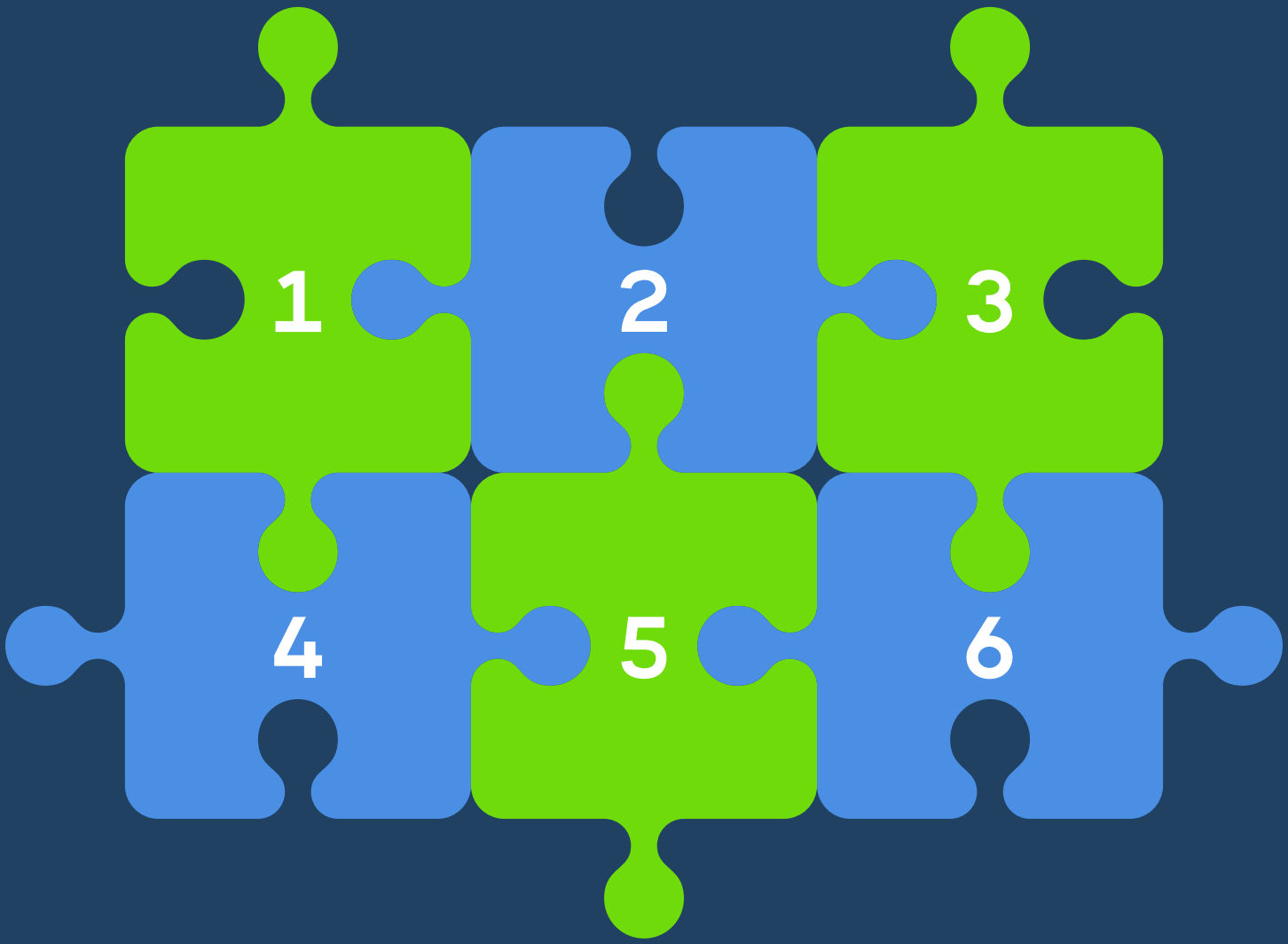
CoreView

Six vital pieces to the

M&A Microsoft 365 governance puzzle



Introduction

Mergers and acquisitions (M&A) scenarios are challenging for enterprises large and small alike. At the same time, today most enterprises have or are moving to SaaS productivity and collaboration/communication applications – of which Microsoft 365 is a leading light. Microsoft asserts that there are over 300 million monthly Microsoft Teams users and that 200 petabytes (PB) of data are added to SharePoint every month. Microsoft 365 is powering the digital workplace for many organizations.

There are three main scenarios for these organizations using Microsoft 365 during complex processes like Mergers and Acquisitions, including:

- A Microsoft 365-based enterprise buys another Microsoft 365-based enterprise might deal with migration, governance, as well as security and application and user management.
- A Microsoft 365-based enterprise buys a non-Microsoft 365-based enterprise and must deal with migration, governance, as well as security and application and user management.
- A non-Microsoft 365-based enterprise buys a Microsoft 365-based enterprise and must deal with integration issues – and plan for proper governance.

Migration/Integration basics

When bringing on a company using Microsoft 365, the fundamental process of moving that tenant over might look straightforward, and one would think it is just an integration of the tenants. IT chooses which will be the host tenant (likely, the buyer gets this honor), creates dummy users on that side, and then copies the email addresses of the mailboxes. This gets the ball rolling...

As you go deeper, things get more complex. “You may need to onboard folks from the acquired company, merge two environments and govern them, identify security issues, and meet compliance regulations before the deal can be done. If people are let go, offboard safely and address data loss prevention (DLP) issues before they cause problems,” said Kasia Nowicka, Product Marketing Manager for CoreView.

Here are the six steps to take to ensure top-shelf Microsoft 365 governance during the M&A process.

1 Conducting a Microsoft 365 tenant assessment

Assessment of any Microsoft environment is critical because most likely IT teams from each company do not know the details of what each side of the deal has, or how Microsoft 365 is set up and managed, if at all. Luckily, basic analysis and reporting reveal how people use the platform, how they are licensed, the number of users, plus what applications and services are used and what are not. This is also a good time to investigate what toolkits companies have in place, how they are monitoring existing policies, enforcing them and remediating if needed.

If your IT team is taking in and ultimately integrating a new Microsoft 365 tenant, your IT staff should conduct a full and deep analysis. Here are the processes for a proper Microsoft 365 tenant readiness assessment:

Use read-only admin for assessment: It is recommended to have read-only access when analyzing a target company that you have not yet purchased. Fortunately, read-only is a default CoreView RBAC setting to all our Microsoft 365 reports.

Security assessment: Before buying or integrating a company, it is good to know the state of security. Here are some items to look at – their Microsoft 365 Secure Score, Failed Logins, state of MFA (Multi Factor Authentication), Conditional Access, and DLP.

Workload adoption: What is the detailed usage level of key applications such as Exchange, OneDrive, Teams, SharePoint, etc.?

Licenses: Which licenses are currently in the inventory, and what has been distributed? What procedures are in place for purchasing or ordering new licenses, and are there any reconciliation or charge-back processes implemented?

Protocols: Which protocols are utilized for client access to the platform? Specifically for Exchange, which protocol is employed to access mail (MAPI, POP3, IMAP)? Additionally, can we deduce the other access methods currently in use, such as for accessing Teams?

Devices: You cannot protect end users unless you know what devices they have and the state of the operating systems – are they up to date and patched?

Lastly, as part of the assessment, IT should look carefully at how the target company manages their Microsoft 365 environment, including if they have any existing tenant segmentation (either done by Admin Units or other tools), Role-Based-Access-Policies template in place, and any Microsoft 365 or Azure-specific security policies.

2 IT Administration

In cases where a Microsoft 365 shop acquires a non-Microsoft 365 shop, the objective typically involves onboarding the new company onto the selected SaaS platform. This often entails migrating the acquired company to Microsoft 365 as part of the agreement.

One problem is that IT tends to focus on the migration to Microsoft 365 itself, not its actual operation, which should concern IT just as much. Gartner in its 'Market Guide for Cloud Microsoft Migration Tools', put out in February 2019, pinpointed how migration tools are limited to, well, just migration. "Migration of emails, files and application data is a common scenario for cloud office migration, but few vendors move all three workloads using a single tool and even fewer address post-migration requirements of governance," Gartner argued. "Include as part of your cloud office migration strategy the ability to address both short-range (on-premises to cloud office) and longer-range (ongoing platform governance, tenant splits, consolidation or cross-platform shifts) migration demands."

Ignoring these operational issues during migration or integration means living with an insecure, unwieldy and breach-prone SaaS environment.

3 Securing Microsoft 365 before fully integrating acquired tenant

Microsoft 365 security is a challenge – in an M&A scenario or not. Adding a new company to the equation worsens the problem. If you buy a company that is not secure, you take on those vulnerabilities. Consider Marriott. In the midst of the Marriott-Starwood merger, it was revealed that Starwood had experienced a data breach impacting approximately 500 million customers. This incident proved to be unfavorable for Marriott in terms of public relations.

Although this incident did not involve a breach in Microsoft 365, it is important to note that Microsoft's cloud productivity platform is a prime target for hackers and often serves as a source for breaches of enterprise and Personally Identifiable Information (PII) data. Therefore, it requires meticulous protection measures.

Security issues frequently inflict significant damage on acquisitions. In fact, a survey conducted by Forescout reveals that 65% of IT professionals express regret over an acquisition due to inherited security problems.

According to an article in Dark Reading, the acquiring company should carefully examine the security posture of the company being bought. These discovered problems do not always rule out an acquisition but should be addressed prior to the IT integration -- and even be part of a price calculation. "Cybersecurity due diligence should start before any deal is made. You are looking for cybersecurity issues that could rule out a deal or affect the sale price. For instance, Verizon knocked $350 million from its purchase price for Yahoo after two data breaches were discovered," the website argued, adding that survey data "revealed 73% said the discovery of an unknown data breach would be a deal breaker for an acquisition."

In the case of Microsoft 365, audit logs can be examined to determine security history. One can even run a CoreView Health Check, which examines the entire tenant for security issues.

Microsoft 365 Health Check and auditing

The M&A transition is a critical and sensitive time. “Knowing exactly what is happening during that sensitive human resource time is important. The first thing CoreView does as part of a Health Check is turn on auditing for every single workload. That data now exists where it almost certainly did not exist before because, with Microsoft 365, auditing is not turned on by default,” CoreView’s Nowicka explained. “Then CoreView can store that audit information longer, alert on anomalous activities, and expose the full data analytics of the Microsoft 365 E5 suite their users may have. All of this serves to increase security awareness. When people know they are being watched, it improves their behavior. That is why cameras are so prominent at the register in convenience stores. There is a reason why those are not all hidden cameras. It positively impacts behavior.”

A CoreView Health Check fully points out the security issues that you may be inheriting, as well as license savings that can be had.

When you are in the process of negotiating, there are bound to be security issues to explore and tackle. For one, you do not want confidential information being released. Moreover, after an acquisition, oftentimes people are redundant and let go – which raises security issues with data leakage, confidential information shared or stolen, and nefarious acts by disgruntled ex-employees. “Once you’ve acquired a company, oftentimes there are redundancies and people get laid off and that’s where a lot of confidential data gets stolen, leaked out, shared,” Nowicka argued.

A deep analysis of the target tenant can nip these problems in the bud. “What cannot be overemphasized is the ability to look at large volumes of data in detail and extract high impact issues. Looking at the entire file state of an organization, their OneDrive and SharePoint sites, be it on-premises or in the cloud and identifying what sensitive data exists is all absolutely critical. Equally important is identifying potential configuration issues and even recommending a security model for those assets,” Nowicka explained. “Then finally, consider tagging that data or enhancing the metadata so those assets can be found in what is going to be a much larger tenant when the two organizations merge. That must be a key pillar to assessing and creating a merged structure going forward.”

4 Proper and safe onboarding

Once the integration is underway, IT must onboard Microsoft 365 workloads in either direction. “Typically, it is a payment company acquiring a subsidiary. In that case, the subsidiary has a certain involved way of provisioning Microsoft 365 user accounts, mailboxes, SharePoint sites and other functions such as external/ guest users,” Nowicka said.

Workflow and provisioning

Clearly, provisioning is a huge deal during a merger or acquisition. Most companies being bought, if they have Microsoft 365, use provisioning scripts. “However, if IT gives admins the ability to run those same scripts in the new environment, under the native model Microsoft 365 administration model, IT has to offer global admin rights to run those PowerShell scripts,” Nowicka argued. These global rights simply give admins, including those from the target company, way too much power.

By implementing limited rights through Role-Based Access Control (RBAC) and incorporating workflow automation, Microsoft 365 can be effectively streamlined and secured for larger tenants. “With the CoreView workflow model, IT can get very granular. IT could give admin rights to only add telephone numbers for users, which is exaggerating to prove a point. But you really can get that granular,” Nowicka said. “IT also cares how users from the target company access the Microsoft 365 platform. Maybe IT wants to permit web access from home, or allow mobile devices including Androids, Windows mobiles, as well as iPhones. That may not be the policy of the parent company or the acquiring company, or it could be a merger with peers. Just knowing what those policies are and being able to see them firsthand versus calling the admin saying, ‘Okay, how do you do stuff?’ is important. On that, CoreView can be very specific and detailed.”

Finally, licensing is a key part of the onboarding/provisioning process. “CoreView helps with initializing their onboarding in phases. For instance, IT could give user permissions just to do licensing – for now. IT can create license pools for usage. IT can provision out of their corporate licenses instead and gain efficiency from that. Or IT could let someone create users and change passwords – but just for their group. Here, Virtual Tenants, license pools and functional access control, all come into play,” Nowicka said.

5 Looking at licensing

Conducting a license analysis not only identifies savings but also shows if the licenses of the target company match the needs of the buyer. Say the buyer tends towards high-end E5

licenses, while the target company makes do with E3 or even E1/F1. Or the reverse, where the target overspends on high-end licenses they don't need.

There are also benefits through the unified purchasing of licenses – these are only truly realized if you have controls in place via license pools.

6 Maintaining what you integrated/ migrated securely

Secure Delegation

When bringing on a new tenant, Microsoft 365 IT pros should apply the least privileged access model, segmentation of audit logs, and smart and secure provisioning to make the combined tenant safe and effective.

Part of this is making sure the administration itself is safe. Here, delegating admin responsibilities means less micromanaging at the top and more uptime in the field – and better security against IT insider threats and admin errors. You can assign access by role, so you have fewer global admins and better security. Meanwhile, CoreView can manage multiple tenants all within the same portal instance.

By giving all your tenants one place to do their work, you ensure that no matter a person's access level or sub-pool, they are never confused about where to access reports and perform management tasks.

CoreSuite allows global IT administrators to delegate control over all aspects of the management interface, including reports, custom PowerShell scripts and everyday admin functions.

By partitioning your tenant, you can limit access to specific geographies. Here, CoreView enables Virtual Tenants and license pools. These groups can be automatically governed by filtering via Azure AD (Active Directory) attributes such as department, city, cost center, etc.

The delegation is fully integrated. CoreView supports delegation in entirety of our platform, so you can make delegated workflows consistent across your company. Learn more about delegation.

License optimization

Managing licenses can be challenging for IT, not only within their own tenant but also in the target company's environment. However, imagine the convenience of easily identifying inactive Microsoft 365 licenses for both your organization and the target company, and seamlessly reallocating them. With the help of CoreView, you can effortlessly locate inactive, oversized, and duplicated Microsoft 365 licenses, and perform reallocation tasks without needing to leave the management platform. This prevents overspending and helps you identify departments with low adoption.

Finally, you can determine the itemized cost of licenses by business unit, location and more. CoreView lets you insert the net costs for your license SKUs into reports broken down by specific attributes like business unit, department, location and team.

That way you can see how costs are actually distributed.

You can also base Microsoft budgets and chargebacks on actual usage. Each department in your company uses Microsoft 365 differently. Make your budgets and chargebacks more accurate with SKU data mapped to your business units, departments, locations and more.

Offboarding through workflow

M&As often involve layoffs. Fortunately, employee offboarding can be done safely, securely, and easily through CoreView's workflow. Workflow templates automate both provisioning and de-provisioning. And with automation, IT ensures users have the right licenses to access the right infrastructure. IT can "clone" users or create them from templates to reduce errors and speed provisioning. With this approach, IT automates the entire user lifecycle: onboarding, configuration, provisioning, and removal.

Workflows make it exceptionally easy to manage end users. Some provisioning processes can include 50 or more steps – all of which can be triggered by a single click – with full auditing implemented by default. This saves admin time and ensures these processes are error-free.

The Final Analysis

One key lesson from the M&A experience is that deep, actionable, and consolidated reporting is critical to maintaining and governing Microsoft 365. At the same time, when companies merge, there are advantages to having a single tenant by allowing employees of the combined entity to collaborate – such as with Microsoft Teams. The companies really come together through a single address book, and standard ways of sharing documents, files and data.

Now that we have walked through all six integration and Microsoft 365 M&A governance steps, what does it all mean? "These steps help from a security aspect, a provisioning aspect, and for economies of scale by bringing the licensing purchasing power under a central authority. That typically has with it an economy of scale, increasing collaboration, allowing the collaboration to occur so that you realize the value of Microsoft 365 in a single tenant," Nowicka argued.

All this IT M&A legwork greatly eases the transition. Plus, IT is more comfortable knowing what the target company has for users, licenses, workloads, directories, security policies, administrative practices, configurations, and data sharing, such as through SharePoint or OneDrive.

Learn more about Microsoft 365 administration with a CoreView **demo**.