Office 365:
Compliance and Security Considerations

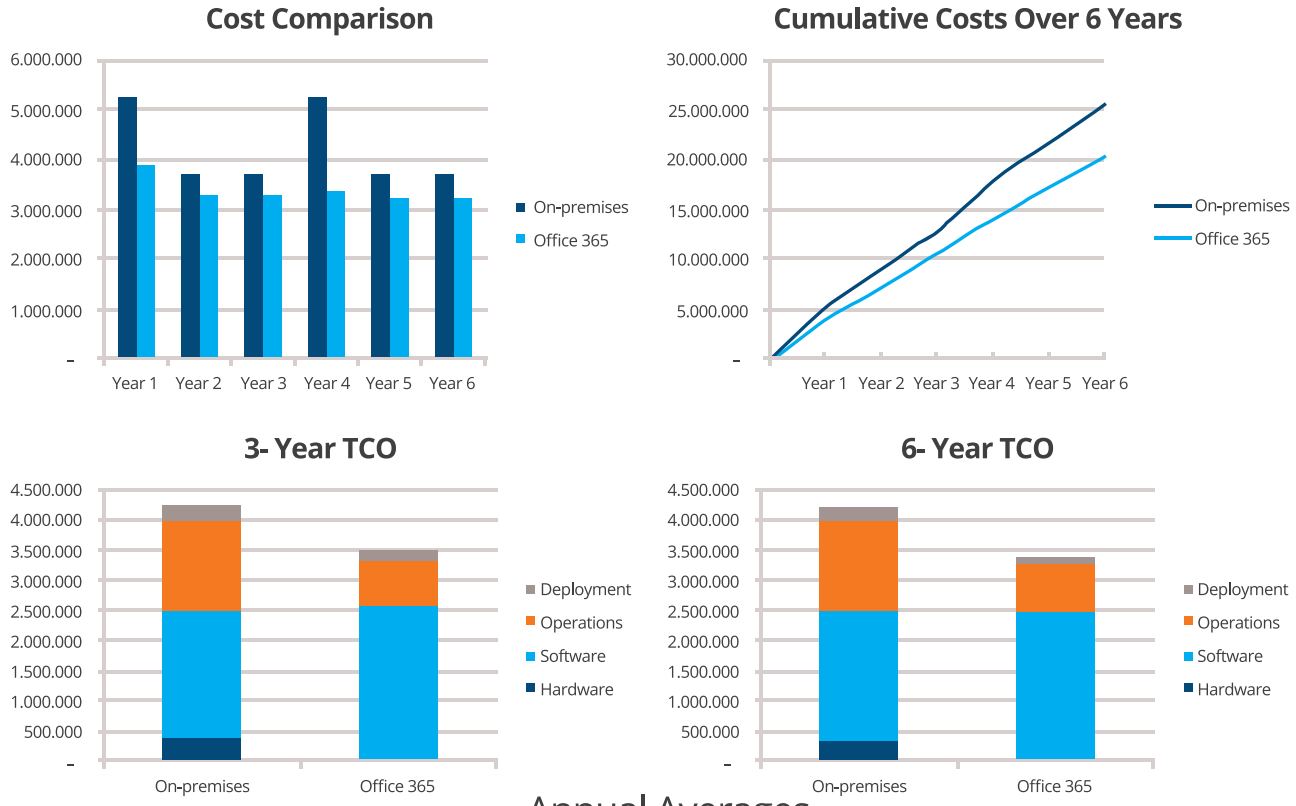
Lumen21

The advent of cloud technology has brought new capabilities that **can improve the cost structure of information technology, reduce time-to-market for new business initiatives, and enable rapid implementation of new business tools.** But it also has brought challenges as well, chief among them concerns about the security and privacy of systems and data within the cloud. But these risks can be greatly minimized by taking proper steps when implementing the given solution, allowing the advantages to far outweigh the challenges. Educating ourselves and understanding what we get out of the box and what additional controls we need to implement is the key.

Take, for instance, the growing popularity of software-as-a-service. One highly-desirable product is **Microsoft Office365.** When we hear about this product it brings to mind a number of **advantages; no on-premise equipment, someone else manages that environment, pay-per-user reduces waste, it includes an integrated office productivity suite with Outlook, Excel and Word, and upgrades to newer versions are automatic.** All of these things provide value, but it is the extensive list of additional capabilities that create the trap that lessens an organization's ability to properly and securely implement this solution.

The fear we often face is to think that per user cost will become more expensive. But it is the on-premise solution that is more expensive after including the licensing that is needed to provide all the components that would be required to have a functional, secure and compliant offering. **Components such as data loss prevention, encryption, two factor authentication, malware and antivirus are necessary.** And let's not forget the items that we don't have to consider in a software-as-a-service cost (such as on-premise infrastructure and capacity, system administration, and upgrade costs). The case is very strong for choosing the solution-as-a-service offering, however the service needs to be properly thought through, implemented and managed, particularly if you are in regulated industries such as healthcare or financial services, or are subject to PCI Data Security Standards.

Numerous studies have been done evaluating the on-premise versus **Office365** cost. Forrester TEI estimated that on average the value savings of moving to Office365 was about $750.00 annually per user. The **Office365** Total Cost of Ownership (TCO) tool evaluating a 5,000 user employee organization supports similar savings as the Forrester study found. Certainly the results can differ depending on a given client environment. If we focus on just four major cost areas: Hardware, Software, Operations and Deployment, we can see significant benefits for the **Office365** solution:



Annual Averages

Example of a cost comparison of Office 365 vs. On-premises for a 5,000 employee company (results based on Office 365 TCO tool, will may based on environment)

4 costs areas

- Hardware
- Software
- Operations
- Deployment

Given the potential cost benefit, there is value in accepting the challenge of implementing **Office365** in a secure and compliant manner. The good news is that **Office365** is a wonderful product, very rich in functionality, and **it provides plenty of components that allow you to truly realize productivity, security, and compliance,** even if you are part of a regulated industry. But…and there is a "but". These capabilities often need additional modules such as mobility, end point protection, or strong access controls to be implemented and configured while taking into consideration your operations, business, and regulatory needs. And the services must be monitored, managed and reported on an ongoing basis. It's a process…it's not magic and it just does not happen automatically.

Microsoft does provide the components that you need in order to address your regulatory and security needs. However, Microsoft can't protect you if you don't implement the right components that are needed for your given environment, or if those components are not properly configured and managed by your organization. **Compliance, Privacy and Security as it relates to Office365 has two critical parts:**

1. Microsoft efforts that include their technology, controls, their policies and procedures that come with their offering out-of-the-box.

2. Your own company controls that you must implement to customize or adopt the **Office365** environment based upon your organization's compliance and security requirements.

The second point is the one to which companies fall victim by not completely addressing the potential risks. How about employees accessing **Office365** through personal smartphones, computers, or even public computers at Internet cafes or libraries? What about the movement of Excel spreadsheets via email with private company info including PHI or PII? If that doesn't keep you awake at night, what if the portable device is lost or stolen? **Microsoft** provides tools to address these issues, but companies need to act in order to accommodate their specific company requirement for compliance and security.

Office365 has become much more than email, the Office suite, and the reduction of on premise infrastructure. O365 offers additional components that represent a very robust business solution for mobility, messaging, video, calling, texting, and security.

ATA

Advance Threat Analytics provides a simple and fast way to understand what is happening withinyour network by identifying suspicious user and device activity with built-in intelligence and providing clear and relevant threat information on a simple attack timeline.

EMS

Enables Intune for end-point protection for managing anti-virus and anti-malware. Enables AzureActive Directory Premium and reporting capabilities. Configures Information Rights Management to protect information online

EOP

Exchange Online Protection is Microsoft's cloud-based email scrubbing option for spam and malware, both for email for Office365 and on-premises Exchange Server.

MFA
Azure Multi Factor Authentication helps safeguard access to data and applications while meeting user demand for a simple sign-in process. It delivers strong authentication with a range of easy verification options—phone call, text message, or mobile app notification—allowing users to choose the method they prefer.

Yammer
Microsoft's Social network tool for communication across departments and locations.

Skype
Communication platform that includes phone, video, messaging capabilities.

Organizations are fortunate as well as challenged. Fortunate to have the building blocks of a strong software-as-a-service portfolio within **Office365.** Challenged, to be able properly identify the needed components, configure them, and provide the necessary ongoing management, support and reporting. Organizations would be well advised to carefully plan their needs before actually procuring, implementing, configuring and managing **Office365,** particularly for those in regulated industries such as healthcare and financial services. We suggest the following:

1. Determine the regulatory requirements to which your organization needs to adhere. Evaluate the specific industry guidelines such as **HIPAA** and **FFIEC** for healthcare and financial services for those operational components that your **Office365** environment will be serving.

2. Based upon this regulatory evaluation, determine the complete set of components that must be part of your given **Office365** build. Remember, its more than email and Office. This should include a BAA agreement that is satisfactory to an organization for those in the healthcare verticals.

3. Configure the needed components, taking into account the regulatory policies that you will support and attest to, as well as the associated processes that will be required for daily operations and management.

4. Migrate your environment using either automated tools provided by **Microsoft,** or manually, depending on the level of control that best fits your company needs.

5. Provision users with the required credential and authentication controls.

6. Go live, be sure to implement processes to track, monitor and manage the system on on-going basis.

Office365 provides a strong option for adding business value, and makes a good economic case for organizations. But you can't assume that **Microsoft** will automatically provide all the things your particular environment needs to address as part of your compliance and security requirements. **Office365** is powerful and highly capable, but it does not just happen without proper understanding, needed components, configuration and operation, particularly if you are in a regulated industry. Remember, compliance is not a statement, it's a process.

Lumen21 is a company that specializes in the area of IT Security and Compliance. Lumen21 has a series of solutions and services for used by Healthcare organizations in order to leverage newer technology while meeting its regulatory and security responsibilities. Lumen21's Compliant Cloud Computing Solution is truly HIPAA compliant and also maps to NIST SP-800-144, NIST SP 500-299 standards as well as it complies with or exceeds the Cloud Security Alliance Framework (CSA). Lumen21 enables the process of compliance and allows a healthcare company the ability to measure, monitor, report and improve that process. Lumen21 offers its O365+ Compliance Service leveraging Microsoft products such as O365 Enterprise, Enterprise Mobility, Device management and Azure Storage, implementing the necessary controls that are configured and monitored to meet regulatory standards. That is why at Lumen21 we believe HIPAA compliance is not a statement, it's a continuous process that is vetted and certified. You can learn more about our solutions that can help you meet regulatory compliance in your It operations as well as enhance your security by reaching out to us at sales@lumen21.com or visit us at www.lumen21.com HIPAA compliance is not a statement, it's a continuous process that is vetted and certified. You can learn more about our solution by reaching out to us at sales@lumen21.com or visit us at www.lumen21.com