

White Paper

Navigating divestiture migrations: Pointers for success

Two previous papers delved into managing, planning, and executing migrations with a focus on merger and acquisition (M&A) scenarios. This paper pivots to hone in on divestitures, where an organization spins out one or more business units into other organizations. As with M&As, thorough discovery, careful scoping, and meticulous pre-planning are essential before initiating the process of migrating mailboxes, documents, and files. The ground covered in those previous papers also applies here. But in the experience of BitTitan — especially with some tricky, high-stakes projects — divestitures are a little different and there are some specific things an MSP and migration team need to be alert for.

Understanding the landscape

In a divestiture, a business entity has made a decision that one or more of its business units are not core to the fundamental business, and sells or transfers it to another entity that can bring more focus and ultimately create more value. There are three broad types:

- A carve-out sells the business unit to a third party
- A spinoff turns a business unit into an independent operating company.
- A breakup separates the parent company into multiple independent companies

In all of these scenarios, the business unit being divested has been dependent on some of the services and processes of the parent company — a set of dependencies often termed entanglement. The divesting company (divestor) and acquiring company (acquirer) enter into a transition services agreement (TSA) that establishes the conditions, milestones, and timeline for how the divested business unit will be disentangled from the divestor and serviced under the acquirer's umbrella.

IT roles and responsibilities

When an MSP takes on a divestiture migration, it is brought in to execute some of the terms of the TSA. The migration of the users and data is just a small part of handing over the IT assets and operations. This means the divestor's CIO in particular is burdened with all of the details that go into disentangling the processes and fulfilling all the other terms of the TSA. Bringing an MSP on board to handle the migration frees the CIO to focus on the bigger issues, rather than how to staff up to manage a huge migration project. Therefore, the more the MSP can do to reassure and demonstrate to the CIO that things are in good hands, the better it is for everyone.

The in-house IT teams still have a big role to play in identifying the data, users, and systems that need to be migrated, and that in turn drives the migration plan and timeline. After assisting in the discovery phase, the degree to which existing IT teams take part in the migration is a tradeoff involving costs, time, and staff availability. Once the proposal has been accepted and the MSP moves into scoping the project, the roles and responsibilities begin to crystallize and turf battles may begin. This is where a strong MSP can step up, assert ownership where it matters, and protect all parties by heading off issues that might delay or jeopardize the entire project.

At the extreme, there have been cross-border divestiture scenarios where there were so many local IT staffs and stakeholders involved and the pressure to meet the target date was so extreme that the MSP was given the keys to make all the judgment calls and take complete ownership of the entire migration.

Discovery and scoping

Most MSPs that specialize in migrations have developed and follow a standard operating plan which is good to a point, but it's a mistake to limit the discovery questions to what has been written down. There have been many, many migrations where the existence of an ancient, legacy system with old data that the organization still relied on was uncovered only after the migration was complete. Oftentimes, the data exchange between the legacy and current production systems was automated using pointers, so the dependency on the legacy system was overlooked or forgotten. The bottom line for the MSP is, even after you think you have all the answers, keep asking questions.

One significant item to address early-on is identifying the Destination environment. It could be an Office 365 environment, or a Domino environment. Files may be stored on local drives, Google Drive, Teams, OneDrive, SharePoint, or any number of combinations and permutations. In general, migration to a greenfield environment is easier than to a pre-existing one that has already been configured. While it can be a chore setting up a net-new environment to match the licensing, security parameters, workflows, and settings to replicate what the users are accustomed to, that process is fairly straightforward. Moving to an existing setup requires discovery of the Destination environment as well as the Source, which is often more time-consuming.

Some acquirers see the migration as a great time to do a technology refresh, which adds extra steps and another layer of planning. There have also been migrations where users of extremely current systems were being migrated to systems that were truly ancient, adding to the complexity, costs, and knowledge base required to pull off the migration successfully.

End-user issues

Be aware that ownership can be an issue in a divestiture and individuals may not be happy with someone digging into their systems. Diplomacy can be a vital skill. Usage patterns and organizational culture may also come into play. What are the implications for the migration plan if the divestor had no data policy and users were accustomed to storing their data and files on local machines, while the acquirer expects everything to be stored centrally?

In the end, the major questions that drive the migration itself and the strategy involve the amount of data, and the end goal which is where the acquirer wants the data to reside. A second layer is around security parameters, group policies, workflows, permissions, and the other considerations that describe how the acquirer expects to operate from a functional and security perspective.

Security and legalities

There are legal aspects to divestiture migrations because the TSA is a contract between the two business entities. Country-specific regulations may also come into play, or legal differences between countries may dictate that some data cannot be migrated.

Sometimes, the migration deadline and legal closure of the divestiture are on the same day. More often, once the divestiture deal is signed and closed, the TSA specifies a set period of time, typically between six and twelve months, to fully separate the divestor and acquirer. A quick takeover is to the benefit of both parties. The agreement likely includes a schedule with milestones, and possibly financial incentives for terminating services early or penalties if services need to be extended. There may also be legal deadlines imposed by regulators.

Confidentiality and data integrity

The divestiture plan may have been publicly disclosed, or kept confidential. If confidential, it is typically publicly announced when the definitive agreement to divest has been signed between the divestor and acquirer. Since the migration of the data is part of the TSA, once the announcement is public, rogue users are a liability risk under terms of the agreement.

In most divestitures, news about potential layoffs is held until the data migration is complete. Otherwise, to-be-terminated employees have the opportunity to take revenge by deleting key records, emails, and documents, and otherwise sabotage both parties — especially if they have higher privileges or administrative rights. To guard against the consequences of early leaks or gossip about post-divestiture employment plans, extra attention needs to be paid to security in the timeframe leading up to the migration. If the organization being divested is on Office 365, it may be prudent to put mailboxes on litigation hold, even at the cost of extra licensing.

Email issues and business continuity

Completing a successful divestiture migration that goes according to plan and has the acquirer's staff working productively on day one requires attention to details. Here are some of the seemingly simple issues that might be overlooked.

Address conflicts. Role addresses, proxy addresses, and individual accounts with similar names in the divestor and acquirer need to be spotted and accounted for before the mailboxes are actually migrated, or there's a risk of populating a mailbox in the Destination with someone else's email.

Addressing conventions. This is an elementary example of the sometimes-thorny issues that come up when one organization joins another. This has happened in larger migrations where the divested business unit has been using `firstname.lastname` for 20+ years, the acquirer uses `firstname_lastname`, and nobody wants to change.

Federated accounts. If either organization has established guest accounts or uses federation to extend access to trusted business partners, it should be brought up early in the discovery process. That is especially true if the organization being migrated wants to preserve the continuity of their operation straight through the migration with continuous access for business partners.

Increasingly, organizations are using federation to enable collaboration with partners. Happily, there are also strategies that draw on federation, in conjunction with a migration tool's ability to convert between mailboxes of different types, to make the migration smooth and seamless for users inside and outside of both organizations.

Migration execution

Knowing the data sizes, and identifying which data is most important for keeping the business running are the keys to developing a sound migration plan that will keep the business running while minimizing the chances that throttling will come into play.

During the migration, it's important not to rely solely on a dashboard, even though that's tempting if the overriding concern is with meeting a deadline. Keep an eye on the logs including the data sizes, counts, and exception reports, and don't assume that all of the data in a batch has been migrated successfully. Errors that prevent files from being copied are inevitable. There can also be XML files, contacts, and calendar items that aren't translated to the Destination. End-users are quick to notice a few missing items after their data has migrated and complain. This is where end-user communication before and during the migration makes all the difference in setting expectations and keeping the finger-pointing in check.

End-user training

If the divestiture means admins and end-users are moving to an unfamiliar environment and applications, the TSA should and likely does include provisions for end-user application and IT system management training. Portions of the training will likely fall to the MSP, who should embrace it as an elemental part of the migration, and not an after-thought. Amid the technical details, it's easy to lose sight of the big picture — migration isn't just about moving mailboxes, files, and folders. It's about moving a thriving, productive business into a different tenant.

Working with BitTitan and MigrationWiz

The MigrationWiz Tenant Migration Bundle is an excellent option for an MSP tackling a big divestiture project because pricing is per-user and the bundle can be applied to migrations that involve any combination of mailboxes, Microsoft SharePoint, or Microsoft Teams. The migrating client or MSP doesn't have to produce counts of Teams groups or SharePoint libraries to arrive at a cost for the migration. The bundle makes pricing predictable, and decreases the chances that there will be a need to procure additional licenses to complete the migration and the delay that comes with it.

The MigrationWiz GUI and the extensive logging capability built into MigrationWiz is a major advantage before, during, and after the migration. The point-and-click experience is highly streamlined, in comparison to trying to manage a migration using scripting solutions and is much appreciated by MSPs who have taken on a high-stakes project with exacting deadlines.

Finally, engage with the BitTitan Customer Success team early on in the project. Even if you don't need the support right away, enlisting them and getting them familiar with your project can pay dividends well before it's time to deploy MigrationWiz.

**To find out more, speak to a CCS Media
Datacentre & Networking Specialist**

call: 01246 200 200

email: letstalk@ccsmedia.com

visit our website at [ccsmedia.com](https://www.ccsmedia.com)

