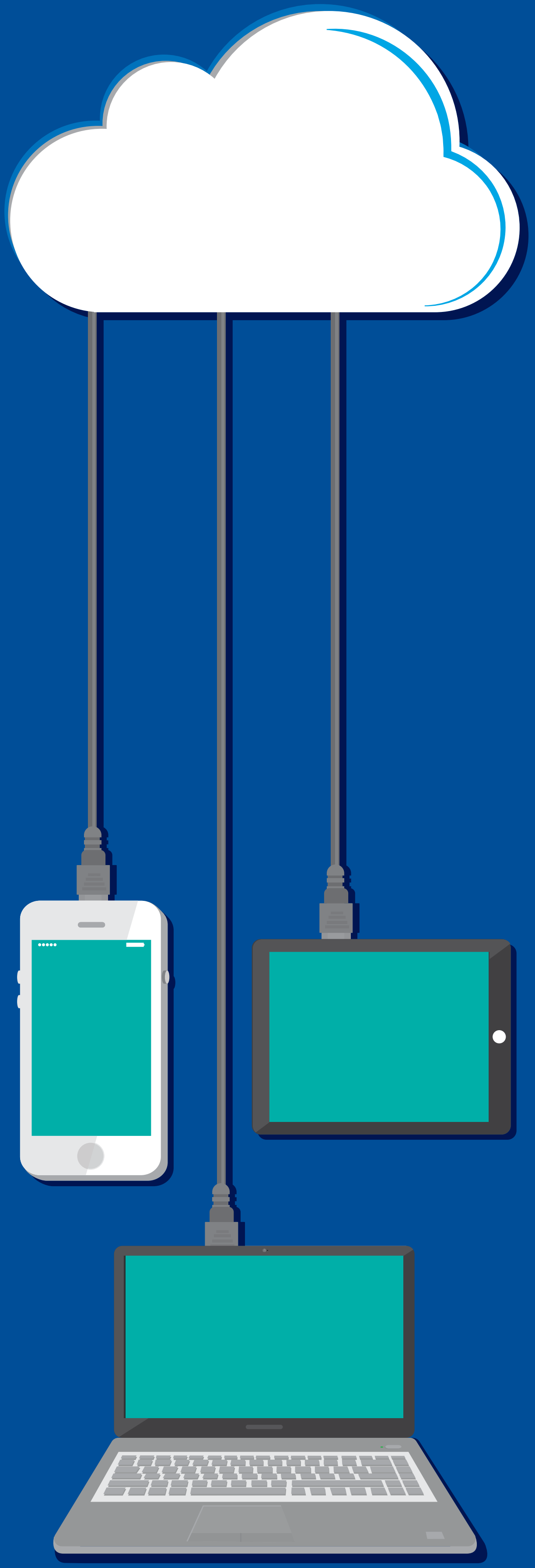
KPMG

Moving to the cloud with confidence

Proactive risk management drives confidence in cloud



kpmg.com

Introduction

It's official: Cloud computing has gone mainstream. With rapid growth in both spending and revenue, the public cloud services market is forecasted to be worth more than $200 billion in 2019.[1] Organizations are turning to cloud computing to drive ongoing innnovation; increase agility and responsivness; achieve greater elasticity and scalability; accelerate product development; and reduce cost.

But even as the market for cloud services has matured, and more organizations have implemented cloud computing solutions, risks remain. In 2018 alone, an unsecured Amazon S3 server exposed the personal information of tens of thousands of FedEx customers. An issue with Google Cloud Platform caused outages for Google Cloud Networking, App Engine and Stackdriver, shutting down official help channels. And users of Microsoft Azure in the South Central U.S. were left unable to access cloud services for nearly four days due to an issue with cooling systems in the data center.

Businesses operating in the cloud will likely experience an outage, breach or another form of failure at some point—but that doesn't mean you should fear moving to the cloud.

There's no denying that the cloud has increased the potential for both internal and external threats to the organization. However, being proactive with your risk approach can help you safely unlock the benefits of cloud technology. Adopting a "cloud-first" mentality has become key for outpacing competitors.

Today's cloud is much more rich and nuanced than it was at its inception over ten years ago. Cloud consumers now have more native options, stronger security and privacy tools, and enhanced measures for detecting, responding to and preventing security breaches. As the processes, regulations and knowledge surrounding the cloud continue to improve, these advances have increased customer confidence and eased the burden for IT functions.

With the pressure on IT to be agile, deliver increasing value, and improving maturity in cloud technologies, now is an opportune time to reap the benefits of cloud technology. Businesses that haven't yet started the journey need to ask: at this stage of the game, which of our processes make sense to move to the cloud, which cloud service providers (CSP) should we use and how can we manage the risks?

In this paper, we explore how the cloud and its reputation have changed over the past few years, and offer steps and guidelines to create sustained business value for those ready to make the move.

Cloud is fundamental to achieving business priorities

CIO expect to move **nearly 1/2** of their applications to a public cloud by 2020

70% of IT leaders report moderate or significant investment in cloud over the next three years.

In 2020, worldwide spending on cloud services and infrastructure will grow **21%** annually-nearly **7X** the rate of overall IT spending growth

Source: Worldwide Semiannual Public Cloud Services Spending Guide, International Data Corporation, February 2017

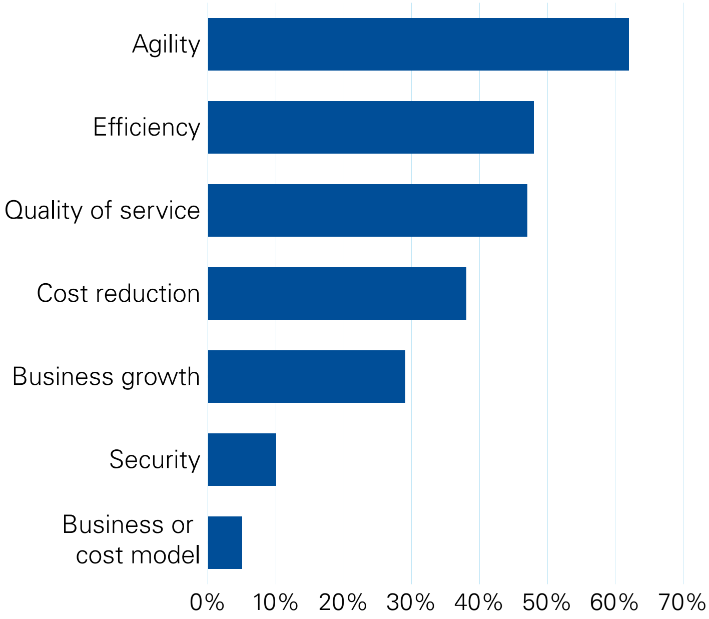
[1] Forecast Analysis: Public Cloud Services, Worldwide, 2Q18 Update, Gartner

KPMG

What is drawing businesses to the cloud?

With age comes experience and with experience, understanding. As a relatively new technology, the cloud has undergone extensive scrutiny and rightfully so. Many businesses were, and remain, hesitant to move their data from a local or on-premises data center to a public space that is seemingly beyond their control. But increased transparency, advancements in cloud processes, tools and platforms, and the emergence of modern development practices have led to a better understanding of the cloud—and increased investment.

Figure 1: Key drivers for enterprise cloud migration initiatives



Source: HFS Research, 2018

According to a 2018 survey by HFS research (See Figure 1), the two key drivers for overall cloud adoption are the need for agility and efficiency. It should be noted that many enterprises have migrated to the cloud for greater security—reinforcing the notion of a maturing approach to cloud adoption. Further proof is that a surprisingly high number of companies operating in highly regulated industries are migrating workloads to the public cloud.[2]

With security representing a significant priority, CSPs have undergone thorough audits and have addressed the requests and concerns of businesses by improving tools and features and adding new applications. For example, providers now allow cloud consumers to create and control their own encryption keys. Five years ago, providers would include an encryption option, but they would control the key. Machine learning, a form of artificial intelligence that employs a sophisticated array of algorithms to learn from data, is another added feature that helps proactively detect and prevent threats.

CSPs continue to develop new security, risk and compliance software tools, with features and functions to address the requirements of various industries, including a variety of preventative and detective measures. And while risk management is still primarily the responsibility of the user organization, CSP's have invested significantly in their own internal security and are making strides to make consumer responsibilities for security less cumbersome.[3]

[2] HFS Research, 2018

[3] Oracle and KPMG Cloud Threat Report, 2018

How companies are successfully leveraging the cloud

During the early days of cloud computing, companies moved to the cloud with little understanding of the risks or how to optimize processes. What these businesses failed to understand is that new technology alone does not improve performance. Organizations are realizing they must redesign existing processes and operating models to achieve the potential benefits of cloud technologies.

Businesses can create a hybrid cloud environment that enables them to operate with a combination of on-premise, private and third-party cloud services tailored to fit their specific needs.

It's important to keep in mind, however, that hybrid cloud approaches and multiple CSPs require a new management framework and an overall governance approach that help control the increased complexity.

New tools also allow businesses to integrate their multi-cloud ecosystem with what they have on-premises. Although it was possible to integrate cloud solutions from multiple CSPs in the past, the process was manual and time-consuming. Now that it is easier, quicker and more secure, we encourage businesses to choose cloud solutions based on the strengths of the individual solution, rather than going all-in with a single cloud provider. This diversified CSP strategy ensures a cloud ecosystem that is more likely to meet your business needs.

A well-planned suitability assessment can help determine how to optimize business processes using the hybrid approach, as well as manage the associated risks and inevitable complications effectively. Organizations that plan to leverage more than one cloud environment, including SaaS, IaaS and PaaS, need a sound strategy to ensure accountability, controls and security.

But even companies that have not yet made the move to the cloud are putting in the work to understand the cloud more fully. Just over half (51 percent) of respondents indicated that thorough audits of the security of on-premise versus cloud security increased their confidence in the cloud.[4] The emergence of new organizational roles, such as Cloud Security Architect, and various risk management mechanisms and tools from CSPs, offer businesses an in-house resource for understanding compliance and security and operating in the ever-evolving regulatory landscape.

Introducing the Cloud Security Architect

The role of the Cloud Security Architect (CSA) has become a central and strategic position for meeting security and compliance milestones. Businesses are assembling teams to assess security protections, configurations and key controls, and manage costs through budgeting and tracking. This leads to a better understanding of shared accountability requirements, and provides a framework for protecting the organization from cyber threats.

[4] Survey Report: Behind the Growing Confidence in Cloud Security, 2018

No matter which cloud environment an organization adopts, it is critical to understand the shared responsibilities between the customer and CSP. More importantly, a strong governance and third-party risk management process must account for the blurred lines of responsibility.

Shared security responsibility model

On-premises	**IaaS**	**PaaS**	**SaaS**
Users	**Users**	**Users**	**Users**
Data	**Data**	**Data**	**Data**
Applications	**Applications**	**Applications**	Applications
Operating system	**Operating system**	Operating system	Operating system
Network	**Network**	Network	Network
Hypervisor	Hypervisor	Hypervisor	Hypervisor
Infrastructure	Infrastructure	Infrastructure	Infrastructure
Physical	Physical	Physical	Physical

■ **Customer responsibility** □ Cloud provider responsibility

Source: Microsoft Corporation

Wherever you are in your cloud journey, avoid these common pitfalls:

- Underestimating the need for investment in retraining people or hiring for cloud catalyst roles including cloud security, risk and compliance functions
- Underestimating the total cost of ownership
- Failing to perform a suitability assessment for cloud workloads
- Treating the cloud IAAS and PAAS migration as a one-time lift-and-shift initiative. Successful migrations typically leverage a multi-stage transitional process involving multiple architectural patterns such as refactoring
- Limited understanding of the shared responsibility model. Many incorrectly presume that cloud-service providers will assume responsibility for the security and resiliency needs for their entire technology stack
- Neglecting to modify processes, workflows and existing reference architectures. Not integrating cloud native tools with existing tools, and processes where appropriate.
- Not engaging all three lines of defense in the transformation process; while the first line generally feels the growing pains, the second and third lines have been slower to embrace change due to lack of expertise and an already full agenda.
- Under appreciating the impact of cloud migration on Sarbanes Oxley audits, privacy and other regulatory compliance matters

The cloud journey checklist

It's important to take a holistic and structured approach when moving applications and workloads to the cloud. Your IT and business units should collaborate to understand the cloud journey from the beginning—when cloud is merely a consideration—to the end—when measuring transformation success. You can achieve this shared understanding through robust planning, piloting and assessments.

Steps to accelerate and enhance your cloud journey

Understand your current landscape and future priorities. Design a governance framework that supports the needs of the business while supporting agile development. This helps establish a cloud strategy and common framework. Businesses should determine if they have the skill set available internally or there are gaps that need to be filled via training or catalyst hires. Put a governance process in place to vet security and reliability of cloud service providers as well as cloud migration initiatives. Unmanaged cloud vendors might expose the organization to significant financial implications and reputational risks. But too hard or too many rules won't allow cloud vendors to add value. The key is to strike the right balance between too restrictive and too lax.

Build supporting processes and tools. This involves: evaluating different approaches; performing due diligence on tools and vendors; defining cloud architecture principles; designing secure baseline configurations for each cloud product and service to meet information security and privacy requirements; and choosing which solutions work for your business. Further, to optimize the cloud investment, companies should take a risk-based and value-driven approach to design. After all, spending $1000 to address a $100 problem is imprudent. And remember: Security focused on technology alone will fail. It is critical that the risk management framework supports the strategic direction of the organization—enabling a cloud-first mindset that supports change.

Create a detailed roadmap for what can go in the cloud. Assess your current portfolio of applications and decide whether to upgrade applications or move-to-the-cloud. With the increasing maturity of cloud technology, a growing number of best-of-breed applications are available as SaaS solutions. For infrastructure and platform migration for applications, decide what cloud migration pattern (life and shift, refactor etc.) to adopt for each application.

Design and integrate cloud solutions. Integration of cloud solutions is typically more efficient than implementation of legacy technology. However, you must focus on requirements such as identity and access management, and resiliency to ensure that the relevant security, privacy and resiliency controls are in place.

Continuously log and monitor your cloud defense. With an increase in the threat surface, as well as a massive sprawl of potential data ingress and egress points, remaining engaged every step of the way is critical.

Agile and seamless security that enables innovation. Cloud security must incorporate the same agile development process that engineers and project managers embrace. In short, the security architecture you build should empower business transformation outcomes.

Why KPMG

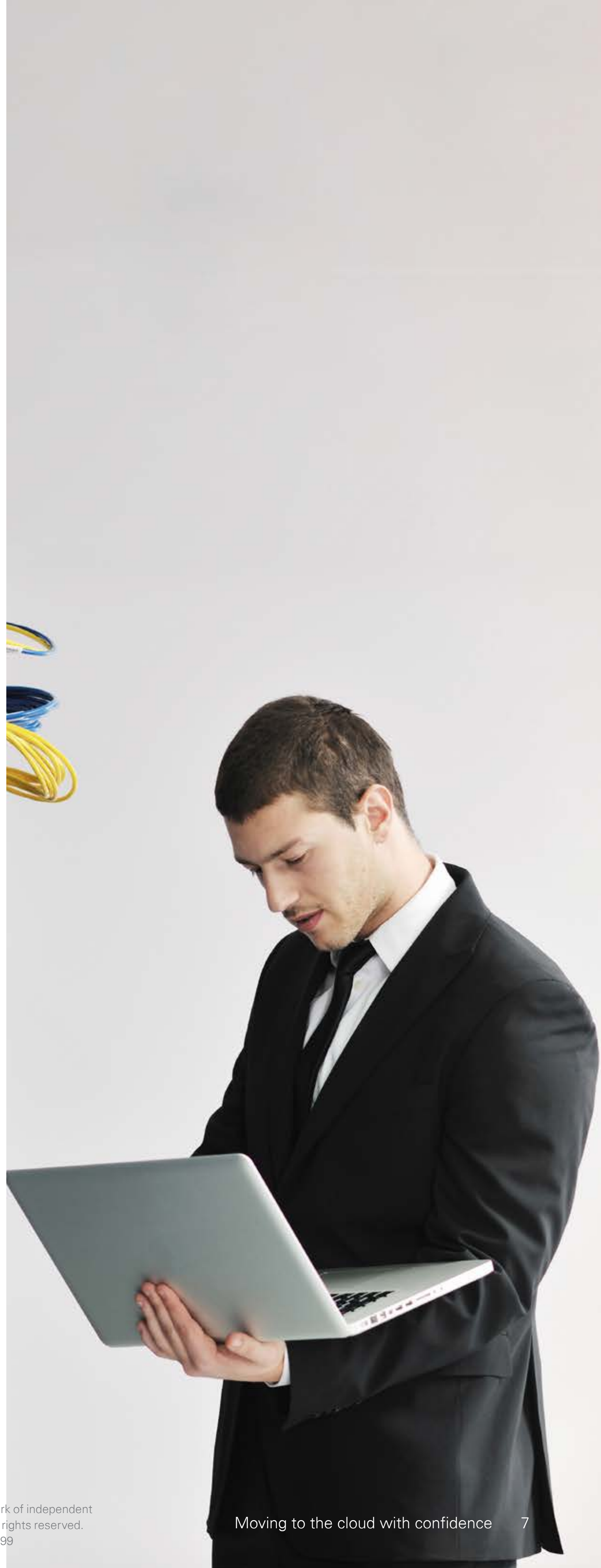
KPMG has developed, deployed, and refined through hundreds of client engagements, a cloud migration, transformation, and risk management approach.

We help clients manage the complexity of cloud usage by providing the structure, approach and discipline required to define and implement an effective hybrid cloud delivery model, including a hybrid cloud infrastructure automation strategy, to better realize the benefits of the cloud while mitigating unintended consequences.

By conducting impact assessments, establishing target operating models based on our hybrid cloud life cycle management framework, building transformation road maps, and creating business cases that justify their plans, we help organizations align their cloud strategy with their business needs.

We have helped CSPs evolve their products and tools and heighten security. By working with CSPs, we've developed a deep understanding of what customers get by working with providers—and what you don't get. Additionally, our alliances with several key CSPs give us insight into the future direction of the cloud and its potential business impact.

To learn more about creating an effective cloud strategy and managing cloud risk, please visit our portal page



Contact us

Sailesh Gadia
Partner, Advisory
T: 612-305-5087
E: sgadia@kpmg.com

Contributors

Vishi Bindra
Director, Advisory

Josh McKibben
Director, Advisory

Some or all of the services described herein may not be permissible for KPMG audit clients and their affiliates.

kpmg.com/socialmedia

The information contained herein is of a general nature and is not intended to address the circumstances of any particular individual or entity. Although we endeavor to provide accurate and timely information, there can be no guarantee that such information is accurate as of the date it is received or that it will continue to be accurate in the future. No one should act upon such information without appropriate professional advice after a thorough examination of the particular situation.