IDC ANALYZE THE FUTURE

IDC ANALYST CONNECTION

Sponsored by: Oracle

There are many advantages to migrating to the cloud. When selecting a cloud service provider, financial institutions must take into account security capabilities, service-level agreements, and compliance requirements.

Demystifying Cloud Compliance for Financial Institutions

May 2021

Questions posed by: Oracle

Answers by: Steven D'Alfonso, Research Director, Compliance, Fraud and Risk Analytics Strategies

Q. What are the top concerns and common misconceptions that arise when a financial institution (FI) assesses a cloud service provider (SP)?

A. FIs have indicated to IDC that security is a top concern of public cloud adoption. Interestingly, they have also identified security as a key benefit of adopting cloud. Despite the dissonance between those two sentiments, both statements can be true. Financial institutions will often acknowledge that cloud providers have better security technologies than the institutions themselves because the providers' sole focus is infrastructure and datacenter security. IDC believes that the stated security concerns arise out of a lack of trust rather than reflecting reality.

Financial institutions' top concerns include data exposure and breaches, malware, data in transit risk, and compliance risk. In addition, financial institutions are concerned with costs associated with migration and data transfer. Often, security risk managers are concerned with giving up control for the management of risk, security, and compliance.

There are common misconceptions related to cloud security and compliance. Security staff often mistakenly have an expectation that the cloud SP will follow the bank's internal policies. In reality, the cloud SP will apply its own best practices across its cloud infrastructure. The cloud SP's application of its security controls will provide a consistent, scalable, secure, and compliant environment. This environment is often in stark contrast to the disparate security technologies and dashboards that a bank's security team must manage for its on-premises infrastructure. This approach will provide the bank with a simplified way to monitor security controls. A related misconception is that bank security staff may believe that security compliance is entirely provided by the cloud SP. In reality, the cloud SP will provide controls under a shared responsibility model.

Further, many have a perception that regulators will not view moving important workloads to the cloud as prudent or that FIs must obtain a regulator's approval before engaging a cloud SP. Neither perception is accurate. There has been a rapid shift to the cloud, particularly of critical workloads across the financial services industry. In addition, regulators would not provide approval for an FI to use a cloud SP. However, regulators do require that an FI perform and document appropriate due diligence and put in place processes for ongoing monitoring of the cloud SP relationship.

Q. What is a financial institution's typical process for evaluating a cloud SP?

A. Financial institutions are required to conduct and document a prudent risk assessment of any service provider — particularly one as critical as a cloud SP that is providing critical infrastructure and security technologies. An FI will likely have a standard policy on performing a third-party risk assessment, but how should an FI specifically evaluate a cloud SP?

An FI should develop a security questionnaire to query the cloud SP about security elements that are important to the FI. As part of that questionnaire, an FI should assess how the cloud SP tracks regulatory changes that would be relevant to the FI. The cloud SP should be able to provide a description of its regulatory intelligence and change management processes. Likewise, a cloud SP should provide evidence of compliance certifications, such as the Payment Card Industry Data Security Standard (PCI DSS) or the System and Organization Controls 2 (SOC 2). For regulatory requirements for which there is no certification, a cloud SP may provide a white paper or some other content as evidence of compliance.

Beyond compliance-related inquiries, FIs should interrogate the cloud SP's transparency related to risks that will affect them. Key risks may include employee and management turnover and depth of industry-related experience within the ranks of their staff, as well as the cloud SP's experience in working with FIs. Additionally, the cloud SP should provide guidance on infrastructure reliability supported by service-level agreements (SLAs), the ability to scale its infrastructure, the methodology used to quantify and manage risk, the extent to which third-party partners are used, and the cloud SP's openness to allow the FI the right to audit.

Q. How does utilizing a cloud SP reduce a financial institution's level of responsibility for security- and compliance-related activities within a shared responsibility framework?

A. A financial institution can never avoid or transfer liability for its compliance risk; however, a key benefit in using a cloud SP is the transfer of certain compliance-related activities. When an FI uses a cloud SP, it passes the responsibility for most physical and infrastructure controls to the cloud SP. The cloud SP assumes responsibility for the expense and effort of maintaining infrastructure security compliance as well as related disaster recovery planning and testing. The FI and the cloud SP will operate together under a shared responsibility model. The FI's level of responsibility declines based on the cloud deployment method selected. An infrastructure-as-a-service (IaaS) model transfers the least amount of responsibility to the cloud SP; a platform-as-a-service (PaaS) model transfers more responsibility to the cloud SP, and a software-as-a-service (SaaS) model transfers the most responsibility. The cloud SP should outline in specific detail its responsibility under the applicable regulations that affect the FI.

For example, the PCI DSS is a very rigid security standard with 12 requirements and multiple subrequirements. The cloud SP and the FI must clearly agree on responsibility for compliance with each element of the standard; responsibility can be delineated between the cloud SP or the FI or can be the joint responsibility of both. The cloud SP should briefly describe what it does for each element of the requirements where it has full or partial responsibility. For example, under PCI DSS 7, there are multiple requirements related to restricting access to system components and cardholder data. The cloud SP should describe how it controls access to the underlying infrastructure for authorized personnel, while the FI is responsible for managing and restricting access to authorized users. In addition, the cloud SP should clearly outline, in its reporting, the roles and responsibilities between the user and the cloud SP.

Q. How does a cloud SP provide assurance over and manage its area of the shared responsibility?

A. Financial institutions' IT managers and line-of-business managers want to know how their data is protected. Senior management and board members have a keen interest in how a cloud SP provides assurance that it will not only protect the FI's data but also help the organization meet increasingly stringent and complex security and compliance requirements.

There are several ways in which a cloud SP can provide assurance to its FI customers related to its responsibilities under the shared responsibility framework. At a minimum, a cloud SP should assist the FI in developing a mapping of all security risk controls to specific regulatory requirements based on the regulatory jurisdictions in which its customers operate. Second, a cloud SP should provide a right to audit for all externally facing regulatory alignment documents such as white papers and industry best practices. Third, a cloud SP should provide independent audit and compliance program certifications such as PCI DSS, SOC 2, and ISO to ensure adequacy of its controls.

Q. What are financial institutions' best practices to satisfy financial services regulators' requests when using a cloud SP?

A. Regulators, regardless of the agency or jurisdiction they represent, will seek to understand and be comfortable with an FI's third-party risk assessment process. This is especially true for vendors that provide critical technology and services or have a responsibility to protect consumer data.

As a best practice, an FI should have a clear and comprehensive description of its risk assessment process; the stakeholders involved; the request for proposal (RFP) and the process used to distribute it; and the processes for collecting responses and analyzing the collected information. A description of the process for vendor due diligence and selection must also be included. Further, SLAs with the vendor should be assessed, including the methodology for monitoring compliance with the SLAs and the risk associated with SLA noncompliance.

Another required practice for many FIs will involve providing notification of the existence of a third-party service relationship to certain regulatory agencies within a specific period. For example, in the United States, the FDIC and the SEC require notification within 30 days of contract signing. Typically, the notification will require a description of the services being performed. Using the documentation created during the risk assessment process will be an efficient way to relay the nature of the relationship.

While there are certain reporting requirements when using a cloud SP, there are other reporting requirements that are ongoing, such as New York's cybersecurity regulations for financial services companies that require annual certification confirming compliance. A cloud SP can simplify an FI's security ecosystem by providing a consolidated view of controls through a single dashboard. The consolidated view can help streamline efforts to meet regulatory reporting requirements as well as senior management and board member reporting requirements.

About the Analyst

Steven D'Alfonso, *Research Director, Compliance, Fraud and Risk Analytics Strategies*

Steven D'Alfonso is a Research Director with IDC Financial Insights responsible for compliance, fraud, and risk analytics strategies. His coverage area includes research on technology solutions aimed at solving key issues facing financial institutions around GRC regulations, financial crime, and risk management.

MESSAGE FROM THE SPONSOR

Oracle Cloud Infrastructure's built-in security and compliance solutions protect your most valuable data in the cloud. Oracle's approach leads with security first, built on our decades of experience securing data and applications. Oracle Cloud Infrastructure delivers a more secure cloud to our customers, build trust, protect their data and:

- Strengthens security posture and reduces risk
- Reduces complexity and prevents human error with automated security tools
- Provides continuous protection with always-on encryption and continuous monitoring

Visit the Oracle Cloud Infrastructure security webpage to learn how Oracle Cloud Infrastructure is designed to protect our customers' data.

IDC Custom Solutions

IDC Research, Inc.
140 Kendrick Street
Building B
Needham, MA 02494
T 508.872.8200
F 508.935.4015
Twitter @IDC
idc-insights-community.com
www.idc.com