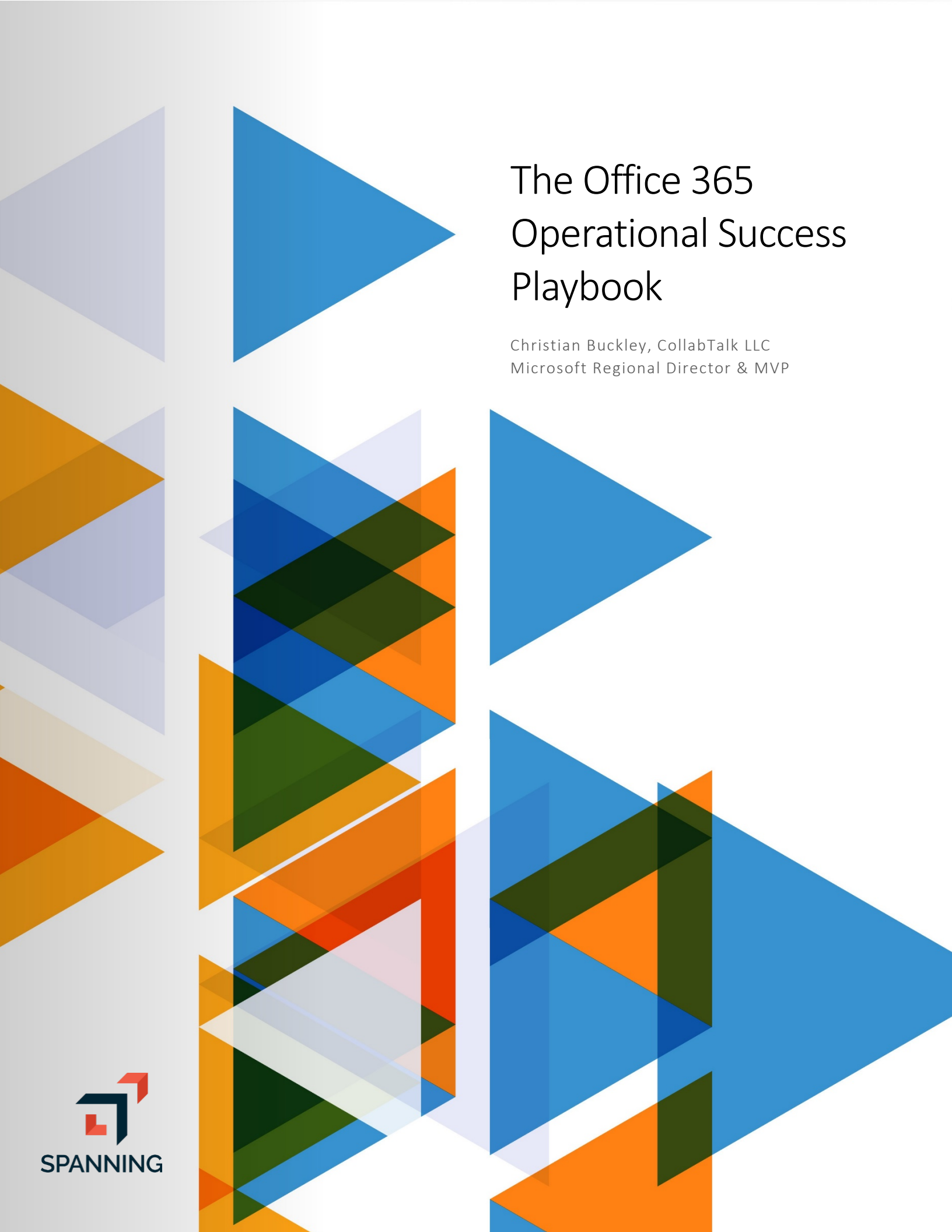
The Office 365 Operational Success Playbook

Christian Buckley, CollabTalk LLC
Microsoft Regional Director & MVP



SPANNING

Contents

This whitepaper is based on two recent independent research efforts:

Organizational Security & Compliance Practices in Office 365 (March 2019), sponsored by Spanning, RecordPoint, tyGraph, Rencore, and Microsoft.

Improving Governance in Office 365 (March 2019), sponsored by Spanning, Rencore, tyGraph, and Microsoft.

Why Operational Guidance is Needed

According to recent research, the number one area of concern identified by Office 365 customers as they began planning for their move to the cloud is security and compliance[1]. Cloud security and compliance is an important topic across every industry and company size as increasing cost efficiencies and dramatically improved productivity drive organizations towards the cloud.

As our cloud efficiency grows and end user productivity increases, so does our need for an increased focus on change management and operational improvement. The better we understand and leverage the technology we have in place, the more value we deliver to our teams – requiring us to be thinking about additional ways that we can improve upon our business outputs. We live in a hyper-competitive world, and few companies will ever have the luxury of sitting still for very long. The competitive landscape does not stay idle: technology will continue to innovate, and your employees will not remain satisfied with the current slate of tools forever. Life is an escalator — it's always moving up, or down. If you come to a stop, people will find their own path forward, with or without you.

Looking at the Office 365 platform, with the core workloads of Exchange, SharePoint, OneDrive, and Skype, they include decades of on-premises history with robust and mature security, compliance and governance capabilities as standalone offerings. Customers around the world have come to rely on the on-premises versions of these tools, but they are quickly moving to the cloud, which requires a review – and possibly a re-thinking – of operational practices to ensure our environments remain secure, compliant, and well-governed.

While the Office 365 platform inherits the robust and mature security, compliance and governance capabilities of its on-premises standalone predecessors, customers need to include a review their security, governance and compliance requirements as they migrate to Office 365 to ensure that requirements are being met and any gaps can be managed.

A Change Management Mindset

If moving to the cloud was not complex enough, our end users are leveraging more devices than ever before – some of them personal devices. Here's the problem: How do we know if our systems are compliant if our end users are using whichever tools and whatever devices they want? Is there a documented governance model, are these policies and procedures being regularly reviewed, and how often are changes made to the model? Do these documents and processes reflect the current standards governing our systems, or were they antiquated and irrelevant as soon as they were published? How are changes and updates to policies and procedures identified, much less implemented?

Most documentation comes with an expiration date due to changing business requirements and shifting legal and regulatory constraints. The fact is that our operations are a living, breathing, ever-changing activity — and yet lessons learned through our day-to-day project experiences are seldom reflected in our documentation, causing new projects and teams to reinvent the wheel each time.

[1] https://spanning.com/resources/reports/organizational-security-compliance-practices-office-365/

Beyond capturing corporate and system requirements, your operational management activities necessitate having strong governance and change management models. This is especially important if you have open policies about the tools and devices end users can adopt, as an increasing number of companies support. Part of change management is having a clearly defined and communicated plan. With an overarching view of your systems and controls, your team will better understand and more quickly recognize where changes are necessary. Maintaining a blueprint of your operational management activities means that you can more proactively monitor and manage your business systems and the technology platforms you have come to rely upon.

Of course, compliance is easier when people can locate the policies — and they have a shared understanding of the overall governance and change management model. To be effective and successful, these operational activities must be an active and transparent part of the organization's day-to-day management conversation and culture. People need to know where to go find the latest policies and procedures, but they must also see the impact of business change and have trust in the system.

The Modern Workplace

Within organizations around the globe, one common trend in collaboration is the increasing focus on employee adoption. The reason for this focus is simple: You can spend all the money in the world on technology, but if your employees don't use it, you've failed. Organizations are questioning the value of their structured collaboration platforms, many of which evolved from outdated intranet portals and a presenter/audience content distribution methodology. While organizations have had some degree of success with these models, there has been a noticeable enthusiasm gap with end users — and the grand vision of many of these platforms as "the" place where employees gather to collaborate has not been achieved. As a result, the focus has shifted to end user adoption, with Microsoft developing experiences that not only support the rapidly changing collaboration expectations of users, but to develop interconnected tools that will continue to deliver value.

Office 365 Primary Workloads

Microsoft has long been at the forefront of the modern workplace, and Office 365 continues to be Microsoft's collaboration and productivity centerpiece for enterprises and small to mid-sized businesses around the world. Within the core Office 365 platform are some of the most widely-used and supported solutions available within each collaboration sub-category:

SharePoint

SharePoint is a web-based document management and storage system that powers the intranets of almost 90% of the Fortune 500 companies. It also increasingly provides the document infrastructure to the other workloads within Office 365.

Exchange / Outlook

Email remains an important aspect of the modern workplace. Exchange is the server-based software component, while Outlook is the desktop email client.

Teams

Teams is the relatively new chat-based workspace in Office 365 that brings together people, conversations and content—along with the tools that teams need—so they can easily collaborate to achieve more. Teams reduces context switching by integrated with the familiar Office applications and is entirely built for the cloud.

Yammer

Another cloud-based platform is Yammer, an enterprise social networking service used for private communication within organizations.

OneDrive

OneDrive is a file hosting service and synchronization service that allows users to store files and personal data in the cloud, share files, and sync files across their mobile devices, Windows and macOS computers, and the Xbox 360 and Xbox One consoles.

Azure

Azure is a set of cloud services to help you build, manage, and deploy applications on a massive, global network using your favorite tools and frameworks.

Microsoft 365 vs. Office 365

Another common question from end users: What is the difference between Office 365 and Microsoft 365? To clarify, Office 365 is a line of subscription services offered by Microsoft as part of the Microsoft Office product line and is included within the broader Microsoft 365 offering.

The Office 365 brand includes plans that allow use of the download-able Microsoft Office software suite over the life of the subscription (monthly and annual subscription plans available), as well as cloud-based software-as-a-service products, such as Teams, Yammer, and SharePoint. One benefit of using cloud-based services is that the Office 365 solution includes automatic updates at no additional charge, rather than needing to pay for new licenses each year.

By comparison, Microsoft 365 is a more comprehensive offering for the enterprise or mid-sized company requiring desktop and mobile device support, and more. As shown in the following Figure, Microsoft 365 includes Office 365, Windows 10, and Enterprise Mobility + Security, giving administrators more visibility across each workload, and providing a richer, more collaborative experience for end users.

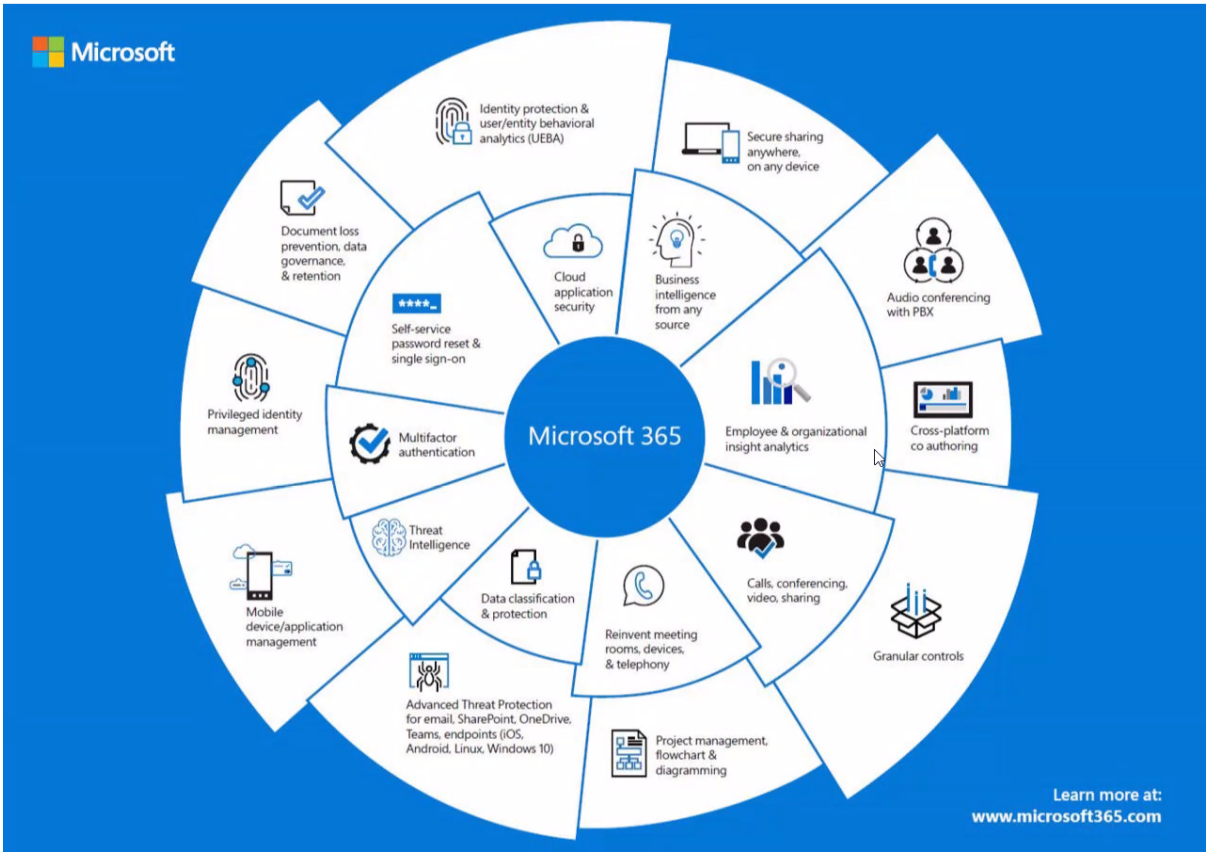


Figure 1 - The Microsoft 365 offering

Microsoft's Strengths

Microsoft has a number of core strengths that are helping to accelerate the maturity of their cloud platforms, with Office 365 at the center:

Business-focus

One of Microsoft's core strengths comes from its extensive product base, which is especially attractive to enterprise customers who already use Microsoft products and are invested, with an estimated 1.2 billion Office users and 60 million Office 365 commercial customers.

Privacy

With far too many public failings of tech companies to secure their customer data, Microsoft has made data privacy a major priority. For every web application that touches Azure, Microsoft outlines exactly how they manage customer data within their datacenters, giving customers control over where it is geographically located, who has access, and how it should be managed.

Expansion of PaaS and IaaS

Microsoft Azure originally started as a Platform as a Service (PaaS) offering but has since moved toward Infrastructure as a Service (IaaS). With tight integration between Azure and existing Microsoft products, the platform has grown exponentially and is now the #2 cloud platform behind AWS.

High availability and scalability

Microsoft's huge (and growing) global footprint gives the company a distinct advantage over most customers in its ability to provide high availability and redundancy through Azure through its datacenters around the world. There are currently 54 Azure regions available in 140 countries with up to 1.6 Pbps of bandwidth in a region. Because of this footprint, Azure can scale up or down quickly to meet the needs of even the most volatile businesses.

Security as design principle

Microsoft has invested heavily and focused on improving the security of its cloud products because hackers are becoming more sophisticated and organized. Microsoft offers three levels of security, namely physical security, logical security and data security.

The Risks of Modern IT

Microsoft cloud infrastructure investments give customers a solid base upon which they can build, but there are always risks associated with change. Business transformation through technology is happening faster and more pervasively than any other point in history. In today's connected, mobile, application-based world, organizations must constantly innovate to satisfy the appetite for customers who expect quick and reliable service at their fingertips, on any device they choose. With the latest advancements in cloud technology, the ability to modernize for better security, greater functionality, and workforce efficiency is now within reach of organizations of all sizes.

In our most recent research, survey respondents were asked to identify their biggest security challenges. At the intersection of their responses was a lack of proper planning and governance:

Table 1 - What are your biggest security challenges?

Survey Responses	%
Shadow IT - apps being used but not under IT management	15.90%
Lack of security training for all employees	15.61%
Lack of security policies and controls	13.58%
No monitoring solution specifically looking for data and security breaches	13.29%
Lack of adequate encryption	10.12%
Data protection and recovery from loss	8.96%
Mission critical applications running on legacy hardware	8.67%
Mission critical applications not running latest version or patched	7.23%
Firewall and Protection platforms out of date	4.91%
Other	1.73%

When it comes to facilitating innovation, having a solid IT management strategy is essential. Today, IT infrastructure is the foundation upon which a company can continue to transform products and services, accelerate operations, and empower users to do more with less. But there are a number of risks that can also slow down or halt any progress if not properly mitigated:

Shadow IT

Shadow IT may not be a problem within the individual workloads of Office 365 and the Microsoft Office family of productivity tools, but the use of unauthorized third-party tools and cloud-based services is a problem within most organizations, regardless of company size or industry because they often circumvent security and compliance protocols.

Rapidly changing standards

Security and compliance are rapidly evolving areas within the collaboration technology sector. However, many organizations have become overly reliant on the tools and platforms they use, assuming they will provide the right levels of security and compliance coverage. Unfortunately, it is far too common that companies do not take action on gaps in coverage until a security breach has taken place, or under the threat of fines due to non-compliance.

Pace of change of innovation

The rate at which new technologies are made available through the cloud can be staggering. How you manage your collaboration platform — from engineering activities, to risk management and compliance audits, to the overall change management and IT

ticket prioritization — is essential to managing this pace of change. Transparency is often missing. People don't like to be left in the dark. Share what is happening within the platform so that people have a clear understanding of what works and what doesn't and share their feedback and experiences.

Internal and external threats

Every organization maintains trade secrets and other sensitive information that, if compromised, could cause them to lose their competitive advantage or even cease to operate. Regardless of the technology platform used, it is critical that companies can trust that it will not leak out sensitive information – whether internally by managing access and permissions controls or configuring solutions to reduce external threats by preventing unauthorized release of sensitive information.

Failure of strategy and/or ability to execute

Finally, one of the greatest risks to modern IT is inaction. Rarely is this intentional, but unfortunately it can be fairly common as organizations become overly reliant on the out-of-the-box security and compliance capabilities of the platforms and services they use without fully understanding the gaps within their own unique business requirements. Taking the time to properly plan, or to properly execute on a plan, can be viewed as time-consuming or costly – and then skipped over.

The tools you deploy should enable you to improve upon key business processes. Your platform should enable quicker, more detailed collaboration between co-workers, partners, and customers, allowing you to do more, and do it better and more accurately. This also goes back to end user adoption — the better and more clearly you can align how your platform works to how your business works, the happier your employees will be. Good collaboration streamlines business, through things like workflow and process automation, forms and wizards to walk you step-by-step through data entry and by putting social activities at the center of everything you do, so that your content has better context, and is more searchable, more findable.

However, good collaboration should not come at the expense of secure, compliant, and well-governed solutions. There needs to be a balance to claim operational success.

Designing Operational Success

Your collaboration platform is the hub for workplace productivity. It is where your information workers connect, share, and get work done. While the leading tools and services enable you to quickly launch and add users, your long-term success requires more thoughtful steps and business alignment. Planning is the key to success — and having a strategy for each of the potential risks outlined in the previous section will ensure that your collaboration environment meets or exceeds your end user expectations and will continue to support your growing needs.

Proper planning is also essential because Office 365 is continually evolving, as well. With customers around the world with many different standards and regulations guiding them, Microsoft is constantly reviewing how their platform handles your information assets, adding to the list of compliance and security standards supported while at the same time expanding their data center footprint to reach customers in under-served areas of the world. While Microsoft's efforts should inform your organizational security and compliance planning, your overall strategy should include a more holistic and comprehensive review of industry research and trends, expert guidance, and your own internal experiences.

Focus Areas for Successful Office 365 Management

Organizations that are considering moving to the cloud entirely or using a hybrid model need to understand the differences between reporting, compliance, and governance capabilities within their existing on-premises and online tools and platforms and set expectations about what can be managed out-of-the-box – and where third-party solutions will need to be utilized.

Much of the administration experience inside of Office 365 streamlines and automates tasks that you previously had granular control over within the individual on-premises workloads. From an auditing and compliance perspective, this means you need to understand:

1. Your organizational requirements, standards, and policies.
2. What capabilities are possible within each of your hybrid components, from discovery through technical enforcement.
3. What can be managed centrally versus within each individual system or component, and by whom.

Whether your environment is on-premises, in the cloud, or in a temporary or permanent hybrid state, it is critical that organizations clearly understand their security and compliance requirements, and whether these requirements are being met. All planning should begin with a detailed, step-by-step review of security and compliance policies and procedures, mapping out how each of them is currently accomplished. As organizations consider moving to the cloud, they should use this baseline to understand how each will be accomplished within the future environment, and how current metrics and key performance indicators (KPIs) will be updated.

Security

The topic of cyber-security has become more visible in the past several years due to major breaches that have compromised the personal identity of millions of customers. Most organizations gather information about who they do business with, such as banks with credit card applications or software companies with customer logins and passwords, which requires that every company be vigilant in their security measures. Companies have an ethical obligation to safeguard their customers personal information.

What Microsoft provides

Microsoft Office 365 handles both trade secrets and other sensitive information, and it is critical that companies wanting to benefit from the platform can trust that it will not leak out sensitive information. You can find an overview of the Office 365 Security and Compliance Center at https://docs.microsoft.com/en-us/office365/securitycompliance/

Additionally, Microsoft provides additional security guidance for several leading sectors:

- Public Sector details can be found at http://bit.ly/O365_PublicSector, including links to the Office 365 US Government service plan, and plans for Germany, China (21Vianet), and other Public Sector options.
- Education Sector details can be found within the service plan details at http://bit.ly/O365_EDU.
- Financial Services Sector details can be found within the Microsoft Trust Center overview at https://www.microsoft.com/en-us/trustcenter/cloudservices/financialservices
- Healthcare Sector details can also be found within the Microsoft Trust Center overview at https://www.microsoft.com/en-us/trustcenter/cloudservices/health

Potential gaps that organizations should plan for

According to our recent research, two areas that organizations need to supplement to ensure that their unique security requirements are being met include:

1. Monitoring solutions that actively look for security breaches
2. Data protection and recovery from loss and lack of adequate encryption

Compliance

Commercial organizations have regulations and policies that they must comply with to operate businesses in various industries. These policies can be a mix of external regulatory requirements that vary depending on industry and geographical location of the organization and internal company-based policies.

Office 365 provides built-in capabilities and customer controls to help customers meet both various industry regulations and internal compliance requirements, staying up-to-date with many of today's ever-evolving standards and regulations, giving customers greater confidence.

What Microsoft provides

Microsoft undergoes third-party audits by internationally recognized auditors as an independent validation that they comply with all policies and procedures for security, compliance and privacy. Office 365 utilizes a control framework that employs a strategic approach of implementing extensive standard controls that in turn satisfy various industry regulations. Office 365 supports over 900 controls that enable Microsoft to meet complex standards and offer contracts to customers in regulated industries or geographies, like ISO 27001, the EU Model Clauses, HIPAA Business Associate Agreements, FISMA/FedRAMP.

Where Microsoft is putting most of their resources is in expanding the Office 365 Security and Compliance Center (https://protection.office.com/ requires Office 365 login), which is your primary portal for protecting data within Office 365, and for managing all of your auditing and compliance requirements.

Potential gaps that organizations should plan for

According to our recent research, the top three most widely cited compliance challenges identified by the survey respondents include:

1. End users don't classify data correctly and/or take required actions (38%)
2. Content stored in legacy content systems (35%)
3. Content spread across multiple workloads (34%)

Governance

Good collaboration is definitely a cultural skill. The organizations who are best at collaboration are often those with mature cultures that have clearly defined governance and change management models that facilitate understanding and execution. Governance can be viewed as an umbrella term to describe multiple areas it involves such as data governance, IT governance, information governance, etc. Furthermore, governance has a range of definitions based on which sector it is describing such as the public, financial, and healthcare sectors.

The first step to building a healthy governance strategy is always to sit down and discuss various organizational requirements and differences between teams and come to a shared understanding — before any solution is proposed.

What Microsoft provides

Microsoft's approach to governance in Office 365 has been to invest in two primary areas: the Administration Console, and in expanded documentation through https://docs.microsoft.com/en-us/office365/admin/admin-overview/

Governance is a broad topic, and for many years the partner community – ISVs (independent software vendors), SIs (strategic integrators, or consulting companies), and the MVP community – have provided content, tools, and expertise to help manage any and all gaps within the platform. However, Microsoft has stepped up their game in this

area, investing heavily in the overall management experience of the platform, as well as the documentation in support of the features and tools that they bring to market.

Potential gaps that organizations should plan for

In our recent research, when asked whether their organizations are generally good at managing governance activities across the various Office 365 workloads, the majority of respondents felt they were "Average," "Good" or "Excellent." However, based on the collective responses to the more granular questions about specific governance activities within each workload, the confidence level of respondents was not so high.

Table 2 - State of overall governance readiness

Answer	%
Very poor	2.33%
Poor	30.23%
Average	30.23%
Good	27.91%
Excellent	9.30%

One of the difficult lessons for many organizations, as with most user-driven technologies, is that technology is often unleashed without proper planning or governance processes in place. As a result, many administrators find themselves in reactionary modes and having to quickly research and retroactively apply standards across their environment. Even the most proactive, process-oriented organizations struggle from time to time with managing governance across rapidly deployed collaboration platforms and services, many of which are being acquired and deployed without the prior knowledge or oversight of the IT team.

A good governance strategy will outline the ways in which you intend to uphold policy and ensure your platform is performing optimally. Healthy governance is essential to any successful platform. A strong governance strategy can have a direct impact on end user adoption and productivity, the level of management support received for current and future IT initiatives, and your ability to see measurable business value.

Governance should be a priority no matter what tools or platform you deploy, but certainly should be at the forefront of any decisions to roll out companywide social tools. The recommendation is to begin by clarifying and documenting your permissions, information architecture, templates, content types, taxonomy within each workload—and ownership of each—and then map those requirements to your platform roadmap. Define what policies, procedures, and metrics are necessary to manage your entire environment, and then look at what is possible across your many different tools and platforms.

Implementation Action Plan

There is no tool or platform in the world that will address every possible security, compliance, and governance requirement or scenario. The key to operational success is to properly plan and regularly review your assumptions and strategies, and to incorporate end user feedback into the process. In our most recent research, we asked respondents to share the factors that influenced their success, and provide these key takeaways as a checklist for your operational planning efforts:

Planning	
Have a holistic approach	Organizations should look at Office 365 as an integrated business solution rather than through functional silos or individual workloads. Review the end-to-end experience as well as individual workloads within your existing or future governance oversight committee meetings, as the review and management of security and compliance issues will likely comprise a large portion of your ongoing operational activities. Develop metrics for each workload that will be meaningful at the company-level, as well as the business unit or team-level and provide deeper insights into how different user groups are adhering to company security and compliance standards.
Prepare for changing information needs	There's a reason why agile development is becoming so pervasive — the rate at which our business needs change is increasing. A key to keeping people engaged is to ensure that the right data is available and in a timely manner. This is another great example of where regularly talking with your employees or end users will impact how they view and participate within your collaboration platform. No matter how well you document the requirements of your system, end user needs will change.
Manage organizational and cultural differences	We live in a "fix it" culture where problems surface, and we immediately want to run to them and solve them. But sometimes the best way to solve a problem is to allow the participants to find their own path. And if people understand that there is a method (or process) for resolving their differences, they are less likely to use a policy disagreement as a reason to disengage.

Inventory Assessment / Audit	
Conduct a detailed self-assessment.	Regularly conduct a detailed assessment of your systems and tools, information architecture, and business goals to better understand what is in place today, how it maps across to the Office 365 tools and capabilities, and where there may be gaps. With this baseline in place, you will be able to properly plan for future system and tool deployments and business requests.

Identify feature gaps and create an operational strategy	By regularly auditing your systems and identifying needs gaps, you allow IT Managers and other key business stakeholders to understand the features and limitations of each workload within Office 365 (For example, OneDrive can only restore deleted files for 93 days[2]) and more transparently manage employee expectations.
Expand your information architecture	Technology is changing so rapidly, the information architecture designed for your earlier SharePoint deployment is likely out of date and should be updated to reflect the growing usage of other workloads, such as Teams, Yammer, OneDrive, and others. Whether or not your organization uses a formal intranet, understanding where your information assets sit and how to access them is essential.
Conduct scheduled inventory audits	Cleaning up content and verifying classifications will strengthen your overall information architecture (IA), improving search results while also ensuring that content lifecycles are compliant. Setting security and compliance policies is difficult when managers and employees do not know the state and disposition of their information assets. Audits provide visibility, and present opportunities to re-evaluate the priority of information assets, as well as to make policies and procedures around the content lifecycle clear to everyone.

Training	
Invest in training and adoption	Do not assume that the initial training conducted when Office 365 was initially rolled out will be sufficient for long-term success. Provide a blend of self-help and ongoing productivity training for all employees, and leverage some of the "Customer Success" best-practices provided through Microsoft and the expert community to look for ways to continually inspire and encourage end users to collaborate and stay engaged.
Create a training plan to better disseminate policies and procedures	Training should not happen one-time (usually at launch). Make awareness of security and compliance standards part of a mandatory education plan. Training plans that incorporate multiple tools and distribution methods are always more effective than simply providing a digital training PDF or posting a single training video to the company intranet. Organizations should take the time to create training assets that match the learning culture within the organization, providing self-help tools (videos, content, internal quizzes) and both formal and informal sessions (classroom, brown bags, ask me anything (AMA) discussions) to reach the broadest audience.

[2] https://support.office.com/en-us/article/restore-deleted-files-or-folders-in-onedrive-949ada80-0026-4db3-a953-c99083e6a84f

Treat people like adults	Depending on the culture of your organization, this may not be an issue, but it's worth pointing out that people feeling like they are not taken seriously or are being marginalized is often a sign of micro-management. The best-run collaborative platforms are the results of clear rules and guidelines and then getting out of the way to let people work. Effective managers are clear on what needs to be accomplished, but do not dictate *how* people accomplish their work.

Governance and Change Management	
Create (or improve / extend) your governance committee	The overall governance of your Office 365 environment has less to do with the technology and more to do with the practices and procedures you put in place to administrate your information assets. One of the essential steps to successful Office 365 governance is the creation of an oversight committee, tasked with the ongoing operational review of the platform as it is planned, deployed, extended, and supported. The goal of this team is to regularly review the state of operations, monitor changing business needs and evolving technology capabilities, ensure that information architecture, security and regulatory requirements are being met, and to track end user adoption and engagement.
Keep pace with change	Supporting transparency and holding the organization accountable is especially critical as the pace of the Office 365 change release process is incredibly fast (including monthly and weekly builds), and organizations can easily miss key improvements or new features if they fail to stay on top of these releases.
Incorporate change management into your culture	An effective change management process is the key to transparency and should be led by your IT organization or Project Management Organization (PMO) to provide a formal front-door process for business and feature requests, to provide issue tracking and status updates, and to work with end users and management alike to ensure that what is delivered meets expectations.
Provide transparency	People do not work well in an information vacuum. Take away transparency and people will go around you to try and solve their issues on their own. It's amazing how quickly a planned and articulated communication strategy can affect how people react to the state of a project. The more you involve people in the process, the more likely they are to support that process and stay engaged.
Stay on schedule	Communicate your schedule for delivery of new features, new content, lifecycle or permissions changes, and similar activities to ensure you are meeting your end user expectations. If your communication channels are open and people feel confident in their ability to voice opinions, you may be more capable of handling any schedule slips — but your goal should always be to hit that delivery schedule.

Innovation	
Better leverage the latest technology	Microsoft tries to provide business guidance and user scenarios for all new features and capabilities, documenting administrator and end user guidance to help customers quickly adopt. Organizations should constantly pilot these new capabilities, creating an environment where new features are quickly tested and deployed. Companies that can successfully adapt and adopt will have a distinct competitive advantage over those who fail to keep up. This is especially true with security and compliance features, which can have an immediate financial impact through risk reduction.
Pay attention to industry trends	As with the changing information needs for your end users, it is important that you are aware of industry trends and innovations that may evolve or disrupt your platforms. A great example has been the disruption of traditional enterprise content management (ECM) platforms by social collaboration tools. Be aware of improvements to your key workloads and stay ahead of your end users by testing out new solutions. If your team recognizes that you are constantly evaluating new technologies, looking for ways to improve and to stay on top of industry trends and best practices, they will be less likely to let their attention wander.
Focus on business outcomes, not technology	Be careful to balance your use of metrics with end user feedback, working collaboratively to improve employee experiences. Taking the time to understand the root cause of issues and focus on outcomes rather than the process of getting there (and nitpicking the mistakes made along the way) often proves to employees that you are making an effort to do the right thing, encouraging them to provide more information and helping to solve problems faster and, ultimately, helping to build trust within your collaboration platform.

Summary

Once you have the ability to view and understand your operational indicators, and to generate scenarios and contingency plans based on these strategies, you will be positioned to efficiently and effectively plan for obsolescence, as well as develop new product and feature strategies – and unlock unrealized revenue that had otherwise been lost within the shuffle of deficient lifecycle planning.

Much like an organization's operational excellence strategy, we as individuals need to be constantly looking for ways to improve our own roles. Change is a fact of life — and one of three constants in life (along with taxes and death). To succeed in collaboration overall and to help end users stay engaged and productive, you will need to establish healthy habits and best practices.

The fundamental role of management is to watch for and mitigate risks — and yet the level of engagement of end users is rarely a risk mentioned in most organizational planning sessions. Engagement should be one of your primary organizational metrics. Clearly defined governance and consistent communications are at the core of end user engagement issues. If you're experiencing serious issues with end user engagement, the first step is always to get a clear picture of where things are today — and be honest about what you see. Only with awareness can you begin to take the right steps forward and build out healthy collaboration practices within your organization.

The result of changing your operational activities toward a productivity focus means a higher return on investment (ROI) for the platform overall, because it will have a direct impact on platform usage. And when more people are using the platform, your company will get more out of the platform. You'll see these benefits through faster employee on-boarding and training, more business output and stronger platform usage — all of which means a faster realization of the financial investments you've already made in the Microsoft stack. But remember that there is no end to your operational focus. Your business is constantly changing, the technology is constantly changing, and your end user needs are also constantly changing.

About the Author

Christian Buckley is a Microsoft Regional Director and Office Apps & Services MVP, and the Founder & CEO of CollabTalk LLC, an independent research and technical marketing services firm. You can find him online at www.buckleyplanet.com and @buckleyplanet

About Spanning

Spanning Cloud Apps, a Kaseya company, is the leading provider of backup and recovery for SaaS applications, helping organizations around the globe protect their information in the cloud. The company provides powerful, enterprise-class data protection for Microsoft Office 365, G Suite, and Salesforce. With data centers located in North America, the EU, and Australia, Spanning Backup is the most trusted cloud-to-cloud backup solution for thousands of companies and millions of users around the world. Learn more at www.spanning.com. Follow Spanning on Twitter @spanningbackup.

www.Spanning.com