KPMG

How to manage five key cloud computing risks

kpmg.ca

Sai Gadia is a leader in KPMG LLP's (KPMG) Emerging Technology Risk Services practice focused on Cloud Risk Consulting services. He has almost 20 years of experience helping enterprises deliver efficient and effective IT and risk management results. He is the architect of KPMG's Cloud Governance and Controls Assessment (CGCA) global framework, which provides KPMG's clients with the tools, resources, and data for cloud computing governance initiatives. Sai also leads KPMG's innovation efforts to research and analyze disruptive technologies such as blockchain.

Contact: sgadia@kpmg.com

How to manage five key cloud computing risks

Cloud computing is the top technology that is disrupting enterprise and consumer markets around the world, thanks to its ubiquity and widespread usage. Within just a relatively short period of time, cloud computing has accelerated in implementation, becoming a key part of IT and business strategy. In the near future, cloud computing will continue to enable the integration of emerging technologies and shape new business models as a strategic advantage.

As the industry matures, there has been a rapid expansion in service offerings. The large cloud service providers (CSPs) that entered the market with SaaS offerings, e.g., Salesforce.com, are integrating backwards into PaaS, with Salesforce.com's PaaS offering. Likewise, Amazon Web Services (AWS), which started off largely as an IaaS provider, now offers not only PaaS but also SaaS solutions. From a risk perspective, there is some gradient across the different service models, but the deployment model is where the risks vary widely.

However, while cloud computing provides many benefits, at the same time, it introduces major risks on several crucial fronts that need to be governed and managed by user organizations. Well-managed organizations must understand and mitigate these risks to better leverage their cloud computing initiatives. Five major risks are:

1. Data security and regulatory
2. Technology
3. Operational
4. Vendor
5. Financial.

"Uber, the world's largest taxi company, owns no vehicles. Facebook, the world's most popular media owner, creates no content. Alibaba, the most valuable retailer, has no inventory. And Airbnb, the world's largest accommodation provider, owns no real estate. Something interesting is happening."

— Tom Goodwin, senior vice president of strategy and innovation at Havas Media

Why companies look up to the cloud

Organizations can realize significant benefits by leveraging cloud computing in their technology and business processes, namely, scalability, flexibility, and lower capital investment.

There are many small and medium enterprises that have been using the cloud exclusively and have no on-premises servers and related assets. Interestingly, one of the first large companies to shut down its last data center was Netflix in 2015.

However, organizations need to be careful. Much like a failed investment or a poor business decision, not knowing or miscalculating the far-reaching implications of such disruptive technology can leave organizations irrelevant and struggling to keep up.

In the last few years, the popular notion was that public cloud is inherently risky, and risk management for cloud computing is primarily the responsibility of CSPs. However, with CSPs increasing their focus on risk management in the last few years, they have thrived. According to a Cloud Security Alliance survey, *The Cloud Balancing Act for IT: Between Promise and Peril*, about 65 percent of IT leaders surveyed think that the cloud is as secure or more secure than on-premises software.

This fact is also reinforced by industry surveys, including KPMG's 2015 – 2016 Higher Education Industry Outlook survey, where a majority of higher education administrators are comfortable using the cloud and data protection assurance provided by CSPs. In fact, one of the greatest barriers to adoption has become the lack of clear understanding of the shared-responsibility model under cloud computing.

According to the same survey from Cloud Security Alliance, the top barrier to stopping data loss in the cloud is a lack of skilled security professionals. It is relatively easy for untrained public cloud users to expose their organization to significant direct risks such as financial loss or indirect risks such as loss of reputation.

That is why each organization must understand and mitigate the risks associated with cloud computing.

According to a September 2015 Gartner report, "through 2020, 95 percent of cloud security failures will be the customer's fault."

Clouds are secure: Are you using them securely? Gartner, September 22, 2015

KPMG

Five key cloud computing risks

Let us look at five different types of risks and how they apply or vary by cloud deployment models.

Data security and regulatory risk

Data security and regulatory risk can be associated with loss, leakage, or unavailability of data. This can cause business interruption, loss of revenue, loss of reputation, or regulatory incompliance.

Regulatory risk is associated with noncompliance with various national/geographic regulations, industry, or service-specific legal and regulatory requirements such as the Gramm-Leach-Bliley Act (GLBA), Sarbanes-Oxley Act (SOX), Health Insurance Portability and Accountability Act (HIPAA), or the European Union (EU) Data Protection Directive.

One of the most significant new regulatory schemes is the EU General Data Protection Regulation (GDPR) that was recently adopted by the European Parliament, which introduces extensive requirements for any organization doing business in Europe or storing data about EU residents. This requires a new level of tracking data and related consent which requires special considerations when using cloud computing. The consequences for non-compliance are dire, including fines up to 4 percent of global annual turnover/revenues or €20 million, whichever is higher.

According to the Cloud Security Alliance's *Cloud Adoption in the Financial Services Sector* survey in March 2015, data protection is a preeminent security concern for the financial sector moving to the cloud. In particular, data protection standards and relevant laws were "top of mind" for survey respondents. Industry regulation drives compliance requiring financial institutions to implement specific security measures to consider migrating to cloud services. At the top of the list were data protection (75 percent), corporate governance (68 percent), PCI-DSS (54 percent), and national regulations (47 percent).

According to the Cloud Security Alliance survey *The Cloud Balancing Act for IT: Between Promise and Peril*, the primary obstacle to moving systems of record to the cloud noted by 67.8 percent of companies was the ability to enforce their corporate security policies. Cyber attacks are not the only concern companies have when it comes to moving their systems of record to the cloud—61.2 percent of companies see compliance with regulations as a major barrier to cloud adoption.

For a private cloud, the data risks do not change as much compared to traditional computing, as organizations have better control and understanding on how various government rules, laws, and regulations apply to them. Further, there is no comingling of data across multiple cloud users. However, additional risks apply to private external cloud:

- Lack of visibility into controls over initiation, authorization, recording, processing, or reporting of transactions
- Unauthorized data access by a service provider and/or less control over who sees what data—e.g., the service provider might be using contractors or third parties.

For a public cloud, the data risks associated with the private external cloud apply. Additionally, the following risks apply:

- Data leakage or access risks due to multitenancy/shared infrastructure between different organizations
- Lack of flexibility over data protections mechanisms, such as encryption and implementation of specific controls by data type. Different organizations might have different encryption and control requirements, and a public cloud provider may not be able to customize their infrastructure or provide customers the control over encryption keys. This is particularly relevant in case of solutions delivered under SaaS and PaaS models.

Our view on how to manage this risk: *In KPMG's experience, leading organizations have mature data protection and regulatory compliance programs staffed with talented individuals who have sufficient authority and clear responsibilities. Such organizations also leverage leading third-party or homegrown automated tools and continuously improve their capabilities.*

Technology risk

Technology risk can be associated with constantly evolving technologies and lack of standardization in how they integrate or interoperate. Technology risks could lead to costly rearchitecture efforts for adoption or integration with new technology.

For a private cloud, a technology risk could be:

- A constantly evolving technology landscape that might require the organization to upgrade or rearchitect its computing resources and retrain its technology support staff
- A potential for human error due to the number of configurable points and frequency of deployments.

For a public cloud, the evolving technology risk might be lower, as service providers would have to worry about upgrading/rearchitecting their computing resources and retraining the support staff. However, in a public cloud, other technology risks might be introduced, such as:

- Constantly evolving technology features might require the organization to rearchitect its cloud applications much more frequently compared to mature technologies. We have noted several situations where the organization's cloud architecture was defined before advanced security and control features were introduced, and management had not updated the cloud architecture to take advantage of these advanced capabilities offered by the vendor for free or at a nominal cost. For example, AWS introduced hundreds of enhancements to its cloud services in 2015
- Limitation on what and how much an organization can customize (infrastructure, platform, or applications), depending on which service model the organization is using
- Due to the use of multiple cloud providers and potentially hundreds to thousands of server instances in the cloud, CSP dashboards for cloud management might provide limited visibility. Each public cloud solution vendor typically offers its own administration console. With the rapid rise in the number of SaaS solutions in use at organizations, this is increasingly becoming a daunting task due to the lack of a single/consolidated management dashboard.

Our view on how to manage this risk: *In KPMG's experience, leading organizations recognize that cloud will require the role and responsibilities of in-house IT professionals to evolve and are making the necessary investment to train individuals and encourage the adoption of innovative technology. In the process, they are also increasing alignment with the vision and business of the organization.*

Operational risk

Operational risk can be associated with execution of IT services and tasks that the business relies upon. Migration to cloud has also brought to the forefront a new approach called *DevOps,* where development and operations responsibilities are merging. This allows deployment times to be cut down to days rather than weeks or months. It can have an impact on IT operations, and development teams will need to be trained in cloud deployment and systems management in the cloud, although it will be less about managing IT hardware and network.

For a private cloud, some of the operational risks are:

- Suboptimal service reliability and uptime since it might be cost-prohibitive for an organization to employ leading technology for cloud computing that could provide better service reliability and uptime.

For a public cloud, some of the operational risks are:

- Lack of customized service level for different IT services, which might require the organization to choose a proximate acceptable service level, including those related to application availability and disaster recovery
- Lesser control over quality of service
- Reduced control on critical application availability and disaster recovery.

Our view on how to manage this risk: *In KPMG's experience, leading organizations have also adopted the agile development methodology as well as the DevOps model for cloud deployments. Such organizations are now using the learning from pilot projects to shape the enterprise development methodologies of the future.*

Vendor risk

Vendor risk comes from leverage or association with vendors. Unforeseen vendor circumstances such as bankruptcy, lawsuits, SEC probe, or any other act of defamation for the vendor could significantly damage an organization's reputation and goodwill. This risk would apply to private external cloud and public cloud computing scenarios due to association with and reliance on service provider(s).

Due to the ease of access to IaaS there has been a mushrooming of innovative SaaS start-ups—some with unique solutions that meet needs that the traditional vendors had left unaddressed. Some of these vendors might not be sustainable for large organizations looking to exchange increasing amount of data while meeting stringent control requirements.

With the use of third parties for cloud computing, there is dependence on service providers to ensure they have adequate controls in place to comply with various laws, rules, and regulations:

- According to Skyhigh Networks' Cloud Adoption Risk Report, Q4 2015, there are over 16,000 cloud services available, and the average organization now uses 1,154 cloud services
- According to the Wall Street Journal's CIO Journal blog, "Cisco Systems Inc.'s Vice President and Chief Information Security Officer Steve Martino discovered 607 cloud services when the company began to use a security broker. About half of those were cloud services that Cisco already had a relationship with so it meant investigating a few hundred other services, said Mr. Martino, speaking at the RSA conference"
- A lot of organizations are grappling with Shadow IT, which magnifies the organization's risk due to use of public cloud solutions that have not been vetted from a risk lens. According to Skyhigh Networks, fewer than 1 in 10 providers store data at rest encrypted, and even fewer support the ability for a customer to encrypt data using their own encryption keys.

Our view on how to manage this risk: *In KPMG's experience, leading organizations take a long-term strategic view to manage their relationships with CSPs. Such companies are actively engaged and are shaping the road map of CSP's service offerings to help accelerate their move to cloud while being offered better tools by the CSP to efficiently manage risks.*

Financial risk

Financial risk can be associated with overspending and loss of revenue. According to the North Bridge and Wikibon's Future of Cloud Computing Survey in December 2015, the cost of cloud services is three times as likely to be a concern today versus five years ago.

For a private cloud, the financial risks are:

- Underestimating initial cost to build a private cloud
- Continuing to carry the capital expenditure related to hardware and software.

For a public cloud, the financial risks are mainly related to the variable nature of costs—that is, running up the cost of using public cloud due to poor planning and requirements from the business. As an analogy, think electricity. A consumer may use an electric heater all day during winter without knowing the cost incurred until the electricity bill shows up at the end of the month. Managing cloud costs needs a level of focus, skill, and tools that were not required in the past.

Our view on how to manage this risk: *In KPMG's experience, leading organizations have assigned individuals with the responsibility for budgeting, tracking, and managing cloud costs. Such organizations are also making use of advanced third-party analytical tools available to manage cloud costs.*

Summary: Five key risks of cloud computing

Risk dimension	Deployment model		
	Private internal	**Private external**	**Public**
Data and regulatory	– Similar to traditional computing	– Data leakage from a malicious insider – Unauthorized data access by the service provider – Lack of visibility into cloud operations and ability to monitor for compliance – Dependence on a service provider to ensure adequate internal controls	– Data leakage from a malicious insider – Unauthorized data access by the service provider – Data leakage across shared infrastructure – Lack of flexibility for encryption, data control – Lack of visibility into cloud operations and ability to monitor for compliance – Dependence on a service provider to ensure adequate internal controls
Technology	– Evolving technologies could require rearchitecture and/or retraining	– Evolving technologies could require rearchitecture and/or retraining	– Limitations on customization of service offerings – Compatibility with other cloud providers – Limited choice or technology and related tools
Operational	– Service reliability and uptime	– Service reliability and uptime	– Lack of service-level customization – Control over quality – Control over application availability and disaster recovery
Vendor	– Similar to traditional computing	– Association and reliance on a service provider	– Association and reliance on a service provider
Financial	– Underestimating initial costs – Continuing to carry capital expenditures of hardware and software	– Underestimating initial costs – In some cases, continuing to carry capital expenditures of hardware and software – Contract modification or cancellation fees – Additional overhead of managing service provider(s)	– Contract modification or cancellation fees – Runaway costs from poor planning and periodic monitoring – Additional overhead of managing service provider(s)

As we have seen in the chart on the previous page, contrary to popular opinion, not all risk management is the responsibility of CSPs. On the contrary, most of the risks are to be managed by cloud users via various risk management mechanisms, including leveraging the tools offered by CSPs. Leading CSPs understand the importance of controls and continue to invest heavily in this area, including providing automated tools to cloud users to manage their risks.

Case study No. 1: Obtaining greater value from cloud computing

Industry: Data and technology services

At a large data and technology services company, cloud (infrastructure, platform, and software) services were being procured without the necessary governance and oversight, leading to significant risks to business operations and regulatory requirements. KPMG performed cloud discovery leveraging automated tools to provide the client with a broad view of cloud usage as well as the risk exposure associated with cloud use within the enterprise. For a selection of CSPs, KPMG utilized its CGCA framework and provided the client with risk-ranked observations and recommendations covering the areas of cloud governance, logical access, data protection, change management, and vendor monitoring. The results of this assessment are helping the client obtain value from cloud computing and better manage risks.

Case study No. 2: Prioritizing investment in controls and compliance monitoring strategy

Industry: Global oil and gas

For a global oil and gas company, the company had started leveraging several CSPs without a compliance monitoring strategy and program, leading to risks to the organization. KPMG assessed maturity against Cloud Security Alliance Cloud Controls Matrix and provided detailed observations and recommendations that helped the client prioritize investment in controls and compliance monitoring strategy.

Case study No. 3: Increasing security to mitigate risk

Industry: Financial services

At a financial services company, the board of directors was concerned about risks related to the use of cloud computing to host customer confidential data and its linkage to cybersecurity. KPMG assisted the internal audit department with obtaining a better understanding of the use of AWS cloud by its organization across governance, logical security, change management, service-level management and cost management areas. The company's internal audit department was able to assess and report on whether the company had adopted the cloud-shared responsibility model in making secure, effective, and efficient use of AWS.

Conclusion

Disruptive technologies are revolutionizing business and life as we know it. These technologies are empowering consumers and forcing enterprises to adapt or be left behind.

A risk-based approach to data protection assumes greater significance with emerging technologies—including cloud computing. You need to know what your crown jewels are, where they are located, and whether they are adequately secured!

Cloud user organizations need to balance supporting innovation in the cloud with having a risk-based governance structure that includes policies, procedures, and personnel. Just saying no to the immense potential of cloud solutions also leads to uncontrolled Shadow IT.

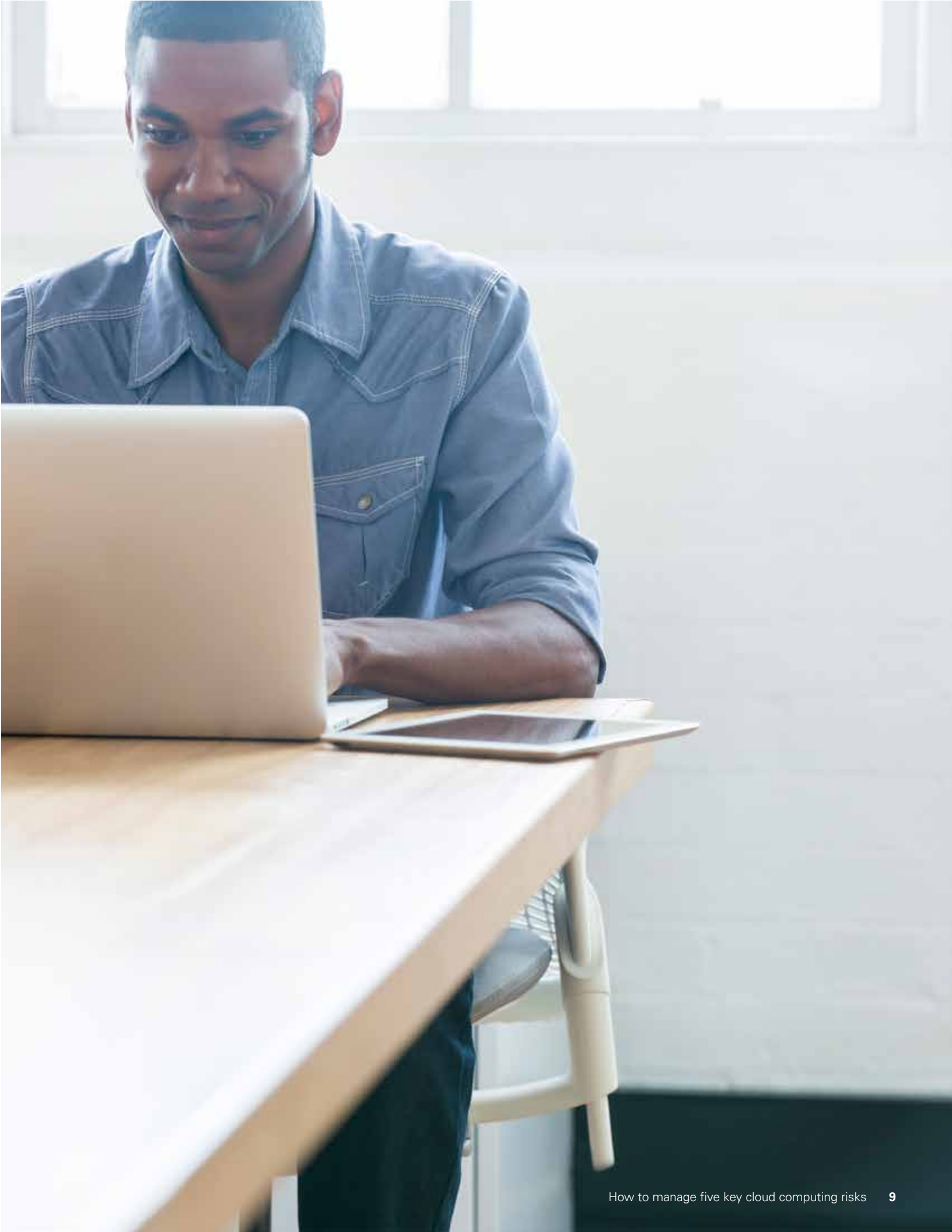
Information security, risk management, and internal audit departments can help their organizations realize and maximize the benefits of cloud while balancing risk rather than hindering the process.

Questions for consideration

KPMG has significant experience assisting organizations in many industries with enhancing the power of cloud while balancing risk. Organizations can achieve tangible benefits from emerging technologies. When turning IT risk into opportunity, an organization must demonstrate effective IT compliance through governance and controls, data integrity, security and privacy, and supplier management compliance needed to embrace disruptive technologies. KPMG's Emerging Technology Risk services help clients recognize and responsibly manage these risks.

Organizations should consider how the five major risks can be mitigated to achieve the numerous benefits of cloud. Here are some questions for your organization to consider:

Questions	Risk category				
	Financial	Vendor	Data	Operational	Technology
Who is responsible for cloud strategy, and is that aligned with the business strategy?	X	X			X
Do you have a road map for cloud transformation, including migration strategy and approach?				X	X
Have your existing governance policies and processes been updated to include cloud and reflect the opportunities and risks that are unique to cloud?	X	X	X	X	X
Are security and risk professionals involved in cloud governance?		X	X	X	X
Are your cloud management processes well designed such that your enterprise users can follow them, e.g., they are simple and repeatable, or are they opaque and cumbersome?		X	X	X	X
Do you understand the data protection requirements of your stakeholders (customers, regulators, etc.), and are you confident that your CSPs are following those requirements?		X	X		
Do you understand the third parties that host your data, and are they protecting it in accordance with your data security requirements?		X	X		
Are you aware of the various tools, techniques, and other automation resources available to harness the power of cloud?	X	X	X	X	X
Are your internal audit and risk management departments prepared to navigate your organization on the cloud journey?	X			X	



Contact us

Francis Beaudoin
National Lead,
Technology Risk Consulting
KPMG in Canada
T: 514-840-2247
E: fbeaudoin@kpmg.ca

kpmg.ca