Free technical checklist

M&A IT Integration and Carve-Out Readiness Checklist

What to establish before signing, what has to work on Day 1, and the carve-out traps that surface late.

IT is rarely the reason a deal is done and frequently the reason it is painful. Tenant to tenant migration has ordering constraints that are not obvious, licences do not move between tenants, and a carve-out has to separate things that were never built to be separable. This checklist covers thirteen areas from pre-close discovery to post-close operations, with the Microsoft sequencing constraints stated explicitly rather than discovered during a cutover weekend.

Version 1.0. Published 24 August 2026.
Prepared for Corporate development, integration leads, CIOs and IT directors working a merger, an acquisition, a divestiture or a carve-out where Microsoft 365 and Azure estates have to combine or separate.
simplicityitinc.com

Contents

How to use this checklist

This covers thirteen areas from pre-close discovery through to post-close operations. Not every area applies to every transaction, and a carve-out uses domains 11 and 10 far more heavily than a straightforward acquisition does.

Use it twice. Once during diligence, where the value is in finding out what you are buying and what it will cost to integrate, and again during planning, where the value is in sequencing. Several items in domains 2, 3 and 7 are ordering constraints rather than tasks, and an integration plan that gets the order wrong discovers it during a cutover weekend.

Record an owner, a status and a date against each item. In a transaction the owner matters more than usual, because the two sides have different information and the person who can answer an item is frequently not the person holding the plan.

Items marked Product describe behaviour Microsoft documents and cite the article. Items marked Practice are Simplicity IT delivery judgement.

What this checklist does not do

- It gives no timeline and no cost. Both depend on user count, mailbox sizes, data volume, hold status, application estate and business constraints. This document contains the questions that determine those numbers. Anyone offering the numbers before asking the questions is guessing.
- It is not legal, tax or regulatory advice. Several items will surface questions for counsel. They are flagged as such rather than answered.
- It does not cover the commercial or people dimensions of an integration, which are usually harder than the technical ones and are somebody else's checklist.
- It assumes a Microsoft estate. An organization running substantially on other platforms will find the identity and data principles transfer and the specifics do not.

SECTION 1

Domain 1. Pre-close discovery

What you need to know before signing. Discovery access is usually constrained during diligence, so the priority is the small number of facts that change the price or the plan.

DS-1 Item 1

User, mailbox and device counts are established from the systems rather than from headcount.

WHY IT MATTERS	Headcount, licence count and active mailbox count routinely differ by a wide margin, and every migration estimate is built on the wrong one of the three unless someone checks.
HOW TO VERIFY	Entra user count by enabled state and last sign in, licence assignment report, device inventory. Compare all three against the headcount you were given.

DS-2 Item 2

Data volume is measured by workload: mailboxes, OneDrive, SharePoint, Teams and file servers.

WHY IT MATTERS	Volume drives migration duration more than user count does, and a small organization with twenty years of archives is a larger job than a large one without them.
HOW TO VERIFY	Admin center usage reports per workload. Ask specifically about archive mailboxes and file servers, which are frequently omitted from the first answer.

Source 10

DS-3 Item 3

The application estate is inventoried, including the applications IT does not know about.

WHY IT MATTERS	Applications, not mailboxes, are what make integrations run long. The ones nobody listed are the ones that stop a department working on Day 1.
HOW TO VERIFY	Entra enterprise applications, expense records for software subscriptions, and a direct question to each department head about what they pay for.

DS-4 Item 4

Existing security incidents, breaches and outstanding remediation are disclosed.

WHY IT MATTERS	You inherit the incident history along with the estate, including any dwell time that has not yet been discovered.
HOW TO VERIFY	Ask directly and in writing. Review the security posture score and any outstanding recommendations for signs of long standing neglect.

DS-5 Item 5

Contractual and regulatory obligations attaching to the data are identified.

WHY IT MATTERS	Client contracts, sector regulation and data protection obligations constrain where data can move and who can hold it, and they do not stop applying because a transaction happened.
HOW TO VERIFY	Counsel reviews client contracts for assignment, data location and subprocessor clauses. This is a legal question surfaced by an IT checklist, not an IT decision.

DS-6 Item 6

Legal holds and retention obligations in force are listed with the matters that created them.

WHY IT MATTERS	A mailbox on hold can block or complicate migration, and holds outlive the matters that created them because nothing visibly breaks when they do not.
HOW TO VERIFY	eDiscovery holds, retention policies and labels, with the matter and date for each.

Sources 7, 13

SECTION 2

Domain 2. Identity and directory

Identity is the first thing to plan and the last thing you can change cheaply. Several items here are ordering constraints.

ID-1 Item 7

The target identity model is decided before any migration work begins.

WHY IT MATTERS	Whether users end up in one tenant, stay in two, or run as a multitenant organization determines almost every subsequent decision. Reversing it later means redoing the work.
HOW TO VERIFY	A written decision naming the end state, with the reasoning and the person who approved it.

Sources 9, 16

ID-2 Item 8

Cross-tenant identity mapping is completed before workload licences are applied to the target users.

WHY IT MATTERS	Microsoft documents that identity mapping must run before licensing the target users, so those users remain in the correct state for the migration to attach to. Licensing them early is a common and expensive ordering error.
HOW TO VERIFY	Confirm the mapping process and its position in the runbook, explicitly ahead of licence assignment.

Source 12

ID-3 Item 9

The source of authority for identity is known on both sides, including any on premises directory and its synchronisation.

WHY IT MATTERS	An on premises directory that still authoritatively owns attributes will overwrite changes made in the cloud, quietly and repeatedly.
HOW TO VERIFY	Identify the synchronisation service, what it writes, and whether writeback is enabled.

ID-4 **Item 10**

Naming, addressing and the primary domain end state are agreed in advance.

WHY IT MATTERS Email addresses are the most publicly visible part of an integration and the hardest to change twice. Domain moves also have their own sequencing, since a domain can only be verified in one tenant at a time.

HOW TO VERIFY A written naming standard, the domain cutover plan, and the decision on whether legacy addresses are retained as aliases.

Source 9

ID-5 **Item 11**

Cross-tenant access settings are configured for the collaboration required during the transition.

WHY IT MATTERS The two organizations have to work together from Day 1, usually long before the migration completes. Left at defaults this is either too open or blocks the collaboration people need.

HOW TO VERIFY Entra external identities, cross-tenant access settings on both tenants, configured deliberately in both directions.

Source 5

ID-6 **Item 12**

Privileged access in both tenants is reviewed, and administrative rights held by departing staff or the seller are enumerated.

WHY IT MATTERS In a carve-out the seller frequently retains administrative access to the divested estate long after close, sometimes by oversight and sometimes because nothing was written down.

HOW TO VERIFY List every privileged role holder in both tenants with their employer after close.

Sources 3, 4

SECTION 3

Domain 3. Microsoft 365 tenant strategy

How the two tenants relate, and in what order their contents move.

TN-1 **Item 13**

The tenant end state is chosen deliberately: consolidate, coexist, or operate as a multitenant organization.

WHY IT MATTERS Consolidation is the most work and the cleanest outcome. Coexistence is faster and leaves permanent complexity. Choosing by default is choosing coexistence.

HOW TO VERIFY A written decision with the reasoning, approved by someone who owns the consequences of the ongoing operating cost.

Sources 9, 16

TN-2 Item 14

Licences are purchased in the target tenant. They are not transferred.

WHY IT MATTERS	Microsoft states that licences cannot be moved between tenants. Every migration plan that assumes otherwise has a hole in its budget.
HOW TO VERIFY	Confirm target tenant licence procurement is in the plan and the budget, with the timing set against the migration schedule rather than close.

Source 9

TN-3 Item 15

Mailboxes migrate before or alongside Teams content, not after.

WHY IT MATTERS	Microsoft documents that Teams chat and channel content depends on Exchange Online mailboxes, which sets the ordering. Moving Teams first produces content with nothing underneath it.
HOW TO VERIFY	Check the runbook sequence explicitly. This is one of the ordering errors that is only discovered at execution.

Sources 9, 13

TN-4 Item 16

OneDrive and SharePoint are migrated together.

WHY IT MATTERS	Microsoft documents that they share a permissions model, so separating them in the schedule risks inconsistent permissions between content that references itself.
HOW TO VERIFY	Confirm the schedule keeps them in the same wave for a given population.

Sources 14, 15

TN-5 Item 17

Migration tooling is chosen and its limits understood before the plan is committed.

WHY IT MATTERS	Native and third party tools differ in what fidelity they preserve. Discovering that a tool does not carry something you needed is a discovery best made before the schedule is published.
HOW TO VERIFY	Review the migration orchestrator and the alternatives against the specific fidelity requirements, particularly version history, permissions and metadata.

Sources 10, 11

TN-6 Item 18

A pilot wave of real users is run before the first large wave.

WHY IT MATTERS	The problems in a migration are specific to the estate, and no amount of planning finds them as quickly as twenty real users with real content and real complaints.
HOW TO VERIFY	Confirm the pilot is a genuine cross section rather than the IT team, who have unrepresentative content and unrepresentative patience.

SECTION 4

Domain 4. Endpoints and devices

The machines people actually work on, which is where an integration becomes visible to everybody at once.

EP-1 Item 19

Device inventory covers what exists, what state it is in, and what manages it.

WHY IT MATTERS	Devices at end of life, unmanaged, or joined to a directory that is going away are all Day 1 problems, and they are only distinguishable in advance.
HOW TO VERIFY	Management console inventory cross referenced with asset records and, where they disagree, with a physical count.

EP-2 Item 20

The device migration approach is chosen: re-enrol, rebuild, or replace.

WHY IT MATTERS	Each has a different cost, a different disruption profile and a different duration. Choosing per device class rather than uniformly is usually cheaper than either extreme.
HOW TO VERIFY	A written approach per device class, with the user disruption stated for each.

EP-3 Item 21

Encryption keys and recovery keys are accounted for before devices change tenant.

WHY IT MATTERS	A device whose recovery key lives in a directory the organization is leaving is a device that cannot be recovered after the leaving. This locks people out permanently.
HOW TO VERIFY	Confirm recovery keys are escrowed somewhere that survives the transition, and test a recovery.

EP-4 Item 22

Local data on devices is identified and handled.

WHY IT MATTERS	Users keep material locally regardless of policy. A device rebuild without that consideration destroys work, and the complaints arrive individually over the following months.
HOW TO VERIFY	Confirm known folder redirection or an equivalent is in place and has actually synchronised, per device, before any rebuild.

EP-5 Item 23

Endpoint security tooling on both sides is compared and a target state chosen.

WHY IT MATTERS	Two agents from different vendors on one device is a support problem, and a gap between removing one and deploying the other is an exposure window.
HOW TO VERIFY	Name the target tooling and the transition sequence per device class, with no gap in coverage.

SECTION 5

Domain 5. Networking and connectivity

The connectivity that has to exist on Day 1, and the overlaps that prevent it.

NW-1 Item 24

IP address ranges on both sides are compared for overlap.

WHY IT MATTERS	Overlapping private ranges prevent the two networks connecting without translation or renumbering, and both are long lead time work. This is the first thing to check and it is regularly checked last.
HOW TO VERIFY	Obtain the addressing schemes from both sides and compare them directly.

NW-2 Item 25

Name resolution across the combined estate is designed.

WHY IT MATTERS	Two organizations with internal domains that must resolve for each other is a design question, and left to chance it produces failures that look like application faults.
HOW TO VERIFY	A written DNS design covering forwarding, conditional resolution and the internal namespaces on both sides.

NW-3 Item 26

Site to site connectivity required for Day 1 is identified and has a lead time attached.

WHY IT MATTERS	Circuits and appliances have procurement lead times measured in weeks. A close date does not move for them.
HOW TO VERIFY	List the connections needed for Day 1 with the lead time and order date for each.

NW-4 Item 27

Remote access for the combined population is planned.

WHY IT MATTERS	Users on either side needing resources on the other is the normal state during a transition, and access designed only for the end state fails throughout the middle.
HOW TO VERIFY	Confirm the transition state, not only the end state, has a working access design.

NW-5 Item 28

Physical sites being retained, closed or divided are known, with dates.

WHY IT MATTERS	Property decisions drive network decisions and are made by people who do not tell IT until the lease is signed.
HOW TO VERIFY	Obtain the property plan and map it against the network plan.

SECTION 6

Domain 6. Applications and licensing

The domain that determines the duration of the whole programme.

AP-1 Item 29

Every business application has a named owner and a decision: keep, migrate, consolidate or retire.

WHY IT MATTERS	Applications without an owner do not get decided, so they get kept by default, and the promised consolidation savings never materialise.
HOW TO VERIFY	The inventory from DS-3 with an owner and a decision against every line, no blanks.

AP-2 Item 30

Software licences are checked for whether they survive a change of control.

WHY IT MATTERS	Many agreements are not assignable, or reprice on a change of ownership. This is a common source of unbudgeted cost that appears shortly after close.
HOW TO VERIFY	Counsel and procurement review the agreements for assignment and change of control clauses. Prioritise the largest by value.

AP-3 Item 31

Applications authenticating against the directory being retired are identified.

WHY IT MATTERS	Every one of them needs reconfiguration, and each is an outage for its users if the directory goes before the reconfiguration does.
HOW TO VERIFY	Entra enterprise applications and any on premises federation configuration, cross referenced with the application inventory.

Source 4

AP-4 Item 32

Integrations between applications are mapped, including the informal ones.

WHY IT MATTERS	A scheduled export that has run for six years, maintained by nobody, is exactly the thing that breaks silently and is noticed at a month end.
HOW TO VERIFY	Ask each application owner what talks to their system, then check for scheduled tasks and service accounts nobody claims.

AP-5 Item 33

Line of business applications with no cloud path are identified early.

WHY IT MATTERS	One application that cannot move sets the floor for how long the old environment must be kept, and therefore for the cost of the whole transition.
HOW TO VERIFY	Identify them, then price keeping the environment they need for the duration required.

AP-6 Item 34

Application data ownership after separation is agreed where an application serves both parties.

WHY IT MATTERS	In a carve-out an application often holds records belonging to both the retained and the divested business in the same tables, and separating them is a data project, not a configuration change.
HOW TO VERIFY	For each shared application, a written statement of who gets what data and how it is extracted.

SECTION 7

Domain 7. Data migration

Moving the content, and knowing afterwards that it arrived.

DM-1 **Item 35**

What migrates and what is archived is decided before the schedule is built.

WHY IT MATTERS	Migrating everything is the default and it is the most expensive option. It also carries forward every permissions problem the source estate had.
HOW TO VERIFY	A written scope with the exclusions named, approved by the business owners of the excluded content.

DM-2 **Item 36**

Mailboxes on hold or subject to retention are identified before scheduling.

WHY IT MATTERS	Hold status can block or complicate a mailbox move, and the affected mailboxes tend to belong to executives and legal, who are the least tolerant of a failed cutover.
HOW TO VERIFY	Cross reference the hold list from DS-6 against the migration waves.

Sources 7, 13

DM-3 **Item 37**

Permissions are reviewed before migration, not carried across and reviewed later.

WHY IT MATTERS	A migration duplicates the source permission model into the target. Oversharing that arrives in the new tenant is oversharing you now own, and remediating post migration means doing it while people are using it.
HOW TO VERIFY	Run sharing reports on the source estate and remediate the worst before the wave, not after.

Sources 8, 15

DM-4 **Item 38**

Fidelity requirements are stated: version history, metadata, permissions, timestamps.

WHY IT MATTERS	Tools differ in what they preserve, and the requirement is frequently discovered only when a user notices something missing weeks later, at which point the source may be gone.
HOW TO VERIFY	A written fidelity requirement, checked against the chosen tool before the tool is chosen.

Source 10

DM-5 **Item 39**

Verification is defined before the migration, including who signs off that a wave succeeded.

WHY IT MATTERS	Without a definition, success means the tool reported no errors, which is not the same as the content being correct and complete.
HOW TO VERIFY	A written verification method with a sample size and a named business signatory per wave.

DM-6 Item 40

The source environment retention period after migration is agreed.

WHY IT MATTERS	Decommissioning too early destroys the only remaining copy of something someone needed. Keeping it indefinitely costs money and leaves an ungoverned estate nobody patches.
HOW TO VERIFY	A written date per workload, with the owner who authorises decommissioning.

SECTION 8

Domain 8. Security posture

You inherit the weaker of the two postures at the moment the networks join.

SC-1 Item 41

Both estates are assessed against the same baseline before they are connected.

WHY IT MATTERS	Connecting a well governed estate to an unassessed one exports the risk of the second into the first, immediately and in both directions.
HOW TO VERIFY	Run the same assessment on both and compare. Do it before connectivity, not after.

SC-2 Item 42

A compromise assessment is considered for the acquired estate.

WHY IT MATTERS	An acquisition inherits any existing intrusion, including one nobody has detected. Discovering it after the networks join makes it your incident and your notification obligation.
HOW TO VERIFY	Scope a compromise assessment proportionate to the deal value and the sector.

SC-3 Item 43

Multifactor authentication and Conditional Access are aligned to the stronger baseline across both populations.

WHY IT MATTERS	A combined estate defends at the level of its weakest access path, and attackers find that path faster than integration programmes close it.
HOW TO VERIFY	Compare the policies on both sides and apply the stronger set to both populations, with a plan for the exclusions.

Sources 1, 2

SC-4 Item 44

Data classification and protection are extended to acquired content rather than assumed to arrive with it.

WHY IT MATTERS	Labels do not survive a tenant move as a matter of course, and unlabelled acquired content sits alongside labelled content looking identical.
HOW TO VERIFY	Confirm the labelling approach for migrated content and whether the source labels map to the target taxonomy at all.

Source 6

SC-5 Item 45

Incident response covers the combined estate from Day 1, with one path and one set of contacts.

WHY IT MATTERS	Two incident processes during an integration means an incident on the boundary belongs to neither, which is where the delay comes from.
HOW TO VERIFY	One written process naming who is called, effective on Day 1 rather than at the end of the programme.

SECTION 9

Domain 9. Day 1 continuity

What must work the morning after close. The discipline here is separating that from what merely should work, because trying to do everything on Day 1 is how organizations do none of it well.

D1-1 Item 46

Everyone can sign in and reach what they need to do their job.

WHY IT MATTERS	It is the whole of the Day 1 test as far as staff are concerned, and everything else in the programme is invisible to them by comparison.
HOW TO VERIFY	Test with real accounts from each population and each role, on the actual devices, before the day.

D1-2 Item 47

Email flows correctly to and from both organizations, including to the addresses clients already hold.

WHY IT MATTERS	Mail is the most visible external failure. A bounce to a client on the day of announcement is a commercial problem, not a technical one.
HOW TO VERIFY	Test inbound and outbound in both directions, including legacy addresses and any distribution lists that appear on published material.

D1-3 **Item 48**

The two populations can find and communicate with each other.

WHY IT MATTERS It is the first thing people try, and failure signals that the integration is not under control regardless of what else is working.

HOW TO VERIFY Confirm directory visibility, chat and meeting invitations work across both tenants before the day.

Source 5

D1-4 **Item 49**

Support knows what changed, and users know how to get help.

WHY IT MATTERS Day 1 volume goes to whoever answers, and a service desk that has not been briefed learns about the integration from the tickets.

HOW TO VERIFY A briefed service desk with a written list of known changes and a documented escalation path, in place before the day.

D1-5 **Item 50**

Anything customer facing that carries branding or addresses has been reviewed.

WHY IT MATTERS Signatures, portals, published contact addresses and automated notifications all carry the old identity, and the announcement is exactly when people look.

HOW TO VERIFY Walk the customer facing surfaces as a customer would, before the day.

D1-6 **Item 51**

What is explicitly not being done on Day 1 is written down and communicated.

WHY IT MATTERS Unstated scope becomes assumed scope, and the assumption is discovered as a complaint on the day.

HOW TO VERIFY A published list of what changes on Day 1 and what does not, circulated to leadership before the day.

SECTION 10

Domain 10. Transitional service agreements

Where one party runs IT for the other for a period after close. Every item here is delivery practice, and every one of them is a question IT should answer before the agreement is signed rather than after.

TS-1 **Item 52**

The services being provided are specified at a level of detail that would settle a dispute.

WHY IT MATTERS	A transitional agreement saying IT services will continue is an agreement about nothing, and the disagreement arrives in month two.
HOW TO VERIFY	Read the schedule. If it does not name systems, volumes and response expectations, it is not specific enough.

TS-2 **Item 53**

The duration and the extension terms are realistic against the migration plan.

WHY IT MATTERS	Transitional agreements are routinely signed for a period shorter than the work takes, and extensions are priced when the buyer has no alternative.
HOW TO VERIFY	Compare the term against the migration schedule, including its contingency. If they are the same length, the term is too short.

TS-3 **Item 54**

Data access boundaries during the transition are defined and enforced technically.

WHY IT MATTERS	The providing party has administrative access to the receiving party's data, and that party may be a competitor after close.
HOW TO VERIFY	Confirm the boundary is enforced by access control and logged, not only asserted in the agreement.

TS-4 **Item 55**

Exit criteria are defined, so both parties can tell when the agreement ends.

WHY IT MATTERS	Without criteria the agreement ends when one party stops paying, which is a dispute rather than an exit.
HOW TO VERIFY	A written definition of done per service, agreed by both sides in advance.

TS-5 **Item 56**

The cost is understood by both sides, including the cost of the providing party's staff time.

WHY IT MATTERS	Providing transitional services consumes the seller's IT capacity, which is usually the same capacity needed for their own separation work.
HOW TO VERIFY	Confirm the providing party has resourced it separately rather than absorbing it.

SECTION 11

Domain 11. Carve-out specific risks

Separating an estate that was never designed to come apart. These items do not appear in a merger checklist because they do not arise in a merger.

CO-1 Item 57

Shared infrastructure is identified along with which party keeps it.

WHY IT MATTERS	Domain controllers, file servers, network appliances and management platforms typically serve both businesses, and only one can keep any given instance.
HOW TO VERIFY	An inventory with a retained or divested decision against every shared component, and a plan for whichever side loses it.

CO-2 Item 58

Shared data is separable, and someone has confirmed it rather than assumed it.

WHY IT MATTERS	Records for both businesses in one system, in the same tables, referencing each other, is the normal state and it is a data engineering problem with a real cost.
HOW TO VERIFY	For each shared system, confirm a separation method exists and has been tested on a copy.

CO-3 Item 59

Enterprise agreements covering both businesses have a separation path.

WHY IT MATTERS	Volume licensing, support contracts and vendor agreements are usually held by the parent. The divested business may have no agreement at all on Day 1.
HOW TO VERIFY	List agreements by holding entity and identify what the divested business needs to procure independently, with lead times.

CO-4 Item 60

The divested business has the IT capability to operate independently, or a plan to acquire it.

WHY IT MATTERS	A carved out business often loses the shared services that ran its IT, and discovers this after the transitional agreement expires.
HOW TO VERIFY	Compare the roles the divested business will hold against the roles required to run its estate. Name the gap.

CO-5 **Item 61**

Intellectual property and records ownership are settled where systems hold both parties' material.

WHY IT MATTERS	Email archives, document repositories and code repositories rarely divide cleanly along the transaction line, and both parties may have a legitimate claim to the same item.
HOW TO VERIFY	Counsel establishes ownership rules, then IT applies them. In that order.

CO-6 **Item 62**

Residual access held by the separating party is enumerated and has a removal date.

WHY IT MATTERS	Accounts, keys, certificates, VPN access and administrative rights persist long after separation because nothing prompts their removal.
HOW TO VERIFY	A written list with a removal date and an owner for each, and a verification that the removal happened.

Source 4

SECTION 12

Domain 12. Governance and decision rights

Who decides, how quickly, and on what authority. Integration programmes rarely fail on technology and frequently stall on unmade decisions.

GV-1 **Item 63**

One person owns the IT integration and has the authority to decide.

WHY IT MATTERS	Two organizations produce two IT leaders with different views, and without a single owner every difference escalates and waits.
HOW TO VERIFY	A named individual with written authority, not a steering committee.

GV-2 **Item 64**

Decisions have a defined turnaround, and there is a path for when the deadline passes.

WHY IT MATTERS	A migration wave waiting on an unmade decision consumes the same budget as one that is progressing.
HOW TO VERIFY	A decision log with dates requested and dates answered. The gap between them is the measurement.

GV-3 Item 65

The integration budget includes the operating cost of running two estates during the transition.

WHY IT MATTERS	Duplicate licensing, duplicate infrastructure and duplicate support run for the length of the programme and are routinely omitted from the business case.
HOW TO VERIFY	Check the business case explicitly names the duplicate running cost and the assumed duration.

GV-4 Item 66

Change control operates across both estates during the transition.

WHY IT MATTERS	A change made on one side during a migration wave is the most common cause of a failed cutover, and it is usually made by someone who did not know the wave was running.
HOW TO VERIFY	One change process covering both estates, with a freeze period around each wave.

GV-5 Item 67

Communication to staff is planned, and IT knows what has been said before it is said.

WHY IT MATTERS	IT receives the consequences of every announcement immediately, and an unbriefed service desk learns the news from the users.
HOW TO VERIFY	Confirm the communication plan is shared with IT ahead of each announcement rather than at the same time.

SECTION 13

Domain 13. Post-close operations

The part after the cutover, which determines whether the integration delivered what the business case promised.

PC-1 Item 68

The combined estate has one operating model and one support process.

WHY IT MATTERS	Two ways of working that persist past the integration are the integration not having happened, and the duplicate cost continues indefinitely.
HOW TO VERIFY	One documented operating model with named owners, in effect rather than drafted.

PC-2 Item 69

Decommissioning of the source estate has dates, owners and a completion check.

WHY IT MATTERS	Undecommissioned environments continue to cost money, continue to need patching, and continue to hold data nobody is governing.
HOW TO VERIFY	A decommissioning plan with dates, and a verification that each item actually went.

PC-3 Item 70

Licence positions are trued up after consolidation.

WHY IT MATTERS	Duplicate and unused licences persist after migration because nothing prompts a review, and the consolidation savings in the business case depend on this step.
HOW TO VERIFY	A licence review after each major wave, with the reduction actioned rather than noted.

PC-4 Item 71

Governance established during the integration continues afterwards.

WHY IT MATTERS	Controls put in place for the transition lapse when the programme closes, and the estate drifts back toward the state that made the integration difficult.
HOW TO VERIFY	Confirm the controls have transitioned to a permanent owner with permanent funding.

Source 6

PC-5 Item 72

The business case is reviewed against what actually happened.

WHY IT MATTERS	Nobody checks, which is why the next integration is estimated with the same optimism as this one.
HOW TO VERIFY	A review at six and twelve months comparing promised against delivered, with the variance explained.

The ordering constraints, collected

These are the items where getting the sequence wrong costs rework rather than time. Each is documented by Microsoft and cited in the item it comes from.

- Identity mapping runs before workload licences are applied to the target users. Licensing them first is the most common ordering error in a tenant to tenant migration. See ID-2.
- Licences are purchased in the target tenant. They do not transfer, and a plan assuming otherwise has a gap in its budget. See TN-2.

- Mailboxes migrate before or alongside Teams content, because Teams chat and channel content depends on Exchange Online mailboxes. See TN-3.
- OneDrive and SharePoint migrate together, because they share a permissions model. See TN-4.
- Permissions are remediated before migration, not after, because a migration reproduces the source permission model into the target. See DM-3.
- Legal holds are identified before waves are scheduled, because hold status can block a mailbox move. See DM-2 and DS-6.
- IP range overlap is checked at the start, because renumbering or translation has a lead time that a close date will not accommodate. See NW-1.

Claims and their basis

Every claim this document makes about itself is listed here with what it rests on. Nothing here is a claim about your organization, a guarantee of compliance, a predicted saving, or a promised outcome.

Microsoft 365 licences cannot be transferred between tenants.

Microsoft states this in the tenant to tenant migration guidance. Licences must be purchased in the target tenant. Cited.

Mailboxes migrate before or alongside Teams content.

Microsoft documents that Teams chat and channel content depends on Exchange Online mailboxes, which sets the ordering. Cited.

No timeline, cost or success rate is given for any migration.

Deliberate. Duration and cost depend on user count, mailbox size, data volume, hold status, application estate and business constraints. The checklist gives the questions that determine those numbers, not the numbers.

Sources

Every source cited in this document, numbered in the order it is first referenced. The numbers on the items above point here. Each source was checked on the verification date shown. Microsoft documentation changes, so re-check anything you are about to act on.

1. Common Conditional Access policies
Microsoft Learn. Verified 2026-08-24.
https://learn.microsoft.com/entra/identity/conditional-access/concept-conditional-access-policy-common

2. Common Zero Trust identity and device access policies
Microsoft Learn. Verified 2026-08-24.
https://learn.microsoft.com/security/zero-trust/zero-trust-identity-device-access-policies-common

3. Start using Privileged Identity Management
Microsoft Learn. Verified 2026-08-24.
https://learn.microsoft.com/entra/id-governance/privileged-identity-management/pim-getting-started

4. Best practices for Microsoft Entra roles
Microsoft Learn. Verified 2026-08-24.
https://learn.microsoft.com/entra/identity/role-based-access-control/best-practices

5. Configure cross-tenant access settings for B2B collaboration
Microsoft Learn. Verified 2026-08-24.
https://learn.microsoft.com/entra/external-id/cross-tenant-access-settings-b2b-collaboration

6. Get started with Microsoft Purview
Microsoft Learn. Verified 2026-08-24.
https://learn.microsoft.com/purview/purview-where-to-start

7. Learn about retention policies and retention labels
Microsoft Learn. Verified 2026-08-24.
https://learn.microsoft.com/purview/retention

8. Turn external sharing on or off for SharePoint and OneDrive
Microsoft Learn. Verified 2026-08-24.
https://learn.microsoft.com/sharepoint/turn-external-sharing-on-or-off

9. Microsoft 365 tenant-to-tenant migrations
Microsoft Learn. Verified 2026-08-24.
https://learn.microsoft.com/microsoft-365/migration/microsoft-365-tenant-to-tenant-migrations

10. Microsoft 365 migration overview
Microsoft Learn. Verified 2026-08-24.
https://learn.microsoft.com/microsoft-365/migration/microsoft-365-migration-overview

11. Migration orchestrator overview
Microsoft Learn. Verified 2026-08-24.
https://learn.microsoft.com/microsoft-365/migration/migration-orchestrator-1-overview

12. Cross-tenant identity mapping
Microsoft Learn. Verified 2026-08-24.
https://learn.microsoft.com/microsoft-365/migration/cross-tenant-identity-mapping

13. Cross-tenant mailbox migration
Microsoft Learn. Verified 2026-08-24.
https://learn.microsoft.com/microsoft-365/migration/cross-tenant-mailbox-migration

14. Cross-tenant OneDrive migration
Microsoft Learn. Verified 2026-08-24.
https://learn.microsoft.com/microsoft-365/migration/cross-tenant-onedrive-migration

15. Cross-tenant SharePoint migration
Microsoft Learn. Verified 2026-08-24.
https://learn.microsoft.com/microsoft-365/migration/cross-tenant-sharepoint-migration

16. Cross-tenant multitenant organization migration
Microsoft Learn. Verified 2026-08-24.
https://learn.microsoft.com/microsoft-365/migration/cross-tenant-multitenant-migration

About Simplicity IT

Simplicity IT Inc. is a Microsoft-focused managed services, security and implementation company. We began in 2011. We assess, implement, migrate, integrate, secure, govern and operate Microsoft cloud environments, and we design the human approval points that keep automated work accountable.

If this document was useful

Book an M&A IT discovery session at simplicityitinc.com/contact/

Related reading

- M&A IT integration and carve-out separation, simplicityitinc.com/solutions/ma-it-integration/
- Zero Trust architecture and Entra ID, simplicityitinc.com/solutions/zero-trust-m365/

Privacy

We use your details to send you this resource and occasional related guidance. We do not sell your information and you can ask us to delete it at any time by emailing hello@simplicityitinc.com.

What requesting this document does not do

Requesting a resource does not create an account, a trial, a subscription, partner status, or an engagement. It sends you a document.