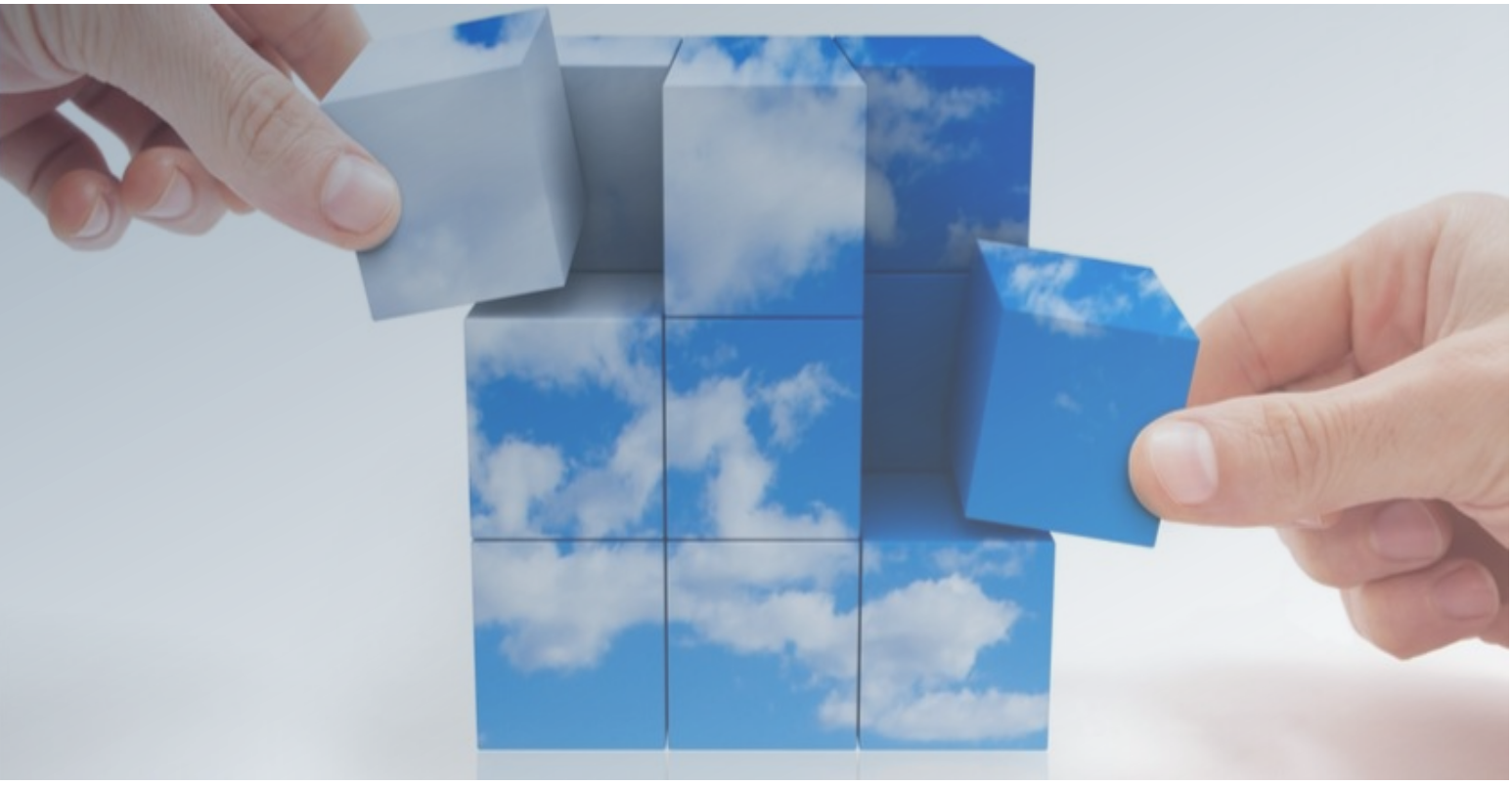
# Adopt a Shared Responsibility Model for Complete Cloud Data Security

## FIVE KEY CONSIDERATIONS TO BUILD A MORE POWERFUL CLOUD DATA SECURITY INFRASTRUCTURE

It's been a troubling year for everyone in business. One of the stressors has been the explosion of people needing to work remotely in order to support business continuity. Thankfully, remote working is possible due to technical advancements in cloud migration and virtualization. However, it raises the issue of whether this data flowing to the cloud from a diversity of remote sources is fully protected and secure.

Data security in the cloud, in essence, operates with a virtual line of demarcation. Cloud providers like Azure handle the infrastructure - hardware security, as well as the security of compute, storage, database and networks. Once data arrives in the cloud, however, its fate is in the hands of the customer.

A powerful data security strategy understands this duality and embraces a *shared responsibility model.* Here, the cloud provider is responsible for the secure infrastructure of the cloud. The customer on the other hand takes primary responsibility for protecting user data, platforms, applications, identity access management, as well as the operating system, network, firewall configuration and other components.



## FIVE PRACTICES FOR BETTER CLOUD DATA SECURITY

Migrating to the cloud has offered tremendous advantages to organizations in terms of scalability and support for exponentially larger data workloads. The cloud also delivers greater options for business continuity and data recovery when a disruptive event occurs. This year has proven working remotely via the cloud can also help with economic survival. The expectation is that remote working will remain a more dominant factor in the workforce even as businesses transition back to a 'new normal' environment. In fact, Twitter and other companies have announced permanent work-from-home options.

With this shift to more remote working, it is a good time to think about data protection in the cloud and what organizations need to do to better shore up defenses against costly data breaches and/or data loss. Productivity via the cloud, whether remotely or on-site, depends on executing the best possible data security strategy.

Here are five key considerations to build a more powerful cloud data security infrastructure:

1. ***Develop a comprehensive plan.*** Take another look at your cloud provider(s) agreement and identify where they can help you to improve security, and where you may need to add technology and solutions to your overall strategy. In the shared responsibility model, you need to know where the cloud provider's agreed upon responsibility ends and yours begins. Then you can better integrate your provider's security controls into your overall security strategy.

   Using this greater detail from your cloud provider, you can develop a plan to include:

   - An assessment of new assets that need to be budgeted for. i.e., threat detection and response software, automated patching updates, swapping out high-risk legacy hardware for more secure devices.
   - Forecasting of your organization's potential workforce shift to determine the longer-term effects and needs of remote working and related devices.
   - Alignment between IT, security and HR on a timetable to execute security improvements. This may entail giving employees new devices, training on new software and security protocols and budgeting priorities.

2. ***Understand your compliance requirements.*** Reassess your compliance needs and then identify and use the tools your cloud provider makes available to help you monitor and prove compliance. Azure Policy is one tool offered to centralize compliance data for quicker auditing and tracking. It enables policy creation at the core of Azure and supports ongoing enforcement by setting guardrails on resources.

3. ***Know your risk tolerance.*** Fully understand what data you need to secure and what risks you are willing to accept for that data. Map out your data risk tolerance by data type and the strategy you will implement to protect it. By classifying your data based on its sensitivity such as personal identifiable information (PII) or HIPAA regulated health records, you'll have a strong idea of which data sets you need to best protect.

**ipm SUCCESS BRIEF**

IPM accelerated cloud adoption for a **U.S. based Insurance Company** following findings from a detailed security assessment.

**Remote working will remain a more dominant factor in the workforce even as businesses transition back to a 'new normal' environment.**

4. ***Design and implement technology controls.*** Organizations can use managed services and solution providers to help design and execute a cloud security plan and help navigate the complexities of cloud data security protocols. This plan can include application and access controls needed to further ensure sensitive cloud data is not compromised and can be recovered. Given the expected increase in remote users, it is imperative to limit access to applications in accordance with work productivity needs. Phishing attacks and malware introduction into networks are a common result of inadequate control at the device endpoint.

5. ***Develop a continuous monitoring program.*** Security threats and risks function in a fluid environment. This demands regular assessment of the controls in place and the agility to adapt as situations change. It includes evaluation of your threat response system, secure onboarding and offboarding of employees' devices, timeliness of all patching updates and due diligence in making use of updated security controls across all major programs.

## TAKE THE TEAM APPROACH TO DATA SECURITY

When developing your cloud security plan, it's important to recognize each of the differences you need to account for compared to the plans applied to your on-premises data. Security plans that were first built to apply controls for on-premises data will need to evolve to support your new cloud model. Ask where each control falls in the new shared responsibility model so that you can appropriately document where the control is being met. Trust an expert security consultant to help you through this process because even with the best technology, there is no replacement for experience.

The shared responsibility model can also be looked at as shared collaboration. But be sure that you have everyone you need on your security team to be successful because every change you make has implications. By including an expert IT security consultant on your team, along with your cloud providers, solution providers, enterprise IT and security staff, you'll avoid the gotchas and know in advance how changes may impact your environment, and your security posture.

After all, everyone sharing responsibility for security wants the same thing: a productive, secure environment in which workers and enterprises thrive. If this year has taught us anything, it is teamwork is the path to economic survival. Looking ahead, improved cloud security, better access controls and continued vigilance will be the foundation for success.

***Safeguard Your Business without Compromising Productivity***

Read how to optimize security and productivity to realize better business outcomes.

*Download PDF*

IPM is a US-based IT Consulting partner with 35 years' experience planning, deploying and supporting all aspects of IT infrastructure for our customers. We enable customers to transition to the cloud by selecting the right cloud model for their goals. We partner with best of breed technology partners to help organizations collaborate and be more productive, wherever they are working. Security is the cornerstone of all of the solutions we develop with a special focus on highly regulated industries and compliance. With strong partnerships and certification at the highest levels with partners including Microsoft, DellEMC, Citrix, VMware and Amazon, we have the ability to create and deliver secure IT solutions to meet your business needs and project budgets.

ipm

151 W. 30th Street, 8th Floor | New York, NY 10001
646.421.2801 | www.ipm.com | services@ipm.com