McKinsey Digital

How CIOs and CTOs can accelerate digital transformations through cloud platforms

To capture the real value from cloud, companies need to focus their investments and build a cloud-ready operating model.

by Jayne Giezmo, Mark Gu, James Kaplan, and Lars Vinter

September 2020

It has been more than a decade since the first corporate experiments with external cloud platforms, and the verdict is long in on their business value. Companies that adopt the cloud well bring new capabilities to market more quickly, innovate more easily, and scale more efficiently—while also reducing technology risk.

Unfortunately, the verdict is still out on what constitutes a successful cloud implementation to actually capture that value. Most CIOs and CTOs default to traditional implementation models that may have been successful in the past but that make it almost impossible to capture the real value from the cloud. Defining the cloud opportunity too narrowly with siloed business initiatives, such as next-generation application hosting or data platforms, almost guarantees failure. That's because no design consideration is given to how the organization will need to operate holistically in cloud, increasing the risk of disruption from nimbler attackers with modern technology platforms that enable business agility and innovation.

Companies that reap value from cloud platforms treat their adoption as a business-technology transformation by doing three things:

— Focusing investments on business domains where cloud can enable increased revenues and improved margins

— Selecting a technology and sourcing model that aligns with business strategy and risk constraints

— Developing and implementing an operating model that is oriented around the cloud

CIOs and CTOs need to drive cloud adoption, but, given the scale and scope of change required to exploit this opportunity fully, they also need support and air cover from the rest of the management team.

Four failure modes prevail

Over the past 20 years, there have been multiple disruptions in the way large enterprises host applications—from expensive proprietary processors to commodity x86 architectures, from proprietary operating systems to open-source Linux, and from servers dedicated to a single application to many virtual machines running on a single server. Together these changes have transformed the cost structure of application hosting. Twenty years ago a single small application might run on a $25,000 server. Today, a similar-size application might run on a $5,000 server shared with ten other applications.

Unlike past successful programs to adopt Linux, x86 processes, or server virtualization, implementing cloud is more challenging. First, the thousands of applications a large enterprise might have built over the past three decades need remediation or re-architecting to run efficiently, securely, and resiliently in the cloud. In some cases, companies have found existing applications cost more to run in the cloud before remediation.[1] Required investments often result in an unexciting ROI for cloud migration, at least for companies that have already aggressively optimized their on-premises infrastructure environment. The cost economics of cloud adoption can be much more attractive for companies that can use it as a forcing mechanism to optimize their infrastructure environment or to avoid making a large data-center capital investment.

Second, the economics, skills, processes, and organizational changes required are too complex and span too many different parts of the business for infrastructure heads to manage on their own.

These realities have led an overwhelming majority of large institutions to experience one or more of the following failure modes:

— *Pilot stall:* Companies have succeeded in implementing a few greenfield applications on public-cloud platforms, but the value derived from these programs has been limited. This makes further progress impossible because tech leaders cannot make a convincing business case to extend the use of the cloud

[1] In the cloud, charges for applications consumer hosting, storage, and network services are based on usage ("by the drink"). Therefore, applications not designed for efficient resource usage can run up large bills with cloud service providers.

platform into the heart of IT's technology environment.

— *Cloud gridlock:* Cloud initiatives become jammed up in long queues because IT cannot build out the automation or reference architectures required to use public-cloud-platform services in a secure, resilient, and compliant fashion.

— *No value from "lift and shift":* The migration of significant portions of the technology environment—largely by replacing on-premises virtual machines with off-premises ones without taking advantage of cloud-optimization levers—has failed to significantly reduce costs or increase flexibility. Support for cloud initiatives subsequently collapses.

— *Cloud chaos:* Tech leadership does not have an aligned vision and does not provide the required guidance or management oversight, leaving developers largely to their own devices in configuring cloud services. This leads to very divergent approaches and tooling with significant security, resiliency, and compliance risks.

As a result, although cloud service providers (CSPs) are growing quickly, enterprise cloud adoption has consistently lagged predictions. Multiple surveys performed by McKinsey indicate that large companies host 10 to 15 percent of their applications in the cloud but continue to host the core of their technology environment in traditional data centers.[2]

Using cloud to enable digital transformation

Only 14 percent of companies launching digital transformations have seen sustained and material performance improvements.[3] Why? Technology execution capabilities are often not up to the task. Outdated technology environments make change expensive. Quarterly release cycles make it hard to tune digital capabilities to changing market demands. Rigid and brittle infrastructures choke on the data required for sophisticated analytics.

Operating in the cloud can reduce or eliminate many of these issues. Exploiting cloud services and tooling, however, requires change across all of IT and many business functions as well—in effect, a different business-technology model.

Success requires CIOs and tech leaders to do three things.

1. Focus cloud investments in business domains where cloud platforms can enable increased revenues and improved margins

The vast majority of the value the cloud generates comes from increased agility, innovation, and resilience provided to the business with sustained velocity. In most cases, this requires focusing cloud adoption on embedding reusability and composability so investment in modernizing can be rapidly scaled across the reset of the organization. This approach can also help focus programs on where the benefits matter most, rather than scrutinizing individual applications for potential cost savings (Exhibits 1 and 2).

— *Faster time to market:* Cloud-native companies can release code into production hundreds or thousands of times per day using end-to-end automation. Even traditional enterprises have found that automated cloud platforms allow them to release new capabilities daily, enabling them to respond to market demands and quickly test what does and doesn't work. As a result, companies that have adopted cloud platforms report that they can bring new capabilities to market about 20 to 40 percent faster.[4]

— *Ability to create innovative business offerings:* Each of the major cloud service providers offers hundreds of native services and marketplaces that provide access to third-party ecosystems with thousands more. These services rapidly

[2] McKinsey Cloud Cube Survey; see also Arul Elumalai, James Kaplan, Mike Newborn, and Roger Roberts, "Making a secure transition to the public cloud," January 2018, McKinsey.com.
[3] "Five moves to make during a digital transformation: McKinsey Global Survey results," April 2019, McKinsey.com
[4] Cameron Coles, "11 advantages of cloud computing and how your business can benefit from them," McAfee, June 9, 2015, skyhighnetworks.com.

Exhibit 1

Cloud benefits vary by consumption models.

Increasing agility, automation, access to innovation, and scalability

Consumption model		Traditional	Lift-and-shift virtual machines	IaaS	PaaS	FaaS
Application maturity	Application architecture	Multi-tier	Multi-tier	Fault-tolerant machine images	Loosely coupled services, using containers	Event driven, serverless, fully stateless
	Automation of app-development operating model	Traditional, bespoke development	Traditional, bespoke development	Move toward product-based, agile development	Move toward DevSecOps	Move toward proprietary, cloud-native development
Infrastructure maturity	Tenancy	Dedicated	Dedicated or shared	Dedicated or shared	Mostly shared and managed	Shared
	Hosting	Mostly on-premises, co-location	Off-premises[2]	Off-premises[2]	Off-premises[2]	Off-premises[2]
	Automation of infrastructure operating model	Basic automation, but with people-dependent processes	Basic automation, but with people-dependent processes; continuous integration	Fault-tolerant and resilient infrastructure (eg, mature auto-scaling); CI/CD[3]	Highly automated; default use of native managed services (eg, stateless, self-healing); CI/CD[3]	3rd-party orchestration; no management needed from the customer; CI/CD[3]
Run-rate benefits & KPIs	% productivity increase vs IT spend	Baseline	–5–0%	10–20%	20–30%	30–40%
	Time to market	Quarterly	Quarterly	Monthly to every 2 weeks	Every 2 weeks/ as needed	Daily/multiple times a day
	Change vs run ratio	30:70	30:70	40:60	50:50	70:30
One-time transition costs	% transition cost vs IT spend	Baseline	10%	10–20%	20–60%	80–120%
	IT payback period[1] (varies by workload type)	N/A	May not pay back	1–2 years	2–3 years	2–3 years

[1]IT benefits only (infrastructure and application development/maintenance); does not include business-acceleration benefits.
[2] Primarily off-premises; can be on-premises or edge for specific regulatory, security, or network-connectivity-constrained situations.
[3] Continuous integration/continuous delivery.

Exhibit 2

Cloud investment priorities vary by domain.

Cloud-based Mostly SaaS-based

Research	Development	Supply chain	Commercial	Enterprise
Discovery	Medical affairs	Plan	Marketing	Finance
Pre-clinical operations	Regulatory affairs	Source	Service	Human resources
Translational science	Pharma-covigilance	Make	Sales-force execution	Legal
	Clinical operations	Deliver	Commercial operations and partner relationship	Facilities and real estate
		Ensure quality	Global education	Public relations

evolve and grow and provide not only basic infrastructure capabilities but also advanced functionality such as facial recognition, natural-language processing, quantum computing, and data aggregation.

— *Reduced risk:* Cloud clearly disrupts existing security practices and architectures but also provides a rare opportunity to eliminate vast operational overhead to those that can design their platforms to consume cloud securely. Taking advantage of the multibillion-dollar investments CSPs have made in security operations requires a cyber-first design that automatically embeds robust standardized authentication, hardened infrastructure, and a resilient interconnected data-center availability zone.

— *Efficient scalability:* Cloud enables companies to automatically add capacity to meet surge demand (in response to increasing customer usage, for example) and to scale out new services in seconds rather than the weeks it can take to procure additional on-premises servers. This capability has been particularly crucial during the COVID-19 pandemic, when the massive shift of digital channels created sudden and unprecedented demand peaks.

A financial-information provider determined that moving its customer-facing applications to the cloud could enable much faster and less costly responses to market opportunities. For example, hosting these applications in the cloud meant that the cost of setting up operations in a new country would be negligible, when it had traditionally cost at least a million dollars. A health-insurance carrier examined

its current project portfolio and found that several billion dollars in additional revenues could be accelerated by cloud adoption. Moving the systems that help them interact with healthcare providers has proven to be especially attractive because of the ability to accelerate the onboarding of new providers.

2. Select a technology, sourcing, and migration model that aligns with economic and risk constraints

Decisions about cloud architecture and sourcing carry significant risk and cost implications—to the tune of hundreds of millions of dollars for large companies. The wrong technology and sourcing decisions will raise concerns about compliance, execution success, cybersecurity, and vendor risk—more than one large company has stopped its cloud program cold because of multiple types of risk. The right technology and source decisions not only mesh with the company's risk appetite but can also "bend the curve" on cloud-adoption costs, generating support and excitement for the program across the management team.

If CIOs or CTOs make those decisions based on the narrow criteria of IT alone, they can create significant issues for the business. Instead, they must develop a clear picture of the business strategy as it relates to technology cost, investment, and risk.

Where to use the different "as-a-service" options

Just as CIOs and CTOs have long had to make buy-versus-build decisions, in the cloud they must determine whether to procure software-as-a-service (SaaS) offerings or build their own applications to run on infrastructure-as-a-service (IaaS) or platform-as-a-service (PaaS) services hosted in the cloud. CIOs should work with senior business leaders to determine which business domains have differentiated processes requiring bespoke software and domains that can be supported by SaaS offerings. SaaS has gotten the most traction in functional domains such HR and customer relationship management (CRM), but there are increasingly capable vertical-specific SaaS packages in many sectors as well.

Which services should be indexed in cloud

There are multiple architectural models for running bespoke needs in cloud, each with its own benefits and drawbacks. A clear understanding of what these are is crucial for CIOs who want to create a tailored approach to cloud that embeds operational efficiencies during migration to maximize the benefits:

— Consuming traditional virtual machines has the lowest transition costs and implies the lowest level of vendor lock-in but, depending on the application, may not provide much benefit in terms of agility or time to market.

— Using CSP native compute (IaaS) with third-party-provided cloud-ready images provides the lowest level of vendor lock-in and limits changes to the infrastructure, providing low levels of benefit for imported availability and maintenance, if deployed with automation.

— Refactoring applications to use containerization enables far greater agility, flexibility, scalability, and sustainability with increased productivity. Exact experience varies,many with most companies seeing a 12–18-month payback period. When containerization is designed and run with clearly defined standards, it can provide a predictable pathway to support the repatriation of containerized applications from one cloud provider to another. Containerization is most suitable for applications but requires code refactoring during migration from traditional environments. Containerization provides optimized efficiencies, scalability, and abstraction with cost efficiency.

— Rewriting an application to be cloud native requires the highest investment but yields the largest improvements in both agility and total cost of ownership. This often requires using proprietary services from a CSP, which may create an unacceptable vendor dependency for some companies.

How to address the loss of the traditional physical-security perimeter

Migrating to the cloud moves applications outside the company's network perimeter and creates a new security paradigm.

CIOs and CISOs will need to identity how much dependency they will build into the existing legacy network design and traditional security systems. There tend to be three options:

— *Route traffic through proprietary data centers.* About 75 percent of large companies route all cloud traffic through their data center, which attempts to leverage existing traditional perimeter protections. This approach can add 10 to 20 percent to hosting costs and add significant latency, reducing the quality of a user's experience. In addition, securing cloud requires the deployment of native networking and security tooling to protect cloud activities in parallel. For this reason, fewer than 20 percent of CISOs expect to use this option in the future.[5]

— *Rebuild the security perimeter in the cloud.* More than two-thirds of companies will take the time and invest enough to adopt native network flows using native tooling and configurations with mature full-stack DevSecOps orchestration. Integration with security-service SaaS providers and targeted compliance tooling will be used to protect the dynamic perimeter.

— *Build "zero-trust applications."* Roughly one-fifth of companies will build zero-trust applications that do not require a network perimeter. Most CISOs believe this model provides the best combination of cost and protection. However, it depends on sophisticated application-development skills that many companies will struggle to develop.[6]

How many CSPs to engage

There are a number of major CSPs and several smaller ones. Using multiple CSPs increases engineering and integration costs. Conversely, focusing on one CSP may limit access to some types of innovation and will lock the company into the single provider, which has often been painful in the traditional on-premises world.

Smaller and less technologically sophisticated companies seem to be gravitating toward using a single CSP. Larger companies, however, with hundreds of millions of dollars in technology-infrastructure spend, are more inclined to use multiple vendors, though they will often start with a single CSP. The largest banks, for example, often put significant effort into using multiple vendors, each best suited to different types of workloads.

While some paint an idyllic picture of companies "cloud bursting" (using a mix of private and public cloud hosting to manage peaks of demand) their applications in real time to whichever CSP can provide the lowest-cost capacity, we have not observed this occurring except for very specialized workloads.

How to migrate existing applications

At the highest level, companies can choose to focus remediation on security and compliance fixes and then optimize systems once they are running, or they can choose to optimize as they go. There is no single right answer here; companies must choose the type of risk they wish to underwrite. Migrating and then optimizing later can help break through the gridlock many companies have experienced with their cloud programs. But this approach requires accepting that some applications may cost more in the short term and aggressively preventing application teams from moving on after migration and neglecting to optimize their systems in the cloud.

[5] James Kaplan, Mike Newborn, and Roger Roberts, "Making a secure transition to the public cloud," January 2018, McKinsey.com.
[6] Ibid.
[7] Technical debt is the implied cost of rework caused by implementing a quick but brittle or otherwise architecturally suboptimal solution.

3. Change operating models to capture cloud value

Capturing the value of migrating to the cloud requires changing both how IT works and how IT works with the business. The best CIOs and CTOs follow a number of principles in building a cloud-ready operating model:

— *Make everything a product.* To optimize application functionality and mitigate technical debt,[7] CIOs need to shift from "IT projects" to "products"—the technology-enabled offerings used by customers and employees. Most products will provide business capabilities such as order capture or billing. Automated as-a-service platforms will provide underlying technology services such as data management or web hosting. This approach focuses teams on delivering a finished working product rather than isolated elements of the product. This more integrated approach requires stable funding and a "product owner" to manage it.

— *Focus on developer experience.* CIOs must redesign the technology delivery processes "end to end," using cloud-native practices to create a "delightful" developer experience. Applying developer journeys to workflows with modern tooling drives organic adoption and sustainable velocity.

— *Integrate with business.* Achieving the speed and agility that cloud promises requires frequent interaction with business leaders to make a series of quick decisions. Practically, business leaders need to appoint knowledgeable decision makers as product owners for business-oriented products. These are people who have the knowledge and authority to make decisions about how to sequence business functionality as well as the understanding of the journeys of their "customers."

— *Ensure cloud is fully software defined, automated and abstracted.* On-premises environments are often slow and rigid due to complex dependencies between software layers, physical hardware, and security components. In cloud, top-performing IT organizations shift to defining everything as software or "as code" to ensure sustainability using abstraction and automation across three design tenants:

- Cloud scale-out abstracts its infrastructure as code (IaC) to tools that offer multi-CSP and SaaS vendor support (such as Terraform or Ansible) so teams can unify on a common approach that embeds co-creation. Continuous integration/continuous delivery (CI/CD) automates the provisioning of infrastructure and delivery of applications with embedded risk assessment and security governance "in pipeline" using DevSecOps.

- Repeatable patterns (such as logging or building virtual private clouds with defined networks) and security guardrails (such as at-rest encryption or inspection tooling) are coded into reusable components that are published to the IaC tool, which teams can then use in a self-service manner in their platform builds, driving consistency.

- Paper-based reference architectures are converted to codified blueprints using modern architectures (containerization, for example) that are composable so teams have the flexibility to swap in and out new capabilities and custom integrations during provisioning.

— *Secure cloud by design.* CISOs must redesign cyber programs, update policies, and modernize controls to build security seamlessly into cloud. This includes shifting risk as early in the provisioning process as possible by embedding guardrails, governance, testing, and security assessment in line to drive uniformed compliance. Infrastructure and security teams should strive to eliminate the human "middleware"

[7] Technical debt is the implied cost of rework caused by implementing a quick but brittle or otherwise architecturally suboptimal solution.

and prevent risk before deployment to deliver consistently secured, scalable environments that operate at velocity.

— *Be agile everywhere.* Traditional infrastructure, networking, and security teams must adopt iterative ways of working and codification, utilizing modern development practices of continuous integration and delivery, ensuring cloud builds use a layered approach so changes can be applied granularly with limited dependency or impact on applications and workloads.

— *Drive cloud skill sets across development teams.* Traditional centers of excellence charged with defining configurations for cloud across the entire enterprise quickly get overwhelmed. Instead, top CIOs invest in delivery designs that embed mandatory self-service and co-creation approaches using abstracted, unified ways of working that are socialized using advanced training programs (such as "train the trainer") to embed cloud knowledge in each agile tribe and even squad.[8]

— *Build engineering skills and culture.* Some companies have seen technical execution as a commodity and outsourced and offshored development activity but retained business analysts and project managers. Others have rewarded IT staff for deep skills in specific vendor technologies. In contrast, as cloud is based on everything as software, its operating model requires everyone to be software engineers who can traverse multiple technology stacks to deliver integrative solutions, with the primary attribute being that everyone can code and understands modern development practices. But some engineers' deep subject-matter expertise aligns to cloud providers, and others' to bespoke product engineering. One institution has set the aspiration that 80 percent of its technology staff will regularly code.

— *Take a risk-based approach.* To prevent security, resilience, and compliance concerns resulting from cloud adoption, top CIOs work closely with their CISOs to develop a clear-eyed view on risk and have rigorous discussions about the best mechanisms for aligning decisions about their technology environment with their risk appetite.

One CTO at a natural-resources company took many of these principles to heart in developing an effective cloud-optimized operating model. He led the implementation of agile ways of working for business "product owners," application development, infrastructure, and security. In particular, he invested in unifying a software-defined approach to cloud with infrastructure as code to embed reusability and composability with end-to-end automation, so that developers could provision workloads on cloud with dedicated as-a-service business platforms securely and resiliently. As a result, the company was able to release new capabilities in days rather than months, while limiting risk and technical debt.

How CIOs and CTOs can join forces with leadership to succeed

Given the economic and organizational complexity required to get the greatest benefits from the cloud, heads of infrastructure, CIOs, and CTOs need to engage with the rest of the leadership team. That engagement is especially important in the following areas:

— *Technology funding.* Technology funding mechanisms frustrate cloud adoption—they prioritize features that the business wants now rather than critical infrastructure investments that will allow companies to add functionality more quickly and easily in the future. Each new bit of tactical business functionality built without best-practice cloud architectures adds to your technical debt—and thus to the complexity of building and implementing anything in the future. CIOs and CTOs need support from the rest of

[8] The ACG Blog, "Why 'central cloud teams' fail (and how to save yours)," blog entry by Forrest Brazeal, April 23, 2020, acloudguru.com.

the management team to put in place stable funding models that will provide resources required to build underlying capabilities and remediate applications to run efficiently, effectively, and safely in the cloud.

— *Business-technology collaboration.* Getting value from cloud platforms requires knowledgeable product owners with the power to make decisions about functionality and sequencing. That won't happen unless the CEO and relevant business-unit heads mandate people in their organizations to be product owners and provide them with decision-making authority. Some companies have explicitly combined tech and business teams.

— *Engineering talent.* Adopting the cloud requires specialized and sometimes hard-to-find technical talent—full-stack developers, data engineers, cloud-security engineers, identity and access-management specialists, cloud engineers, and site-reliability engineers. Unfortunately, some policies put in place a decade ago to contain IT costs can get in the way of onboarding cloud talent. Companies have adopted policies that limit costs per head and the number of senior hires, for example, which require the use of outsourced resources in low-cost locations. Collectively, these policies produce the reverse of what the cloud requires, which is a relatively small number of highly talented and expensive people who may not want to live in traditionally low-cost IT locations. CIOs and CTOs need changes in hiring and location policies to recruit and retain the talent needed for success in the cloud.

— *Rational risk assessment.* It's not uncommon for security, resiliency, and compliance concerns to stop a cloud program in its tracks. CIOs and CTOs can help leaders to understand risk issues and how to mitigate them, and how to work with CEOs and other business leaders to place cloud risks in the context of existing on-premises risks.

The recent COVID-19 pandemic has only heightened the need for companies to adopt digital business models. Only cloud platforms can provide the required agility, scalability, and innovative capabilities required for this transition. While there have been frustrations and false starts in the enterprise cloud journey, companies can dramatically accelerate their progress by focusing cloud investments where they will provide the most business value and building cloud-ready operating models.

Jayne Giezmo is a digital expert in McKinsey's Brisbane office; **Mark Gu** is an associate partner in the New York office, where **James Kaplan** is a partner; and **Lars Vinter** is a partner in the Copenhagen office.