WHY COMPLIANCE MATTERS IN THE CLOUD

Compliance in the cloud: myth or reality

Most compliance standards governing the management of IT infrastructure were not designed with cloud in mind. Compliance standards are predominantly concerned with maintaining the protection and integrity of data ... not locking down virtual environments. Therefore, as organizations look into adopting cloud services for better scalability and lower IT costs, they are confronted with a myriad of unanswered questions regarding compliance in the cloud.

Using the cloud means moving from a dedicated environment where a company has complete control to an environment where that control often belongs to someone else. Although that may sound negative, if the move is to a provider that is well-versed in regulatory standards, and offers a compliant environment, this can actually be positive.

The need for compliance
Regulated industries or businesses that have strict security policies each have their own compliance checklists to follow. The regulatory mandates with the most severe penalties for non-compliance are the Health Insurance Portability and Accountability Act (HIPAA) healthcare regulations, the Federal Information Security Management Act (FISMA) standards for government contractors, the Payment Card Industry Data Security Standard (PCI-DSS) for organizations that handle cardholder information, and the Sarbanes-Oxley (SOX) accounting regulations for wholly-owned or partially-public companies.

These regulations have a common objective: the implementation and enforcement of policies. Compliance with these regulations involves maintaining specific certification standards and ensuring best practices.

• HIPAA requires that healthcare businesses hold onto patient documents for six years.
• FISMA requires each government agency carefully document and continuously review its information security strategy.
• Businesses that process credit transactions are required to track all access to cardholder data via PCI-DSS regulations.
• SOX mandates that an organization is responsible for any accounting or financial wrong, even those of a third party.

Each regulation is about mitigating risk and creating a strong foundation of people, processes, and technology.

The consequences of not being PCI compliant range from $5,000 to $500,000, which is levied by banks and credit card institutions.
Regardless of the type of cloud you are considering — whether private, public or hybrid clouds — the shift to virtualized environments presents new challenges across the spectrum of governance, risk and compliance (GRC). Addressing GRC requirements requires appropriate assessment criteria, relevant control objectives and access to the necessary data. Various standards organizations provide guidelines to assist companies with GRC. The Cloud Security Alliance, for example, publishes a questionnaire titled “Consensus Assessments Initiative Questionnaire” addressing the relevant points around PCI-DSS compliance. This questionnaire acts as a guide to assist organizations with PCI-DSS compliance.

The Health Insurance Portability and Accountability Act (HIPAA) recently adjusted its auditing policies to include cloud. The new HIPAA Omnibus rule, which went into effect on March 26th, 2013, expands the definition of a “business associate” and has a number of key changes if you are either a public cloud provider or user of public cloud services. It puts into place heightened protocols for how patient information is shared as well as how notifications about breaches need to be handled.

The “cloud first” mandate by the federal government has put the spotlight on the Federal Information Security Management Act (FISMA). FISMA is a federal law which mandates a set of processes that must be followed for all information systems used or operated by a US Government agency or by a contractor or other organization on behalf of the US Government.

The mandate focuses on information security and requires stringent documentation and implementation to maintain the confidentiality of information. FISMA requirements encompass all information and information systems that support the operations and assets of the government agency and any operations provided to the government by another agency or contractor.

FISMA compliance requires ongoing evaluation and remediation of risks, including on-going reporting and monitoring of the documents stored either on-premise or off-premise. Agencies must monitor compliance for documents stored in the cloud or elsewhere.

Companies that fall within SOX must ensure their service providers have all the necessary processes in place to adhere to SOX compliances. Many rely on a set of auditing standards, called Statement on Standards for Attestation Engagements (SSAE 16). SSAE audits and reports on a companies internal controls over its processes and handling of information.
How the cloud affects compliance

While an organization’s struggle to keep pace with governance and compliance standards can be difficult, these issues get even more complicated when it comes to public, multi-tenant cloud environments. From the infrastructure perspective, cloud computing heavily leverages resource pools in a variety of technologies — compute, storage, backup, and network — for real-time allocation in an automated and logically-diversified environment, accommodating a variety of applications. With their virtual back-ends, clouds are dynamic, with resources that can be pooled within and across multiple data centers to provide an environment that responds to user needs.

For this reason, a company has to be careful. It is possible that their data and applications might meet required compliance standards while on their own servers, but not when they move to a cloud due to exposures that may exist there or along the way. Likewise, if data and applications meet standards while in the cloud, they may not meet them when they move back to the company’s data center, requiring a re-audit. To maintain end-to-end compliance when employing cloud technology, multiple levels of security must be set in place. For example, the transport media must be secure and data must be encrypted once it leaves the data center, with encryption keys under enterprise control.

Achieving compliance in this kind of virtual environment involves setting up the proper framework, with the cloud service provider’s physical infrastructure acting as the foundation. This infrastructure should have measures in place for protecting the data centers from natural disasters, assuring reliable electrical power (such as backup distribution systems) in the event of outages, and backing up data in the event of a hardware failure. Personnel-wise, a cloud service provider needs to have process and policy guidelines in place covering such matters as employee authorization to access the data center and how internal security reviews are performed and reported.

Service providers for cloud need to offer transparency into the infrastructure and services so customers with regulatory requirements can determine which cloud offering, if any, address their specific needs.

Providers of cloud infrastructure need to understand the regulatory standards their customers are subject to, however the burden of compliance remains with the customer.

Data protection and integrity do not just apply to regulated industries.

Even non-regulated businesses should leverage standards-based systems to ensure the security of their data.
Myth vs Reality

Organizations want (and need) the obvious and oft-stated advantages of cloud, but it cannot be implemented blindly. It must be carefully planned. For both regulated and non-regulated business, the benefits of working within a standards-based and regulations-compliant cloud solve many of the challenges that face decision makers.

There are many myths spanning compliance regulations of SOX, FISMA, HIPAA, PCI-DSS, etc. With the plethora of regulatory requirements we cannot cover them all but we have outlined a few of the top myths below. You need to understand the issues (and myths) surrounding compliance before moving your workloads into cloud.

Myth: Any security is good security

While it’s true that security is a good thing when talking about your infrastructure, when in a regulated environment there is no such thing as “good enough”. You cannot check the box. Organizations need to properly ensure that data is protected. This means making sure your network is safe from malware and attackers, ensuring that your antivirus software is up-to-date and addresses security threats. You also need to address the security behaviors of your entire organization. How and what information is being shared? Who has access and how is the data being protected from unauthorized access? Does your organization have network segregation? Are they using VLAN tagging? VLAN tagging allows different parts of your network can be logically separated into distinct “VLANs” and create small quarantine zones between sets of machines that cannot speak to one another. This reduces data exposure, yet still allows internet connectivity for critical updates.

Recommendations:
• Get a commercial security firewall
• Employ a managed switch that can handle VLANs
• Invest in anti-malware/anti-virus software

You need to understand the issues (and myths) surrounding compliance before moving your workloads into cloud.
Myth: Who needs encryption?

Many organizations place too much emphasis on physical security when it comes to protecting their data. Physical tools like 24/7 monitoring and surveillance, locks, and restricted access are all great, but physical restrictions are only one line of defense. How do you protect your data from those who attempt to gain access via your system remotely?

Security breaches happen too frequently. According to the Ponemon Institute’s 2013 report, ‘The Post Breach Boom’, data breaches are increasing. Respondents indicated data breaches have increased in both severity and frequency in the past 24 months. Considering, it takes organizations an average of three months to discover a malicious breach and even longer to resolve it, that can have a detrimental impact on compliance as well as revenue. Of the 3,529 IT and IT security professionals polled, 63 percent indicate that knowing the root causes of breaches helps to strengthen their security posture. However, only 40 percent of the respondents believe that they have the tools, budget and expertise to identify the root cause of a breach. The impact of breaches goes beyond missed revenue — malicious breaches have an average cost of $840,000, while non-malicious data breaches average $470,000. The damaged reputation, lost productivity, and brand all have serious repercussions.

Recommendations:
• Understand encryption requirements of specific regulations
• Explore options for encrypting data at rest as well as data in motion
• End-to-end encryption services that ensure data is controlled all the way until end-user authentication are critical to passing regulatory compliance requirements
• Address how your organization handles other forms of communication such as instant messaging services, backups and storage

Myth: One vendor or product will make us compliant.

With the incredible interest in compliance in the cloud driving the market, many providers offer an array of “compliant-capable” products. However, it is not feasible that one vendor or one offering can address the many requirements of regulatory mandates. There is no ‘silver bullet’ towards the various standards. Instead of relying on a single product or vendor, you should implement a holistic security strategy that focuses on the ‘big picture’ related to the intent of the specific regulatory requirements you need to address.

As stated earlier, the customer, not the cloud provider, has the burden of compliance. There are many areas of gray within the current regulatory standards, but you don’t want to hinge your compliance status on a platform or device claiming to be 100% compliant.

Recommendations:
• Utilize industry guidelines and professional services to identify gaps in your current compliance and security posture
• Develop a feasible plan to address any gaps in compliance and establish an on-going Governance, Risk, and Compliance project to keep up with regulatory updates
• Work closely with cloud service providers or 3rd party vendors to understand where their responsibilities lie versus what you are responsible for
• Work with any 3rd parties to walk through an audit and understand how all elements of an audit are addressed
4

Myth: I only need to worry about the technology when considering compliance

The technology and corresponding infrastructure is only one piece to the compliance puzzle. A compliant organization must also address the people and process, as well as technology. An organization can develop and implement a rock-solid governance, risk and compliance posture, but unless employees and vendors follow the policies and procedures, they cannot achieve compliance.

Employees that do not maintain the proper security, do not handle mission critical information in the right way can open your organization up to security breaches. What kind of processes are in place to ensure the proper handling of data? What documentation do you have in place that supports the proper protection of your data? How are passwords protected? How is access to systems addressed?

Recommendations:
• Develop a good password policy and system for maintaining. Make sure all employees keep passwords confidential and do not write them down or share them with anyone. If employees are writing passwords on post it notes, you need a better password policy
• Educated employees, vendors, and partners on your security policies and expectations. Everyone working for your organization needs to follow and understand the procedures in order to ensure proper security
• Self audit. Perform internal audits to make sure all procedures are understood and being followed

5

Myth: I only have to care about compliance if I’m regulated

Everyone should care about the protection and integrity of data. Governance, risk and compliance programs and standards are not just about “regulated” industries, although those are the industries that are officially required to pay attention. Adherence to strict process and security policies allows even non-regulated organizations to protect data and avoid the risk of non-authorized access. A strong security posture mitigates risk associated with threats.

Recommendations:
• Develop and follow a “best practice” approach to security and data protection. Understand security standards and how they are best implemented. Understand your responsibilities versus those of your partners in meeting security requirements
• Challenge your service provider to demonstrate how they provide a secure environment

The impact of breaches goes beyond missed revenue — malicious breaches have an average cost of $840,000, while non-malicious data breaches average $470,000.
Compliance in the cloud: myth or reality

Conclusion

Thriving in the cloud
For any business, both regulated and non-regulated, the protection and integrity of data, is critically important. Organizations cannot sustain a negative finding from an auditor or a breach in security that could result in disrupted operations, fines, lost sales, or a damaged reputation.

At Sungard Availability Services, we continuously refine our infrastructure and processes to support our customer’s compliance requirements, best practices, and standards of our customers.

We have built our data center facilities and our Enterprise Cloud Services platform to address a broad range of IT industry standards and best practices for security, resilience, and performance. In addition to auditing our data centers for ISO 20001 and SSAE 16 Type II, we have achieved PCI-DSS compliance our Enterprise Cloud Services platform, giving us the ability to help customers ensure our customers are receiving the best in governance, risk-management, and industry compliance to enable them to thrive and grow.

For more information please visit our website at:
www.sungardas.com/cloud