Microsoft Azure

Microsoft Azure Guidance for Sarbanes Oxley (SOX)

Microsoft

Abstract

This document is intended for Azure customers who are considering deploying applications subject to SOX compliance obligations. It provides customer guidance based on existing Azure audit reports, as well as lessons learned from migrating internal Microsoft SOX relevant applications to Azure.

November 2017

Contents

Introduction

The Sarbanes-Oxley Act of 2002 (SOX) is a US federal law administered by the Securities and Exchange Commission (SEC). Among other things, SOX requires publicly traded companies to have proper internal control structures in place to validate that their financial statements reflect their financial results accurately. As cloud adoption gains momentum, more and more customers are exploring how to migrate applications and workloads subject to SOX compliance obligations to the cloud. This paper provides guidance to customers on how to leverage Azure's existing compliance reports when addressing their own SOX compliance obligations. It draws on internal Microsoft experience with migrating SOX relevant applications to Azure. Moreover, this paper provides migration best practices, including SOX compliance implications, reviews of two publicly available case studies, and lessons learned from Microsoft's internal migration projects.

Customers are wholly responsible for ensuring their own compliance with all applicable laws and regulations. Information provided in this document does not constitute legal advice, and customers should consult their legal advisors for any questions regarding regulatory compliance.

Leveraging SOC attestation for SOX compliance

SEC does not define or impose a SOX certification process; instead, they provide broad guidelines for publicly traded companies to determine how to comply with SOX reporting requirements. Consequently, there is no SOX certification or validation for cloud service providers; however, Azure can help customers meet their obligations under SOX, which is heavily influenced by customer's internal processes especially when it comes to controls for financial reporting. For example, SOX requirements involve internal customer controls for the preparation and review of financial statements, and especially controls that affect accuracy, completeness, effectiveness, and public disclosure of material changes related to financial reporting. Customers enquiring about Azure SOX compliance should review the Azure SOC 1 Type 2 attestation that is based on the American Institute of Certified Public Accountants (AICPA) Statement on Standards for Attestation Engagements 18 (SSAE 18) standard (see AT-C Section 105) and the International Standard on Assurance Engagements No. 3402 (ISAE 3402). This attestation has replaced SAS 70, and it is appropriate for reporting on controls at a service organization relevant to user entities internal controls over financial reporting. Customers can download this attestation report from the Trust Center.

Azure maintains a SOC 1 Type 2 attestation that covers at least a 3-month run window (audit period) across a broad portfolio of customer-facing services that can be used to build a wide range of applications. All Azure SOC reports (SOC 1 Type 2, SOC 2 Type 2, and SOC 3) are produced by an independent third-party auditing firm. Azure services in scope for SOC attestations are tracked on the Trust Center, which also provides download links to the actual attestation reports. Customers should review these reports to learn about control objectives and effectiveness of controls owned by Microsoft, as well as complementary user entity controls and user entity responsibilities. For example, there are IT controls under customer's responsibility that impact SOX compliance, such as user access to cloud resources, and appropriate auditing of these controls need to be developed by the customer as part of any SOX migration strategy.

Shared responsibility implications for SOX compliance

NIST SP 800-145 defines the following cloud service models: Infrastructure as a Service (IaaS), Platform as a Service (PaaS), and Software as a Service (SaaS). The shared responsibility model for cloud computing is depicted in Figure 1. With on-premises deployment in their own datacenter, customers assume the responsibility for all layers in the stack. As workloads get migrated to the cloud, Microsoft assumes progressively more responsibility depending on the cloud service model. For example, with the IaaS model, Microsoft's responsibility ends at the virtualization (Hypervisor) layer, and customers are responsible for all layers above the virtualization layer, including maintaining the base operating system in guest Virtual Machines. With finished cloud services in the SaaS model such as Microsoft Office 365 or Dynamics 365, Microsoft assumes responsibility for all layers in the stack; however, customers are still responsible for administering the service, including granting proper access rights to end users.

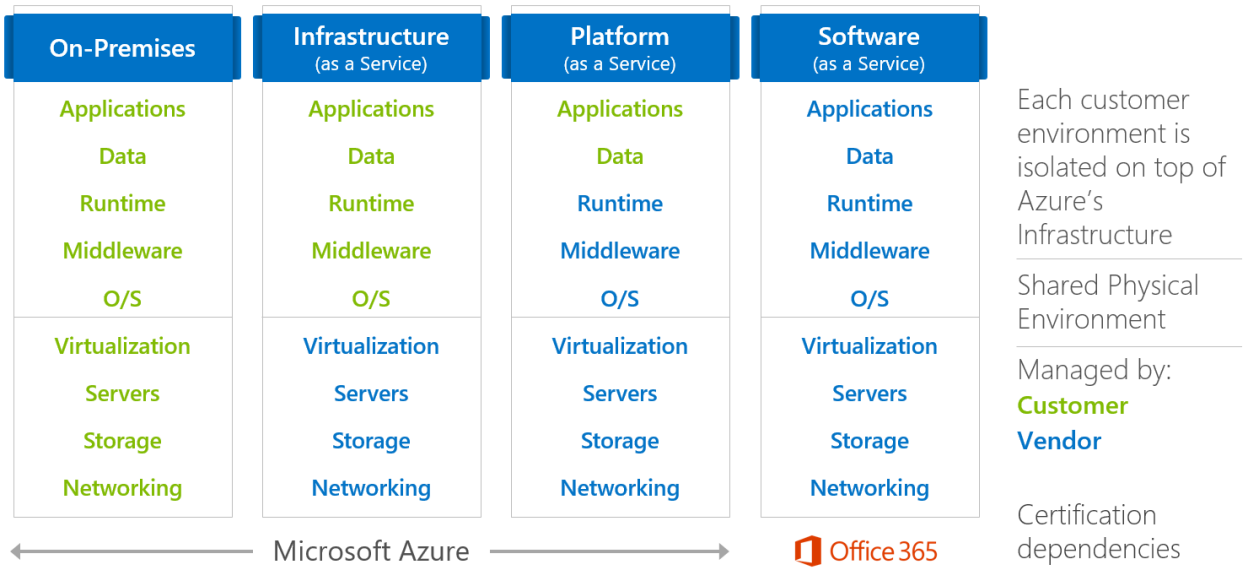

Figure 1: Shared responsibility model in cloud computing

The concept of shared responsibility extends also to certification dependencies and compliance obligations. When customers subject to SOX compliance obligations deploy applications to Azure, they take control dependencies on Microsoft. Customers are ultimately responsible for meeting their SOX regulatory requirements; however, they inherit various controls from the underlying cloud platform and can leverage Azure's existing audits for assistance. For more information on shared responsibility, read the Microsoft whitepaper Shared Responsibilities for Cloud Computing.

To help customers with their SOX obligations, Microsoft maintains a SOC 1 Type 2 attestation covering most of the generally available Azure services that customers can leverage to build applications. These services span all platform features, including Compute, Storage, Networking, Databases, Security and Identity, Monitoring and Management, etc. It is crucial for customers to understand clearly what IT controls they need to implement and monitor, as failure to do so may result in internal control deficiencies even while Azure platform controls owned by Microsoft are operating effectively. Controls owned by customers are driven primarily by customers internal processes involved with financial reporting.

SOX related Azure case studies

Last year, Microsoft published two case studies for business critical, financial applications that were migrated to Azure. They provide useful insights into migration strategy, business benefits, and significant cost savings when running applications in the cloud. These case studies are reviewed below.

Microsoft Treasury

Microsoft Treasury is responsible for managing the financial assets of the company. It supports:

- More than US $300 billion annual cash movement.
- Annual portfolio trades per year totaling approximately US $600 billion.
- Operations in 191 countries and in more than 30 currencies.
- Approximately 2,000 bank and custody accounts and relationships with 95 banks.
- More than 10,000 wire transfers processed per year.

In 2016, Microsoft moved 100% of Treasury's infrastructure to Azure IaaS, thereby reducing infrastructure costs by 20% and infrastructure footprint by 61%. Using "lift and shift" concepts, this stage was completed relatively quickly, with minimal downtime and no business interruption. Next, by assessing what applications could leverage Azure PaaS features, engineers redesigned the application portfolio using Azure PaaS services to build a more functional and unified environment. The combined effect was to create a much more cost-efficient, agile, and scalable Treasury app environment, all in under 8 months. For more information on this cloud migration, read the case study Migrating business-critical Treasury applications to Microsoft Azure.

Microsoft Finance

Microsoft Finance, which handles the company's international taxes, was faced with rapidly changing tax laws and data growth for periodic reporting of sales or income taxes, as well as complying with audits. With Microsoft revenue approaching US$100 billion in 2015, the data volume was at 6TB, with expected growth to 100TB over the next few years. Microsoft transformed the Finance department's traditional data warehouse infrastructure into a centralized, cloud-based big data system using Azure SQL Database and HDInsight. Microsoft also took advantage of Azure App Service to create APIs for a web-based interface, as well as Power BI for self-service analytics.

Once live, the system delivered significant productivity improvements when responding to international audit requests. For example, the Finance team used to capture tax information in a spreadsheet that was then provided to the tax authorities. Some of the queries that took six hours or more were reduced to around 10 minutes with the new system. Moreover, Microsoft Finance now has the same level of deep granularity across all the different billing systems, with the insight and agility it needs for data-driven decisions that ultimately improve global business processes. For more information on this cloud transformation, read the case study Microsoft IT builds a big data tax solution for Finance with Azure.

Lessons learned from Microsoft SOX migration efforts

Listed below are some of the lessons learned based on Microsoft internal SOX migration projects.

- **Aim for PaaS** – PaaS migration is highly recommended compared to an on-premises "lift and shift" migration to IaaS, since there are fewer SOX IT controls to implement within a PaaS environment.
- **Engage in early planning** – Ensure early planning to allow adequate time for scoping and implementing SOX controls. Project teams need to account for potential issues relating to control implementation and deployment that may delay the project.
- **Avoid 4th quarter** – Given the potential for major business impact if there are deployment issues, Microsoft avoids 4th quarter migrations of applications that require SOX compliance.
- **Complete a security review** – In addition to SOX requirements, applications migrating to Azure should complete a security review and remediate all identified issues prior to deployment.
- **Scope to SOC 1 Type 2** – Only use SOC 1 Type 2 certified Azure services to host or process financial data. If Azure services are not in scope for the SOC 1 Type 2 audit, additional SOX controls may need to be in place to ensure protection.
- **Maintain control mapping** – Establish how Azure SOC controls map to customer control environment. Monitor this mapping over time for potential impact.
- **Document controls** – SOX owners need to document and implement IT controls prior to deployment. Project teams must document the test plan to ensure test procedures are implemented and operating effectively.
- **Perform a dry run** – SOX owners need to perform a dry-run test of the SOX controls and produce adequate evidence to ensure it satisfies SOX audit requirements prior to deployment.
- **Automate SOX controls** – Where possible, automate SOX controls to ensure consistent operating and testing of the controls.

Summary

Customers looking to migrate applications to Azure that are subject to SOX compliance obligations can get useful insight into best practices and business benefits based on Microsoft internal SOX migration projects. They can leverage the existing Azure SOC 1 Type 2 attestation when assessing their own SOX compliance requirements. This attestation is appropriate for reporting on controls at a service organization relevant to user entities internal controls over financial reporting. It is important for customers to internalize the concept of shared responsibility in the cloud when developing a successful SOX migration strategy.