KPMG

Improving cloud ROI —

and why CIOs are the ones to do it

Improving cloud ROI

Whatever the technology, we've found that chief information officers (CIOs) and other IT leaders have always been focused on delivering value. In last year's KPMG Technology Survey, "proven return on investment (ROI)" was the most common motivation US respondents provided when asked about their technology investment choices.[1]

Yet it's rare we speak with any business leader who doesn't say they wish they had a better ROI from their cloud spend. So why the disconnect? If ROI is a primary focus, why haven't they been able to meet ROI expectations?

The cloud promised every business enormous efficiencies and massive savings, largely based on its Software-as-a-Service (SaaS) model. Yet SaaS solutions may have created a false sense of simplicity. Cloud and SaaS providers can make it seem easy. We believe this may be at the heart of challenges.

As many organizations now rush to implement artificial intelligence (AI), any illusion of IT simplicity is rapidly dissolving. Now is the time for organizations to rethink the role of IT—and for IT leaders to play a more important role in delivering value.

[1] Source: KPMG US Technology Survey Report, 2023

The impact of shadow IT

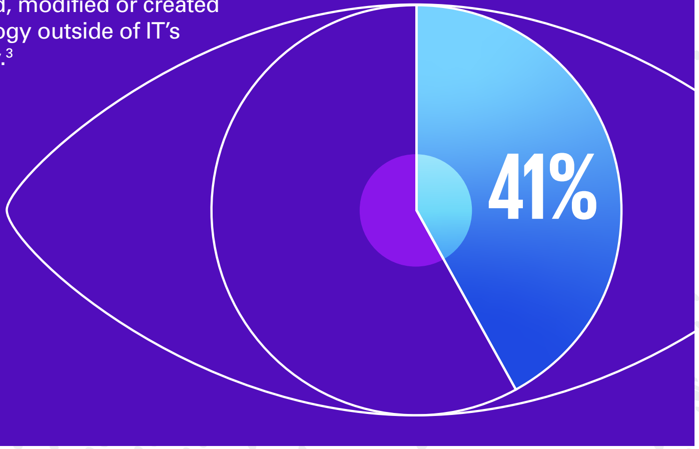
The ability for a business organization to implement a SaaS solution without IT involvement has led to the growth of “shadow IT” organizations, moving both control and budget from IT leaders’ purview out to individual business units.

It’s a trend that built steadily over the last decade. In 2018, a Harvey Nash-KPMG CIO survey found that two-thirds of all respondents reported having more than five percent of their IT spend managed outside their department.[2] In 2023, Gartner reported that 41 percent of employees acquire, modify or create technology outside IT’s visibility.[3]

As one might expect, this trend had an impact on the influence of IT leaders. The 2020 version of the Harvey Nash-KPMG CIO survey noted that the “changing nature of technology [has] removed many of the certainties that have fueled the importance of the CIO role.” It also found that board membership for CIOs was down from 71 percent in 2017 to 61 percent in 2020.[4]

Out of sight, out of control

In 2023, 41 percent of employees acquired, modified or created technology outside of IT’s visibility.[3]



The recent explosion of generative AI (genAI), however, may have reversed this trend. It has exposed many of the weaknesses of shadow IT by putting the growing complexity of businesses’ IT infrastructures into the spotlight. Many businesses have recognized the enormous challenge that multiple shadow IT organizations can create when trying to identify, access and manage the data genAI requires. Many have recognized the security and compliance risks of having multiple shadow IT organizations. But few appear to have recognized the ROI challenges they may have created.

How AI is pulling back the curtain

It’s undeniable that cloud and SaaS solutions can greatly simplify both technology implementation and ROI realization. The business might implement a SaaS solution for handling human capital management, for example. It could see the efficiencies or added capabilities the solution would offer, understand the associated licensing costs, calculate ROI, and justify the expense. IT’s involvement might be limited.

Today that same SaaS solution may offer an AI-driven option to improve decision-making. The business can still clearly estimate its financial benefits and understand its per-seat licensing costs. But licensing costs may be just the tip of the iceberg when calculating ROI.

[2] Source: Harvey Nash/KPMG CIO Survey, 2018

[3] Source: *Gartner Unveils Top Eight Cybersecurity Predictions for 2023-2024*, March 28, 2023

[4] Source: *The slow deathe of the CIO in financial services and the rise of C-level tech influence*, Andrew Jenkins, Finance Derivative, July 11, 2023

The impact of shadow IT continued

With the growing popularity of genAI, it's highly likely multiple business units will be considering similar solutions. Each request may be ROI-justifiable on its own, but not when viewed in context. The business as a whole doesn't likely need five different genAI assistants or five different data analytics solutions. Individual business units won't understand the implications of their decisions or be able to recognize overlapping synergies. While chief operating officers (COOs) may be able to fill the role of "centralized synergy keeper," the complexities don't stop there.

As new technologies and delivery models evolve, it's more important than ever for companies to rely on the expertise of the CIO. At right, for example:

Modern data fabric and AI

Few AI features can be implemented or delivered as discretely as a SaaS solution. To support the new AI feature, data may need to be moved or rationalized. New controls may need to be put in place. Data egress costs across multiple cloud providers may need to be factored in. There may be increased runtime costs for ancillary systems or increased training and support costs for IT personnel. Reliance on legacy systems, customizations, and other proprietary solutions must be factored in. The list goes on.

Hybrid and multi-cloud management

Delivery model complexity—the combination of public cloud, private cloud, hybrid multicloud, on-premise—is not something the business can see or be expected to understand or account for. The business will continue to know what functionally it needs to achieve business outcomes—that won't change. But IT leaders are better positioned to continually assess the implications for the larger strategic vision, understand how to address the technology complexities associated with achieving those goals, and determine the most ideal path forward in the most economically sustainable way.

As new technologies and delivery models evolve, it's more important than ever for companies to rely on the expertise of the CIO.

Transforming IT into a force for optimization

IT leaders are ideally positioned to be the heroes in this story, but two things must change. First, businesses must revisit the role of IT and that of its leader within the organization and restore some of the responsibility and authority that may have slipped away in recent years. Second, IT organizations must be prepared and fully equipped to handle that responsibility.

The latter is no small challenge. With a mandate to manage a holistic view, IT leaders must prioritize their efforts. We see several key areas where IT focus and expertise may be best applied to help deliver greater business value from cloud technology:

Addressing the explosion of data

In the last three to five years, data growth has been astronomical at every one of our clients. Few anticipated that data would grow at such a rapid pace, and managing this growth has become a major challenge.

It's more than just speed and volume. Some may have migrated an application to the cloud, but failed to modernize the application, creating a data silo. Similarly, some have failed to modernize the data to harness its power, turning it into something more meaningful that would provide more insights into their business, which in turn is value realized. Data sources are often widely dispersed, in on-premise systems, in public and private clouds, and across multiple cloud providers, which can make it challenging to ingest, align and standardize data.

Many organizations suffer from a lack of data quality, a lack of trust in data and low data literacy. There may be large, operationally complex and slow data pipelines causing timing collisions. Technology sprawl with many manual operational touchpoints and workarounds put in place over the years can add to the complexity. Tightly coupled technology stacks can inhibit modernization efforts and planning flexibility. Data security and privacy risks abound.

Despite the complexity, there are solutions at hand designed to address the challenge. A low-code integration-Platform-as-a-Service (iPaaS) solution combined with an application programming interface (API) management platform (APIM) can dramatically speed and simplify the "plumbing" required to connect all of the disparate pieces. A modern, cloud-based data platform can then be used for real-time, automated extraction of data from each technology platform, and translated into a common data model. That provides one centralized, rationalized set of data, regardless of the complexity or diversity of the underlying technology ecosystem. It can also enable DataOps—the same DevSecOps automation and control principles and processes used for software, including Agile and CI/CD, to be applied to data.

Where CIO expertise can help

Data strategy and architecture

CIOs can help define the business case, data and technology architecture, standards for data usability, consistency and integrity, metadata standards, ETL/ELT data processing standards, data security standards, and data modeling plans.

Modern data fabric

CIOs can lead the design and implementation of a cloud-based data architecture and integration strategy, improve data uniformity, accuracy and integrity, and map the flow of data between applications and data stores.

Advanced data integration

CIOs can eliminate data siloes by connecting applications and their data across hybrid cloud, multicloud and on-premise environments with an application programming interface (API) architecture.

Transforming IT into a force for optimization continued

Adapting to the cloud business model

Cloud providers make money through consumption. Anytime a server is on and running, even if it's not being used, the meter is running and the costs are climbing. That's different than if the same server were in an on-premise datacenter where it wouldn't matter if it were on or not.

This fundamental difference in cost models requires IT organizations to approach how they build and operate applications differently in the cloud in order to control costs. However, we often see IT organizations fail to take these things into consideration. Is my server on or off? Am I using this application only when I have a need? How do I know? Is it designed to automatically scale up and down based on demand?

In our experience, it's rare to find IT organizations with the skills required to completely rethink the way they approach application design to make it fully cloud-optimized. Simply running an application originally designed to run on-premise in the cloud can be very costly—potentially significantly more costly than hosting it on-prem, depending on the application's design. As you might expect, this also has tremendous implications for deciding what legacy applications should and shouldn't be moved to the cloud.

A cloud-native approach extends to taking advantage of some the newer capabilities being offered by the major hyperscalers, such as containerization and infrastructure as code, as well as features such as artificial intelligence or blockchain services. It requires adoption of IT automation such as DevSecOps. It also requires discipline to control development of custom features because that can limit the ability to take advantage of prebuilt services and their updates. Limiting desired customization may require accommodations by the business side and therefore alignment of expectations.

We've seen a bit of skepticism that there's really ROI to be mined here. It's tempting to consider this solely as a "people" challenge—having legacy people who are trying to develop and operate for the cloud when the two don't match. While that's true to an extent, we've seen organizations hire new people and bring in technology experts in the field yet still struggle to get the value out and to make the progress that they want. Inevitably in these cases, it's a strategy, process, policy and culture issue, something deeply ingrained into the IT organization itself.

Where CIO expertise can help

Cloud modernization and migration

CIOs can oversee the migration and modernization of the application portfolio to the cloud, modernize storage platforms, and update middleware and application integrations.

Cloud-native development

CIOs can help define target architectures, implement modern IT service delivery practices and take advantage of cloud-native services including API-driven microservices, containerization, infrastructure as code (IaC), and low-code and AI-generated automation.

Cloud emerging technology

CIOs can develop business value-led strategies, integrated architectural designs, ROI models and roadmaps for execution of leading-edge technologies such as internet of things (IoT), edge computing, digital twins, and augmented and virtual reality.

Transforming IT into a force for optimization continued

Implementing FinOps processes and technologies

ROI challenges often simply boil down to too much spending and too little oversight. But as they say, you can't manage what you can't measure. Without clear visibility and proper governance controls, it's easy to overspend on cloud.

Can you identify and measure key areas such as the percentage of oversized instances, orphaned resources or usage during weekdays versus weekends that are bleeding ROI? If you set a baseline hourly cost of running a server or a container and advise all teams to comply with that objective, how will you monitor results, allocate spending and strive to ensure that your goal is being met over time?

The bleeding of ROI isn't always so directly measurable. Without the proper controls, security teams may operate in reactive mode, and recurring defects and productivity losses can hamper efficiency and effectiveness. Insufficient controls and lack of standardization in data platforms can also make it difficult to leverage advanced analytics and extract essential insights. It's not enough to simply know what your total cloud spend is at any moment. Visibility into where your cloud spend is going, monitoring activity at a granular level, and responding as needed as workloads and objectives change are essential capabilities.

FinOps has emerged as the modern solution to these challenges. FinOps aligns cloud spending with business objectives and helps to ensure that cross-functional teams work harmoniously to enhance financial control and predictability, reduce friction and deliver products and services faster.

FinOps success requires visibility of assets through IT asset management and the use of appropriate tools, technologies and tagging, including automation capabilities. Unfortunately, there are many examples of businesses with multi-cloud environments that are using tools and capabilities provided by their cloud vendors with little to no success. In comparison, platform-independent observability tools can gather data from all available sources and analyze that data for precise visibility into cloud processes, trends, issues and areas requiring improvement. They can enable more sophisticated forecasting beyond simple trend analysis, such as "what-if" analysis.

These tools and the insights they provide are indispensable. Yet without the ability to respond to them, these insights are reduced from extremely valuable to merely interesting.

IT leaders must optimize cloud operations, with visibility into risk controls and vulnerabilities, to help teams be more proactive in addressing risks and defects, with a focus on value instead of capabilities. Modern delivery practices such as Agile and CI/CD are required to help optimize developer productivity, leveraging automation and AI capabilities to enable code quality improvement and proactive discovery of software deficiencies. Data management teams must have data foundational capabilities, including data quality, data cataloging, master data management and data observability.

But with the technology enabled and the principles applied, the resulting well-governed and monitored cloud estate, employing automated controls to reduce and govern cloud spend, can unlock a significant amount of value.

Where CIO expertise is needed

Cloud governance and optimization

CIOs can help implement operational controls, define and automate governance policy and processes, and establish transparency and visibility into inefficiencies, security vulnerabilities and cloud costs. They can implement compliance tools and controls designed to protect the enterprise and its systems with proactive vulnerability detection, and help verify control consistency across modern delivery practices.

Transforming IT into a force for optimization continued

Recognizing—and correcting—bad decisions

In some cases, the lack of value realization simply boils down to poor decision making during initial cloud migration. A business may have chosen the wrong applications to move. They may have chosen the wrong partners. However, given the maturity of cloud technologies, the vendors providing them, and the people within companies who are now better educated and have more experience in making decisions that are better for the business.

With such experience under their belts, some organizations are now embarking on what they call "cloud 2.0" because they've already been down the path before. In many cases, this requires a complete rethinking of their cloud strategy. It can be a tough journey. Inertia is a powerful force, it's never easy to admit defeat, and the sunk-cost fallacy can have a powerful grip on even the most intelligent leader. Knowing when and on what specific technologies and strategies to throw in the towel is a critical decision.

Where CIO expertise is needed

Hybrid and multi-cloud management

CIOs can lead efforts to develop a successful cloud placement strategy with the right mix of on-premise data centers, private clouds and public clouds tailored to the organization's operational requirements that accounts for financial and operational requirements, business needs, technical debt and legacy systems.

Migration that's effective not just from a technology perspective, but also from a financial one, requires a methodology designed for both. It must help you understand your application and data dependencies. It must help you select the application that makes sense to move to the cloud. It must help you understand the upstream and downstream implications of moving these applications, and how to do so in a way that drives efficiencies through a FinOps process.

Cloud affinity also falls into this bucket. It's not uncommon to find an IT organization committed to a particular cloud hyperscaler through no reason other than tradition or inertia but where that provider may not be the best match for their business needs. It's also not unusual for clients to have hundreds of different products on three different clouds plus on-prem. This may be the result of mergers and acquisitions, business-led initiatives outside of IT control, a deliberate strategy to avoid having all their eggs in one basket, or just a natural build-up of cruft over time.

In either case, a complete reexamination of the cloud strategy may reveal significant efficiencies. Based on the industry, the nature of the business, strategic business objectives, and technology requirements, one particular cloud hyperscaler may be more ideally suited than others to handle its workloads, modernize data, and modernize services and application. Identifying all of the variables that go into such a decision and matching business requirements to the strengths and features of leading platforms is no small task. We developed a custom tool called Cloud Compass to help clients assess the options because spreadsheets alone were not capable of handling the complexity.

Transforming IT into a force for optimization continued

Undervalued value

At the top of almost every technology leader's list of priorities—even before ROI—is uptime. Keeping the lights on is mission number one, which includes cyber resilience and disaster recovery strategies and capabilities. But these may not be as sexy as a new genAI solution, or fully appreciated by the business as a true source of value—at least, that is, until a breach or failure occurs. While security and reliability may be undervalued, they're the essential foundation to all technology ROI.

The basic functions that cloud service providers handle, such as vulnerability patching, can create a false sense of security. But as fallout from one recent global crisis involving a vendor rolling out a defective automatic software update illustrates, the consequences of sudden disruption to IT systems can be dire. With headline-grabbing examples of security breaches of cloud environments and failures of critical code, the responsibility for cyber security and reliability is far broader—and it falls on the IT leaders' shoulders to manage. The scale and complexity of cloud security, underpinned by a fundamentally new technology stack and new skills required to operate it, make it an extraordinarily challenging task.

Where CIO expertise is needed

Cloud data security and compliance

CIOs can establish the appropriate governance of the cloud security function and build the underlying control and compliance structure. They must modernize security processes with automation accelerators and security and compliance "as code" solutions to help keep pace with the ever-changing nature of cloud investments, and increase the velocity of successful product deliveries.

Cloud resiliency

CIOs can lead efforts to identify critical business functions, determine maximum allowable downtime based on the regulatory, operational, financial and reputational impact of an outage, and evaluate resiliency architectures and disaster recovery plans. They must implement solutions for application, product and process-centric recovery measures, along with the development of recovery plans and testing procedures.

While security and reliability may be undervalued, they're the essential foundation to all technology ROI.

How KPMG can help

With more than 5,000 dedicated cloud professionals backed by a powerful ecosystem of global alliances, KPMG LLP offers a robust collection of business, technology, and data resources and capabilities designed to help you maximize the value of your cloud investment and become the driving force behind your organization's cloud ROI.

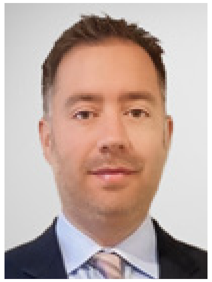
Data strategy, architecture and implementation: We can help you accelerate your genAI efforts and unlock value trapped in your data, starting with a solid data strategy. We can help connect data across hybrid cloud, multi-cloud and on-premise environments with an API architecture. With our KPMG Modern Data Platform (MDP), we can help you apply modern DevOps principles such as Agile and CI/CD to your data. We can help enable data foundational capabilities, including data quality, data cataloging, master data management and data observability, and practices, processes, and technologies for building sophisticated analytics solutions and machine learning models.

Cloud modernization: We can help you migrate your applications to cloud and modernize them to take advantage of cloud-native services. We can help you develop flexible, resilient and scalable cloud-native applications built on a modern architecture, backed by modern software development and delivery practices, including DevSecOps and continuous delivery. We can help optimize your developer productivity, leveraging automation and genAI capabilities to enable code quality improvement and proactive discovery of software deficiencies.

FinOps: With our established track record of building and implementing cloud financial management strategies, we can help you implement an effective FinOps model to help identify and remove excess costs from your existing cloud environments and prevent costs from spiraling out of control in the future.

Security and resiliency: We can help with compliance tools and controls designed to protect your enterprise and its systems with proactive vulnerability detection, and help verify control consistency across modern delivery practices. We can help you optimize cloud operations with visibility into risk controls and vulnerabilities, and help your teams be more proactive in addressing risks and defects, with a focus on value instead of capabilities.

Contact



Kevin Martelli
Principal
Cloud Practice Lead
kevinmartelli@kpmg.com

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

Learn about us in: in | **kpmg.com**

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.