
KPMG
Accelerating your journey
to the public cloud

As cloud adoption continues to expand and accelerate, upgrading and migration adds a host of new challenges to businesses.

Whether it's using infrastructure-as-a-service (IaaS) to shift legacy applications to the cloud, software-as-a-service (SaaS) to upgrade to more modern application alternatives, or features such as containers and microservices to develop new cloud-native applications, enterprises from a wide range of industries are increasingly turning to public clouds. Data-center-hosted applications will likely soon be the exception, not the rule.

While public clouds free the IT organization from the management and maintenance of compute, network, and storage resources, they don't free the business from the risks and responsibilities associated with migrating or upgrading enterprise applications. If anything, as cloud adoption continues to expand and accelerate, they add a host of new challenges to its plate.

These issues stem from scaling cloud adoption across the entire enterprise, including front-, middle-, and back-office applications, which presents numerous challenges for chief technology officers (CTOs), chief information officers (CIOs), business leaders, and controls teams. Managing cloud adoption at scale and pace requires many critical components to help reduce the associated risks. Organizations need to also consider their shared responsibility model with the cloud service providers.

Cloud adoption requires proper governance. A well-constructed governance process can help keep your cloud adoption aligned with enterprise standards for acceptable use. It can help provide engineers with the right training, help provide transparency to stakeholders to maintain confidence in the migration program, and accelerate adoption. KPMG specialists see a Cloud Center of Excellence (CCoE) as the foundation for this governance. The right leadership can help drive agreement on which cloud services will be used, how technology will be deployed, how a team will support the effort, and how costs will be managed.

An effective CCoE can bring together your existing enterprise policies, processes, and stakeholders, but you must update these elements for a cloud model, whether it's migration of conventional workloads (via IaaS) or modernization to cloud-native applications (serverless, containers, microservices, etc.). Tasking the CCoE with overseeing the modernization of the process is a critical first step to align the entire enterprise on the journey to cloud. As part of the CCoE it is important to have shared responsibilities with the lines of business and not have a fully centralized model.

Determine a shared definition of success. A cloud adoption program can affect various stakeholders differently. All stakeholders should agree upon a shared definition of success before the first application is deployed into a public cloud. In order to evaluate if the program achieves the desired outcomes, it's important to create definitions that are measurable. Establish baselines of the current technology ecosystem in order to compare your end state. Some factors that can be investigated to determine success are application availability and resiliency, business process responsiveness, speed of application feature deployment, and customer experience. The CCoE should manage stakeholder engagement and help ensure each constituency is bringing their requirements, expectations, and priorities into the decision-making around cloud adoption. If done right, the technical implementation will flow more smoothly from a clearly understood definition of success.

All stakeholders should agree upon a shared definition of success before the first application is deployed into a public cloud.

Investing the time to adapt to new security patterns and cloud security features

Engage security and risk departments early and often. Security, risk, and compliance teams should be engaged early in the cloud adoption program to address issues such as data protection, controls, auditability, and identity and access management. Late engagement with your security team could result in resistance and delays in moving workloads to the cloud. Adapting to new security patterns and cloud security features can take time in your organization. Early and frequent engagement is imperative to meet your timelines. By using policy as code (PaC), you can help build confidence with your risk and security teams for how new cloud services can be provisioned and maintained within the guardrails of compliance requirements. PaC can help you enforce recommended security practices and compliance requirements without slowing down development. This practice can also create consistency and compliance within a DevSecOps mode of operations.

Get the disposition right. The proper disposition of your application portfolio requires a detailed roadmap and a rolling wave plan. The plan should include each application's strategic hosting destination, and should align to business needs, technology strategy, cloud adoption policies, constraints, and rules of acceptable use. Make sure to ask yourself whether the application will be retired, remain in place, moved as-is, modernized, or take one of the many other paths to cloud. Take the time to perform an application analysis and disposition effort, including the interdependencies that make up a business ecosystem, before moving any workloads.

Effective portfolio analysis should include both technical and business considerations. Without accounting for business needs and business relationships within the application portfolio, your move to the cloud is far less likely to succeed. The sources of data needed to perform this broad analysis properly are often diverse and scattered throughout the enterprise. Infrastructure data from a configuration management database (CMDB) or other inventory source is commonly the easiest to include. However, because many enterprises treat cloud adoption as an infrastructure change, this source can have a disproportionate impact on disposition decisions.

For an adoption program to be successful, you should include a broader collection of data in the disposition analysis than the infrastructure inventory alone. This data should include application architecture sources to help understand each system's in-depth architecture. A keen understanding of business ecosystem information is needed so applications are not treated as an isolated component. This is a critical step to help avoid splitting a complex business process apart during the migration waves. You should also pay attention to policy, governance, and controls requirements so that disposition decisions will comply with enterprise requirements for data protection, tech governance, and terms of acceptable use of cloud services.

Making plans for FinOps

Transparent reporting of program health is essential. Understanding the progress and health of each application's move or modernization, as well as the broader health of each wave's progress, can help enable leadership and stakeholders to see the risks that need attention as they arise. And a monitoring and tracking structure should be in place to enable visibility into each application and wave as they move to the cloud.

It's not uncommon to see organizations trying to track and report their cloud modernization and migration efforts through spreadsheets because they lack modern tooling. For proper reporting, we recommend implementing modern tooling and establishing common T-minus plans for similar application types.

A T-minus plan is designed to establish critical-path milestones and timings required to achieve a planned cutover date, post-go-live outcomes, and successful handovers to business as usual (BAU). Applications should be grouped into waves by technical constraints and dependencies, functional dependencies, or complexity. Each wave should have a common T-minus plan that applies to each app. Effective T-minus plans can help enable realistic multiyear wave schedules that balance velocity and the business's ability to adapt to change.

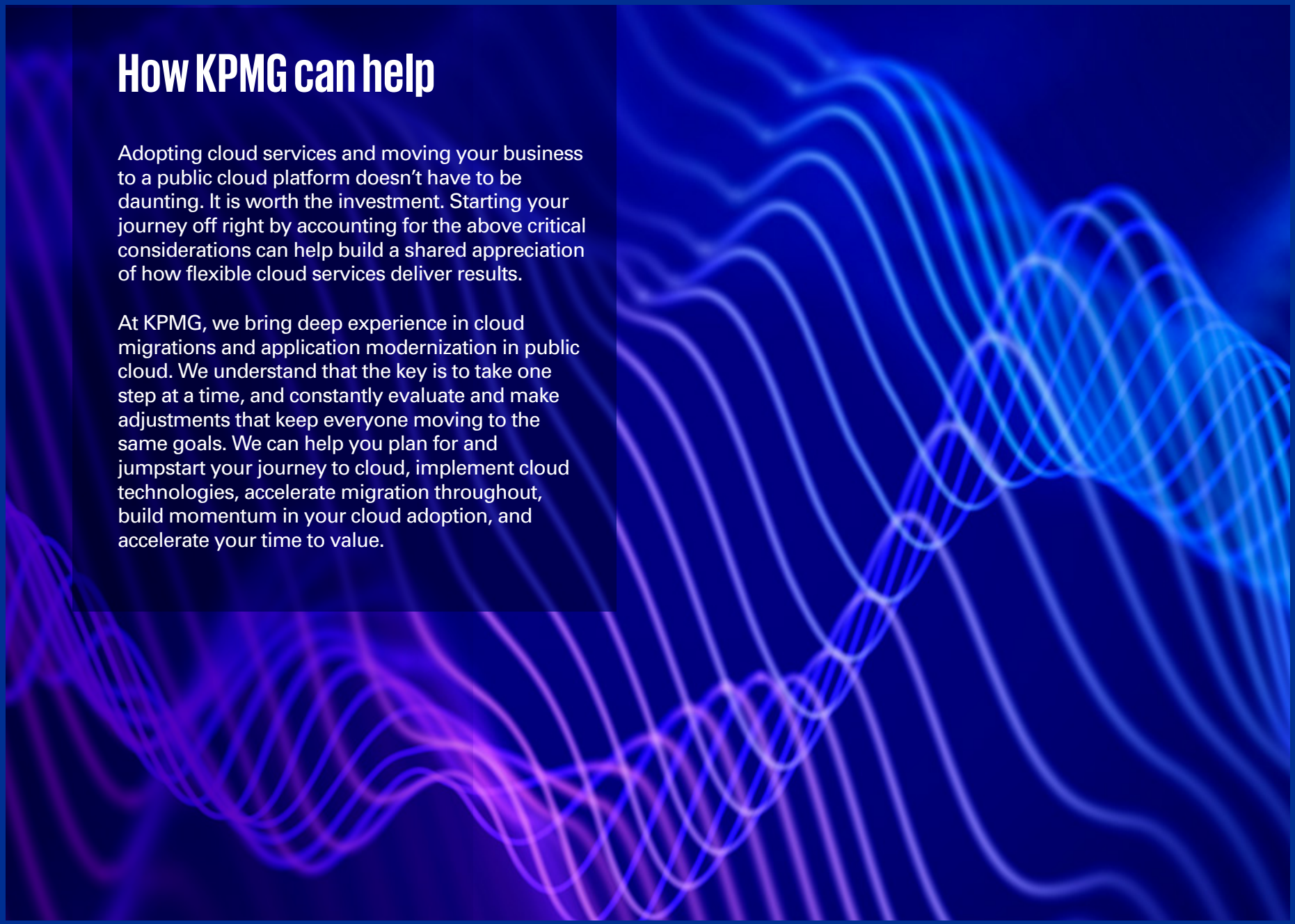
Implement cloud FinOps before cloud services are activated. One of the many benefits of public cloud services is full cost transparency of the services you activate. Most organizations don't plan for and implement cloud financial management or "FinOps" (a portmanteau of "finance" and "DevOps"). FinOps tooling can help you measure, report, analyze, and optimize your cloud spend. A common pattern observed across organizations is to activate cloud services, then wait several months to examine the monthly cloud spend to find an alarmingly higher-than-expected expense. IT teams should become fiscally knowledgeable and responsible for the cloud architectures, services, and solutions that are deployed. Once implemented, a FinOps process should be maintained to optimize public cloud use over time.

Applications should be grouped into waves by technical constraints and dependencies, functional dependencies, or complexity.

How KPMG can help

Adopting cloud services and moving your business to a public cloud platform doesn't have to be daunting. It is worth the investment. Starting your journey off right by accounting for the above critical considerations can help build a shared appreciation of how flexible cloud services deliver results.

At KPMG, we bring deep experience in cloud migrations and application modernization in public cloud. We understand that the key is to take one step at a time, and constantly evaluate and make adjustments that keep everyone moving to the same goals. We can help you plan for and jumpstart your journey to cloud, implement cloud technologies, accelerate migration throughout, build momentum in your cloud adoption, and accelerate your time to value.



Contact us

To learn more about how KPMG can help accelerate your journey to the public cloud, please contact:

Kevin Martelli
Principal,
Advisory, Lighthouse
KPMG in the U.S.
kevinmartelli@kpmg.com

Craig Hays
Managing Director,
Advisory, Lighthouse
KPMG in the U.S.
craighays@kpmg.com

Damian Smith
Director, Architect
Advisory, Lighthouse
KPMG in the U.S.
damiansmith1@kpmg.com

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

kpmg.com/socialmedia