Organizational Security & Compliance Practices in Office 365

Research conducted by CollabTalk LLC
and the BYU Marriott School

Commissioned by Spanning, RecordPoint,
tyGraph, Rencore, and Microsoft

SPANNING

RecordPoint

tyGraph

Rencore

Microsoft

CollabTalk

Table of Contents

ABOUT COLLABTALK

CollabTalk LLC is an independent research and technical marketing services company, founded with the goal of empowering customers to create and manage effective and engaging content and marketing strategies. CollabTalk focuses on tools and trends in the enterprise collaboration, social, and business intelligence ecosystems, and provides community-driven events, original research, and thought-leadership content.
For more information, visit https://collabtalk.com.

Introduction

The number one area of concern identified by customers as they began planning for their move to the cloud is security and compliance. Cloud security and compliance is an increasingly important topic for all industries as increasing cost efficiencies drive organizations towards the cloud. "End-user spending for the information security market is estimated to grow at a compound annual growth rate of 8.5% from 2017 through 2022 to reach $170 billion in constant currency."1

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 relied on the on-premises versions of Exchange, SharePoint, OneDrive, and Skype, and are now deciding whether to adopt them as online services via the Office 365 platform. 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.

This research focuses on how organizations have evolved (or not evolved) their governance planning and activities as they've moved from on-premises environments to the cloud (primarily Office 365), and seeks to provide CIOs, IT management, and security and compliance officers with a better understanding of the impacts of not evolving.

Methodology

For this research project, CollabTalk partnered with the Marriott School of Business at Brigham Young University to conduct primary research that included surveys, interviews with customers, partners and Microsoft Most Valuable Professionals (MVP's), and secondary research of academic and industry research and content to answer key questions surrounding the level of governance awareness and readiness from a cross-section of Office 365 customers around the world.

The goal of this research is to examine how organizations are managing security and compliance today, looking specifically at the evolving patterns of end user and team collaboration, and identifying the changing workplace habits that are impacting costs and risks due to security and compliance gaps in the business processes and technologies used. While the primary focus of this research will be on SharePoint customers, which is where most governance activities are generally managed, the research will look at the broader enterprise collaboration story, encompassing Office 365, Windows, and mobility.

Some of the questions we plan to address:

- How do IT organizations assess and tackle security and compliance problems?
- What is the "business view" of security and compliance?
- How do viewpoints of security and compliance change between industries?
- What are the common workplace scenarios that are undergoing change, and what is the cost/impact of these changes (or lack of change)?
- How much is the work that we do changing due to these standards?
- What industry trends are important to consider?
- Where does security and compliance with Office 365 need to be improved?

Overall, our findings reveal that security and compliance is a topic that is highly misunderstood. Most organizations believe that security is an area of continuous improvement but see compliance as adherence

[1] https://www.gartner.com/doc/3883783/forecast-information-security-worldwide-

to standardized laws. Both security and compliance are aspects of corporate risk management, and security is more prioritized because the effects of security failings are costlier than the effects of compliance failings.

Demographics

In order to answer key questions, the research team conducted a detailed survey with IT professionals, c-level executives, and compliance officers globally. The data represents 195 responses across 19 industries. Additionally, pulse surveys were conducted in APAC and the EU, asking fewer but more granular questions about their security and compliance activities and confidence in Office 365 capabilities, providing the research team with another 76 responses and additional perspectives. The companies represented range from under 50 employees to more than 10,000 employees, running environments that range from legacy hardware to cloud and hybrid.

Respondents were surveyed as representing their own companies, or for consultants, their current clients rather than an aggregate of past clients. The following figures are provided as a demographic overview of the survey respondents:

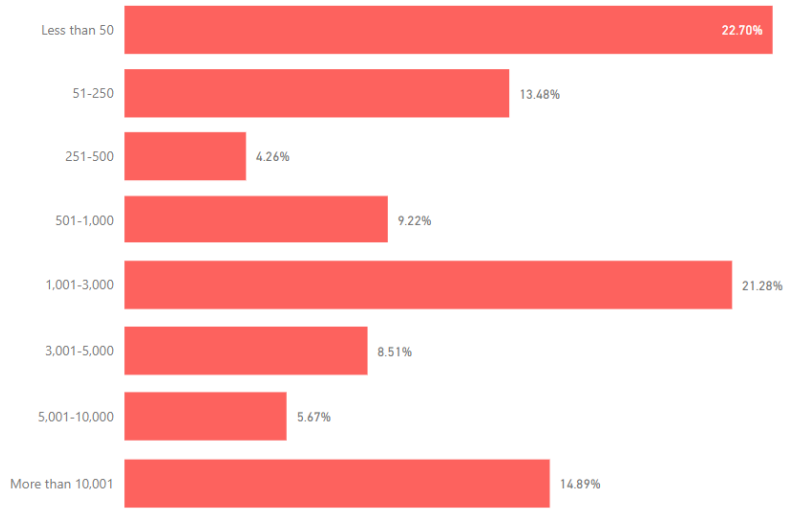


Figure 1 - Company size of survey respondents

The global cloud security market size was valued at USD 4.88 billion in 2016. It is expected to rise at a compound annual growth rate (CAGR) of 13.9 percent until 2024. Cloud computing security, also known as cloud security, incorporates all plans, policies, and their execution controls essential to safeguard and protect application data, infrastructure as well as compliance adherence associated with cloud. (Research, n.d.)

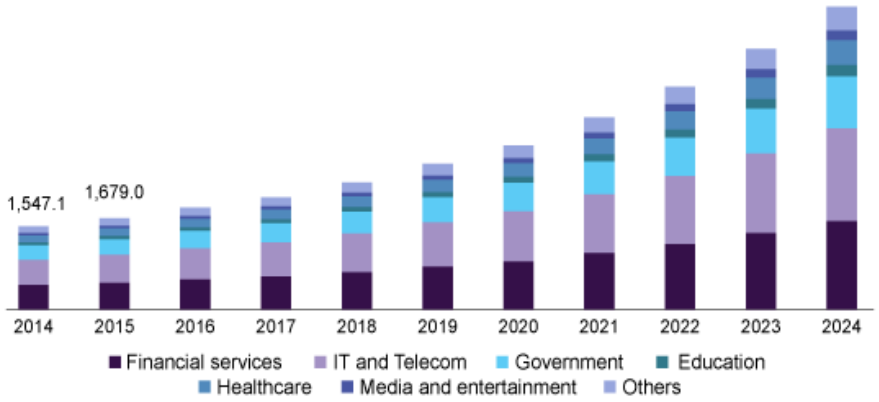


Figure 2 - US cloud security market size, by application, 2014-2024 (USD Million)

IT and Telecom and Financial Services are the two largest application segments in the market. They are likely to remain prominent throughout the forecast period. There is expected to be an exponential increase in spending on cloud services across industries. From a report, it is expected to reach $160 billion by the end of 2018, an increase of 23.2 percent from 2017 and reach $227 billion by 2021. (Zola, n.d.)

Survey respondents came from a variety of industries, although "Technology" is a broad category that consists of Information Technology and services, consulting, and cloud-based solutions and providers.

Table 1 - Industries represented by survey respondents

Answer	%
Healthcare	2.74%
Finance or Insurance	6.16%
Public Sector or Government	29.45%
Resource Industries (Oil & Gas, Mining, Utilities)	6.85%
Education	6.16%
Entertainment and Recreation	0.68%
Manufacturing	2.74%
Technology	26.71%
Retail	1.37%
NGO	2.74%
Services	6.16%
Non-profit	2.74%
Other	5.48%

Rather than ask survey respondents to identify the versions of platforms and tools used, since the primary scope for this research was Office 365, we asked respondents to identify the state of their move to the cloud, providing more granularity to their responses, as shown in Table 2 - *Environments in use from survey respondents* below. Based on this, the top three environments identified by respondents were:

1. Hybrid solutions (combination of Office 365 and on-prem components) (22.99%)
2. Other public cloud solutions such as Box, Dropbox, G Suite (17.24%)
3. Cloud-based CRM such as Salesforce, Microsoft Dynamics Online (14.18%)

What this helps illustrate is that customers that maintain a single OEM vendor relationship (for example, only using the Microsoft technology stack) are no longer typical. Furthermore, the majority of environments are currently leveraging or are planning to move to hybrid scenarios[2]. Due to multi-vendor and hybrid complexity, organizations need to understand their security and compliance requirements beyond the out-of-the-box capabilities supported by individual workloads.

On the topic of multi-vendor usage, some of our research advisory panel were surprised by some of the data points. For example, Jussi Roine (@JussiRoine), Chief Research Officer at Sulava Oy in Helsinki, Finland and a Microsoft Regional Director and MVP commented:

> *"Very surprised to see "other public cloud solutions such as Box, Dropbox, G Suite" so high. It's expected but still, it's surprising especially for companies that are already using Office 365."*

Less surprising, however, was the hybrid data. As stated by Eric Overfield (@EricOverfield), President of PixelMill in Davis, California, and a Microsoft Regional Director and MVP:

> *"On-prem is not going anywhere soon, over 60% are utilizing hybrid solutions."*

Table 2 - Environments in use from survey respondents

Answer	%
On-premises Microsoft solutions only	6.13%
Office 365 only	9.20%
Hybrid solutions (combination of Office 365 and on-prem components)	22.99%
Other dedicated cloud solutions, such as Rackspace or other private hosters	13.41%
Other public cloud solutions such as Box, Dropbox, G Suite	17.24%
Legacy Enterprise Content Management platforms such as Documentum, FileNet, HP TRIM	11.11%
Microsoft Cloud for Government for U.S. Federal, State, and Local Government	2.68%
Cloud-based CRM such as Salesforce, Microsoft Dynamics Online	14.18%
Other	3.07%

As *Table 3* shows, the vast majority of survey respondents are using the Office 365 Enterprise (E Plans) licensing, which is where Microsoft and partners have been directing customers as they provide the most comprehensive set of features and solutions.

[2] CollabTalk, 2017. "Understanding the State of Hybrid SharePoint Ecosystem"

Table 3 - Office 365 licensing from survey respondents

Answer	%
Office 365 Small Business (P Plans)	4.71%
Office 365 Midsize Business (M Plans)	3.53%
Office 365 Enterprise (E Plans)	78.82%
Office 365 Kiosk (K Plans)	7.06%
Other	5.88%

With our focus on security and compliance, it was expected that a sizeable percentage of respondents would consist of compliance and records management personnel (24%), executives (13%) and senior managers (11%), and consultants (11%), together comprising two-thirds of all respondents and interview participants.

Table 4 - Roles of survey respondents

Answer	%
Senior Leadership/Executive	13.33%
Director/Senior Manager	11.33%
IT Manager	9.33%
Compliance Officer / Legal / Records Manager	24.00%
Team Lead	8.00%
Engineer/Developer	3.33%
Project/Product Manager	6.67%
Consultant	11.33%
Information Worker	7.33%
Other	5.33%

Commenting on the role of upper management, Nicki Borell (@NickiBorell), a Microsoft Regional Director and MVP, and co-founder of Experts Inside commented:

> Security and Compliance topics are still not under the focus of top-level management. They know about it, and they know they should take care of it, but they don't really engage in it. The solution is to be honest, show upper management the data breach examples, and talk about the story behind these topics.

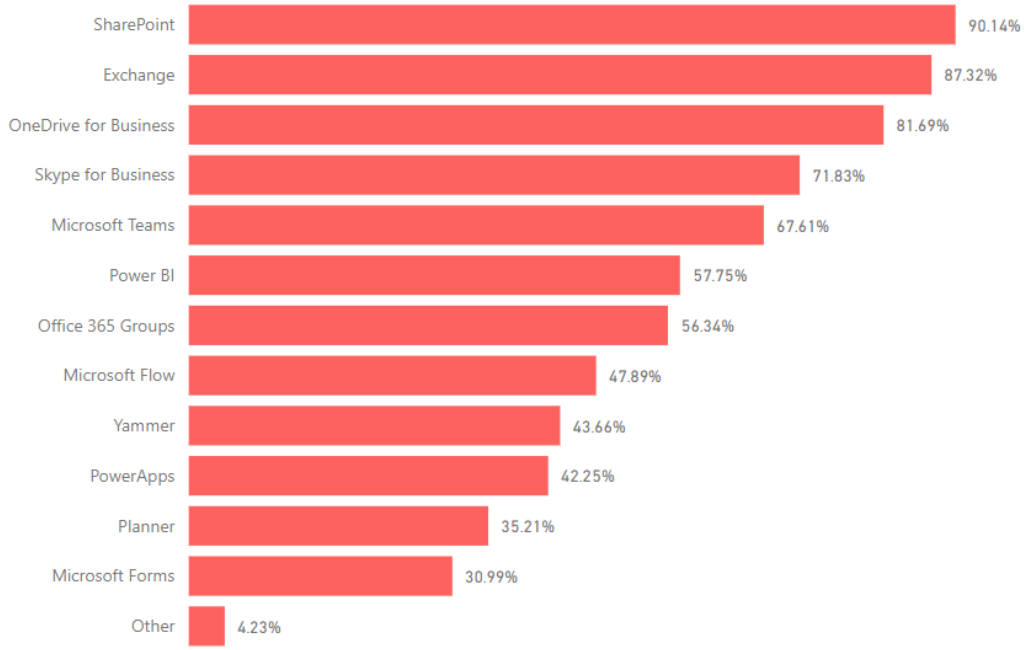
Another interesting data pivot point is shown in Figure 3, which allowed the research team to explore survey responses based on primary workload, as well as by role, company size, and other demographic details. Where this comes into play later within this research is around confidence levels in specific Office 365 security and compliance capabilities, and whether these workloads are perceived as “high” or “low”

risk against organizational requirements. Several of the research advisory panel were surprised by some of the responses within our sample size.

For example, Antonio Maio (@AntonioMaio2), a Microsoft MVP and an Associate Director & Senior Enterprise Architect at Protiviti, shared his feedback:

> *"This result is surprising, because when looking at moving into the Microsoft Cloud from a SaaS perspective, from our experience the general approach that most organizations follow is to migrate Exchange first, then OneDrive for Business and then SharePoint. Exchange and OneDrive for Business tend to migrate first because you are typically migrating a person's mailboxes or a person's dedicated network file share. The fact that those entities are tied to a person tends to make the migration process simpler to plan and execute, and organizations don't tend to take the opportunity to re-organize or clean those up the way they do with SharePoint sites. As a result, as organizations make their journey to the cloud, we tend to see most already have Exchange and/or OneDrive for Business, as opposed to SharePoint."*

Figure 3 - Which Microsoft workloads are currently used within your organization?



Less surprised about the high number of responses for Microsoft Teams was Jussi Roine:

> *"Teams is fast closing in on SharePoint. People might not realize O365 Groups is partially the same category. Planner remains a niche, but it would be interesting to ask how many respondents use Project Online with Planner – which seems to be growing."*

Insights and Definitions

Throughout our research, one theme was consistently expressed by respondents as well as our advisory panel: Security and Compliance should not be the sole responsibility of IT, as summarized in comments made by Antonio Maio:

> *"We see a lot of conversations happening about data security and compliance at the C-suite and board level these days. It has become a priority for executives in many organizations to evaluate and improve the security posture and regulatory compliance controls of their companies. I believe this is in part the reason why we have compliance officers and senior leadership factoring so highly in this survey.*
>
> *"This is driven in part by the constant data breaches we see at many major enterprises, and leadership's desire to protect their business reputation. This is also driven by new regulations that are designed to protect personal data for the individual, such as the General Data Protection Regulation (GDPR) out of the EU and the California Consumer Privacy Act or 2018 (AB 275), with their wide-ranging mandates and extreme fines.*
>
> *"We also see circumstances where IT managers or IT team members have a very good sense for the organization's security exposures, but they have a difficult time starting a conversation with their internal legal or compliance departments. From the point of view of raising the conversations about security and compliance within organizations, the fact that so many in a leadership or compliance position are responding to this type of survey is a positive result."*

Security and compliance are rapidly evolving areas within the collaboration technology sector. Many organizations are overly reliant on the tools and platforms they use to provide the right security and compliance coverage. Unfortunately, it is far too common that companies do not do more in these areas until there has been a security breach, or under the threat of fines due to non-compliance. For example, organizations that do business in or with customers in the European Union scrambled to understand and prepare for the General Data Protection Regulation (GDPR) which went into effect in May 2018, rather than proactively create data management policies and procedures to meet these and future industry and governmental changes.

The Office 365 platform supports customers around the world with many different standards and regulations guiding the handling of information assets. As such, Microsoft is constantly 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, a more holistic and comprehensive review of industry research and trends, expert guidance, and your own internal experience.

Industry Perspectives

As mentioned, it can be important to understand and periodically review major trends and issues within your own and parallel industries. As part of our secondary research, we looked at the topics of security and compliance in several of the leading industries to identify definitions and trends that span all industries, as well as any factors that were unique to a single industry.

We've highlighted some of this research within four key sectors: Public (Federal, State and Local Government), Education, Financial Services, and Healthcare.

Public Sector

In one presentation given to public sector leaders, compliance was defined as:

> *"the process of ensuring and proving that policies (internal and external) are being followed." (Governance, Risk & Compliance for Public Sector, n.d.)*

A secondary definition that clarifies the most important laws to follow is provided below:

> *"For U.S. Federal agencies, the major security and privacy compliance concerns include the Clinger-Cohen Act of 1996, the Office of Management and Budget (OMB) Circular No. A-130, particularly Appendix III, the Privacy Act of 1974, the E-Government Act of 2002 and its accompanying OMB guidance, and the Federal Information Security Management Act (FISMA) of 2002.11 Also of importance are National Archives and Records Administration (NARA) statutes, including the Federal Records Act (44 U.S.C. Chapters 21, 29, 31, 33) and NARA regulations (Title 36 of the Code of Federal Regulations, Chapter XII, Subchapter B)." (Jansen, 2011)*

From this information, we can infer that the public sector focuses strictly on compliance to specific and extensive regulation, and that the internal processes are not focused on as much as in the Financial Sector.

In our survey, we generally found that members of this industry noticed less clear ownership of security and compliance, focusing more on product lifecycle, and a much higher spread in security and compliance confidence levels between products.

- Specific compliance threats that are larger for this industry than with other industries: Content lifecycle (e.g. all content is retained forever)
- Specific security threats that are larger for this industry than with other industries: No monitoring solution specifically looking for security breaches
- An overview of the Office 365 Security and Compliance Center can be found at https://docs.microsoft.com/en-us/office365/securitycompliance/
- Additional Office 365 security and compliance guidance for the Public Sector can be found at http://bit.ly/O365_PublicSector, which includes links to the Office 365 US Government service plan and plans for Germany, China (21Vianet), and other Public Sector options.

Education Sector

The education industry views compliance very similarly to the public sector. Although there is no definition specific to the industry, the following passage helps to understand the viewpoint of the industry:

> *"In addition to the usual security concerns for any enterprise, educational institutions, by virtue of their diverse operations, are subject to numerous compliance regimes, and when it comes to compliance, universities are well aware that you can outsource responsibility, but you can't outsource accountability." (Sasikala, 2010)*

In addition to this viewpoint, a comprehensive list of other laws and regulations can be found at www.higheredcompliance.com

Compliance in the education sector, similarly to the public sector, is concerned with strict adherence to a large amount of regulations without proactive investments.

In our survey, we generally found that members of this industry noticed security ownership completely by IT departments and about average compliance and security confidence scores.

- Specific compliance threats that are larger for this industry than with other industries: Content lifecycle (e.g. all content is retained forever)
- Specific security threats that are larger for this industry than with other industries: Lack of adequate encryption
- Additional Office 365 security and compliance guidance for the Education Sector can be found within the service plan details at http://bit.ly/O365_EDU.

Financial Services Sector

The financial industry is the most concerned with remaining compliant out of the industries researched here. For the financial services industry, compliance is a proactive endeavor, as described by worldfinance.com

> *"Regulation in the financial services sector will continue to pose a challenge to firms both large and small. Compliance is not just about recognizing the key regulatory pressures facing financial institutions, but also proactively ensuring the company is improving its processes and streamlining its operations. As the challenges around compliance continue to put pressure on firms, finding new solutions and methods will be vital." (World Finance, n.d.)*

For the financial industry more than any others, the focus is on reducing cost and streamlining the internal processes that lead to compliance. Another definition of compliance is given by the International Compliance Association below:

> *"In the context of financial services, businesses compliance operates at two levels. Level 1 - compliance with the external rules that are imposed upon an organization as a whole. Level 2 - compliance with internal systems of control that are imposed to achieve compliance with the externally imposed rules." (International Compliance Association, n.d.)*

Compliance in the Financial Services industry is also meant to preserve reputation. "Protect against loss of reputation" is in the top five priorities for banks in the financial services industry (MetricStream, 2014). Most of this work tends to show in "Level 2" of the definition above, in increasing efficiency of internal processes to more effectively achieve compliance with external rules.

In our survey, we generally found that members of this industry were less familiar (most people not familiar at all) with general trends in security and compliance. Ownership of these problems is at CXO level and CXO's do tend to be somewhat familiar with trends. Security and compliance confidence scores, however, are mostly low.

- Specific compliance threats that are larger for this industry than with other industries: Content lifecycle (e.g. all content is retained forever)
- Specific security threats that are larger for this industry than with other industries: Data protection and recovery from loss and lack of adequate encryption
- Additional Office 365 security and compliance guidance for the Financial Services Sector can be found within the Microsoft Trust Center overview at https://www.microsoft.com/en-us/trustcenter/cloudservices/financialservices

Healthcare Sector

The Healthcare industry's typical definition of compliance is:

> *"The ongoing process of meeting, or exceeding the legal, ethical, and professional standards applicable to a particular healthcare organization or provider...Healthcare compliance covers numerous areas including, but not limited to, patient care, billing, reimbursement, managed care contracting, OSHA, Joint Commission on Accreditation of Healthcare Organizations, and HIPAA privacy and security to name a few. " (Healthcare Compliance, n.d.)*

Although Healthcare is regulated carefully, the Healthcare sector views compliance to these regulations as the extent of their security. In the Compliance Effectiveness Survey, the following conclusion was reached by the researchers:

> *"For any compliance program, a critical measure of success is its ability to prevent incidents from occurring. Determining how many events are avoided is difficult, though. Employees rarely come forward to report, 'I was about to commit a felony and then remembered that compliance training I received.'"*

This statement from an industry-standard source implies that the Healthcare industry views compliance as a type of security, and that compliance to regulation is intended to prevent "incidents", one of the goals of a security strategy.

- There are no specific security or compliance threats that are larger for this industry than with other industries.
- Additional Office 365 security and compliance guidance for the Healthcare Sector can be found within the Microsoft Trust Center overview at https://www.microsoft.com/en-us/trustcenter/cloudservices/health

The Maturity of Office 365 Security and Compliance Standards

To some organizations, moving to the cloud may seem like an unnecessary risk. Microsoft has made huge strides in educating their customers about the stability and security of the cloud, but as our research will help illustrate, there is still much work to be accomplished to help customers understand where their planning and administration efforts may be falling short.

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.

Antonio Maio shared some insights from his consulting work:

> *"We see many organizations struggle with the fact that their organizational data is spread across so many different systems and applications, making it extremely difficult to manage regulatory compliance controls across all of their data in a consistent manner. Along with the wide-spread storage of data, we see organizations struggle with data ownership – having individuals internally identified as data owners, having data owners understand their responsibilities and having data owners take that responsibility seriously. Classification is just one aspect of being able to control data, in that it helps identify the sensitivity of data. However, applying classification across all an organization's information, not just Office documents and PDFs, is a large undertaking. It requires not only users to classify their data but also systems which will automatically classify information, and whole applications to be classified if they store a particular type of data (ex. a CRM system which stores contact and account data being classified as storing sensitive customer information).*
>
> *"Generally, inventorying all the systems and applications within an organization which store information and enable collaboration on that information is an effective place to start. Regular compliance assessments and audits of those systems allows organizations to identify where security gaps exist. Consolidating systems is also a strategy used by many organizations, which then tends to precipitate migration projects to move corporate data to a single cloud environment, like Office 365. As part of a move to the cloud, it is recommended that organizations take that opportunity to improve the maturity of their governance policies and procedures, and implement effective compliance controls as part of a migration or digital transformation initiative."*

Microsoft is making tremendous investments in data security and compliance to ensure that they are compliant with local, regional and international security and compliance regulations and standards. Additionally, they are also creating tools and guidelines to help customers become or remain compliant, as well. Microsoft is investing heavily in this area, because they understand that to convince enterprise customers to give up real or perceived control of their data and environments, the company needs to be a leader in security and compliance.

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

- **Their focus on business**. Microsoft cloud's strength lies in its extensive product base. It is the most attractive solution provider for enterprise customers who already use Microsoft products and are invested (Cloud Cruiser, 2016). There are now 1.2 billion Office users and 60 million Office 365 commercial customers (CALLAHAM, 2016). Both for SMB and Enterprise customers, Microsoft Office products seem to be the foundation for business operations in modern society. In part because of this, Microsoft wants to focus on targeting businesses instead of specific industries or market segments (Carey, 2017).

- **Rapid 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) (Cloud Cruiser, 2016). Microsoft has made Azure, and other cloud services, a high priority and has gained traction with current Microsoft customers because of Azure's tight integration with existing Microsoft products (AFourTech, 2017).

- **Security as design principle.** Due to the technology shift, more and more customers are willing to move their data to the Microsoft cloud. But their major concern is the security issue. Therefore, Microsoft has invested heavily and focused on improving the security of its cloud products. Recently, according to Microsoft, cyber security has become one of their most important design principles and features because hackers are becoming more sophisticated and organized (MPN Team, 2016). Microsoft offers three levels of security, namely physical security, logical security and data security (MS Office 365, 2016). Apart from these, Office 365 also offers enterprise user and admin controls (Dianne Faigel, 2017). See a list of security features in Appendix A.

This research seeks to determine viewpoints on the governance of security and compliance for organizations in the midst of this shift from on-premises environments to the cloud, helping organizations to better understand where they are in relation to recommended security and compliance standards and best practices. It is also important to address any gaps in organizational planning, whether through the upgrading of tools and reports, modifying well-established IT and business processes, or by trying to better understand how Microsoft is evolving and where their various product and support teams are shifting their own focus – which is often a clear signal to customers and partners about how they must also prepare for change.

Security Concerns

Cyber-security has become a hot topic in recent years. IT and executive management are on high alert since the breach of Equifax compromised the personal identity of millions of US customers (Daitch, 2017), with seemingly monthly failures of systems owned by banks, online retailers, and other consumer-based product and service providers.

Cyber-security is defined as:

> "... the protection of computer systems from the theft and damage to their hardware, software or information, as well as from disruption or misdirection of the services they provide"[3]

[3] Wikipedia, https://en.wikipedia.org/wiki/Computer_security

Why is it important to protect computer systems? Many companies gather information about who they do business with, such as banks with credit card applications. If the sensitive information used to identify you gets out to the public, others could claim they are you based on possessing that information. Companies therefore have an ethical obligation to safeguard their customers personal information.

As shown in *Table 5 - What are your biggest security challenges?*, the leading cause of concern from our survey respondents is "Shadow IT" (15.9%) followed closely by "Lack of security training for all employees" (15.61%), which could be argued is a clear contributor to the problems with Shadow IT. Shadow IT is defined as:

> *"Shadow IT refers to information technology projects that are managed outside of, and without the knowledge of, the IT department. At one time Shadow IT was limited to unapproved Excel macros and boxes of software employees purchased at office supply stores. It has grown exponentially in recent years, with advisory firm CEB estimating that 40% of all IT spending at a company occurs outside the IT department. This rapid growth is partly driven by the quality of consumer applications in the cloud such as file sharing apps, social media, and collaboration tools, but it's also increasingly driven by lines of business deploying enterprise-class SaaS applications."*[4]

Shadow IT may not be a problem within the workloads of Office 365 and 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.

Companies also have information, trade secrets and other sensitive information about what they are developing, that if also compromised could cause them to lose their competitive advantage or cease to be able to operate. Office 365 handles both information types, and it is critical that companies wanting to benefit from using the platform can trust that it will not leak out sensitive information. However, it can be configured to reduce external threats by preventing unauthorized release of sensitive information.

Table 5 - What are your biggest security challenges?

Survey Responses	%
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%
Lack of adequate encryption	10.12%
No monitoring solution specifically looking for data and security breaches	13.29%
Lack of security training for all employees	15.61%
Lack of security policies and controls	13.58%
Data protection and recovery from loss	8.96%
Shadow IT - apps being used but not under IT management	15.90%
Other	1.73%

[4] SkyHigh Networks, https://www.skyhighnetworks.com/cloud-security-university/what-is-shadow-it/

As stated in the SkyHigh Networks research mentioned above, the problem of Shadow IT is much larger than the response rate in our research would indicate, encompassing several of the other categories. Our advisory panel was not surprised that Shadow IT was at the top of the respondent data.

From Jussi Roine:

> *"Very expected. Shadow IT, together with BYOD (from previous chart) is a persistent problem for organizations. This reflects with the E1/E3 license plans, that often lack the security tooling and mobile device management capabilities."*

From Microsoft MVP Joanne Klein (@JoanneCKlein), an independent SharePoint and Office 365 Consultant and owner of NexNovus Consulting based in Saskatchewan, Canada:

> *"This demonstrates to me the importance of us getting this right! Either we make the sanctioned tools the "tool of choice" for end-users or they will go elsewhere. Having clearly articulated security policy and controls in place and then training end-users is key."*

Added Antonio Maio:

> *"Shadow IT is a very significant problem for enterprises today. As we know, it's very easy for information workers to sign up for their own cloud services, such as DropBox or Box, and use that to collaborate with others both inside and outside of their organizations. As a result, this is starting to drive IT teams, security teams and compliance teams to enable more collaboration solutions which are easy-to-use and corporate approved for their information workers. They are starting to enable external sharing within SharePoint and OneDrive for Business and self-service site creation or team creation for end users. This is happening in an effort to enable the business and information workers with the tools they need or want, so that they can be productive day to day.*
>
> *"However, this also creates challenges for IT, security and compliance teams because they still have a mandate to protect and control corporate information, in part due to internal corporate policies but in many cases also due to regulatory compliance requirements.*
>
> *"We see this driving many organizations to create controls around the self-service model, so that users may still request or create their own collaboration spaces but so that IT, security and compliance teams are still informed and can control these spaces. Security training for employees is a continuing challenge as well. We see more and more organizations requiring employees to take annual information security training in order to improve how information workers manage and security the information they use every day. In addition, monitoring tools such as Microsoft Cloud App Security enable those with a security and compliance mandate to monitor for suspicious behavior, automatically enforce governance policies and use machine learning to adapt automatically to changing threat landscape."*

Eric Overfield provides some thoughts on how to address this growing problem within your own organization:

> *"Shadow IT rears its ugly head. Work with your end users, determine what it is they need, and find a way to provide them a reasonable solution within the framework of your organization's policies and procedures. Shadow IT translates to your employees have jobs to do, while the organization has yet to provide the proper tools or training to address those workloads."*

In a 2017 research conducted by CollabTalk and BYU[5], a survey was used to generate key insights into the perceived gaps in Office 365 security. Most of the responses came from small businesses (less than 50 employees) in the technology sector, many of whom identified as consultants who provided development and deployment services for their customers.

- Barely over half of the respondents use Multi-Factor-Authentication, but it was still the most commonly used product (54%). The next most used was Exchange Online Protection (46%)
- When asked how Microsoft could enhance the security of their products, 83% of respondents that commented requested more assistance in understanding and implementing Microsoft products.

This showed a few important points: only about half of the respondents were willing to pay for additional security features. Also, most of the comments pointed to a general confusion around cyber-security with Office 365 products. In other words, they did not know what was available through the platform, whether these features were all (or in part) in use, or whether the features provided exceed, met, or missed their industry and organizational requirements. This lack of education is emphasized in these additional findings from the survey:

- Of those that thought Microsoft security was sufficient, 80 percent have either not run security checks, or do not know if they have
- Of those that did not think Microsoft security was sufficient, only 29 percent have not run, or do not know if they have run, security checks
- Of those who did not think the current security protection offered by Microsoft was sufficient, 57 percent were not aware of Microsoft's cyber-security division, and 71 percent were not aware of Microsoft's overall security strategy
- Only 39 percent of respondents were aware of both Microsoft's overall security strategy and their cyber-security division (55% at least knew about the C.S. division)
- 100 percent of respondents who had experienced a security breach did not think Microsoft security was sufficient, regardless of the cause of the breach (and vice versa, 100% who did not think the security was sufficient has experienced a security breach)
- 88 percent of respondents who did not experience a security breach either do not currently run security checks or do not know if they run security checks

These results highlight a few important points: Those who are confident in the security of Office 365 products are not as careful in running security checks, while those who are skeptical are more cautious. Those who are skeptical, however, do not seem to be aware of Microsoft's cyber-security efforts. Also, every respondent that had experienced a security breach did not think Office 365 security was sufficient, even though none of the reasons indicated were attributable to Microsoft. Finally, less than half of all respondents were aware of Microsoft's overall security strategy and their cyber-security division.

These results lead us to believe that those that believe Office 365 security is sufficient are very trusting, to the point that they do not run security checks, and also that those who don't believe the security is

[5] CollabTalk, April 2018. "Understanding Microsoft Cloud Services and Security." https://rencore.com/blog/cyber-security-report-understanding-microsoft-cloud-services-and-security/

sufficient are skeptical because they have experienced data breaches. We also learned that there is a perceived gap in security from a lack of education.

Addressing Compliance Concerns

One rapidly evolving area within Office 365 is the expansion of auditing and compliance capabilities. 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 platform 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 admin 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.

Creating a unified administrative experience across on-premises and Office 365 environments is a lofty goal and will require further development and extensibility from Microsoft as well as the partner community. Microsoft is making huge investments in cloud security and compliance, with new hybrid management and security capabilities through the Microsoft Operations Management Suite, targeting three core areas:

1. Insights and Analytics
2. Automation and Control
3. Protection and Recovery

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.

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. To bolster this and to continue earning your confidence, 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.

Key aspects of built-in compliance capabilities include third-party audits that verify that Office 365 meets many key world-class industry standards and certifications. 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[6] 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.

[6] https://products.office.com/en/business/office-365-trust-center-compliance

In addition, Microsoft employs a comprehensive Data Processing Agreement to address privacy and security concerns around customer data, helping customers comply with local regulations. Read more in Microsoft's *Regulatory Compliance FAQ.*

To give customers the most control over compliance in Office 365, Microsoft provides the following:

Data Loss Prevention (DLP)

DLP is a strategy and tools to help administrators control the flow of sensitive or critical information outside of the corporate network.

DLP enables administrators to configure policies based on your organization's compliance needs to help reduce the chance that financial information, personally identifiable information (PII), or other key intellectual property data might be inadvertently released. DLP policy tips place notifications directly into your users' email in order to alert them of a potential risk prior to sending an email. These notifications can also act as an educational tool for employees on your corporate compliance policies.

eDiscovery in the Security & Compliance Center

Electronic Discovery, or eDiscovery, is the process through which electronic records are sought, searched, located, and secured with the intent of using it for legal matters.

This capability on Office 365 allows you to search for content across SharePoint Online sites, Exchange Online mailboxes, OneDrive for Business accounts, or across all of them. The Security & Compliance center allows you to create "cases" which will provide a collaborative space for you to gather key components required for your evidentiary requirements. With eDiscovery in Office 365, you are able to discover any of the content stored in your environment, including archived emails.

Archiving in Office 365

Messaging records management (MRM) is the technology at the heart of data retention in Office 365. The configuration options allow you to apply records management policies to both Exchange Online and SharePoint content in order to specify content that should be retained and clean-up content that is no longer needed. Audit logging and reporting is available to track anything from Administrator actions to document access and deletion. There are many logging and reporting options that can be configured to fit your needs.

Combining email archiving and eDiscovery can make life easier for both users and administrators by reducing the amount of inbox organizing to be done, and automatically applying data retention policies based on the type of content being used. The added benefit of email archiving is that even if your users store emails in independent archive files on local machines or in cloud storage like Dropbox, the archived emails are still within reach of your IT team.

Continuous Compliance Services

Office 365 Security & Compliance provides a framework of processes and controls that Office 365 uses to proactively monitor and manage the platform. With over 900 controls in place, and more being added every month, Microsoft is continually reviewing its own data handling policies and procedures to ensure that evolving customer and industry standards are being upheld.

As new customers are added to the service, each customer agreement details the privacy, security, and data handling processes necessary for you to comply with local data regulations.

Microsoft is constantly reviewing evolving and changing industry standards to ensure that Office 365 compliance framework is current.

Additionally, legal hold and eDiscovery capabilities are built into the system to help you find, preserve, analyze, and package electronic content for legal request or investigation, and Data Loss Prevention to help you identify, monitor, and protect sensitive information.

International Compliance Standards and Certifications

Microsoft recognizes that customers around the world are subject to various laws and regulations. The legal requirements and standards in one country or region may not be applicable in other regions. As Microsoft expands into more regions, countries, and economic zones, the company is constantly expanding their services and capabilities to enable compliance across a wide range of regulations and privacy mandates to meet their customer needs.

The list below provides an overview of some of the leading compliance standards and certifications provides through the Office 365 platform. However, it is ultimately up to the customer to determine whether these standards satisfy your regulatory requirements. You can find out about the latest Microsoft certifications at https://servicetrust.microsoft.com/

- Health Insurance Portability and Accountability Act (HIPAA)
- Data processing agreements (DPAs)
- Federal Information Security Management Act (FISMA)
- Federal Risk and Authorization Program (FedRAMP)
- ISO 27001
- European Union (EU) General Data Protection Regulation (GDPR)
- EU-U.S. Privacy Shield Framework
- Family Educational Rights and Privacy Act (FERPA)
- Statement on Standards for Attestation Engagements No. 16 (SSAE 16)
- Canadian Personal Information Protection and Electronic Documents Act (PIPEDA)
- Gramm–Leach–Bliley Act (GLBA)

Based on our research, Table 6 shows that 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%)

Table 6 - What are your biggest compliance challenges?

Answer	%
End users don't classify data correctly and / or take required actions	37.95%
Content stored in Legacy content systems, such as File Shares, Documentum, FileNet, HP TRIM, etc.	35.38%
Content spread across multiple workloads (Exchange/Outlook, Teams, Yammer)	33.85%
Content lifecycle (e.g. all content is retained forever)	32.82%
Insufficient planning and/or poorly executed compliance strategy	27.69%
Difficulty incorporating conflicting or differing compliance rules across the organization	18.97%
Bring Your Own Device (BYOD) policies and procedures	10.77%
Protecting consumer data	10.26%
Difficulty with business partner or contractor compliance	9.23%
Other (please specify)	2.05%

Our advisory panel had ample feedback for the lack of controls, and over-reliance on end users to "do the right thing" when it comes to compliance. According to Joanne Klein:

> *"This demonstrates to me how the end-user is seen as the key player in compliance and the importance of not only training, but implementing as many automated controls as possible. This will reduce the risk of an end-user not taking the right action on their own."*

More specifically, Microsoft MVP and CTO of Toronto-based 2toLead, Richard Harbridge (@RHarbridge) pointed to the problem end users (and experts alike) have in keeping up with the rapid pace of change in the platform:

> *The biggest issue with a company's security and compliance strategy is the lack of expertise. This space is moving fast. You need to be up to date on what's possible, what works well, what doesn't and what you should prioritize. Many customers just don't have the right people focused on this, or don't support them by modernizing technology faster and more effectively. Most of the issues are worse when you have legacy technology and/or legacy approaches.*

Continued Eric Overfield:

> *"Why is this no shocker that the primary compliance challenge is the lack of end user provided classification and metadata? I only blame the end user to a point, before this point, I look at those that created the system in the first place. What roadblocks were unnecessarily added, or unnecessarily left in place that could be removed. It is incumbent upon the solution architects to consider the end users' experience.*

> *"On the other end of the spectrum, I am also not surprised that few are blaming Office 365 in general. The tools exist, we need to use them correctly. That takes an upfront investment for sure, yet worth it in the long run."*

Going back to the core problem of Shadow IT, Joanne Klein once again identifies the problems that can occur due to a lack of end user education:

> *End-user's general lack of understanding of security and compliance risks needs to be addressed for handling controls, security controls, compliance (retention) controls. You can have all of the advanced tools in place, but if an end-user wants to circumvent the sanctioned tools, they will. However, if they understand the risks in doing that, they will be less likely to do so.*

The Ownership Dilemma

Looking across all security and compliance requirements, there is rarely one role or a single group or program that addresses all of these functions. The executive role of Chief Security Officer is uncommon for most enterprises – and non-existent within smaller companies. Instead, IT teams are tasked with ownership of the technology platforms and physical security operations, with compliance managed through operations, which can sometimes mean the Support team or a formal Project Management Organization (PMO). Without clear ownership and leadership from the top-down, security and compliance are not adequately monitored and managed.

As one respondent summarized, "This needs to change. No longer can IT have ownership of Security and Compliance since this is more than just a technical challenge."

As shown below in *Figure 4,* our survey respondents fit within industry norms, pointing toward IT departments as the primary owner. Surprisingly, executives were identified as the second highest response, which may indicate a slow but steady wave of change as organizations begin to understand the importance of these topics to the company's bottom-line.

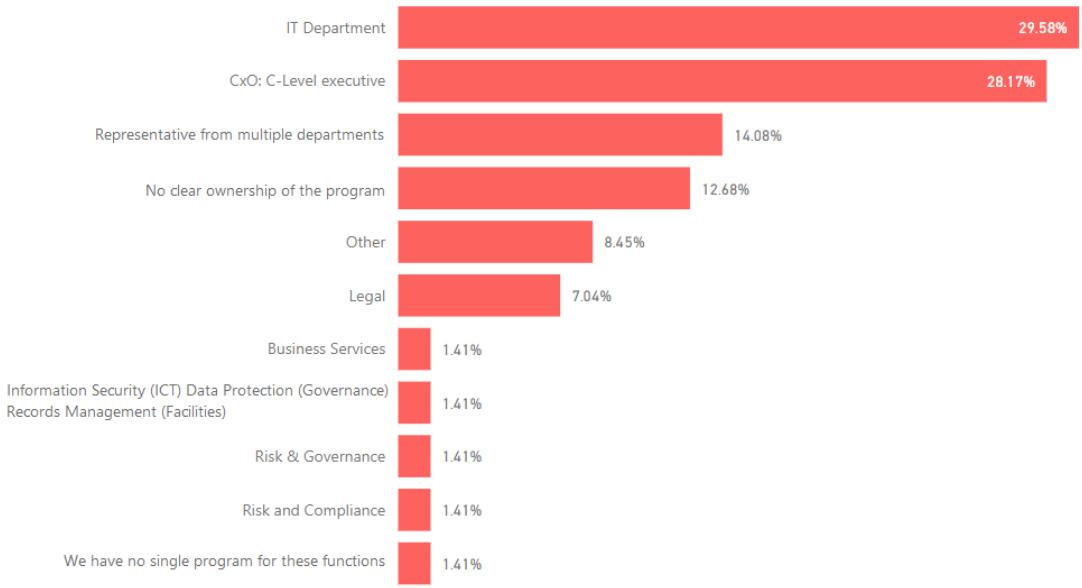


Figure 4 - Who owns security and compliance within your organization?

Antonio Maio points out one of the repercussions of relying too much on IT to manage legal and compliance issues:

> *"This reflects what we see in industry, where IT tends to own security and compliance. However, security and compliance should be owned by a Chief Information Security Officer (CISO), Compliance Team or Legal Team, so that corporate security initiatives have appropriate executive level sponsorship. In cases where IT owns security and compliance, we often see that IT has a hard time starting or carrying conversations with legal and compliance teams in order to get that executive level buy in."*

One of the biggest areas of concern for organizations that surfaced consistently within the individual interviews but was not reflected within the surveys (not included as a possible answer): whether Microsoft will be compliant, or can help them become compliant, to these standards. Respondents wanted to better understand what more Microsoft could do to help manage their security and compliance issues.

One response to this comment is with moving to the cloud itself. Microsoft is able to move much more quickly than individual companies to ensure that rapidly changing laws and standards are being met by the Office 365 platform. Additionally, they are better able to adapt and change to the ever-changing threats that are intentional or unintentional, rolling out updates and improvements to customers as quickly as necessary, providing real-time protection of their data and systems. This is one of the primary benefits of the cloud model – reducing the work and cost of proactive security of your data and intellectual property.

The Confidence Gap

One of the surveys and interview techniques used was to ask broad questions about knowledge and confidence in the functional capabilities of the Office 365 platform, followed by more granular questions to determine how accurately the broader questions were answered. It is very common for respondents to overly attribute positive responses to questions about their company's understanding of their own requirements, the completeness of their planning activities, and whether all available options and features are being utilized.

In other words, respondents will generally paint their organization in the most positive light. By also asking specific questions about core capabilities, we begin to identify a confidence gap across all three areas: most organizations do not fully understand their own requirements, therefore they do not conduct proper planning, and most do not utilize (or are even aware of) all of the features that are available and whether these unused capabilities would help them meet their requirements.

As you can see in Table 7 below, most respondents indicated that they are "Not At All Familiar" or "Somewhat Familiar" with Office 365's security and compliance capabilities.

Table 7 - How familiar are you with Microsoft's security & compliance offerings for Office 365?

Question	Not at all familiar	Somewhat Familiar	Familiar	Very Familiar
Alerts: Alerting on end user and admin actions, as well as content	19.35%	29.03%	29.03%	22.58%
Classifications: Labels and Policies to categorize content and retention	19.35%	32.26%	19.35%	29.03%
Data Loss Prevention: Data Loss Prevention policies for controlling sensitive data such as PII	22.22%	28.57%	28.57%	20.63%
Data Governance: Archive and supervisory review of user's communication	30.65%	37.10%	17.74%	14.52%
Threat Management: Advanced Threat Protection for emails and links. Also, attack simulation for testing end-user security	29.03%	35.48%	22.58%	12.90%
Data Privacy: GDPR Dashboard, and Data Subject Request case management	32.26%	30.65%	22.58%	14.52%
Search & Investigation: Content and Audit Log investigation. eDiscovery and Cloud App Security	20.97%	33.87%	25.81%	19.35%

The question is: how do you interpret this information? Again, if you factor into your analysis the organizational bias that most people have, typically attributing an overly-positive score to their own teams, these numbers are likely top-heavy–which is reflected in the larger gaps in the more granular, feature-specific questions. As Eric Overfield points out, there is a definite education gap:

> *"I am not sure how to interpret this, as across the board only one-third of respondents are claiming to be familiar with each of the different features highlighted. My best guess is that, in general, the available features are not making it into the conversation enough to hit the radars of those responsible for implementing and/or utilizing security and compliance features."*

According to Antonio Maio, however, progress is being made:

> *"We are seeing familiarity with security and compliance capabilities growing, but many organizations are still discovering which security and compliance tools are available to them in the cloud."*

We also asked respondents to share their thoughts on their most-used Office 365 workloads. The purpose of including this question was not to test respondent knowledge of the security and compliance capabilities within each workload, but to gauge their confidence in both security and compliance standards.

Table 8 - How confident are you that the services and solutions are meeting organizational and industry security standards?

Field	Minimum	Maximum	Mean	Std Deviation	Variance
Exchange	1.00	7.00	5.20	1.63	2.67
OneDrive for Business	1.00	7.00	4.64	1.89	3.59
SharePoint	1.00	7.00	4.63	1.84	3.38
Skype for Business	1.00	7.00	4.83	1.70	2.89
Microsoft Teams	1.00	7.00	4.67	1.82	3.32
Office 365 Groups	1.00	7.00	4.70	1.90	3.61
Yammer	1.00	7.00	4.50	2.04	4.16
Power BI	1.00	7.00	4.75	2.10	4.40
Planner	1.00	7.00	4.69	2.08	4.34
PowerApps	1.00	7.00	4.95	2.06	4.26
Microsoft Flow	1.00	7.00	5.09	2.00	3.99
Microsoft Forms	0.00	7.00	4.38	2.34	5.47
Other	4.00	4.00	4.00	0.00	0.00

The advisory panel was surprised by some of these responses, as captured by Joanne Klein:

> *"This one surprises me a bit. Perhaps Microsoft Flow is #1 because there's been a better job at educating people on DLP around it? Generally, it appears non-IT people have the most confidence in the Power Tools."*

While our research did not explore the features and limitations of each of the workloads, what it did provide was a perspective of where respondents are putting their trust – highlighting areas which organizations may want to review and ensure that internal and external requirements are being met.

As one of the fastest-growing products in Microsoft's history, Microsoft Teams landed in the bottom half of the confidence scale. Whether the lower scoring is due to perceptions or concerns over specific security and compliance deficiencies is undetermined within our study, but as Eric Overfield suggests, it's becoming too important a component for organizations to ignore:

> *"As with compliance, we are seeing a lack of confidence around security for Microsoft Teams. There is such room for mistakes with Microsoft Teams that the Compliance Officers must get their heads around. Simply turning off Microsoft Teams, which is destined to be the canvas of the digital workplace, is not an option. Teams provides far too much power for end users to ignore, they will jump instead to other 3rd party solutions, i.e. shadow IT."*

As we explored respondent confidence within the Office 365 compliance capabilities, you can once again see a similar pattern: people have high confidence in their own primary workloads, and low confidence in the systems they do not actively use. As shown in *Table 9* - If audited, how confident are you that your

organization is meeting or exceeding industry compliance standards?, overall respondents are reasonably confident that their primary workloads would pass an unexpected audit.

Table 9 - If audited, how confident are you that your organization is meeting or exceeding industry compliance standards?

	Minimum	Maximum	Mean	Std Deviation	Variance
Confidence level	0.00	7.00	4.13	1.66	2.74

Table 10 - How confident are you that the services and solutions are meeting all organizational and industry compliance standards?

Field	Minimum	Maximum	Mean	Std Deviation	Variance
Exchange	0.00	7.00	4.64	1.71	2.91
OneDrive for Business	1.00	7.00	4.35	1.76	3.11
SharePoint	1.00	7.00	4.29	1.71	2.92
Skype for Business	2.00	7.00	4.73	1.62	2.64
Microsoft Teams	1.00	7.00	4.33	1.77	3.13
Office 365 Groups	1.00	7.00	4.47	1.77	3.13
Yammer	1.00	7.00	4.27	2.00	4.02
Power BI	1.00	7.00	4.18	2.19	4.79
Planner	1.00	7.00	4.06	2.11	4.43
PowerApps	1.00	7.00	4.68	2.18	4.74
Microsoft Flow	1.00	7.00	4.86	2.18	4.75
Microsoft Forms	1.00	7.00	4.50	2.10	4.39
Other	4.00	4.00	4.00	0.00	0.00

Another interesting insight the research team reviewed was how specific roles responded to these questions. Specifically, the differences between respondents identifying as Compliance Officers to Executives (some additional data points are included within the Appendix).

The Compliance Officer is typically a middle-manager role outside of IT, and as shown in *Figure 5,* the confidence that respondents have in some of the newest Microsoft solutions was surprising to our advisory panel, while some of the most mature solutions (SharePoint and Exchange) fall to the bottom half.

Commented Antonio Maio:

> *"Again, I'm surprised that Compliance Officers feel most comfortable in the compliance capabilities of Microsoft Flow. Microsoft Flow is still a relatively young product, and its security and compliance capabilities are still maturing. With Microsoft Flow's ability for any user to send data to any endpoint on the internet, we certainly hope that organizations are using and enforcing the data loss prevention policies that are available with Microsoft Flow in order to mitigate risks of data exposure."*

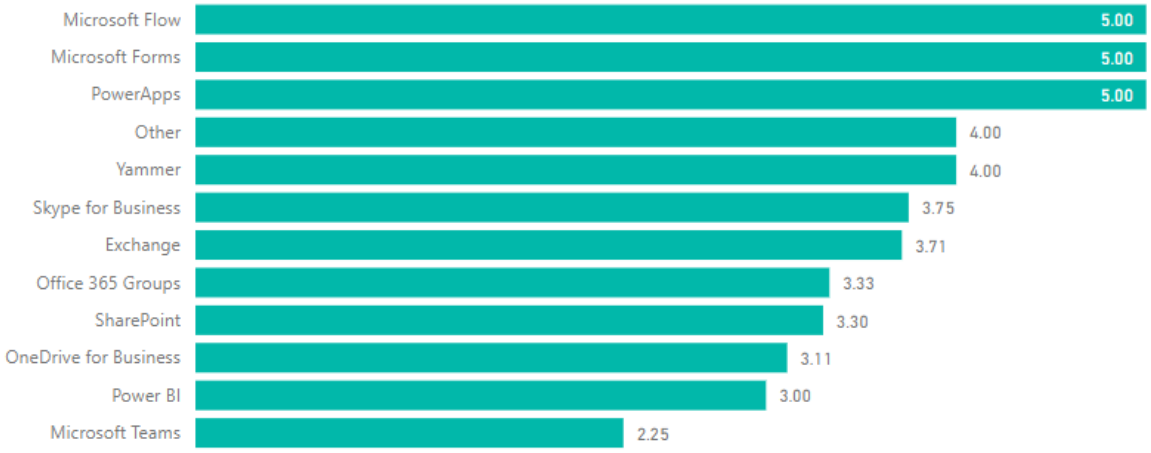


Figure 5 - Confidence by Role: Compliance Officer

What this data illustrates, emphasized by the feedback the panel advisors, is that there is clearly a gap in respondent understanding of the security and compliance capabilities across most of the Microsoft offerings. The research team observed through individual interviews that the more familiar the respondents were with the workload, the more critical they were about granular security and compliance capabilities. The less familiar they were with a workload, the more they trusted in the high-level product marketing messaging—until they were asked more detailed questions about the individual workloads, at which point their confidence levels decreased.

Eric Overfield continued with his commentary on Microsoft Teams:

> *"Compliance Officers lack of confidence in regard to Microsoft Teams is a cause for concern. Teams is being piloted and adopted by hundreds of thousands of organizations. The conversations that are happening there have to be secured and compliancy must be maintained as with any other form of communication or collaboration. Compliance Officer training and support with Microsoft Teams must become top of mind for most organizations."*

The confidence levels from survey respondents identifying as Executives or Senior Leaders was much more in-line with what the advisory panel expected to see from this data, as shown in *Figure 6 - Confidence by Role: Executive / Senior Leader*

Figure 6 - Confidence by Role: Executive / Senior Leader

Stated Antonio Maio:

> *"Confidence in the compliance capabilities of SharePoint is in line with what we see in the market from executives and senior leadership. SharePoint has a long history of storing and enabling collaboration on sensitive data, and its compliance capabilities have evolved significantly over time."*

As stated earlier, the additional questions around the more granular features showed that when asked for specifics versus general confidence / awareness, survey respondents showed less organizational bias, with most answers trending down.

Table 11 - How often do you use the Alerts feature?

Answer	%
Never	39.06%
Sometimes	35.94%
About half the time	9.38%
Most of the time	10.94%
Always	4.69%

Table 12 - Do you use Labels for classification?

Question	Never	Sometimes	About half the time	Most of the time	Always
Office 365 Labels	49.18%	26.23%	6.56%	11.48%	6.56%
Custom or 3rd-party classification solution	63.33%	15.00%	3.33%	8.33%	10.00%

Table 13 - How often do you use the Data Loss Prevention (DLP) feature?

Answer	%
Never	36.67%
Sometimes	26.67%
About half the time	10.00%
Most of the time	13.33%
Always	13.33%

Table 14 - How often do you use these data governance features?

Question	Never	Sometimes	About half the time	Most of the time	Always
PST Import	64.91%	22.81%	1.75%	8.77%	1.75%
Content Archive	42.86%	30.36%	5.36%	12.50%	8.93%
Content Retention	33.93%	23.21%	12.50%	17.86%	12.50%
Content Dispositions	48.21%	19.64%	10.71%	12.50%	8.93%
Supervisory Review	51.79%	21.43%	3.57%	10.71%	12.50%

Table 15 - How often do you use these threat management features?

Question	Never	Sometimes	About half the time	Most of the time	Always
Attack Simulator	50.00%	20.83%	6.25%	14.58%	8.33%
ATP Anti-phishing	42.86%	18.37%	4.08%	18.37%	16.33%
ATP Safe Attachments	43.75%	16.67%	8.33%	12.50%	18.75%
ATP Safe Links	47.92%	14.58%	6.25%	12.50%	18.75%
Anti-spam	27.08%	18.75%	6.25%	14.58%	33.33%
DKIM	44.44%	15.56%	6.67%	17.78%	15.56%
Anti-malware	29.17%	20.83%	6.25%	16.67%	27.08%
Message Trace	29.17%	33.33%	8.33%	18.75%	10.42%

Table 16 - How often do you use these data privacy features?

Question	Never	Sometimes	About half the time	Most of the time	Always
GDPR Dashboard	54.00%	24.00%	4.00%	8.00%	10.00%
DSR Request	64.58%	16.67%	4.17%	8.33%	6.25%

Table 17 - How often do you use these search & investigation features?

Question	Never	Sometimes	About half the time	Most of the time	Always
Content Search	16.33%	22.45%	24.49%	8.16%	28.57%
Audit Log Search	22.45%	26.53%	18.37%	10.20%	22.45%
eDiscovery	26.53%	26.53%	16.33%	6.12%	24.49%
Cloud App Security	32.65%	26.53%	2.04%	18.37%	20.41%

Another interesting data pivot is to understand where third-party tools are in use, which may indicate one of three things:

1. Low confidence in the comparable out-of-the-box features
2. Education / awareness issue with comparable out-of-the-box features
3. Missing features in the platform

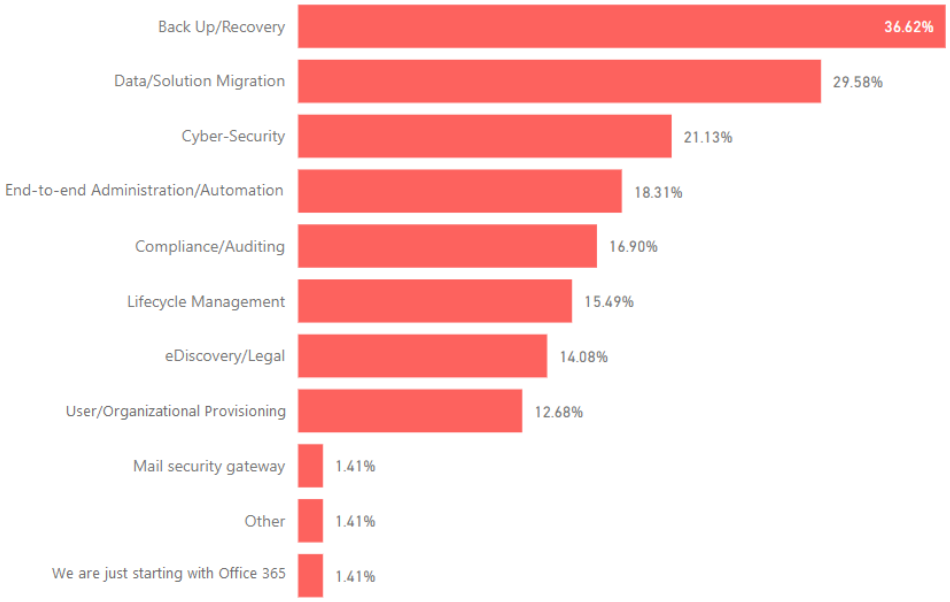


Figure 7 - What other third-party or custom-built solutions does your organization use for security and compliance?

Eric Overfield showed some concern over the low number of respondents using third-party cyber-security tools, stating:

> *"Only 13.5% of respondents are using cyber security 3rd party tools, that appears to me to be far too low than what we would want to see. Security has to be top of mind of organizations."*

However, this may also reflect the strengthening cyber-security story from the out-of-the-box Office 365 capabilities in which customers are finding that they no longer need to purchase additional solutions to augment their platforms. Based on industry data, however, a more likely scenario is that they are not fully

aware of the gaps in their cyber-security strategies and are overly reliant on Microsoft and other key solution providers.

Antonio Maio makes a similar point:

> *"This is an interesting outcome – and is in line with some client environments and the needs of Compliance Officers. Where we recommend backup of content from Office 365, to either on-premises systems or to other cloud hosted backup systems, is to meet specific regulatory compliance needs where maintaining full backups of all corporate content is a strict requirement.*
>
> *"From a security and compliance perspective, our clients are often investing in third-party tools for data loss prevention, identity and access management, and advanced control of privileged user access. As well, as part of digital transformation initiatives, we often see organizations invest in third-party tools for data and solution migration. In addition, we see third-party tool investment in records management tools for compliance with record retention requirements in the Microsoft Cloud continuing to occur. Microsoft's tool set for record retention and record management in their Cloud offerings has made significant advancements recently, but there are still some gaps that require the use of third-party tools."*

As shown in

Table 18 - Reasons for using 3rd party solutions, we then asked the survey respondents to share their reasoning for using these outside tools and solutions. Interestingly, there were no categories in which the majority of respondents believed these third-party tools to be better than what Office 365 provides.

Table 18 - Reasons for using 3rd party solutions

Question	I have a very specific need that only this tool can address	My company bought this tool/legacy application	I believe this tool to be better than what Microsoft can provide in the cloud
Back Up/Recovery	31.82%	45.45%	22.73%
Data/Solution Migration	33.33%	33.33%	33.33%
Compliance/Auditing	23.08%	30.77%	46.15%
eDiscovery/Legal	8.33%	50.00%	41.67%
Cyber-Security	27.27%	27.27%	45.45%
User/Org Provisioning	20.00%	80.00%	0.00%
Lifecycle Management	40.00%	30.00%	30.00%
End-to-end Admin/ Automation	40.00%	40.00%	20.00%

According to Antonio Maio:

> *"This is very much in line with what we see in the market. Third-party tools for data and solution migration are often utilized by consultants working in client environments,*

> *where solutions for backup/recovery are often utilized by internal company staff such as IT managers or administrators."*

Finally, we asked the survey respondents whether they believed the current security and compliance features were sufficient for their organizational requirements. For security features, a strong majority (66.67%) agreed the Office 365 "Definitely Yes" or "Probably Yes" met all of their requirements. However, for compliance features, just under half (45.1%) of respondents agreed that it "Definitely" or "Probably" met all of their requirements, with the largest response being "Might or Might Not." Once again, the research team believes this can be attributed to the education gap around Office 365 compliance capabilities.

Table 19 - Do you think the current security protection for Office 365 is sufficient?

Answer	%
Definitely yes	19.61%
Probably yes	47.06%
Might or might not	19.61%
Probably not	11.76%
Definitely not	1.96%

Table 20 - Do you think the current compliance capabilities in Office 365 are sufficient?

Answer	%
Definitely yes	15.69%
Probably yes	29.41%
Might or might not	33.33%
Probably not	13.73%
Definitely not	7.84%

Overall Analysis and Recommendations

At its core, Office 365 operates some of the most secure data centers in the world, adhering to Microsoft's internally-developed Security Development Lifecycle. Many of the best practices were developed over decades of Microsoft's own enterprise software development efforts, and since the late 1990's, this has included a host of online services. Per the Microsoft Trust Center[7]:

> *Office 365 is verified to meet the requirements specified in ISO 27001, European Union (EU) Model Clauses, the Health Insurance Portability and Accountability Act Business Associate Agreement (HIPAA BAA), and the Federal Information Security Management Act (FISMA). Our data processing agreement details the privacy, security, and handling of customer data, which helps you comply with local regulations.*

The Office 365 platform provides enterprise-grade user and administrator controls, giving organizations the ability to manage and scale their environments with the assurance that all physical, logical, and data security layers adhere to industry best practices (or better). Microsoft makes continuous improvements to the security of the Office 365 platform, from port and perimeter scanning to regular auditing of operator/administrator activities and access.

While organizations need to understand how they are meeting their security and compliance needs today, and how Microsoft can improve on that, customers of Office 365 are ultimately responsible for their own data. Microsoft provides broad oversight of the service plan, including service uptime and SLAs. Customer requirements for security and compliance will likely extend beyond these capabilities – and organizations need to understand the limitations of their service plans and have strategies in place to mitigate these gaps.

However, the top issue identified by respondents was not the technology, but administrator and end user education:

- When asked how Microsoft could enhance the security of their products, 83% of respondent requested more assistance in understanding and implementing Microsoft products.
- Of those that thought Microsoft security was sufficient, 80% of respondents have either not run security and compliance checks, or do not know if they have.
- Of those who did not think the current security protection offered by Microsoft was sufficient, 57% of respondents were not aware of Microsoft's security division.
- Of those who did not think the current security protection offered by Microsoft was sufficient, 71% of respondents were not aware of Microsoft's overall security and compliance strategy.

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. Office 365 provides the tools and capabilities you require to develop sound governance standards and meet your internal and industry-defined governance requirements.

[7] https://products.office.com/en/business/office-365-trust-center-compliance

On the reliance on Office 365 to meet most, if not all, of your security and compliance requirements, Microsoft MVP Erica Toelle (@EricaToelle), a Product Evangelist at RecordPoint in Seattle, Washington, commented:

> *Before the cloud, people managed security and compliance all on their own. Outsourcing this to Microsoft is a good idea. Microsoft has more budget to hire the industry-leaders, so they are more secure. People don't perceive this because their understanding is immature. They don't know how much Microsoft is protecting them or not. They also don't really have complete control over the situation.*

Based on our primary and secondary research, six key recommendations were identified to improve organizational security and compliance practices within Office 365:

1. Approach security and compliance more holistically, looking at it as an integrated business solution rather than through functional silos or individual workloads. Make each topic part of your existing or future governance oversight committee meetings, as 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.

2. Identify feature gaps and create an operational strategy for those gaps, allowing CSOs, 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[8]) and more transparently manage employee expectations.

3. Conduct scheduled inventory audits on a regular basis to help clean up and classify data and improve information architecture (IA) across the board. 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.

4. Create a training plan to better disseminate policies and procedures that moves beyond one-time training and makes 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.

5. Develop necessary governance and change management programs and committees to advance these ideas, support transparency, and to hold the organization accountable. This 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.

---

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

6. **Better leverage the latest technology**, getting "out in front of it" by "dogfooding" the latest features (pilots) to understand how new features can be utilized. More than ever, 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 that create an environment where new features are quickly testing and deployed will have a distinct competitive advantage over those who fail to adapt and adopt new solutions. This is especially true with security and compliance features, which can have an immediate impact through risk reduction.

On the idea of starting your planning with an audit, Eric Overfield stated:

> *"Companies need the right person (expertise) to run audits and decide to dedicate resources to security and compliance. You need someone who intrinsically understands common situations and holes in security. You need to start with an audit, then you need to lock things down. Network, workstations, client data. Go after security first and then compliance."*

Microsoft's high-level guidance for Office 365 on the topics of security and compliance is straight-forward: monitor and proactively manage. Along with your users, data is the lifeblood of your organization. As a result, it's critical to lay the groundwork to lock down access, manage the content (and end user) lifecycle, and protect your system from risk – and external threats.

To accomplish this, Microsoft recommends leveraging the Security & Compliance Center to:

- Set up and monitor alerts
- Regularly review access and usage reports
- Use the Threat Intelligence tools to research and respond to threats
- Filter and quarantine your organization's email
- Follow all of Microsoft's recommendations, based on your license types and usage patterns
- Leverage the new Advanced Security Management features to investigate and mitigate potential issues
- Regularly check your Office 365 Secure Score to identify areas for improvement

A cohesive, holistic and practical approach to governance is required for platforms like Office 365, where the reach is extensive. With the simplification of development practices in the move to a cloud environment, you now are able to more easily shift resources to concentrate on process and governance where doing so was difficult in the past.

When approaching governance of your Office 365 environment, is it important to review your strategy and tactical plans to execute your strategy. Consider each of these four areas:

Foundation

Set the ground rules for how your platform operates and what information technology security parameters it must operate in to remain secure and compliant. Address the structure and support your organization will provide to keep your environment in working order.

Administration

Placing an emphasis on teamwork between your administrative teams will streamline issue resolution and promote the nature of the platform's collaboration core. As with any team environment, definition of roles and responsibilities will be key to success. Also be sure to set a clear vision for the future in order for your administrators to manage your environment with the future in mind.

Communication

One of the clearest forms of collaboration is communication. Be straightforward and open when it comes to your Office 365 platform. Just as nature abhors a vacuum, successful communication requires collaboration with management, stakeholders, and your end users. Bring your voice and vision to the forefront and give your employees a voice in the process.

Adoption

Focus resources on user engagement, awareness and recognition in order to ensure adoption of new features. Empowering your end users will encourage them to explore and become personally invested in the technology and how it can benefit their day to day work.

There are many great online resources available with guidance on how to approach modern governance. While Microsoft provides many of the tools and guidance you need to build and maintain your governance standards, also take advantage of Microsoft's incredibly strong partner ecosystem and community of experts and practitioners to leverage the wisdom of the crowd – in addition to your own internal expertise.

On this point, long-time Microsoft MVP Matthew McDermott (@MatthewMcD), Principal Technical Marketing Engineer at Spanning Cloud Apps, stated:

> *"Companies should invest in personnel and tools to ensure compliance and secure systems. It's not enough, with today's threat landscape, to be reactive. We need to be proactive in our approach to keeping our assets and customer data safe and secure."*

His guidance was echoed by Antonio Maio:

> *"Overall, we see security and compliance knowledge and requirements within the enterprise maturing at a steady pace. As our cloud environments evolve with new capabilities, and as new threats come onto the landscape, there is a need for compliance officers, security teams, IT managers and senior leadership to continue to invest in and mature their understanding of what compliance in the cloud looks like, how they demonstrate compliance in the cloud, what tools are available to them and what tools are right for specific tasks. Annual training for end users on corporate information security policies is still highly recommended for all organizations to address many of the challenges faced. Finally, rolling out new cloud capabilities to end users in a well-defined and controlled manner is also highly recommended, so that information workers have the tools they need to be productive day to day and so that IT, Security and Compliance teams have appropriate controls in place to meet corporate security and compliance requirements."*

The first step in moving forward is to understand your security and compliance goals and priorities.

Advisory Panel

Liam Cleary
CEO/Owner at SharePlicity, and Product Owner - Security at Rencore
Microsoft MVP
@helloitsliam
linkedin.com/in/liamcleary/

Jussi Roine
Chief Research Officer at Sulava
Microsoft MVP & RD
@JussiRoine
linkedin.com/in/jroine/

Eric Overfield
President of PixelMill
Microsoft MVP & RD
@ericoverfield
linkedin.com/in/ericoverfield/

Antonio Maio
Associate Director & Senior Enterprise Architect at Protiviti
Microsoft MVP
@AntonioMaio2
linkedin.com/in/antonio-maio-b082191/

Joanne Klein
SharePoint Consultant at NexNovus Consulting
Microsoft MVP
@JoanneCKlein
linkedin.com/in/joannecklein/

Joel Oleson
Sr. Manager at Blizzard Entertainment
Microsoft MVP & RD
@joeloleson
linkedin.com/in/joeloleson/

Richard Harbridge
CTO at 2toLead
Microsoft MVP
@rharbridge
linkedin.com/in/rharbridge/

Nicki Borell
Managing Consultant at Xperts at Work
Microsoft MVP & RD
@NickiBorell
linkedin.com/in/nicki-borell/

Brian Culver
Enterprise Solutions Architect & Consultant at Expert Point Solutions
@SPBrianCulver
linkedin.com/in/bculver

Sponsors

Microsoft develops, manufactures, licenses, supports and sells computer software, consumer electronics, personal computers, and services. Our mission is to empower every person and every organization on the planet to achieve more.
www.Microsoft.com

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

RecordPoint is a global records management and compliance solution provider and pioneer of cloud-based recordkeeping. Recognized as a Cool Vendor by Gartner in 2018, RecordPoint is leading the way in the content services segment and providing organizations with the ability to manage records from across multiple services and platforms using a single, federated solution.

With support for Office 365, SharePoint, File Shares, E-mail, Box, Dropbox, G-Suite and many other applications, RecordPoint demonstrates how easy federated compliance can be with a modern, trusted cloud solution. www.RecordPoint.com

tyGraph is an award-winning software company that provides intelligent tools for better collaboration, using Machine Learning (ML) and Artificial Intelligence (AI) platforms to extract the strongest signals from the billions of rows of data processed for our customers each month. Many Fortune 500 companies across the globe trust tyGraph to deliver the analytics they need to take action on insights. www.tyGraph.com

Rencore is a software company providing award-winning solutions essential to the SharePoint and Office 365 space. The Rencore Platform is based on four pillars: App Security, App Governance, App Management, and App Modernization. The Rencore Platform securely automates everyday tasks, finds app issues and vulnerabilities in the DevOps process, and discovers and monitors customizations in the Pre-Production, Production or Modernization phases. www.Rencore.com

In-Kind

Redmond
THE INDEPENDENT VOICE OF THE MICROSOFT IT COMMUNITY

SharePoint Fest

sharethepoint
CONNECT · LEARN · EXPERIENCE

European SharePoint Office 365 & Azure Conference