Microsoft

Trustworthy Computing

CISO Perspectives: Compliance in the cloud
August 2013

CISO Perspectives

CISO Perspectives provides insight into some of the key questions facing information security professionals today. These articles are based on interviews and discussions with chief information security officers (CISOs) and information security and risk specialists from Microsoft and the industry.

This article will discuss some of the key challenges, success factors, and potential solutions regarding compliance in the cloud.

Compliance in the cloud

The shift to cloud computing provides an organization with the ability to focus on its core value proposition and allows for far greater flexibility and capital cost reductions. This shift often changes the way that organizations operate, and presents unique challenges to information security professionals.

New operating paradigms demand consideration of different risk factors and additional compliance concerns. For this article we interviewed several information security and risk specialists and surveyed approaches that work for them with regard to the shift to cloud computing.

Location

The inherent flexibility in cloud computing allows an organization to move data, applications, and certain operations to a cloud provider. The fact that such an organization no longer houses data and related functions in its own physical structure leads to the

concern that many current legal frameworks, contractual requirements, and regulatory demands are trailing technological developments in several areas. One such area focuses on national geographical boundaries, such as the EU Data Protection Directive 95/46/EC.[1] Simply put, many laws demand that data shall not cross borders or be shared with other environments in a different national area. (Some laws allow data to cross borders or reside in different locations if followed by a strict pre-approval process.)

"The biggest impediment is clear visibility of where the data is and how it is separated from other data." Thomas Doughty, Vice President and Chief Security Officer of Prudential Financial.

"*Telus Communications had to insist that* [certain] *data must remain within Canada."* Kenneth Haertling, Vice President and Chief Security Officer of Telus Communication.

When geographic location of data is a question, a best practice is to have an open dialogue with the cloud service provider to understand the type of data being stored, where the service provider will process and store the data, and who will have access to it.

Risk assessment

Another challenge is the general requirement for audit, assessment, and verification, such as the one inherent in the Payment Card Industry Data Security Standard (PCI DSS).[2] This requirement generally means that much of the work around audit, assessment, and verification must be performed by each individual data-owning organization, to satisfy their own unique risk acceptance criteria and the unique regulatory environment that applies to the organization. One approach is to apply the process described in the International Organization for Standardization / International Electrotechnical Commission 27001:2005 (ISO/IEC 27001:2005) standard.[3] This provides an industry accepted method to managing information security risk.

As a way to help organizations recognize and mitigate cloud-specific risks, the *Cloud Security Alliance (CSA)* developed a controls framework called the *Cloud Controls Matrix (CCM).* The CCM provides organizations with a standards-based framework that incorporates cloud services.

The goal of the CCM is to reduce the risk of an organization failing to consider important factors when selecting a cloud provider. It provides visibility into how participating cloud providers operate, particularly in the areas of security and compliance controls. The CSA's

---

[1] EU Data Protection Directive 95/46/EC http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:31995L0046:EN:HTML

[2] Payment Card Industry (PCI) Data Security Standard (DSS)https://www.pcisecuritystandards.org/

[3] the International Organization for Standardization / International Electrotechnical Commission 27001:2005 (ISO/IEC 27001:2005) standard http://www.iso.org/iso/catalogue_detail?csnumber=42103

Security, Trust & Assurance Registry (STAR)[4] contains detailed responses to more than a hundred self-assessment questions that were posed to cloud service providers about cloud security controls.

The purpose of STAR is to reduce much of the effort, ambiguity, and cost associated with getting the most relevant questions and information about cloud providers' compliance, security, and privacy practices. Access to the registry is free, and it helps cloud customers compare services from different participating cloud providers.

If you are considering using a cloud service provider, check to see whether they have submitted answers to the CSA STAR so you can learn more about their security and privacy practices and compliance-supporting controls. If the cloud provider has not submitted a self-assessment to the CSA STAR, you can use the free framework provided by the CSA to ask the cloud provider the questions that are relevant to your organization. Understanding how your cloud provider manages security and privacy to support your compliance efforts can help to minimize potential future problems.

By referencing the CSA's cloud controls matrix through STAR, organizations can reduce or eliminate the cost of engaging outside expertise to select an appropriate cloud provider and rely instead on combined efforts that represent years of expertise in the field.

Due diligence

A key consideration for CISOs is what data to move to the cloud and what data to keep on-premises. In our conversations with CISOs we identified two key approaches for identifying and reducing risk and ensuring compliance in the cloud.

The first approach is to use existing due-diligence processes, including the identification of the process owner, the data owner, and the risk elements, when deciding what to put in the cloud.

Thomas Doughty adds "*Due diligence is a central requirement, while impetus* [to move to the cloud] *is decentralized*." This view leads to an increased focus on monitoring and documenting the due diligence process.

This increased focus is a challenge for CISOs, because the pace and frequency of due diligence processes continues to increase as organizations discover the many benefits of shifting additional workloads to the cloud. These benefits include faster provisioning, increased capacity, increased flexibility and cost savings, to name a few. In addition, many

[4] CSA's Security, Trust & Assurance Registry (STAR) https://cloudsecurityalliance.org/star/

cloud consumers say that they believe the level of security they get from their cloud provider is better than that of their on-premises operations.

A greater challenge exists for CISOs in industries that are highly regulated: "*Companies subject to tighter regulations have more to consider when they move to the cloud,"* says Mark Estberg, Senior Director, Global Foundation Services at Microsoft. The STAR framework, which Microsoft participates in, allows an organization to follow a well-documented process, including a check list that helps them more thoroughly document their due-diligence process.

A different approach that's used by other CISOs we spoke with stems from an organizational demand for rapid provisioning times: *"How do you come up with the right security controls and still keep provisioning time to less than 24 hours?"* asks Kenneth Haertling. He suggests that there might be a need, at times, to build new, virtualized security frameworks that use new and potentially virtualized controls. After all, as John Meakin, Chief Information Security Officer, Royal Bank of Scotland, says, *"Security implications vary wildly across different implementation schemes"*.

Contracts and agreements are important vehicles for clarifying security responsibility and risk assignments between organizations that use cloud services and cloud providers. The STAR registry allows cloud service providers to provide customers with visibility into their security, privacy, and compliance commitments and capabilities.

Whatever the approach, all the experts we spoke with agreed that offering risk-based weighting and consideration is a better approach than treating compliance with a regulatory approach. As Kenneth Haertling succinctly put it: *"Is this [the risk profile] really a risk profile you can accept?"*

For more CISO Perspectives, visit http://aka.ms/cisoperspectives