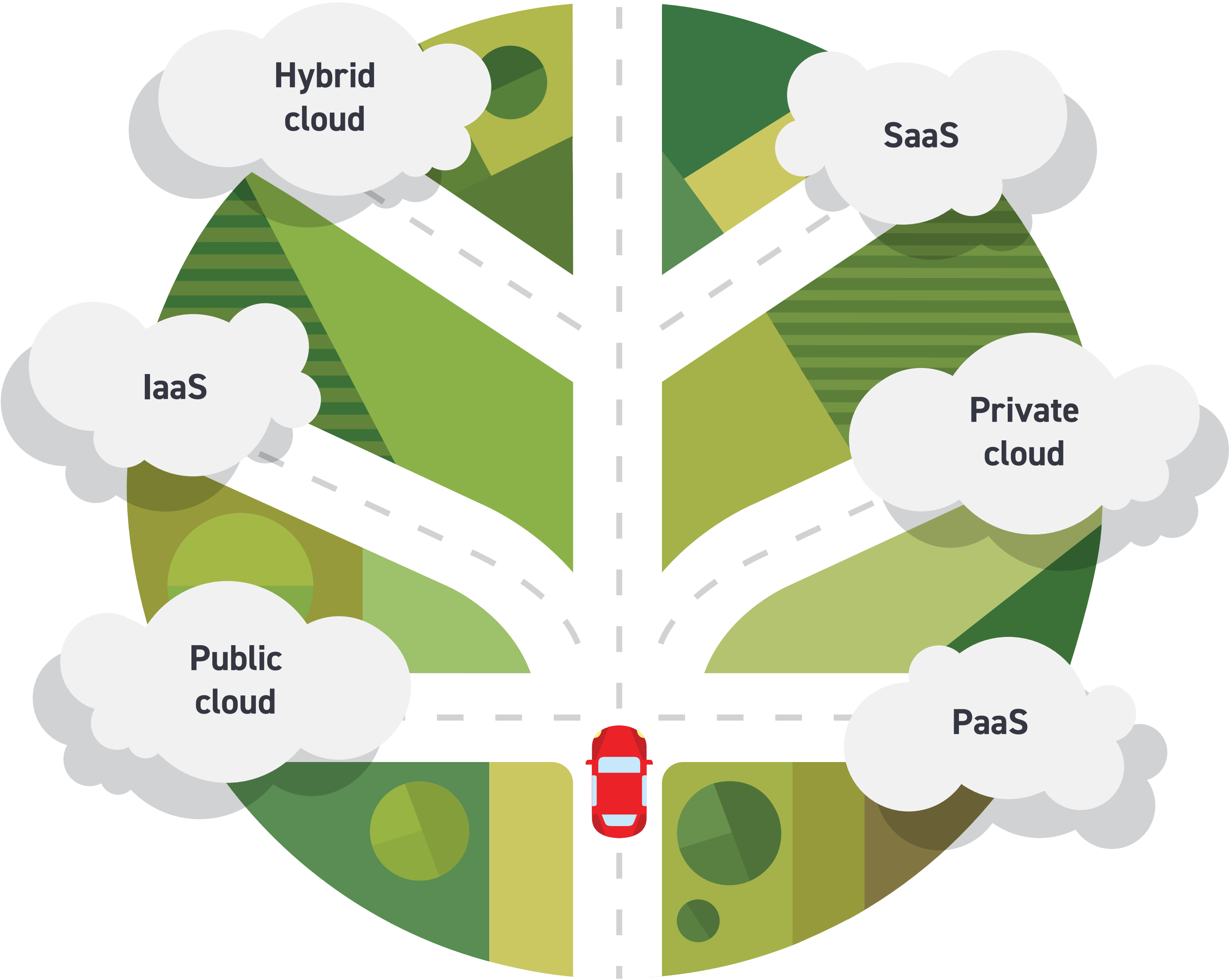
Deloitte.



The cloud is here: embrace the transition

How organizations can stop worrying and learn to "think cloud"

Clouds in the forecast

The emergence of cloud computing has business and information technology (IT) leaders asking fundamental questions: How can we better understand the risks and opportunities that cloud computing presents? How do we take advantage of these opportunities, not fall behind, and not make costly mistakes? How do we survive and thrive in the cloud?

The growth and maturation of the cloud marketplace has not only proven the viability of commercial cloud offerings but also represents a fundamental shift in technology management philosophy. With traditional practices garnering limited return on investment and providing limited business agility, organizations are moving away from the do-it-yourself mentality and toward using technology services from cloud services providers (CSPs), who can do things better, faster, and often cheaper.

While many organizations are apprehensive about adopting these types of services, the cloud is an inevitable part of IT service-delivery models of the future. In fact, your organization is likely already in the cloud, with employees having the ability to procure cloud-based solutions with the swipe of a credit card, whether sanctioned by your IT team or not. This creates risks related to 'shadow IT', or solutions adopted without the consent and/or approval of IT.

Moreover, your technology vendors are going to the cloud. Cloud deployments are becoming ubiquitous with commercial off-the-shelf offerings, while on-premise deployments are becoming the exception.

Some notable examples of leading software deployed via cloud services include business productivity suites (such as Google G Suite, Microsoft Office 365), customer relationship management (e.g., Salesforce.com), enterprise service management (e.g., ServiceNow), talent management (e.g., SuccessFactors, Taleo), and even full suites of Enterprise Resource Planning (ERP) solutions. This list is rapidly expanding as software companies begin the transition from delivering their software as on-premise installations to software as a service (SaaS) delivery models.

Embracing the cloud will soon be a matter of sheer survival. Competition, disruption, and transformation are compelling companies to continuously improve their operations to drive agility, savings, efficiency, and enhanced customer experience. For many organizations, differentiation is no longer just a concern for the marketing department but the key to surviving a fast-evolving marketplace.

Whether they want it or not, and whether they're ready or not, the transition is well underway. Businesses must start "thinking cloud" if they want to survive.

The cloud's sunny side

Many leaders may be used to viewing IT as a roadblock, an impression no doubt molded in part by the fact that anything new needed to go through extensive upfront planning, procurement, and implementation cycles. Cloud computing, on the other hand, may be seen as the opposite—as an enabler.

It can play a key role in the optimization and development of new business models thanks to several key capabilities:

- **It reduces the time it takes to get to market:** Turn-key computing solutions shorten the ideation-to-implementation cycle. Bonus: these solutions operate on a subscription basis, so there is no burden of long-term capital investments.
- **It offers scalability:** By being able to provide extra technology resources whenever required, organizations can accommodate sudden spikes in demand.
- **It limits capital investment:** The ongoing nature of cloud expenditures enables organizations to focus their time, effort, and resources on using IT services rather than conducting extensive planning exercises to secure funding and/or implement IT infrastructure.
- **It stimulates innovation:** CSPs introduce new features and functions on a regular basis; some have launched more than a thousand features in a single year. In addition, they free organizations to redirect IT roles away from operations and toward developing capabilities in such areas as the Internet of things (IoT), machine learning, and artificial intelligence (AI).

What is cloud computing?

The National Institute of Standards and Technology in the United States defines cloud computing as a model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources that can be rapidly supplied and released with minimal management effort or service-provider interaction[1].

Common characteristics of cloud computing include:

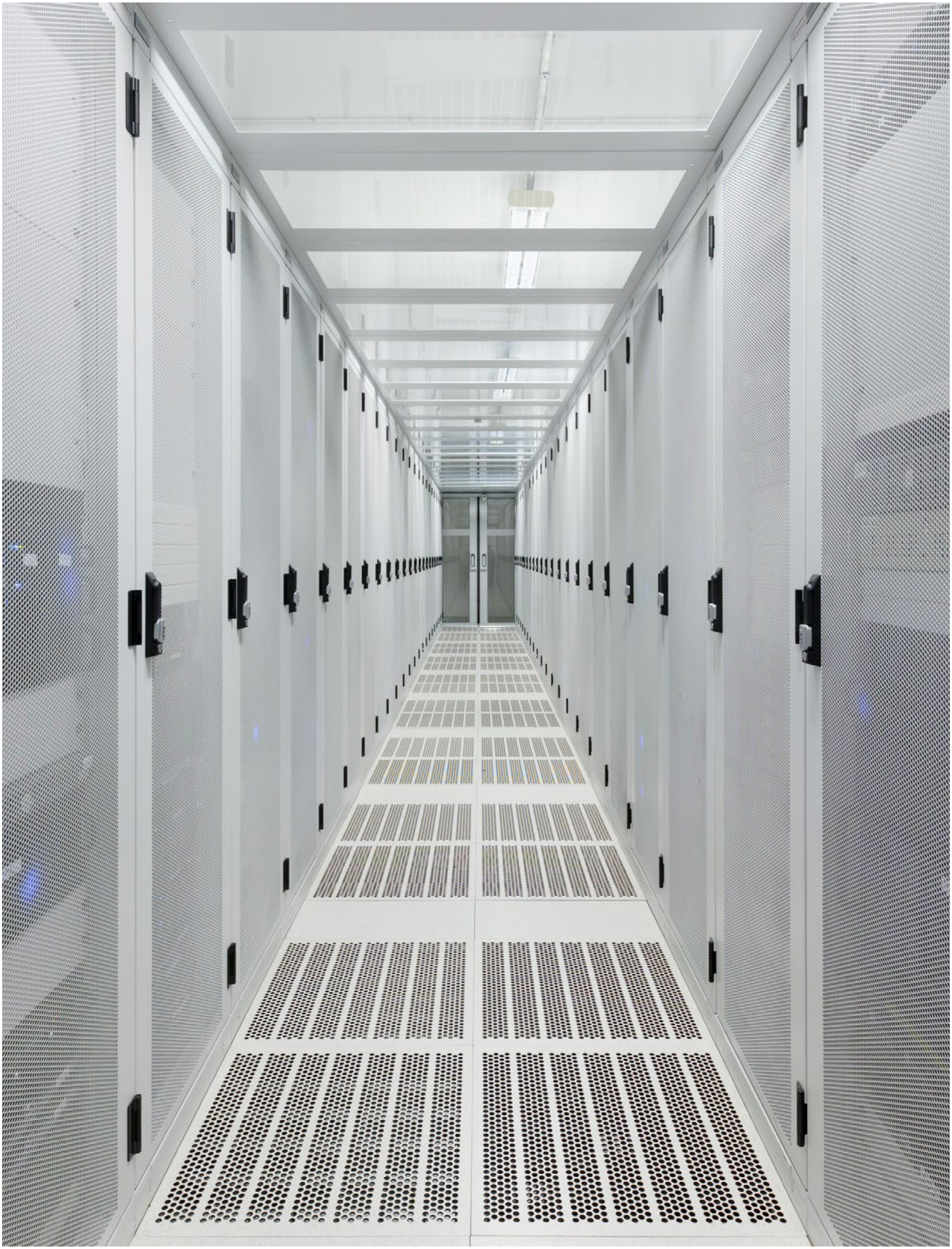
Measured service
Cloud systems automatically control and optimize resources, and they can monitor, control, and report usage, which provides transparency for both the provider and the consumer.

Rapid elasticity
Based on demand, resources can be supplied and released to scale rapidly.

On-demand self-service
Users can provide their own computing capabilities as needed with each service provider, with no need for human interaction.

Broad network access
Access is available over the network and through various client platforms (e.g., mobile phones, tablets, laptops, and workstations).

Resource-pooling
The provider's computing resources are pooled to serve multiple consumers, with resources reassigned according to demand.



Avoid common pitfalls

Adopting an entirely new way of doing things is not without potential headaches. There are numerous hazards to adopting cloud, from not realizing the expected savings to being trapped in a relationship with a single vendor to compliance and regulatory issues.

Fortunately, there are ways to avoid or mitigate such less-than-ideal situations.

The following are some of the most common pitfalls of cloud adoption:

- **Anticipated cost savings don't materialize**
- **Vendor lock-in**
- **Data security and privacy**
- **Compliance and regulatory risks**
- **Hybrid cloud integration**

Anticipated cost savings don't materialize

A key tenet of the cloud computing value proposition is cost reduction. Large CSPs, particularly those that provide infrastructure as a service (IaaS), are commonly cited as being capable of delivering computing at a price point internal IT organizations can't match. In addition to operating leading and optimized IT infrastructure, CSPs can take advantage of economies of scale and offer competitive pricing. So while consumers understandably expect to realize these cost savings, many of them find in reality that not only are there are no cost reductions but indeed cost *increases* of up to 20 percent[2].

CAUSES

Cloud adoption costs — Implementing public cloud resources may require technology investments (network redesign, identity and access management toolset, for example) and staff (new roles, training) to enable proper management of a hybrid IT environment. In some instances, these investments can be significant; they must be taken into consideration when estimating potential cost savings.

Limited governance — Uncontrolled usage of cloud services can significantly increase the costs because they're billed on a pay-per-use basis (e.g., per user/per resource/per hour), and sometimes include charges based on consumed bandwidth. These costs can dramatically change the business case, if they are not properly understood and proactively managed. Cloud environments offer the benefit of scalability but the cost implications must be clear and known in advance.

Unsuitable workloads for public cloud environment — On-premise deployments may be are better suited for some workloads, such as those that have high-resource utilization and extensive, complex integrations. The vendor may also not have selected the most appropriate cloud model, as each model has different cost/benefit drivers.

PREVENTATIVE MEASURES

Financial analysis — A business case should be developed to justify the migration of workloads to cloud environments to mitigate risks related to cost management. The financial analysis should align with the organization's cloud strategy, provide guidance on in-scope cloud service models and workloads that can be migrated, and account for additional investments in people, processes, and technologies. Revisit the business case after the transition, to validate its realization.

Workload analysis — A technical review of the proposed workloads to migrate to the cloud should be completed. Leverage methodologies and toolsets that look at multiple facets of the proposed workloads such as performance, application architecture and integration requirements to name a few. Also, use this as an opportunity to rationalize duplicative applications within the enterprise

Governance processes — Governance processes specific to the consumption of cloud services should be developed: who is able to request them, how many resources can be provided, and what approval(s) are required. In addition to setting quotas, providing visibility and reporting usage will help to hold users accountable.

Cloud optimization tools — As the usage of public cloud services grows, so too does the need for tools and capabilities to help companies more effectively manage expenses. Capitalize on tools to reduce cloud expenses by identifying and right-sizing overprovisioned resources, take advantage of pricing changes, and identify ways to use and release IT resources more cost-effectively.

CASE STUDY:

A healthcare company[3]

Challenge — The operating costs for cloud services were preventing an organization from meeting its budgetary target. Moreover, the services were under-performing.

Solution — The organization reviewed its predominantly Amazon Web Services (AWS) cloud infrastructure and determined a few things needed to change. These included reconfiguring the existing cloud infrastructure, creating detailed future spend projections, implementing VPN/network improvements, and conducting regular and ongoing staff training on cloud usage.

Result — Implementing the fixes reduced monthly operating costs by 30 percent and drove the consolidation of the existing IT infrastructure footprint by 25 percent.

Vendor lock-in

Becoming dependent on a single vendor is a situation no company wants to find itself in, in any area of business. Vendor lock-in can manifest in many forms, but two of the more likely forms involve technology and contracts. With technology lock-in, the challenges relate to repatriating or migrating a large IT service portfolio built on a specific cloud platform to another CSP and/or in-house.

Being locked into a contract can have a number of consequences, including significant financial penalties for terminating services early, an inability to renegotiate pricing if commercial costs change throughout the duration of a contract, and an inability to migrate to an alternative CSP that offers more attractive services.

CAUSES

Market consolidation — The IaaS market has consolidated significantly over the last few years, and trends suggest only a handful of very large CSPs will eventually operate in this space. Customers who were early adopters of IaaS and made considerable investments may be required to move to alternative CSPs in the near future as the market continues to consolidate.

Limited cloud standards and interoperability — The lack of coordinated cloud standards across cloud service providers has made it difficult for organizations to move workloads between CSPs and/or to private clouds.

PREVENTATIVE MEASURES

Multi-cloud and multi-vendor strategy — A hybrid cloud strategy consisting of a manageable number of different vendors and cloud services will help reduce vendor lock-in. While this may increase the complexity, management requirements, and integration requirements of the overall IT environment, it will provide the flexibility to select the most appropriate vendors and the ability to switch CSPs with eyes wide open.

Multi-cloud managed services — Using services that work across multiple CSPs for various cloud functions is also a good strategy. By maintaining a diverse and vendor-agnostic set of cloud services, organizations can lessen their reliance on a single vendor and reduce the requirements related to cloud service migration.

Market-leading vendors — Soliciting cloud services from established vendors such as Amazon Web Services, Microsoft Azure, among others, will limit risks of being subjected to the ongoing cloud market consolidation.

Containerization and open source technologies — Technical solutions can help protect against vendor lock-in. For example, Docker, a containerization technology, has a solution that increases workload portability while simultaneously reducing licensing and IT operations costs. OpenStack, another open source toolset, provides application programming interface (API) capabilities, which can increase the ease in which workloads can be moved across various cloud environment. Other solutions include VMware on AWS and Azure stack.

Mature vendor management capabilities — The demand for effective vendor management capabilities increases in direct correlation with the volume of cloud services in operation. In addition to understanding the cloud marketplace and the suitability of cloud services for industries and functions, it is critical to approach cloud service contracts as an ongoing set of relationships—consistent monitoring of the cloud market, particularly in more nascent segments, is necessary.

Cloud procurement tools and techniques — Cloud solutions are often difficult to evaluate due to variables across IT infrastructure, service levels, cost, and performance. Providing a baseline set of business requirements, as well as using cloud-ready market solicitation tools and techniques, will help companies make a fair comparison of vendor offerings.

CASE STUDY

A gaming and entertainment organization[4]

Challenge — As the volume and complexity of online games grew, a gaming and entertainment organization found it difficult to scale its IT infrastructure. This affected the front-end performance of its online games. To overcome this issue, developers sought the convenience of a database-as-a-service (DBaaS) model while maintaining complete control over its technology stack in an attempt to maximize flexibility and limit issues related to vendor lock-in.

Solution — The organization migrated its data to a multi-tenant cloud platform, which provided the development teams with the ability to build their own database service for all the company's studios and developers. This empowered the teams to use dedicated cloud infrastructure to store unique data sets and, therefore, increase the front-end performance of its games.

Result — The operations teams retained complete control and access to their code throughout their technology stack while simultaneously having access to a scalable and flexible cloud service. The organization also consolidated its IT environment, which has improved performance and reliability.

Data security and privacy

Businesses have shifted from assessing whether they should use cloud computing to planning how they are going to make it an integral part of their IT infrastructure.

For all the advantages of storing data in the cloud, it is equally important to understand and mitigate risks related to moving corporate data out of a carefully built and secure on-premise environment. Losing operational control of such data may make it vulnerable to external security and privacy threats, if adequate safeguards and controls are not enforced. Furthermore, public cloud architectures are dynamic, which can make security and privacy measures both cumbersome and expensive.

CAUSES

Data storage on shared compute infrastructure — Many public cloud environments require data to be stored on shared infrastructure managed by the CSP, representing a fundamental shift from traditional IT practices. While the client's IT team has access to and control of public cloud usage through administration web-interface or API scripts, both the environment and the API scripts can be vulnerable to cyberattacks.

Multi-tenancy — Public CSPs use multi-tenancy to optimize server workloads and reduce costs by sharing workloads across multiple environments. This practice can potentially result in side-channelling, an IT security threat that occurs when an attacker is able to obtain information through a shared tenant's node.

PREVENTATIVE MEASURES

Strong data encryption and continuous monitoring — As data moves outside a company's secure perimeter, it must be encrypted using methodologies such as cryptography and tokenization and further secured by controls like digital certificates and multi-factor authentication. Monitoring tools must also be put in place to reinforce traditional anti-virus and anti-spam tools like intrusion detection, denial-of- service (DoS) attack monitoring, and network traceability tools. It's important for organizations to stay current and adopt the security innovations from leading vendors.

Understanding of the cloud security and privacy operating model — It's critical for businesses to understand their cloud providers' security and privacy architecture in terms of firewalls, intrusion detection techniques, and industry standards and certifications, because they may need to align their own security architecture with the CSP's architectural constraints. Understand what is being signed up regarding contract provisions for data security. In cloud computing, risk management is shared between the user and the vendor: responsibility is transferred but not accountability.

Cloud adoption awareness — Organizations should provide training and create awareness of the risks related to operating cloud solutions. Cultivating a culture of constant vigilance is one of the easiest and most cost-effective methods of securing cloud data.

CASE STUDY

A global investment bank[5]

Challenge — As a global bank's adoption of cloud services increased, so too did its challenges related to managing data security and privacy in a cost-effective manner. The bank requires data-processing capabilities that span multiple privacy jurisdictions, each with their own complex array of regulatory controls.

Solution — The bank turned to a managed cloud security services provider to meet its needs for scalability, global privacy compliance, and cloud adoption. The organization embraced a standards-based, data-centric approach to data security using a combination of encryption and secure tokenization technologies.

Result — With the help of a consolidated, centrally managed cloud security and privacy solution, the bank could offer secure business services to customers across the globe and serve its demanding, diverse client base more simply and less expensively.

Compliance and regulatory risks

Meeting regulatory and compliance requirements in cloud computing is complicated to practice and execute. Compliance covers government regulations, such as Sarbanes-Oxley and the European Union Data Protection Act, as well as industry regulations such as PCI DSS for payments[6].

Moving to a public cloud infrastructure platform requires giving up some level of compliance controls to the cloud vendor, which is a challenging situation for many auditors. CIOs and CEOs want to know how to leap into cloud computing in a way that preserves their good standing in regulatory and compliance functions.

CAUSES

Limited organizational control of cloud purchases and consumption — It's possible for stakeholders to procure cloud services with little oversight from their procurement and IT teams, which has led to many organizations assuming a higher level of risk than with traditional IT procurements. For example, cloud vendors offer data repatriation capabilities for up to 60 or 90 days, but the data may not be returned in a usable format, and the associated metadata may or may not be included.

Limited negotiation with cloud service providers — CSP are typically not open to negotiating their standard terms and conditions. Different kinds of clients use public cloud environments, and providers don't yet offer services customized for unique or specialized requirements.

Rapidly changing landscape — A relatively new market offering, cloud solutions are still maturing in terms of industry standards and operating models. Regulators are also evolving and many don't yet provide clear guidance regarding cloud computing. As various alliances, industry groups, and government agencies continue to develop their standards, organizations must ensure CSPs are keeping pace with compliance and regulatory changes.

PREVENTATIVE MEASURES

Well-defined organizational controls related to cloud purchases and use — With an enterprise risk-management perspective in mind, companies should develop and implement cloud-specific procurement guidelines with preferable terms and conditions as well as create the necessary mechanisms to enable a well-engineered move to cloud.

Cloud vendor landscape evaluations — Organizations should establish fundamental guidelines around compliance and regulatory requirements for cloud services, which will provide a baseline for vendor evaluations. It's critical to understand what to look for in terms and conditions, and determine what constitutes an acceptable level of risk based on business priorities. When evaluating cloud vendors, they should look for baseline compliance requirements such as user identity and access management, data protection and incident response, and data residency requirements, among others.

CASE STUDY

A broadcasting network[7]

Challenge — The value proposition of cloud computing made it an appealing option for replacing an aging email system at a public broadcast agency. It was critical to comply with the regulations and controls imposed on public sector entities.

Solution — A thorough analysis was undertaken to assess the risks of cloud computing, both in general and as it pertained to email and collaboration tools. The agency also developed a formal framework to evaluate cloud-hosted email solutions and the lessons learned along the way helped it identify key criteria around regulatory and compliance requirements.

Result — The analysis of the company's regulatory and compliance requirements enabled it to pick the right public cloud solution and successfully replace its legacy email system within a three-month period.

Hybrid cloud integration

Improvements in cloud computing have not driven organizations to rip out and replace their own IT systems, but it has compelled them to seek the best of both worlds (in some cases, this means taking advantage of the agility, scalability, and performance of cloud services while keeping on-premise systems for storage). This has led to complex hybrid IT environments within many organization, new tools required to manage the hybrid environment and new skills needed architect, secure and manage hybrid cloud solutions (which are in high demand in the market). Integrating new cloud services with on premise IT infrastructure can be complex due to customization and configurations, require additional investment, and be resource intensive to maintain throughout its lifecycle. Companies considering a hybrid model must ensure they understand how cloud applications and services will—or will not—integrate with its existing IT stack and applications.

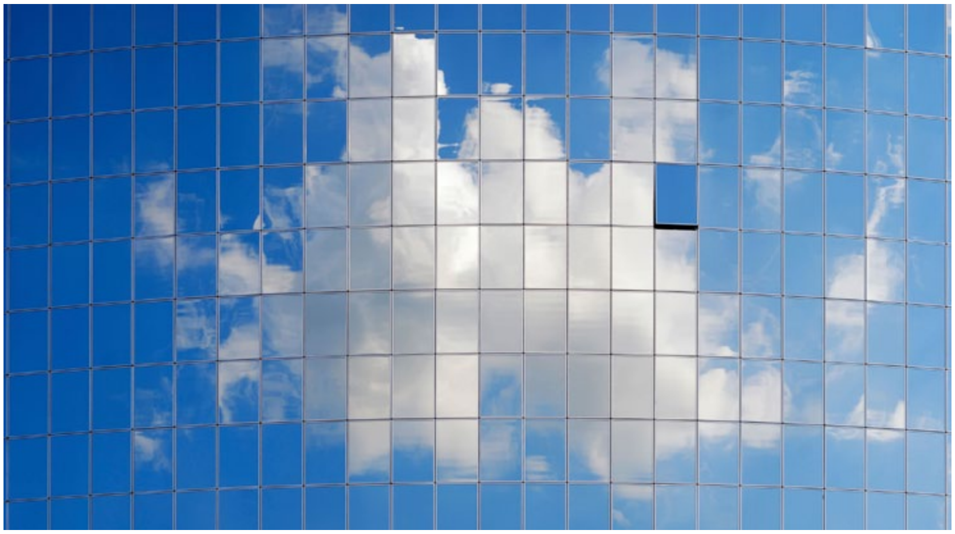
CAUSES

Legacy IT architecture — Business and IT leaders are often reluctant to retire their legacy investments in technology, people, and processes because of concerns about security, risk, upgrade costs, and regulatory compliance. But not cutting the legacy cord cleanly can result in integration problems between cloud applications built on leading-edge IT architecture and older, on premise IT architectures.

Enterprise architecture — In the absence of an enterprise architecture that guides cloud consumption, each business unit might choose a cloud application that's perfect for their purposes, but may not be the optimal choice for the organization as a whole.

PREVENTATIVE MEASURES

Structured cloud governance — Establishing governance and controls provides direction for the organization's cloud adoption. It should consider business process, applications, data, infrastructure, and organizational management controls. Structured governance is required to constantly monitor performance, improve service effectiveness, and align investments with business objectives.



Enterprise cloud adoption guidelines — Guiding principles for the purchase and adoption of cloud solutions should be established for lines of business as part of the enterprise-wide guidelines. Software evaluation and selection decisions must also consider operational performance metrics, not only features and functionalities.

Modernizing operating models and enterprise practices — To improve an organization's integration flexibility, its leadership should consider modernization opportunities and prepare a business case to justify such investments. As the industry moves towards cloud consumption, early investments in upgrading existing enterprise IT architecture would help a company minimize its cloud integration challenges and help accelerate the attainment of benefits.

CASE STUDY

A manufacturing company[8]

Challenge — A manufacturer with more than 200 active on-premises applications, many of which were acquired through mergers and acquisitions, faced integration challenges after it also invested in cloud-hosted applications

Solutions — After looking at various integration platforms, including ETL and data integration vendors, the company engaged a cloud integration service provider to integrate its new cloud infrastructure with existing on-premise systems. The hired provider recommended a structured integration approach and helped develop a baseline cloud architecture that met the company's long-term vision.

Result — With the help of the cloud-based hybrid integration platform and service provider, the company was able to successfully manage its growing cloud and on-premise application integrations.

Doing cloud "right"

Although there are many pitfalls related to cloud adoption, there are also many examples of organizations reaping the benefits. They're using it successfully to transform their service and product offerings to increase customer engagement and revenue, and to increase performance, reliability, and security by eliminating their on-site IT infrastructure operations.

The following case studies demonstrate that when done right, the cloud delivers on its transformative potential and can help enhance IT service delivery.

- **Netflix**
- **Adobe Systems**
- **Matson Inc.**

Case study 1: Netflix[9]

Operating an almost entirely public cloud environment, Netflix has redefined how the world accesses and consumes content. One of the primary drivers for the organization’s cloud adoption, as noted in its 2016 annual report, is the following:

> *“As we scale our streaming service, we are developing technology and utilizing third party ‘cloud’ computing services... If we are not able to manage the growing complexity of our business, including improving, refining or revising our systems and operational practices related to our streaming operations and original content, our business may be adversely affected.”*

For the company, cloud computing is not simply a means to operate information technology but is a pillar of its business. Taking advantage of the benefits of cloud computing (e.g., high availability, scalable IT infrastructure) is a critical success factor for the organization to deliver on its value proposition and maintain its market share.

NOTABLE SUCCESSES

Netflix operates an almost completely public cloud environment. It runs its own content delivery network, called Open Connect, that’s hosted in Amazon Web Services (AWS). Open Connect partners with internet service providers (ISPs) across the globe to securely deliver Netflix services, which are optimized to the specific needs of each client based on its unique network conditions.

The entertainment powerhouse also developed multiple open source solutions (OSS) that have been adopted by organizations worldwide, the most notable of which is Simian Army. This solution is a series of tools that test the tolerance of cloud deployments by randomly shutting down certain systems in order to determine how well they tolerate random failures.

CHALLENGES AND CONSIDERATIONS

Netflix’s streaming services famously crashed on Christmas Eve 2012 when AWS experienced an outage. This not only brought negative attention to Netflix but it also prompted it to bolster its internal testing capabilities. The countermeasures seem to have worked; a recent outage didn’t have any negative impact on users.

A second challenge for Netflix is that it’s hosted completely on AWS. Users who follow such a path are locking themselves into using only one cloud provider.

Case study 2: Adobe Systems[10]

In 2010, Adobe embarked on a research effort to evaluate the effectiveness of its website's sales efforts. Among the many findings, the organization found that although millions of users visited adobe.com every week, most failed to take action.

Acting on these findings, Adobe developed a roadmap to transform its website and evolve the sales model of its software. In partnership with AWS, Adobe launched its cloud-based Creative Cloud Suite in 2013, which helped the organization achieve record levels of revenue in both 2015 and 2016. Using a cloud-driven, subscription-based model, Adobe has been able to increase its user adoption in part due to its flexible licensing agreements and reduced adoption requirements.

NOTABLE SUCCESSES

Enabled by cloud services, Adobe was able to increase user adoption by eliminating its costly one-time licensing costs (which could be upwards of USD$2,500 depending on the application suite) and allowing users to select their preferred applications and subscription licensing model.

The Creative Cloud also gives customers self-service account access and management "anytime and anywhere." It also always has the most up-to-date app versions, since Adobe's DevOps teams can take advantage of highly efficient and agile release-management capabilities.

Adobe managed to transform its commercial product suite and its revenue model using cloud services in less than three years. It's reaped the rewards: the organization has achieved greater levels of revenue and profitability selling their software suite using a subscription-based model than it did selling it as a hard good.

Case study 3: Matson Inc.[11]

In late 2016, Matson Inc., a leading US carrier in the Pacific, closed all four of its on-premise data centres and migrated its entire IT environment to AWS. Matson was already operating a significant application portfolio with AWS, including its customer-facing website and all its mission-critical applications: custom-built order-to-cash booking and billing systems, terminal operations, global equipment management, and US-wide logistics applications among them.

In addition to garnering increased performance, increased reliability, improved security, and IT infrastructure cost savings, the decision to transition entirely to the cloud was primarily driven by industry pressures.

The shipping industry requires advanced IT capabilities to enable the precise tracking of assets and customer shipments as they move around the world. Matson's vessels, shipping terminals, container equipment, and truck shipments all require highly reliable technology to ensure its transportation network operates at world-class levels. Moreover, its customers count on cloud-based applications to provide real-time visibility and analytics to manage their own supply chains.

NOTABLE SUCCESSES

Migrating all the enterprise applications to a cloud environment has enabled Matson to focus on innovating its business services even more. Even better, it reduced its IT costs an impressive 50 percent by closing its four on-premise data centres.

CHALLENGES AND CONSIDERATIONS

The complete migration of Matson's IT environment took more than half a dozen years. Although the shipping company had to operate two IT environments for a long time, this did allow it to carefully manage risks, challenges, and impacts.

Follow the steps

One size does not fit all when it comes to cloud computing. As the offerings become increasingly prominent and vendors continue dictating the pace of cloud adoption, organizations are finding themselves grappling with diverse business needs and challenges.

It needn't be an overwhelming process. Based on our experience, the following steps can help guide organizations on their journey to the cloud:

STEP 1: LEARN

Understand the benefits, risks, and issues associated with cloud computing and install controls to govern the proliferation of cloud services within the organization’s IT environment

STEP 2: PLAN

Based on the organization’s cloud maturity, define a set of strategic objectives and make a prioritized plan to achieve them

STEP 3: FORMALIZE

Develop cloud policies, standards, and an operating model to manage cloud solutions

STEP 4: ADOPT AND MANAGE

Acquire cloud solutions and adopt vendor-provided management tools to supply and manage cloud services

STEP 5: EVOLVE

Enhance service delivery, automate IT management functions, and migrate to cloud environments

Step 1: Learn

One of the most important steps organizations can take in transitioning to the cloud is to find out as much about it as possible. This includes researching the possible pitfalls, discussed earlier in this paper, which must be managed from acquisition to migration.

Various implications should considered when assessing cloud service solutions, such as:

IT security — How are the cloud services secured? Who is responsible for implementing and managing IT security measures?

IT skills — Are the right skillsets in place to plan, implement, and run cloud solutions, and that won't put the organization at risk?

IT support — Who is responsible for providing support? Can the internal IT helpdesk and operations support this solution?

Privacy — Who is managing access to the solution and its data repositories? What regulations and compliance needs must we consider?

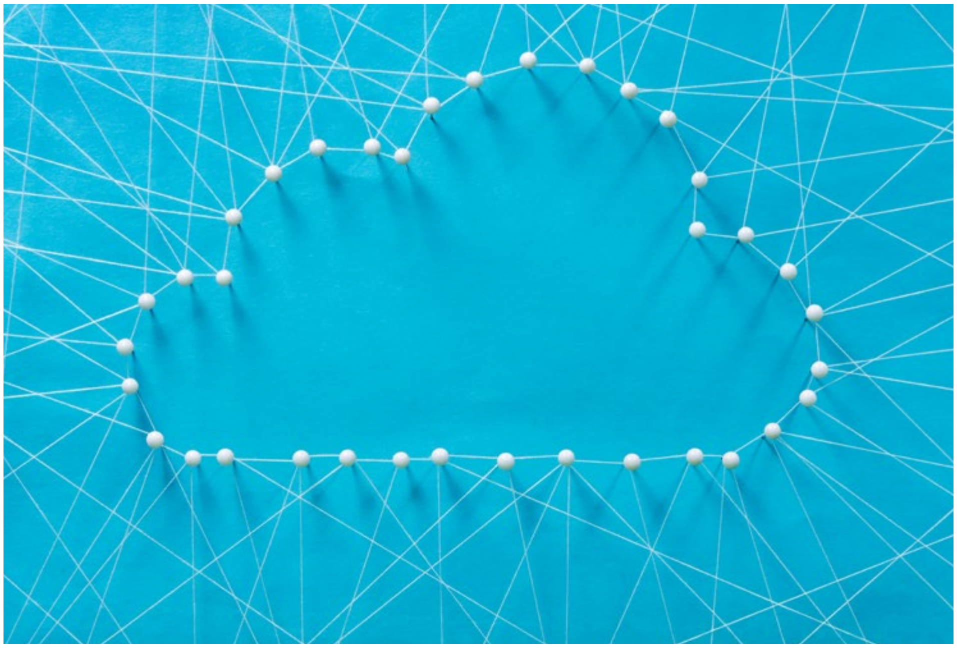
Finance — Who is responsible for financing the solution? How will operating capital be allocated this year and next?

Data ownership — Who retains ownership of data stored in a cloud environment?

Contract management — What are the terms and conditions of the contract? Are they competitive?

Vendor management — How will services provided by the vendor be managed?

Service level management — How will service performance be tracked, monitored, and reported?



Education also plays a critical role in mitigating risks and controlling the proliferation of cloud service usage by an organization's own staff, which gives rise to the so-called shadow IT. Organizations must proactively raise awareness amongst their employees, as many may consider the acquisition and operation of cloud solutions to be no different from traditional on-premise deployments.

By clearly communicating that individual cloud solutions can have fundamentally different management requirements and considerations, organizations can help taper the rise of shadow IT and start implementing informal controls and governance functions. Moreover, including the organization's broader business groups (such as legal and compliance) will help to mitigate applicable risks as accountability is shared across multiple business areas.

This first step does not seek to halt or impede an organization's progress toward cloud adoption. Many organizations want to 'do cloud right' but the reality is that few organizations get it right the first time, so this learning step should complement a company's journey to the cloud while helping to ensure it doesn't go too far down the wrong path.

Step 2: Plan

The second step is initiating planning exercises to identify where the organization is going and the best way to get there. Our experience tells us successful cloud adoption is primarily founded on two things: mature IT fundamentals and solutions that are just the right fit for the organization.

Mature foundational business capabilities and processes—such as vendor management, service management, and demand management, among others—are necessary to support the delivery of cloud solutions. Although cloud-specific capabilities aren't required, managing and operating cloud solutions without such fundamental IT capabilities would risk exacerbating existing IT issues. Companies should conduct a maturity assessment to determine which business capability areas could be hosted in the cloud.

Finding the right fit between functions the company wants to push to the cloud and functions the cloud *can* take on will inform the next steps. As noted earlier, not all workloads are suitable for cloud environments and, similarly, not all cloud capabilities may provide the same level of strategic alignment with an organization's vision. Completing a cloud readiness assessment identifies the gaps the organization may have in its cloud capabilities and defines a roadmap to remediate those risks.

Step 3: Formalize

With a cloud vision and strategy in place, an organization can formalize its cloud adoption through the development of policies and an operating model. The purpose of policy isn't to limit but to enable, since organizations can drive value from their cloud investments through effective policy development.

From experience, we'd recommend taking a proactive approach to cloud policy development. This requires an organization to apply its knowledge of both current and future cloud requirements in order to manage its exposure to risk. Building such a policy typically involves providing guidance in the following areas:

Contract management — What terms, conditions, and clauses must the organization be aware of and actively manage?

Financial management — What are the financial requirements as they pertain to payments, budgeting, and accounting?

Vendor management — What is the organization's role in managing the delivery of cloud services?

Information management — How must data be managed in the cloud?

IT security management — How must data/information be secured in the cloud?

Governance — How will decisions specific to cloud solutions be made? Who holds accountability? How can governance be made flexible enough to manage risk while supporting innovation and cost reduction?

In addition, companies will need to define how they envision the future of cloud within their business and the form it will take within their existing organizational structure. There are two typical options for an operating model: centralized and federated. In a centralized model, a dedicated cloud team is responsible for supporting cloud solutions and supplementing cloud-applicable business activities. With a federated model, cloud-specific roles are assigned throughout cross-functional IT groups to provide guidance and help make each function more cloud-capable.

Selecting and developing the right cloud operating model will depend on an organization's IT maturity, structure, and skillsets, among other considerations. What works for one may not work for another, so it's important to conduct an assessment at the outset to ensure the right resources are put in the right place.

Step 4: Adopt and manage

When organizations have finished preparing the groundwork, the next logical step in their journey to the cloud is to adopt and implement the tools they need to provision and manage their selected cloud solutions. While early adopters have well-articulated visions for how they should manage cloud services, many organizations are not at that level of maturity. They're looking to commercial toolsets to provide guidance. We recommend adopting the various tools provided by CSPs since, given the rapid evolution of cloud services, the market for management tools is still immature.

In our experience, three fundamental capabilities are needed to effectively manage cloud solutions: self-service cloud provisioning, which enables users to request cloud resources by way of a self-service portal; IT orchestration management, which automates processes that manage and execute the creation of requested IT resources (such as virtual machine); and financial management, the processes that track and charge IT costs for cloud resources.

A cloud management platform may be a tempting option, since these are highly capable. But choosing this route at the outset risks investing in a solution that provides limited value relative to vendor-provided tools, is unable to support future cloud services models, and doesn't align with the organization's own cloud management approach.

By using vendor-provided tools as they adopt and integrate cloud services, IT organizations can assess their needs and make an informed decision about whether they need to go to market to acquire a cloud management platform (CMP). The CMP also needs to be supported by a robust cybersecurity platform and competency.

Step 5: Evolve

The last step in the journey is for organizations to take full advantage of the capabilities and the IT environments they've cultivated. The highly scalable and on-demand nature of cloud services make them perfect candidates for **experimentation and innovation**. As cloud environments can be set up for comparatively less investment than in-house deployments and for short periods, they provide low-risk opportunities to try new things. As one of the most significant barriers for innovation is fear of failure, the cloud provides avenues for employees to re-envision business processes and develop proof of concepts for little investment and with limited negative impact.

Modern cloud-based solutions, such as platforms-as-a-service (PaaS), offer organizations the ability **to rapidly transform their operations** with limited procurement requirements and upfront investment. Using various IT capabilities, organizations can digitize their services, such as DevOps, and house them in a centralized system that takes advantage of scalable, available, and secure IT infrastructure.

Since vendors control when software updates are released, organizations will have the most current version available to them at all times. That means users will have leading functions and capabilities at their fingertips, enabling them to improve how they execute their work. Although this may require organizational change management to help staff cope with ongoing change, **modern functionality** creates opportunities for employees to rethink how they do their job.

Finally, since cloud solutions reduce IT operational requirements, organizations can redirect their IT staff to deliver more effective IT and operational services. This can be done by enabling their employees to acquire **new IT skillsets**, such as agile development and prototyping, and to take advantage of **new capabilities**, including portals, resource pooling, and application development.

Conclusion

When done right, the cloud offers transformative opportunities for organizations. We see that demonstrated in the success stories shared in this paper.

However, to be done right, organizations need to approach the cloud with clarity of vision and expectations, knowledge of options, understanding of business drivers (both opportunities and risks), proper planning, disciplined execution, and ongoing, deliberate governance and management.

In today's environment of constant and accelerated technological evolution, it is difficult to comfortably stay on top of all the developments in the cloud ecosystem. Evolving vendor landscapes, new solutions, products and services, constant innovation and disruption seem to offer endless opportunities, but also endless ways to get things wrong. This paper lays out the steps an organization can consider taking to get things right—and to start really "thinking cloud".

Contacts

For more information about transitioning to the cloud, please contact:

Dalibor Petrovic
Partner, Consulting
Western Canadian Technology Strategy & Architecture Leader
dpetrovic@deloitte.ca
780-421-3716

David Brassor
Director, Consulting
Canadian Cloud & Infrastructure Practice Leader
dbrassor@deloitte.ca
416-874-3150

Celia Wanderley
Senior Manager, Consulting
Technology Strategy & Architecture
cwanderley@deloitte.ca
780-421-3640

Arish Kathawala
Manager, Consulting
Technology Strategy & Architecture
akathawala@deloitte.ca
416-601-6506

Daniel Blackburn
Senior Consultant, Consulting
Technology Strategy & Architecture
dblackburn@deloitte.ca
780-421-3617

Endnotes

1. “NIST Cloud Computing Program - NCCP,” National Institute of Standards & Technology, accessed October 24, 2017, https://www.nist.gov/programs-projects/cloud-computing; Deloitte Analysis.
2. “Financial Case for Moving to the Cloud,” Gartner, accessed October 24, 2017, https://www.gartner.com/smarterwithgartner/the-financial-case-for-moving-to-the-cloud/; Deloitte Analysis.
3. “Reducing Operating Costs with AWS,” Cloud Technology Partners, accessed October 24, 2017, https://www.cloudtp.com/doppler/reducing-operating-costs-aws/; Deloitte Analysis.
4. “Why Tomb Raider publishers created their own database service,” Cloud Computing News, accessed October 24, 2017,
5. “Global Investment Bank, Western Europe: Solving Data Residency and Privacy Compliance Challenges,” Voltage Secu rity, accessed October 24, 2017, https://4b0e0ccff07a2960f53e-707fda739cd414d8753e03d02c531a72.ssl.cf5.rackcdn.com/wp-content/uploads/2015/01/Voltage_CS_Global_Bank_WEurope_DataRes_Compliance.pdf; Deloitte Analysis.
6. “PCI Security,” Payment Card Industry Security, accessed October 24, 2017, https://www.pcisecuritystandards.org/pci_security/
7. “Challenging Compliance & Regulation Requirements for Cloud Services Adoption” Canadian Broadcasting Company (CBC), accessed October 24, 2017, http://www.cbc.radio-canada.ca/en/reporting-to-canadians/sync/sync-issue-4-2013/cloud-compliance/; Deloitte Analysis.
8. “Oldcastle increases speed of innovation and delivery of integrations with a hybrid platform,” MuleSoft, accessed October 24, 2017, https://www.mulesoft.com/case-studies/soa/oldcastle-precast; Deloitte Analysis.
9. “Netflix finishes its massive migration to the Amazon cloud,” ARS Technica, accessed October 24, https://www.arstechnica.com/information-technology/2016/02/Netflix-finishes-its-massive-migration-to-the-amazon-cloud/; Deloitte Analysis.
10. “Adobe Takes a Customer-Centric Approach to e-Commerce, Improving Functionality, Revenue, and Customer Satisfaction,” Deloitte, accessed October 24, 2017, https://www2.deloitte.com/content/dam/Deloitte/global/Documents/Technology/gx-cons-adobe-client-spotlight.pdf; Deloitte Analysis.
11. “Matson Modernizes Shipping by Going All-in on AWS Cloud,” Amazon Web Services, accessed October 24, 2017, https://aws.amazon.com/solutions/case-studies/matson/; Deloitte Analysis.

Deloitte.

www.deloitte.ca

Designed and produced by the Deloitte Design Studio, Canada. 17-5346T