Office 365: Trust, Security, and Compliance

Establishing enterprise confidence in Microsoft’s business collaboration cloud platform
Summary

Catalyst

According to Microsoft CEO Satya Nadella, Office 365 is Microsoft’s most strategic API. But to realize the potential of this business collaboration platform, Microsoft and its partners have to convince business and IT leaders that it offers levels of security, privacy, and compliance that are equal to or higher than those of their existing on-premise solutions. Even though a high percentage of enterprises are adopting cloud storage and compute within their businesses, the adoption of cloud-based content and collaboration products is by no means universal. Concerns relating to governance, risk, and compliance with regard to cloud services are understandable, but it is not unusual to find them overstated.

Ovum view

All clouds are not created equal, meaning that the quality of service and support can differ from provider to provider and from region to region. However, the overarching challenge for the industry is still trust, and improving trust will mean business decision-makers are more likely to embrace the benefits of cloud computing, such as lower costs, improved scalability, reduced deployment times, and, somewhat ironically, improved information security management.

Functionality and ease of use are very important from the perspective of the end user when it comes to using services such as Office 365, but organizations need to be confident that cloud service providers such as Microsoft have good governance of the processing of personal and corporate data. Although things are improving, verifying that good governance is in place is still not as easy as it might be.

Security concerns are an important consideration for organizations as they contemplate moving productivity and collaboration applications to the cloud, yet these often overshadow the opportunities that might come from such a move. It is vital, therefore, that business and IT decision-makers have confidence in Microsoft as they consider adopting Office 365, and that Microsoft, in turn, meets expectations related to the processing and management of data when it comes to security, privacy, and compliance.

To address the issues of trust, Microsoft has constructed an effective framework to help it deliver Office 365 in a way that meets enterprise security, compliance, and privacy requirements. This framework is formed through two primary constructs. The first includes service-level capabilities that include technology, operational procedures, and policies. These are enabled by default for all organizations using Office 365. The second is a set of customer controls, which include features that enable organizations to tailor their Office 365 environment to fit specific business and/or regulatory needs.

Key messages

- Senior leadership teams are preoccupied with corporate security.
- By necessity, Office 365 security never adopts a steady state.
- Business continuity demands a pragmatic yet thoughtful approach to data sovereignty.
Cloud service providers that are serious about supporting enterprise customers need to meet compliance obligations.

Office 365 provides an increasing range of in-built compliance capabilities.

Certification of the Office 365 services stack is important from a compliance perspective.

By establishing the Trust Center, Microsoft provides additional insight relating to Office 365 compliance practices.

Moving enterprise collaboration to Office 365 could actually increase corporate privacy controls.

Microsoft will have to keep an eye on changing European data privacy legislation.

Large enterprises are likely to adopt a hybrid approach to Office 365.

**Recommendations**

**Recommendations for enterprises**

Business and IT managers should provide evidence of their commitment to information security through the establishment, implementation, operation, monitoring, review, maintenance, and improvement of a suitable management system.

It is up to business leaders to determine and provide the resources needed to establish, implement, operate, and maintain an information security management system, and to ensure that information security procedures support the business requirements.

Adopting Office 365 does not absolve organizations of their legal and regulatory requirements or contractual security obligations. However, compliance managers should consider the value-add imparted to business operations and offset this against migration and change-program costs.

Organizations should ensure that all staff using business information technologies – whether on-premise or cloud-based – are competent to perform the required tasks. Ovum’s general view is that few organizations regularly assess the competencies of staff performing work that might affect the well-being of the organization.

Business adoption of Office 365 provides organizations with a fresh opportunity to provide training and evaluate the IT literacy, skills, experience, and qualifications of the workforce. Corporate training managers should engage with employees and the IT department early on in order to maximize business returns and minimize any customer disruption.

Office 365 services are often adopted piecemeal, with email considered the low-hanging fruit. However, Ovum believes that organizations should consider a more strategic and holistic approach to adoption, as this is more likely to bring about the step change that so many organizations are searching for.
A new opportunity to consider the organization’s information security management position

Senior leadership teams are preoccupied with corporate security

Ovum’s 2014 survey of 5,000 IT and business professionals revealed that compliance and security were either important or very important challenges for 70% of respondents. Only improved customer satisfaction ranked higher as a business priority. The management of corporate security is clearly important from a business well-being perspective, but it appears to have become a preoccupation, distracting this layer of management from activities that really matter: running the business and moving it forward.

Delivering access to line-of-business applications and information systems is becoming increasingly complex. IT departments are trying their best to accommodate a wide range of end-user device platforms in the wake of formal and more ad hoc “bring your own device” (BYOD) initiatives. This burden is generally being shouldered by IT professionals working in frontline support, as they attempt to help increasingly tech-savvy employees to integrate their new devices with legacy business processes. Device multi-screening is a key element of the modern mobile work style, the benefits of which are generally recognized by employees and their employers. However, every new device introduced to the workplace increases the vulnerability of the organization by exposing attack entry points and data egress points.

The days of IT-controlled device and application provisioning are coming to an end for many organizations, and this means that enterprise mobility management must become a seamless part of the new digital workplace rather than a bolt-on. And lest we forget, businesses and institutions are almost as vulnerable to human error as they are to cyber threats. Employees and contractors are often ill-equipped to deal with targeted attacks, but poor or nonexistent IT training increases the likelihood of accidental data loss or the compromise of sensitive information.

By necessity, Office 365 security never adopts a steady state

As Microsoft endeavors to explain to customers, Office 365 security is an ongoing process – it is not a steady state. This means that it is constantly being reviewed, revised, updated, and enhanced. Microsoft employs some of the industry’s most highly skilled and experienced engineers, and it also engages third parties and subject-matter experts to bolster its own resources. Few enterprises, let alone small and midsize organizations, can hope to match this level of proficiency in their IT departments, and unlike the typical enterprise, Microsoft also strives to keep software and hardware technologies up to date, not all of which are its own.

Like other established cloud service providers, Microsoft has significant experience in building and operating high-availability public cloud services, and the company is constantly updating its approach to meet industry compliance standards. At the service level, Microsoft adopts a layered approach to protect customer data. The strategy also includes tactics to detect, prevent, and mitigate a security breach before it happens.

According to the service security documentation published by Microsoft, the company uses automated, tool-based processes to reduce human error – which was cited by more than one cloud
service provider as a cause of a major system outage. As one would expect, Microsoft regularly conducts penetration tests to improve and develop the way it responds to real-world incidents. Machine-learning and statistical analysis are also used to spot malicious and misinformed actions, including the contextual assessment of scripts, tools, and elevated privileges.

**Business continuity demands a pragmatic yet thoughtful approach to data sovereignty**

Although Microsoft’s Office 365 data centers are geographically distributed, the company takes regional data location considerations into account when storing customer data. All modern data centers are designed to protect operations, data, and services from natural disasters and unauthorized incursion. Only essential staff are granted access to Microsoft data centers, so there are no guided tours, and physical access to the facilities is controlled through the use of multi-factor authentication techniques and security processes. Some of the biometric security technologies now entering the general market were initially developed for these high-security installations. Motion sensors and video surveillance equipment are used to control security alarms, and automated fire prevention and extinguishing systems are used when needed. Equipment is stored in seismically braced racks where the data center is located in an earthquake zone.

Network security is based on the principle that only connections and communications deemed necessary for the systems to operate are allowed. This means that all other ports, protocols, and connections are blocked or disabled. Microsoft’s Office 365 documentation describes how routers, firewalls, and other items of network equipment are strictly controlled with tiered access control lists. Also, networks within its Office 365 data centers are further segregated, with back-end servers and storage devices physically separated from any public-facing interfaces.

Office 365 does not exist in isolation, as end users interact with the service components using the Microsoft Office suite of desktop applications, mobile apps, and web applications. Moreover, each Office 365 component (Exchange Online, SharePoint Online, Office 365 ProPlus, Skype for Business, and Yammer) has its own set of security features that can be configured by the corporate IT department and its system administrators to address specific business needs and compliance requirements. Organizations are also able to control access to content within and beyond the enterprise using Rights Management Service (RMS); Secure Multipurpose Internet Mail Extension (S/MIME); Office 365 message encryption; and Transport Layer Security (TLS) for SMTP email messages to partners and customers.

Microsoft’s RMS provides data protection at the file level and can be deployed as an on-premise implementation (AD RMS) or a cloud-based offering (Azure RMS). Azure RMS is offered as part of Office 365 and presents a viable alternative to complicated on-premise solutions. Using RMS, organizations can encrypt Microsoft Office files, PDF documents, and image files. Users can apply managed access policies to these files that go way beyond the use of traditional document passwords. This technology can be used in conjunction with Office 365’s email services to address data leakage issues and protect corporate intellectual property. It should be noted that Microsoft has recently announced that it is working on customer controlled encryption that allows organizations to control encryption keys while allowing Microsoft the ability to provide data loss prevention (DLP), e-discovery, search and other data insight features in the future.
Compliance is a matter that binds governments, businesses, and institutions

Cloud service providers that are serious about supporting enterprise customers need to meet compliance obligations

Office 365 has to meet a range of compliance obligations in order to satisfy the audit requirements of governments, institutions, and industry best practices. As a result, Office 365 has obtained independent verification, including ISO 27001 and SSAE 16 SOC1 (Type II) audits, SOC2 Type II, and it is able to transfer data outside of the European Union (EU) through the US-EU Safe Harbor Framework and the EU Model Clauses. Microsoft is also willing to sign a HIPAA Business Associate Agreement (BAA) with customers, and has received authority to operate from a US federal agency under the Federal Information Security Management Act (FISMA).

Microsoft has disclosed security measures through the public registry of the Cloud Security Alliance (CSA). The CSA Security, Trust and Assurance Registry (STAR) Program is a set of offerings for cloud provider trust and assurance. The CSA STAR Program is a publicly accessible registry designed to recognize the varying assurance requirements and maturity levels of providers and consumers, and it is used by customers, providers, industries, and governments around the world. STAR consists of three levels of assurance, which currently cover four unique offerings. All offerings are based on a list of cloud-centric control objectives.

Office 365 provides an increasing range of in-built compliance capabilities

With Office 365, Microsoft offers a range of compliance features, including data loss prevention (DLP), eDiscovery, and auditing and reporting functionality. Although malware and targeted attacks can cause data breaches (an area in which Microsoft continues to increase its capabilities), employees and end users are actually a much greater source of data risk for most organizations. Exchange Online provides organizations with DLP capabilities that can identify, monitor, and protect sensitive data and help users to understand and manage data risk. For example, DLP proactively identifies sensitive information in an email message, such as social security or credit card numbers, and alerts users via “Policy Tips” before they send their email.

For business, legal, or regulatory reasons, many organizations have to retain email messages. Messaging records management (MRM), the records management technology in Office 365, enables each organization to control how long to keep items in users’ mailboxes and define what action to take on items that have reached a certain age.

The eDiscovery Center in Office 365 enables compliance officers or human resources staff to conduct eDiscovery tasks without the need for IT department handholding. Using eDiscovery, compliance officers can retrieve content from across Exchange Online, SharePoint Online, and Skype for Business (previously known as Lync). Using Office 365 eDiscovery, compliance officers have a single system for searching and preserving email, documents, and mailboxes.

Office 365’s collaboration features encourage employees to work together beyond the inbox, so Microsoft is introducing new DLP capabilities in SharePoint Online and OneDrive for Business, allowing compliance managers to search for sensitive content through eDiscovery. Windows File
Office 365: Trust, Security, and Compliance

Server has had a feature called file classification infrastructure (FCI) for a while, and Microsoft intends to enable the detection of Windows FCI content classifications for Office documents in Exchange Online, SharePoint Online, and OneDrive for Business. This includes the full range of FCI content classifications, from automatic to manual content tagging. For example, organizations will be able to create an Exchange transport rule that is able to detect the FCI classified Office document as protected health information and apply appropriate action to prevent disclosure.

Microsoft has stated that it will enable DLP natively in Office applications. This will enable organizations to enforce policies for content creation and sharing rights at the time of content creation, and it will provide end users with policy tips, similar to the email experience described above.

Microsoft will initially bring this functionality to Excel, and it will then introduce similar capabilities for Word and PowerPoint. Organizations that employ these new DLP capabilities through Office 365 will gain increased control of sensitive information across desktop, Web, and mobile apps.

**Certification of the Office 365 services stack is important from a compliance perspective**

Both Office 365 and the infrastructure that underpins it (Microsoft Global Foundation Services) employ security frameworks based on the ISO/IEC 27001 family of standards and have been ISO 27001-certified by independent auditors. This certification enables enterprises and potential customers to evaluate how Microsoft meets the standards and implementation guidance against which it is certified.

ISO 27001 defines how to implement, monitor, maintain, and continually improve an information security management system (ISMS). In addition, both the services and the infrastructure undergo a yearly SAS 70 (or successor SSAE 16) audit. The Office 365 Information Security Policy also aligns with ISO 27002, augmented with requirements specific to online services. ISO 27002 is not a certification but provides a suggested set of suitable controls for the ISMS.

Microsoft is unambiguous when it says that its goals are to operate its services with security as a key principle, and to give customers accurate assurances about its security. Microsoft’s Office 365 security response in the context of CSA Cloud Matrix Control states: “We have implemented and will maintain reasonable and appropriate technical and organizational measures, internal controls, and information security routines intended to help protect customer data against accidental loss, destruction, or alteration; unauthorized disclosure or access; or unlawful destruction.” To this end, Microsoft undergoes third-party audits to validate that it complies with its policies and procedures for security, privacy, continuity, and compliance. By using a combination of the SSAE 16 and ISO 27001 audits, Microsoft asserts that customers can verify that its controls are effective and that the management system is appropriate. Microsoft makes these audits available to its customers under a non-disclosure agreement.

Most recently, independent auditors verified that Office 365 (together with Microsoft Azure, Dynamics CRM Online, and Intune) align with ISO/IEC 27018, which provides a uniform, international approach to protecting personally identifiable information (PII) in the cloud. By adhering to this standard, Microsoft’s enterprise customers remain assured that they have full control of their data and that it will not be used for advertising, for instance.

For security and operational reasons, Microsoft does not allow enterprise customers to perform their own audits. However, Office 365 audit reports and certifications are shared with customers. Office 365
contractually requires third-party service providers to maintain and meet the same security and privacy standards as Microsoft employees. In addition, Microsoft requires that these third-parties undergo an annual audit.

**By establishing the Trust Center, Microsoft provides additional insight relating to Office 365 compliance practices**

The Office 365 Trust Center provides information security and compliance professionals with additional information on topics such as geolocation of data, administrator access, and expanded information about compliance practices. It provides existing and prospective customers with information relating to Office 365 compliance standards, including:

- the Health Insurance Portability and Accountability Act (HIPAA)
- data processing agreements (DPAs)
- the Federal Information Security Management Act (FISMA) and the Federal Risk and Authorization Program (FedRAMP)
- ISO 27001
- the European Union Model Clauses
- the US-EU Safe Harbor Framework
- the Family Educational Rights and Privacy Act (FERPA)
- the Statement on Standards for Attestation Engagements No. 16 (SSAE 16)
- the Canadian Personal Information Protection and Electronic Documents Act (PIPEDA)
- the Gramm–Leach–Bliley Act (GLBA).

It should be noted that the Trust Center only applies to specific enterprise and business offerings for Microsoft Office 365 and Microsoft Dynamics CRM Online purchased directly from or provided by Microsoft. The Trust Center does not apply to Office 365 Home, Personal, or University. Also, Yammer operates under a separate privacy statement, so the Trust Center does not apply to any aspect of Yammer Enterprise.

**Organizations that mishandle privacy matters risk losing the trust of their customers**

**Moving enterprise collaboration to Office 365 could actually increase corporate privacy controls**

The cloud-based enterprise collaboration market is expanding rapidly, especially the enterprise file sync and share market, with 40% of enterprises planning investment in this area in the next 12–18 months. Microsoft's offering in this realm is underpinned by SharePoint Online, with OneDrive for Business providing the user-facing component. Ovum’s 2014 global employee study indicates that approximately 90% of those using file sync and share technology for work purposes are using at least one consumer product, with many using three or more. This presents CIOs and information managers with a serious data management problem, as it means that corporate content is residing in unmanaged repositories.
Eager to accommodate the modern mobile work styles of their employees, organizations are evaluating a range of enterprise file sync and share products, and organizations that are using or considering Office 365 are comparing the features and functions of OneDrive for Business against products from vendors such as Box, Citrix, Dropbox, EMC, Google, Egnyte, EMC, IBM, and Intralinks – all of which are headquartered in the US. With an increasing number of EU businesses and institutions looking more closely at their data privacy obligations, enterprise file sync and share vendors must convince European customers that they have these obligations covered, especially with new legislation expected to come into force sometime in 2017 or 2018.

Like many of the vendors listed above, Microsoft is working with authorities and customers in various jurisdictions to ensure conformance to local and corporate data privacy policies. The challenge for CIOs and IT managers is to shepherd employees away from unmanaged consumer services and back on to corporately administered systems. Somewhat fortuitously, the most popular consumer file sync and share produces used in the workplace – Google Drive, Dropbox, and OneDrive – have their managed equivalents: Google Drive for Work, Dropbox for Business, and OneDrive for Business. Apple is the only mainstream file sync and share product provider not yet offering a managed service – a somewhat ironic situation as many organizations are embracing the Apple iPad to either replace or complement the corporate laptop. In many ways, the arrival of Microsoft Office for iPad, along with OneDrive for Business, has added business legitimacy to the iPad and provided organizations with a mechanism for maintaining and even improving data privacy and information security.

**Microsoft will have to keep an eye on changing European data privacy legislation**

Provision for the protection of data privacy in the EU was first made under the Data Protection Directive of 1995. Although this was extended with the so-called E-Privacy Directive of 2002 (which took into account, for instance, the information gathered by cookies), by 2010 there was widespread recognition in Brussels that technology had moved on, and that a new regulatory regime was required to deal with the world of smartphones, tablets, universal broadband connectivity, and, perhaps most of all, of cloud services. Thus in 2012, the European Commission unveiled a draft General Data Protection Regulation (GDPR) that will, once full agreement has been reached with the European Parliament and the European Council, supersede all previous EU legislation on the subject.

Besides bringing the EU’s regulatory stance on data privacy up to date, the GDPR aims to simplify the compliance process by creating a central authority that companies can engage with rather than having to deal with a separate regulator for each of the 28 member states in which they have operations. This same spirit of simplification and centralization also informs the decision to make this piece of legislation a regulation rather than a directive, which becomes operational as soon as it is ratified by the EU authorities.

Data residency is already an issue under current legislation in a number of European countries, and it will become a more stringent requirement across the EU in the GDPR. Data on EU citizens cannot be stored outside the European Economic Area in countries that do not have equally strong data protection standards. Only 11 countries meet the EU’s requirements for an equally stringent data privacy and protection regime, with the US notably absent from the list. This is clearly an issue for the enterprise file sync and share market and for Microsoft, as it ramps up its marketing of Office 365 outside of the US. Although the US does not have a sufficiently strong data privacy regime for the EU’s data residency regulations, cloud service providers that have US-EU Safe Harbor Certification...
are exempt from the data residency requirement – an exemption that is expected to be maintained under the GDPR.

The US-EU Safe Harbor Framework serves as a bridge between the differences in approach to data privacy between the EU’s 1995 Directive and the US government, and also provides a streamlined means for US organizations to comply with the directive. Microsoft has notified the Department of Commerce that it adheres to the US-EU Safe Harbor Framework, so it is legally required to comply with the Safe Harbor Privacy Principles. Microsoft looks across all markets that it targets and serves so that it can determine the unique regulation and certification requirements. From these assessments, a control set is developed that determines what Microsoft has to do to control its products and services, such as Office 365, to achieve regulatory compliance in a given market.

Large enterprises are likely to adopt a hybrid approach to Office 365

The IT departments of large enterprises have to accommodate a myriad of different use cases when it comes to providing enterprise-wide communication and collaboration facilities. Enterprise content management systems have traditionally been considered “systems of record,” requiring stringent management controls and operational rigor. As a result, platforms such as SharePoint Server, once implemented, become tightly fused to the business, providing the bedrock on which business processes are built. Even the corporate email, which is more often than not based on Exchange Server, is perceived as mission-critical by many business managers, and this has resulted in many organizations adopting a hybrid approach to this most likely candidate for total cloud migration. But in practice, organizations have realized that the cloud – even Microsoft’s Office 365 cloud – is not enough.

Large enterprises, especially multinationals, are looking for business collaboration and productivity solutions that offer a broad range of functionality to accommodate their varied business requirements. These companies are looking for flexibility in terms of deployment options and solution architectures that are able to address complex data sovereignty, integration, and information access challenges. Ovum believes that only a hybrid approach can accommodate these business requirements. Some organizations will pursue this hybrid approach by adopting cloud products and on-premise products, while others will adopt products that are designed to embrace both worlds.

The origins of Office 365 are in Microsoft’s on-premise products: SharePoint Server, Exchange Server, and Lync Server. Only Yammer – the adopted enterprise social networking component of Office 365 – is cloud-native. This means that organizations planning to adopt Office 365 will generally adopt a hybrid environment for migration purposes, and thus have in place an architecture that enables complete workloads to be moved back and forth between cloud and the data center. Moreover, this means that business, group, or user data can be stored in the cloud or in the data center when practical, procedural, or privacy requirements dictate. Although Microsoft provides tools to facilitate Office 365 migration, system administrators and IT departments may need to invest in third-party products and solutions to minimize the burden of supporting dynamic business and/or privacy requirements.
Appendix

Further reading

The Impact of EU Data Privacy Legislation on the Enterprise File Sync and Share Market, IT0021-000080 (April 2015)

2015 ICT Enterprise Insights on Enterprise Collaboration, IT0021-000039 (November 2014)

Office 365: Email Migration, Coexistence, and Adoption, IT0021-000035 (October 2014)

Selecting an Enterprise File Sync and Share Product, IT0021-000018 (August 2014)

The Importance of Protecting Content with Information Rights Management, IT0014-002972 (December 2014)


Author

Richard Edwards, Principal Research Analyst, Enterprise Productivity & Mobility

richard.edwards@ovum.com

Ovum Consulting

We hope that this analysis will help you make informed and imaginative business decisions. If you have further requirements, Ovum’s consulting team may be able to help you. For more information about Ovum’s consulting capabilities, please contact us directly at consulting@ovum.com.

Copyright notice and disclaimer

The contents of this product are protected by international copyright laws, database rights and other intellectual property rights. The owner of these rights is Informa Telecoms and Media Limited, our affiliates or other third party licensors. All product and company names and logos contained within or appearing on this product are the trademarks, service marks or trading names of their respective owners, including Informa Telecoms and Media Limited. This product may not be copied, reproduced, distributed or transmitted in any form or by any means without the prior permission of Informa Telecoms and Media Limited.

Whilst reasonable efforts have been made to ensure that the information and content of this product was correct as at the date of first publication, neither Informa Telecoms and Media Limited nor any person engaged or employed by Informa Telecoms and Media Limited accepts any liability for any errors, omissions or other inaccuracies. Readers should independently verify any facts and figures as no liability can be accepted in this regard – readers assume full responsibility and risk accordingly for their use of such information and content.

Any views and/or opinions expressed in this product by individual authors or contributors are their personal views and/or opinions and do not necessarily reflect the views and/or opinions of Informa Telecoms and Media Limited.