EFFECTIVE COMPLIANCE MANAGEMENT ON MICROSOFT AZURE

cloudneeti

ABSTRACT

As a CIO/CTO, you have decided to move your business-critical applications and associated infrastructure to Azure. Azure although provides compliance to its infrastructure, anything you host on top of it will be your responsibility. Azure compliance status does not automatically translate to the services that you build or host on the Azure platform.

AUTHOR

Gururaj Pandurangi
Sunaina Mishra

DATE:

Jan 2018

Table of Contents

1 EXECUTIVE SUMMARY

Using cloud computing services for data and applications subject to compliance regulations requires a high degree of openness and transparency on the part of the cloud service provider. Customer organizations considering the use of cloud services need to think through what use cases make sense today, closely review contracts and service level agreements, understand the compliance requirements and how they are met (or not met) by the cloud service. They should also insist on "right to audit" clauses and general transparency on the controls in use.

2 YOUR RESPONSIBILITIES

Following are the things you need to consider when you host your application on the Azure platform:

- Investment
- Risk
- Time

3 MANAGE INVESTMENTS

> "*Compliance is often determined on three factors, security: data must be safeguarded against all threats to its integrity; permanence: data must be retained in its original state without being altered; and auditability: data must be accessible in a timely manner when required.*"
>
> - Ryan Barrett, Vice President of Security and Privacy at Intermedia

"It used to be that security concerns were the biggest impediments to public cloud adoption. But, in 2017, that will no longer be the case. It is widely accepted that security in public clouds is strong, shifting the top concern to compliance. Organizations moving to the cloud need to be able to demonstrate and provide assurance that they are doing things in a secure and compliant manner. So, whether it is PCI, HIPAA, NIST-800 53 or internal compliance standards, organizations need to be able to demonstrate that they can maintain compliance throughout the fast-pace of change that takes place in the cloud. To solve this, they should turn to security and compliance automation solutions that will help them measure and report with ease." - Tim Prendergast, CEO at Evident.io

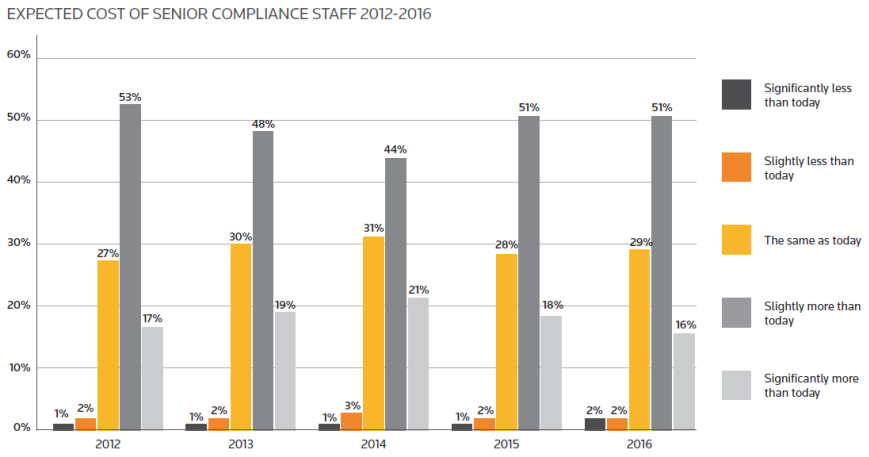
Compliance could cost much when you host your application on the cloud, which includes external and internal costs, automation cost, security cost, etc. Though Azure takes care of buildings, servers, networking

hardware, and the hypervisor, you must manage your operating system, network configuration, applications, identity, clients, and data.

3.1.1 EXTERNAL AND INTERNAL COST

Though Azure facilitates an auditing process, you are required to have your cloud service audited to see that it meets the appropriate requirements, which may relate to IT security or recovery procedures or any other such IT activity that must obey compliance standards. This is in addition to the costs required for your existing on-premises audits. Also, your strategy must be flexible to adapt when internal changes happen, as existing controls may become obsolete.

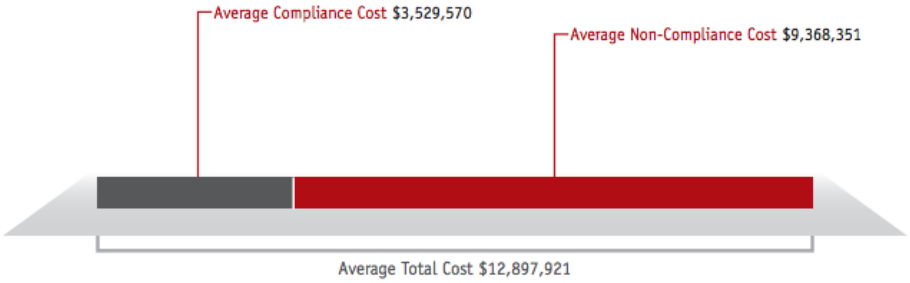
The following graphic shows the cost of recruiting senior compliance staff is increasing year by year:



Source: https://risk.thomsonreuters.com/content/dam/openweb/documents/pdf/risk/report/cost-compliance-2016.pdf

3.1.2 AUTOMATION COST

The automation of compliance technologies is needed to identify suspicious transactions or other anomalous behavior. You need to consider this cost as the compliance costs depend upon the amount of transactions and other data requiring review regularly.



Source: http://www.gigya.com/blog/the-cost-of-non-compliance-putting-a-price-on-privacy/

3.1.3 SECURITY COST

As you make your application available on the Internet, it is open to all. Furthermore, with increasing volumes of data comes increasing costs for licenses and hardware. You must invest in detecting and stopping data theft as fraudsters will seek to steal more than it costs to stop them. Though Microsoft Azure gives you the option to store the encryption keys locally in the same server where you store data, to be compliant with most data security regulations and avoid data breach notification, you must use a way to store their encryption keys and use best practices such as dual control and separation of duties.

Our solution helps in cutting cost and plan better for optimum investment.

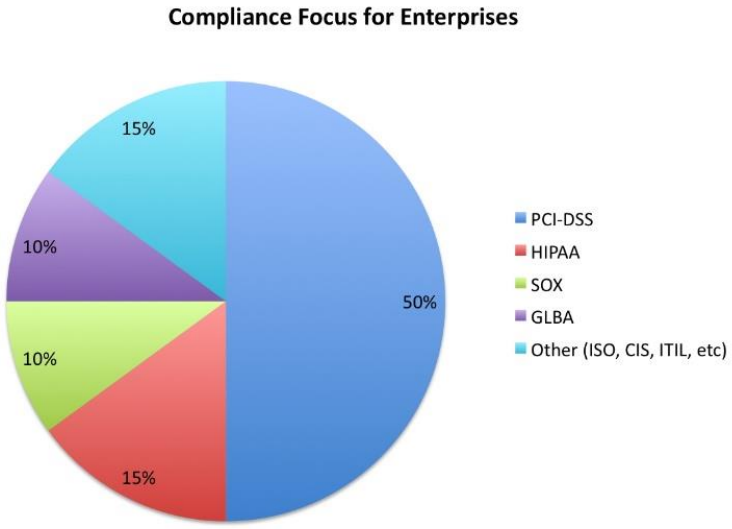
4 MANAGE RISKS

A company might face legal penalties, material loss, and fines if it fails to comply with the industry rules and regulations, internal policies, and best practices. Violating compliance might threat an organization pay penalty for damages and even contract cancellation. This could damage the company reputation and eventually lead to loss in the business opportunities. According to the National Institute of Standards and Technology (NIST), organizations are fully responsible for all compliance-related issues. The cost of not being compliant may result in penalty fees, lawsuits, and bad business reputation.

To manage risks, you might consider the following actions:

4.1.1 ANALYZE SENSITIVE DATA

When hosting in Azure, you are the sole owner of the data stored there. You need to decide if there are any sensitive data that should not be placed in the cloud, such as social security number, bank account information, PCI data, etc. You also need to consider other factors, such as What legal restrictions exist across different countries in which you engage in commerce? Do any countries (or states) have restrictions upon the location in which cloud data are stored? Any of these items could be deal breakers that prevent the use of cloud resources.



Source: http://jameskaskade.com/?p=1768

4.1.2 ENFORCEMENT OF REGULATIONS AT ALL PHASES

Compliance and security are only addressed either at the testing phase or at the last stage of development, which could potentially result in applications that do not identify potential threats. To build good quality and compliant systems, you need to enforce the regulations at all development phases including requirements, design, implementation, and testing phases.

4.1.3 GAP ANALYSIS

You should perform a gap analysis between the specific requirements identified in relevant regulations, and the set of controls provided by Azure. Azure only offers partial compliance, or only on a specific set of services (not all). This means it will be up to you to fill the gaps. You are supposed to close these gaps by deploying specific security controls on your virtual infrastructure. For example, software firewalls and anti-malware software may be deployed as needed in IaaS virtual machine instances to satisfy compliance (and security) requirements.

4.1.4 REVIEW REFERENCE ARCHITECTURE (RA)

Most cloud service providers are required to support multiple regulations to fulfill consumers' needs. The cost of implementing individual regulations can lead to high implementation and maintenance costs, duplication of efforts, and inconsistencies. Many RAs are either incomplete or do not follow standard models or architectures.

You must review the Azure architecture to ensure that it includes major regulation components, stakeholders, cloud components, patterns, and best practices.

4.1.5 CHECK FOR FULL CONTROL AND TRANSPARENCY

The lack of full control and transparency is also one of the compliance challenges in the public cloud. The data stored in the public cloud could be replicated in different regions and / or countries that could violate privacy laws of other countries. Check with Azure team if they ensure the confidentiality, integrity, availability and accountability (CIAA) of your data as per the government and industry regulations.

Our solution helps in cutting cost and plan better for optimum investment.

5 MANAGE INITIATIVES & SCHEDULE

You must undergo many time-taking and rigorous tasks as well.

5.1.1 VULNERABILITY SCANS

It is also worth noting that satisfying many compliance requirements will require regularly assessing the control state for the cloud service at periodic intervals. For example, PCI DSS requires quarterly vulnerability scans be conducted for systems. Even performing vulnerability scans on public cloud services may be an issue, as some cloud services limit the customer's ability to do this in their contract language.

5.1.2 FREQUENT STANDARD RENEWALS

According to a research done by Thomson Reuters more than a third of firms continue to spend a whole day every week tracking and analyzing regulatory change. Keep in mind that compliance is never just a one-time thing. PCI DSS, for example, needs to be renewed each year, involving additional costs.

5.1.3 DOCUMENTING CONTROLS

Paul Nicholson, director of product marketing at A10 Networks, regulatory compliance is time-consuming because organizations often need to comply with multiple regulations with different objectives and

requirements. Not only you need to implement appropriate security, privacy and change management controls, but you also need to document these controls to auditors and regulators.

Our solution helps in reducing time to complete these tasks.

6 REFERENCES

- "A survey of compliance issues in cloud computing", Dereje Yimam and Eduardo B. Fernandez, 2016, https://jisajournal.springeropen.com/articles/10.1186/s13174-016-0046-8
- "Managing Risks and Other Concerns When Moving to the Cloud", The Wall Street Journal, http://deloitte.wsj.com/riskandcompliance/2013/07/09/managing-risks-and-other-concerns-when-moving-to-the-cloud/
- "Is Compliance in the Cloud Possible?", Jim Hietala, 2010, http://www.cso.com.au/article/331534/compliance_cloud_possible_/
- https://msdn.microsoft.com/en-in/magazine/jj991979.aspx
- "The Cost of Compliance in 2016", Loffa Interactive Group, 2016, http://loffacorp.com/the-cost-of-compliance-in-2016/
- "TechTarget Survey: IT risk management, compliance top tasks", Michael Heller, 2015, http://searchsecurity.techtarget.com/news/4500257593/TechTarget-Survey-IT-risk-management-compliance-top-tasks
- "Change control", Margaret Rouse, 2011, http://searchdisasterrecovery.techtarget.com/definition/change-control
- "Here's What the Experts Say about Cloud in 2017", Nicole Henderson, 2016, http://talkincloud.com/cloud-computing/here-s-what-experts-say-about-cloud-2017