manage risk, and communicate progress throughout the Modern Desktop transformation. This planning sub-phase establishes who and what moves when, and ensures that all stakeholders share a common understanding of the rollout cadence.

* + 1. Define User Groups and Device Categories

Begin by segmenting your estate into discrete cohorts, based on business function, device type, and criticality:

* + - 1. User Personas
  + *Remote/Hybrid Workers*: Often highest value for cloud join; ensure network readiness.
  + *Office-Based Knowledge Workers*: May rely on on-prem resources initially; suitable for later waves.
  + *Specialist Users*: Engineering, design, or lab teams with unique hardware or application needs; treat as custom migration tracks.
  + *Front-line Devices*: Shared kiosks or point-of-sale terminals; may require device-based policies rather than user affiliation.
    - 1. Device Categories
  + *New Hardware*: Factory-fresh devices provisioned via zero-touch; ideal for early adoption.
  + *Recently Refreshed Hardware*: Still under warranty, with modern firmware; prime candidates for wave 1.
  + *Aged Devices*: Approaching end of life; evaluate on a case‐by‐case basis—consider repurposing or replacement.
  + *Specialty Devices*: Lab, medical, or ATEX-rated devices requiring bespoke handling.
* For each cohort, capture:
* Number of users/devices
* Operating system baseline (Windows 10 vs. Windows 11)
* Application compatibility considerations
* Connectivity profile (on-prem only, VPN-dependent, direct internet access)
  + 1. Establish Roll-Out Waves and Milestones

Structure your timeline into progressive “waves” to contain risk, absorb lessons learned, and adapt processes:

* + - 1. Pilot Wave
* *Size*: 25–50 devices representative of multiple personas (e.g. remote workers + office workers).
* *Goals*: Validate join workflows, policy application, application deployment, and user support processes.
* *Duration*: 2–4 weeks, with daily status reviews.
  + - 1. Wave 1: Early Adopters
* Cohorts: New hardware devices and remote-first users.
* Goals: Scale provisioning, measure performance, refine automation scripts.
* Duration: 4–6 weeks.
  + - 1. Wave 2: Core Business Units
* Cohorts: Standard office knowledge workers and recent hardware refreshes.
* Goals: Integrate more complex applications, begin decommissioning group policies.
* Duration: 6–8 weeks.
  + - 1. Wave 3: Specialty & Aged Devices
* Cohorts: Specialist and legacy hardware requiring targeted remediation or replacement.
* Goals: Complete device rationalisation, re-image or replace as needed, retire SCCM workloads.
* Duration: 8–12 weeks.
  + - 1. Final Cut-Over
* Scope: All remaining domain-joined devices.
* Goals: Decommission on-prem join services (domain controllers, sync engines), formal sign-off.
* Duration: Defined by SLA with business sponsors (e.g. within 6 months of project start).
  + 1. Map Dependencies and Decision Gates

At each milestone, include clear go/no-go gates aligned to critical prerequisites:

* Network & Connectivity: Proof of internet breakout and proxy configuration for each site.
* Application Readiness: Confirmation that top 20 business-critical apps deploy successfully.
* Support Model: Service desk scripts and escalation paths validated.
* Security Baselines: Conditional Access and compliance policies applied and tested.
* Document these decision gates as part of your project plan, ensuring executive sponsorship at each stage.
  + 1. Communication & Stakeholder Alignment

Embed regular cadence calls and status reports in your timeline:

* Weekly Steering Committee: Review metrics—enrolment success rate, application install rates, helpdesk tickets.
* Bi-Weekly Change Advisory Board (CAB): Approve any scope adjustments, wave sequencing, or exception requests.
* User Communications: Send wave-specific notifications at least two weeks in advance, with links to self-help resources and support channels.
  + 1. Continuous Improvement Loops

After each wave, conduct a “lessons learned” session and refine:

* Update automation scripts to address common failures.
* Adjust wave sizing or length based on throughput and support capacity.
* Revisit device cohorts or application groupings if unexpected dependencies surface.

1. Naming, Tagging & Grouping
   * Device naming template: <SiteCode>-<DeptCode>-<Serial>
   * Dynamic group rules based on device attributes (ownership, join type, OS version) to drive policy and application assignment.

Planning Considerations

* Directory Synchronisation & Filtering
  + Confirm only required OUs and AUttributes sync to Entra ID to reduce clutter.
  + Map custom attributes (e.g. device location) to support dynamic group membership.
* Pilot Execution
  + Run parallel pilots: one cloud-only cohort and one hybrid cohort.
  + Track join success rate, enrolment times, and user-reported issues.
* Fallback Mechanisms
  + Pre-define rollback procedures:
    - Trigger a maintenance window to re-enable on-prem domain join.
    - Use automation scripts to remove stale Entra ID registrations.
* Operational Readiness
  + Train service desk on new join workflows, including common failure modes (e.g. missing device certificates).
  + Update incident management playbooks with Entra ID-specific troubleshooting steps.

Application packaging & deployment approach

Patching strategy and approach

Compliance & Conditional Access strategy

Windows Hello for Business

BitLocker / Encryption

Defender for Endpoint integration

1. Modern Management Foundations to Implement (PC)

Transitioning to a cloud-managed Modern Desktop model requires the implementation of core management foundations within Microsoft Intune and Entra ID. These foundations must align with recognised security and operational standards such as CIS Benchmarks, NCSC End User Device (EUD) Guidance, and Microsoft Security Baselines to ensure a secure, compliant, and supportable environment.

This section outlines the key baseline components that must be in place before devices are migrated, with a focus on security hardening, policy enforcement, automation, and operational governance.

* 1. Intune Tenant Baseline Configuration

A clean and well-structured Intune tenant is essential for policy application, device lifecycle management, and delegated administration.

* **Enrolment Restrictions:** Define supported platforms (Windows, macOS, iOS, Android) and apply corporate vs. personal ownership rules.
* **Naming Conventions:** Implement structured device naming schemes (e.g. <SITE>-<DEPT>-<SERIAL>) for traceability and policy targeting.
* **Scope Tags and RBAC:** Enforce least-privilege administrative access using Role-Based Access Control and Scope Tags to separate environments (e.g. Production vs Pilot).
* **Tenant Branding:** Apply corporate branding and terms of use to enrolment portals for end-user assurance.
* **Audit and Logging:** Enable unified audit logging to meet NCSC guidance around administrative transparency and change tracking.
  1. Entra ID Security Controls

Modern Desktop architecture is inherently identity-driven. A secure Entra ID configuration underpins policy enforcement and access management.

* **Multi-Factor Authentication (MFA):** Enforce MFA on all users. This aligns with both CIS and NCSC MFA guidance for remote access.
* Conditional Access Policies:
  + Block legacy authentication
  + Require compliant device and MFA for access to Microsoft 365 and sensitive services
  + Enforce sign-in risk policies (via Defender for Identity or Identity Protection)
* **Dynamic Device/User Groups:** Automate policy targeting using attributes such as join type, compliance state, or device location.
* **Passwordless Authentication:** Encourage passwordless sign-in with Windows Hello for Business or FIDO2 keys, in line with NCSC’s direction on reducing password reliance.
  1. Device Configuration Profiles

Intune replaces Group Policy with device configuration profiles and CSP-backed controls. These should be mapped against CIS/NCSC policy recommendations to ensure consistent security posture.

* **Microsoft Security Baselines:** Use built-in security baselines for Windows, Microsoft Edge, and Defender as a starting point.
* **CIS/NCSC Custom Profiles:** Where required, use Settings Catalog and custom configuration profiles to implement hardening settings recommended by:
  + CIS Windows 10/11 Benchmarks (Level 1) for enterprise environments
  + NCSC Intune Security Configuration and NCSC EUD Platform Guides for Windows 10/11
* **Wi-Fi, VPN & Certificates:** Deploy secure access profiles using SCEP/PKCS certificate distribution methods to remove reliance on manual config or legacy GPOs.
  1. Compliance Policies and Conditional Enforcement

Compliance policies must codify your baseline expectations for endpoint health and integrate with Conditional Access to enforce Zero Trust principles.

* **Common Policies**:
  + Require BitLocker encryption (aligned to CIS and NCSC disk encryption mandates)
  + Require secure boot, TPM, and up-to-date OS builds
  + Prohibit jailbroken or rooted mobile devices
* **Non-Compliance Actions**:
  + Mark devices as non-compliant after 1–2 missed check-ins
  + Notify user and IT via automated email
  + Lock or remove access to sensitive applications via Conditional Access
* **Compliance Reporting**:
  + Leverage built-in dashboards for compliance posture
  + Integrate with **Microsoft Defender for Endpoint** to adjust device risk scores dynamically
  + Use **Endpoint Analytics** for visibility into configuration drift or remediation success
  1. Autopilot Profile Creation and Enrolment Process

Windows Autopilot enables standardised, zero-touch provisioning, fully aligned with NCSC’s recommended device build principles.

* **Profile Types**:
  + **User-Driven** for corporate laptops and hybrid users
  + **Self-Deploying** for shared devices or kiosks
  + **Pre-Provisioned (White Glove)** for devices built before user delivery
* **Security Alignment**:
  + Enforce BitLocker encryption at OOBE
  + Integrate with Defender AV, EDR and MDE onboarding as part of provisioning flow
  + Auto-assign devices to compliance policies on first login
* **Hardware Hash Import**: Maintain a controlled and validated list of devices in Autopilot using hash uploads or OEM registration.
* **Naming & Group Tagging**: Use Autopilot Group Tags to ensure correct dynamic group assignment and policy scoping.

Devices provisioned via Autopilot should meet **CIS Level 1** benchmarks and be validated using MDM audit logs or security configuration scanning tools.

* 1. Summary

To enable a secure and scalable Modern Desktop model, organisations must establish foundational configurations across **Intune**, **Entra ID**, and related Microsoft cloud services. These include structured enrolment rules, RBAC controls, policy baselines, and secure identity configurations aligned with **CIS Benchmarks**, **NCSC EUD guidance**, and **Microsoft Security Baselines**.

The goal is to create a consistent, compliant, and automation-ready environment where:

* Devices can be securely onboarded and managed from anywhere
* Policies and compliance are enforced through dynamic groups and Conditional Access
* Core configurations (BitLocker, Defender, VPN, Wi-Fi) are centrally deployed and maintained
* Administrative roles and processes follow best-practice security governance

These foundations provide the backbone for all future deployment waves, ensuring repeatability, security, and operational confidence throughout the modernisation journey.

1. Application Modernisation

Modernising the application estate is a critical step in transitioning to a cloud-managed Modern Desktop environment. Legacy packaging formats, infrastructure dependencies, and inconsistent deployment practices must be addressed to enable seamless, policy-driven delivery via Microsoft Intune.

This section outlines the process of auditing, repackaging, and deploying applications in a manner that aligns with cloud-native principles, improves reliability, and supports user productivity across diverse locations and devices.

* 1. Objectives of Application Modernisation

The goal of application modernisation is to:

* Remove dependencies on on-premises infrastructure (e.g. file shares, SCCM distribution points)
* Transition legacy formats (e.g. EXE, MSI, App-V) into Intune-supported deployment models
* Ensure applications are compatible with Entra ID-joined and cloud-managed devices
* Enable self-service and policy-based installation using Company Portal
* Improve patching velocity and reduce update-related disruption
* Rationalise and reduce redundant or unused software
  1. Audit of Existing Applications

Begin by conducting a full application audit to capture:

* **Inventory of Applications**: Extract lists from SCCM, asset management tools, or discovery scripts. Include:
  + Business-critical and LOB applications
  + Productivity tools (e.g. Microsoft 365, browsers, PDF readers)
  + Custom, in-house developed software
  + Utility tools, scripts, and plug-ins
* **Application Metadata**:
  + Name, version, vendor
  + Installer type (MSI, EXE, App-V, MSIX)
  + Update frequency and patch method
  + Target user base or department
* **Installation Method**:
  + SCCM Package or Application model
  + GPO/script-based install
  + Manual or third-party deployment
* **Dependencies**:
  + Licensing servers
  + Local databases or network shares
  + AD group or OU dependencies
* **Usage Data**:
  + Software metering or endpoint analytics to assess active vs unused apps

Rationalise where possible — eliminate duplicate, legacy, or rarely used applications before migrating.

* 1. Packaging for Intune

Applications should be repackaged in formats supported by Intune:

|  |  |
| --- | --- |
| **Format** | **Description** |
| **Win32 (.intunewin)** | Recommended format for complex installers (MSI/EXE/script-based). Requires packaging via the Microsoft Win32 Content Prep Tool. |
| **MSIX** | Modern, secure packaging format. Ideal for new apps or where full control over app updates is required. |
| **Microsoft Store** | Lightweight deployment via private Store or Store integration. Best for well-known apps with existing UWP packages. |
| **Web Apps** | For SaaS or internal web tools. Deploy as shortcuts via Intune. |

There are also third party solutions available for Application Migration from ConfigMgr to Intune, although this should not be performed blindly, and only required and supported apps should be migrated.

For each repackaged app:

* Include silent install/uninstall switches
* Define detection rules (e.g. registry, file path, product code)
* Set requirements (e.g. OS version, disk space, memory)
* Assign to dynamic groups based on device or user attributes, or use filters.
  1. Delivery and Deployment Strategy

A well-defined delivery and deployment strategy ensures that applications are installed efficiently, securely, and in a way that supports user productivity while minimising support overhead. In a Modern Desktop environment, Microsoft Intune replaces the traditional SCCM-centric push model with policy-based and user-targeted delivery mechanisms.

This section outlines how to approach required vs. available deployments, user self-service, automation, targeting, and scalability.

* + 1. Deployment Types

Intune supports two core deployment types, which should be used strategically:

**Required Applications** - These are installed automatically on all applicable devices or users without interaction. Ideal for:

* + Core productivity tools (e.g. Microsoft 365 Apps, Teams, Edge)
  + Security tools (e.g. Defender for Endpoint, VPN clients)
  + Line-of-business (LOB) applications required by default
  + Device enablers (e.g. printer management tools, hardware agents)

**Available Applications** - Made available via the **Company Portal** for user-initiated, on-demand installation. Best for:

* + Departmental or role-specific tools
  + Optional utilities
  + Low-risk software used by small populations (e.g. Notepad++, PDF tools)
  + Tools requiring user acceptance or configuration

***Best Practice***: Offer as much as possible via **available deployment**, empowering users through self-service while reducing support tickets and unneeded installations.

* + 1. Assignment and Targeting

Use dynamic, attribute-based groupings to ensure applications are scoped accurately and efficiently.

* **User-Based Targeting -** Assign apps to Entra ID user groups when the app follows the user across devices (e.g. Microsoft 365 Apps, browser-based tools).
* **Device-Based Targeting -** Assign to device groups when the software is hardware-bound or needs to be installed regardless of who signs in (e.g. drivers, BIOS tools, lab/kiosk software).

**Group Design Considerations -** Create Intune dynamic groups based on:

* + Enrolment profile or Autopilot Group Tag
  + Operating system version or platform
  + Device model, ownership type (BYOD vs. corporate)
  + Department or location (based on Entra ID attributes)

***Best Practice:*** Use Intune Filters to create dynamic deployments.

* + 1. Deployment Automation

To enhance reliability and reduce effort, deploy applications using repeatable automation and assignment practices:

* **Win32 App Packaging Pipelines -** Integrate CI/CD for packaging, versioning, and publishing to Intune via Graph API or scripting frameworks.
* **Detection Logic -** Configure custom rules (registry, file path, product code) to confirm install success. Avoid relying solely on install exit codes.
* **Delivery Optimisation -** Leverage peer-to-peer caching (Delivery Optimization, Connected Cache) to reduce WAN and CDN traffic for large packages.
* **Staggered Deployment (Phased Rings) -** Adopt a ring-based rollout model for required apps:  
  + Ring 0: IT/admin pilot group
  + Ring 1: Early adopters
  + Ring 2: Broad deployment
  + Ring 3: Late adopters or high-risk roles
    1. Resilience and Retry Logic

Intune includes built-in retry mechanisms, but organisations should plan for resilience:

* Ensure apps are marked as **required** with retry enabled in case of temporary failure (e.g. offline device)
* Monitor **install success/failure** via Endpoint Manager reports
* Use **Proactive Remediations** to validate app presence and re-install where necessary

This approach ensures that applications are delivered with high success rates, minimal end-user disruption, and with full visibility across the estate. By aligning deployment types to business need and automating where possible, IT teams can shift from reactive software installs to predictable, policy-driven application delivery.

* 1. Application Compatibility Considerations

Modern desktop environments, particularly those built on Entra ID join and Intune, may surface compatibility challenges with older applications developed for domain-joined, LAN-dependent environments.

**Common Compatibility Issues**

|  |  |
| --- | --- |
| **Compatibility Area** | **Examples** |
| **Authentication** | Apps requiring **Kerberos or NTLM** authentication via domain join may fail on Entra ID-joined devices. |
| **Network Dependency** | Hard-coded references to on-prem servers, mapped drives, or file shares. |
| **Privileges** | Applications requiring **local admin rights** or that attempt to write to protected areas (e.g. Program Files). |
| **OS Compatibility** | 16-bit or 32-bit legacy apps incompatible with Windows 11 or modern hardware. |
| **User Profile Handling** | Apps writing to specific user profile paths (e.g. C:\Users\<username>\AppData) without multi-user support. |

#### Remediation Strategies

* **Refactor**: Work with internal dev teams or vendors to update hardcoded elements or switch to cloud-compatible authentication.
* **Application Proxy**: For internal web apps, use **Entra ID Application Proxy** to publish them securely for modern clients.
* **VPN or Conditional Access**: Maintain minimal VPN access or define **Conditional Access policies** to allow fallback connectivity for transitional apps.
* **Alternate Delivery**: Use **Azure Virtual Desktop (AVD)** or **Cloud PCs** for apps that cannot be replatformed immediately.
* **Run as Admin**: Where absolutely necessary, deploy apps using Intune’s **install context elevation**, and consider endpoint privilege management (e.g. Just-in-Time elevation or integration with LAPS).
  1. Summary

Modernising the application estate is a foundational pillar of the Modern Desktop journey. It involves more than simply repackaging apps — it requires rethinking how applications are discovered, delivered, secured, and maintained in a cloud-first world.

This section outlines a complete approach to:

* Audit and rationalise existing applications, removing legacy dependencies and redundant tools
* Repackage applications using modern formats like **Win32 (.intunewin)**, **MSIX**, and **Microsoft Store apps**
* Deliver software intelligently using a mix of **required deployments** and **self-service via the Company Portal**
* Define robust update strategies to maintain security and compliance across critical and third-party apps
* Address compatibility challenges for domain-dependent or legacy tools, with remediation paths including refactoring, AVD, or conditional access/VPN integration

By implementing a structured application strategy that aligns with Intune and Entra ID, organisations can reduce support burden, improve user experience, and ensure the entire app estate is **secure, scalable, and ready for the future**.

1. Windows Update for Business

Patching Strategy (Rings)

Delivery Optimization

Feature Updates

1. User Data and Enterprise State Roaming

OneDrive Known Folder Move

Edge Sync

Enterprise State Roaming

1. Security and Endpoint Protection

Microsoft Defender AV and EDR configuration

Attack Surface Reduction (ASR)

Firewall

App Control (AppLocker / WDAC)

Admin rights model & LAPS

1. Device Lifecycle Management

Autopilot registration and hardware hash upload

Autopilot Vendor Registration

Deployment of new devices vs. existing re-provisioning

Wipe and redeploy vs. in-place transition

End of Life considerations / processes

1. Reporting, Monitoring & Ongoing Support

Endpoint reporting via Intune & Defender

PowerBI

Health checks and alerting (Endpoint Analytics, Secure Score)

Proactive Remediations

Helpdesk readiness and user self-service tools (Company Portal)

1. Change Management & User Communication

User onboarding and training plan

Communication templates

Executive sponsorship and feedback loops

1. Pilot & Rollout Strategy

Define pilot groups and success criteria (UAT)

Staged migration approach (Rings?)

Post-pilot reviews and scaling to wider estate

1. Known Challenges and Mitigations

Network latency/performance issues

Conditional Access Issues

Firewall / Content Filtering Issues with On Prem LAN

Legacy Network Solution Issues (VPN)

Legacy app compatibility

User resistance and behaviour change

Lack of Modern Desktop mentality / understanding

1. Implementation Checklist

As part of the prerequisites phase, validate the following before proceeding to large-scale Modern Desktop rollout:

* Identity model (cloud-only vs hybrid) is selected and documented
* Directory synchronisation and federation services (if used) are operational and aligned
* Device join methods are confirmed and supported across hardware types
* Licensing tiers and assignments match required feature set
* Conditional Access policies are aligned with onboarding and compliance workflows
* Group structures and role-based access controls are in place and validated
* Tenant settings (naming, restrictions, enrolment policies) are reviewed and documented
* Logging and monitoring are active for critical identity and device events