EVOLVE IP
THE CLOUD STRATEGY COMPANY™

Cloud Brief

Understanding Compliance in the Cloud

Key considerations for ensuring PCI DSS, HIPAA, ITAR and FFIEC compliance with cloud partners.

Introduction

Increasing adoption of the cloud enables IT organizations to lower infrastructure costs and provider greater agility to support users and customers. However, the cloud also increases the complexity of IT security as IT organizations must rely on the cloud service provider's (CSP's) ability to secure data and meet critical compliance standards.

In order for the relationship to work, the client must verify that the cloud services partner not only contributes to its business goals, objectives, and future needs but also meets or exceeds the measures it takes to mitigate risks. In other words, CSP must provide assurances that it keeps client data safe from security threats. Clients should discuss their needs with their provider to determine how the CSP can best provide assurance that the required controls are in place.

Typically, companies try to bolt on security depending on how they've grown. As a result, there are often a lot of chinks in the armor. Often true security involves not just processes and controls, but a true culture change as well. Many companies do not have the IT resources or bandwidth to ensure the data they handle is truly secure.

The need to comply with security standards such as PCI DSS, HIPAA, ITAR and FFIEC often provides companies with a reason to truly examine their security process and culture. It's important to keep in mind that compliance in a cloud environment is a two-way street, meaning both the client and the CSP need to participate. Ultimately, it is the client company that is responsible for complying with industry standards as they are subject to the fines and in some cases criminal prosecution that may result from non-compliance.

It's important to establish and allocate responsibility for security controls at the outset of the relationship with a cloud provider. Typically, management of virtual components, applications and software differs based on the CSPs service and deployment model. As a general rule, SaaS provides the least amount of control for the client and IaaS provides the most but the details of what is included in a particular service model will vary between CSPs. In addition, cloud environments may be deployed over a private infrastructure, public infrastructure, or a combination of both. In any case, clear policies and procedures should be agreed upon between client and cloud provider for all security requirements, and clear responsibilities for operation, management and reporting need to be specifically defined for each requirement.

While many CSPs claim their cloud infrastructure is compliant, it's important to take a closer look. There are various third-party certifiers, as well as agencies and industry groups that offer best practices and guidelines. While each of the various security standards involve a mix of requirements in order to achieve certification, some security mechanisms remain constant regardless of the standard. A closer look at each of the standards, the challenges they present and the questions to ask, will help determine which CSP may best meet your particular compliance needs.

PCI DSS

The Payment Card Industry Data Security Standard (PCI DSS) is a proprietary information security standard for organizations that handle credit cards. This standard is required by the major credit card brands and administered by the Payment Card Industry Security Standards Council. The standard is intended to increase controls around cardholder data to reduce credit card fraud. Compliance audits must be performed annually, either by an external Qualified Security Assessor (QSA) or by a firm specific Internal Security Assessor (ISA).

As mentioned earlier, the more aspects of a client's operations that the CSP manages, the more responsibility the CSP has for maintaining PCI DSS controls. Cloud customers should be sure contracts, memorandums of understanding or SLAs define exactly who is responsible for securing which system components, processes, and documentation.

Potential PCI DSS Challenges

A cloud customer may have little or no visibility into its CSP's underlying infrastructure and the related security controls. For example, CSPs sometimes rely on other third-party companies such as storage providers to deliver their services. Obviously, these types of relationships add to the complexity of the PCI DSS assessment process and extend the number of facilities and services that must be compliant. So it's important to be aware whether your CSP has any third party relationships so you are sure you know where cardholder data is physically stored and when that location may change. For redundancy or high availability reasons, data could be stored in multiple locations at any given time.

Some organizations may turn to data-discovery tools to identify cardholder data in their environments, and to ensure that such data is not stored in unexpected places. However, running such tools in a cloud environment can be difficult and result in incomplete results. Ultimately, it can be challenging for organizations to verify that cardholder card data has not "leaked" into the cloud.

Another challenge for PCI DSS compliance in the cloud is that some virtual components do not have the same level of access control, logging, and monitoring as their physical counterparts. So it can be challenging to verify who has access to cardholder data processed, transmitted, or stored in the cloud environment. In addition, for some cloud deployment models, boundaries between client environments can be fluid. For example, a public cloud environment is usually designed to allow access from anywhere on the Internet.

Nonetheless, your CSP needs to take ownership of access controls and segmentation between clients and verify its security controls are effective. A CSP must provide adequate isolation between individual client environments, between client environments and the CSP's own environment, and between client environments and other untrusted environments (such as the Internet). The CSP is typically responsible for firewall rules, audit logging, documentation, reviews, etc.

At a high level, CSPs can be divided between those that have been validated as meeting a particular level of PCI DSS compliance and those that have not. The recommended practice for clients with PCI DSS considerations is to work with CSPs whose services have been independently validated as being PCI DSS compliant. You need to ask the right questions to ensure: your CSP has selected the right third-party organizations to partner with, provides the necessary controls and visibility into physical security measures to protect their service offerings and offers adequate access controls.

Questions to Ask Your CSP about PCI DSS Compliance

When interviewing CSP's, run through this checklist:

- Are you a registered and participating member of the CSA Security, Trust & Assurance Registry (STAR)?
- Are you contracted with the QSA and certified against all 12 sections of the PCI DSS?
- What does each of your services consist of exactly, and how is the service delivered?
- Are other parties involved in the service delivery, security, or support?
- Do you work with Tier 4 data centers?
- What physical security measures are in place at these data centers?
- Do you have environmental controls and back-up power units in place at all of your data centers?
- How are data center employee background checks performed?
- What do you provide with respect to security maintenance, PCI DSS compliance, segmentation, and assurance, and what am I responsible for?
- How will you provide ongoing evidence that security controls continue to be in place and are kept up to date?
- What will you commit to in writing?
- How is segmentation implemented?
- How are your PCI DSS assessments scoped?
- How are individual PCI DSS requirements validated?
- Which party will perform each validation activity?
- Can I tour the facility to personally meet your team and review the data center design and operating procedures?
- Can we do a full security audit including application penetration testing and vulnerability analysis?

HIPAA / HITECH

Similar to PCI DSS, the Health Insurance Portability and Accountability Act (HIPAA) requires healthcare (or "covered") entities to comply with specific security, privacy and breach notification rules for the storage and transmission of protected health information (PHI) including electronic data. These rules are further strengthened by the Health Information Technology for Economic and Clinical Health (HITECH) Act and defined by the Omnibus Rule to include IT service providers. Those who fail to adhere to HIPAA can suffer from huge fines climbing into the millions of dollars for major violations. As with PCI DSS, cloud customers and providers share the commitment to hosting an application in compliance with HIPAA-HITECH rules. However, there is not an official "HIPAA certification" or "HIPAA certified hosting" designation that can be achieved by CSPs.

PHI includes patient billing and administrative information; utilization and case management data, such as authorizations and referrals; patient health information gathered from or displayed on a website or portal; labs and other clinical data; medical record transcriptions and other kinds of patient reports; and e-mails and voicemails between physicians and patients and between physicians. Because cloud providers typically store, transmit, or process these kinds of electronic PHI (ePHI), they must also comply with HIPAA standards to meet HIPAA compliance. The same risk analysis, administrative, physical and technical safeguards, and ongoing due diligence apply just as much in the cloud provider's data center environment as in a healthcare entities' facility.

Additionally, since cloud providers are considered business associates of healthcare entities, they must have a Business Associates Agreement in place with the healthcare entity, as well as with any subcontractors (for example, backup vendors) that store, process or transmit ePHI of the covered entity or business associate. Cloud providers should help customers ensure that the services provided to them meet the requirements for the administrative, physical, and technical safeguards and standards set forth by the HIPAA, HITECH and Omnibus Acts. Cloud customers are responsible for configuring their applications, platforms, websites and portals in a HIPAA-compliant manner, for restricting and monitoring access to their ePHI data, and for enforcing policies in their organizations to meet HIPAA compliance.

HITECH and HIPAA are separate and unrelated laws, but they do reinforce each other in certain ways. For example, HITECH stipulates that technologies and technology standards created under HITECH do not compromise HIPAA privacy and security laws. A notable difference between the laws is section D of the HITECH Act which contains important provisions that impact covered entities in new and significant ways. Additionally, HITECH also provides newly updated civil and criminal penalties for non-compliance and establishes new requirements for security breach notifications. For example, it mandates that covered entities notify individuals if their PHI has been accessed by unauthorized individuals. Another difference between HIPAA and HITECH is with regard to the accounting of disclosures of PHI. HITECH requires covered entities to account for the disclosure of PHI even when it is done for healthcare treatment or billing purposes.

Potential HIPAA/HITECH Cloud Challenges

Beware of CSPs that claim to be "HIPAA certified." The U.S. Department of Health and Human Services (HHS), the entity responsible for HIPAA, does not require or formally recognize any HIPAA certification programs for CSPs. If a provider is claiming to be HIPAA certified, something is wrong.

Cloud computing is still in its earliest phases of implementation in the healthcare industry and the threat landscape is always changing. As a result, cloud customers may struggle to even understand what is required in order to be compliant, let alone how this may evolve as the threat landscape changes. HIPAA and HITECH are just two of the many regulations that healthcare organizations are required to comply with. Other regulations include PSQIA, Stark, SOX, PCI DSS, and CISP, each of which is stacked with complex requirements, controls and practices, and subject to constant change. Organizations also need to keep track of the variations in regulations from state to state. Understanding which requirements apply to covered entities, and how controls must be implemented can be extremely cumbersome. A cloud provider should be able to demonstrate a commitment to managing the complexities of the evolving compliance requirements and the ability to build and maintain a flexible technology infrastructure that can remain HIPAA compliant over the long term.

Healthcare entities and other organizations often implement more than one cloud solution from several cloud vendors for storage or application development. Each cloud service provider

and subcontractor is obligated to submit to a business associate agreement. This obviously extends the complexity of HIPAA and HITECH compliance for IT organizations.

Questions to ask your CSP about HIPAA and HITECH Compliance

Consider these questions as you speak with CSPs:

- Have you been independently audited against the Office of Civil Rights (OCR) HIPAA Audit Protocol?
- Was a third-party SOC 2 review of the cloud environment performed by an Independent Service Auditing firm?
- When was the HIPAA audit completed and by whom?
- Do you have a thorough BAA (Business Associates Agreement) with documented and communicated policies?
- How many of your clients are in healthcare and how do you facilitate HIPAA compliance with those clients?
- Do you have a Compliance Officer or a designated official responsible for HIPAA/HITECH?
- Do you have a structured security awareness program?
- Do you educate staff on your security awareness program?
- What is your incident response process?
- Do you encrypt data in transit?
- Do you offer secure offsite backups?
- Do you offer disaster recovery or business continuity solutions?
- Will my data be available 100% of the time?
- How do you keep multi-tenant data separate?

FFIEC

The Federal Financial Institution Examination Council (FFIEC) is a formal interagency body empowered to prescribe uniform principles, standards, and report forms for the federal examination of financial institutions and to make recommendations to promote uniformity in the supervision of financial institutions. Agencies on the council include the Board of Governors of the Federal Reserve System (FRB), the Federal Deposit Insurance Corporation (FDIC), the National Credit Union Administration (NCUA), the Office of the Comptroller of the Currency (OCC), and the Consumer Financial Protection Bureau (CFPB). FFIEC guidance, as expressed in its various publications serves as a blueprint for examiners to follow in conducting audits of financial institutions.

If a financial institution fails to comply, it could fail an audit and be prevented from entering new markets, introducing new products, or even merging with or acquiring another institution. The outstanding feature of the FFIEC guidelines from a cloud computing standpoint is the requirement that encryption be used in all online transaction processing (OLTP) done by financial institutions. The level of encryption must be sufficient to prevent unauthorized disclosure within a bank's internal networks and among shared external networks.

Financial institutions like organizations in other industries are moving some data to the cloud to take advantage of the recovery capabilities that the cloud offers. A cloud environment allows companies to recover data at different locations with reasonable recovery timeframes as well as a cost-savings as compared to backing up data within their own environment and restoring it to multiple locations if necessary. However, as previously mentioned, storage of data in the cloud may increase the frequency and complexity of security incidents. The guidance from the FFIEC focuses on data classification, segregation of data and how recoverable it is.

A financial institution's audit policies and practices may require adjustments to provide acceptable IT audit coverage of outsourced cloud computing. For example, it may be necessary to augment the internal audit staff with additional training and personnel with sufficient expertise in evaluating shared environments and virtualized technologies. In addition, in high-risk situations, continuous monitoring may be necessary for financial institutions to have a sufficient level of assurance that the cloud service provider is maintaining effective controls.

As with PCI DSS and HIPAA, the FFIEC guidance dictates that in a multi-tenant cloud deployment, in which multiple clients share network resources, there is increased need for data protection through encryption and additional assurance that proper controls are in place to restrict tenant access solely to their respective data. So, verifying the data handling procedures, the adequacy and

availability of backup data, and whether multiple service providers are sharing facilities are important considerations.

Similar to ITAR compliance requirement, a financial institution's ability to assess FFIEC compliance may be more complex and difficult in an environment where the cloud computing service provider processes and stores data overseas or comingles the financial institution's data with data from other customers that operate under diverse legal and regulatory jurisdictions. A financial institution should understand the applicability of laws and regulations within the hosting countries and the financial institution's ability to control access to its data. Contracts with the cloud-computing service providers should specify the servicers' obligations with respect to the financial institutions' responsibilities for compliance with privacy laws, for responding to and reporting about security incidents, and for fulfilling regulatory requirements to notify customers and regulators of any breaches.

Potential FFIEC Challenges

Unlike the healthcare industry, banking has not been an early adopter of cloud technology. Many organizations are still struggling to understand where their data is being housed and how it's going to be encrypted, both of which are crucial to FFIEC compliance. While CSPs are evolving to meet the needs of financial institutions there is still work to be done.

CSPs should provide contracts that specify their obligations with respect to the financial institutions' responsibilities for compliance with privacy laws, for responding to and reporting about security incidents, and for fulfilling regulatory requirements to notify customers and regulators of any breaches. The contract should also include provisions for logging, reporting, and vulnerability management.

In addition, the potential that data is not completely removed or deleted from the servicer's storage media at the conclusion of a service contract may pose higher risk in a cloud computing environment than it does in more traditional forms of outsourcing. Before entering into a third-party relationship, it is prudent to ensure that the cloud computing service provider can remove Non-Public Personal Information from all locations where it is stored

Questions to ask your CSP about FFIEC compliance

Consider these factors as you seek a cloud partner:

- Are you SSAE 16 compliant?
- What audit and control testing did you do as part of SSAE 16?
- How is data encrypted? Where does it sit? How is it protected?
- Can I have a copy of a recent set of results from a penetration test?
- Who owns the data I store in your cloud?
- How do you segregate each customers' data?
- If services are terminated, what happens to my data?
- Can you tell me about previous instances of tenant data compromises and loss?

Conclusion

The good news is that cloud security practices are oftentimes more rigorous than the security of the customers they serve. Obviously, your CSP's choice of authentication, authorization, and access control mechanisms is crucial, but a lot depends on process as well. Especially the process of establishing which party is responsible for which aspect of the various compliance regulations many industries are subject to. If possible, your company should always back up the data it's sharing with the cloud. It is really difficult to do real compliance. Some businesses try to fake it, covering multiple compliance topics, so conduct your due diligence before trusting your business data with a CSP partner.

For more information about The Evolve IP Compliance Cloud please visit: www.evolveip.net/compliance

About Evolve IP

The Cloud is no longer about buying individual services. It's now about building a strategy around multiple cloud services and integrating them together to make IT more efficient. Evolve IP delivers customized strategies and integrated services for both cloud computing and communications; solutions that are designed to work together, with your current infrastructure, and with the applications you already use in your business. Disaster Recovery, Contact Center, Unified Communications, Desktops, Infrastructure and Identity Management … Experience Cloud as a Strategy™