KPMG

Mastering a multi-cloud environment

Detailed planning and strong controls required

"When it comes to adding an additional cloud to your tech stack, you hear no one saying "the more the merrier"!

Yet here we are in a world where **89%** of organizations around the world employ a multi-cloud strategy.[1]

1 "Flexera 2022 State of the Cloud Report," Flexera Inc., 2022.

Different cloud platforms have different strengths, to be sure, and enterprise-scale businesses may find it advantageous to parcel out their data storage and computing activities on more than one platform based on the unique needs of each application. But over time, the result can be a complex web of information systems that re-creates many of the problems the cloud was intended to solve, from inconsistent policies and controls to poor observability and runaway costs. Without an overarching plan for architecting and managing a multi-cloud environment, one of the most exciting revolutions in computing risks becoming just another resource-draining IT sinkhole that fails to deliver on its promise.

This leads directly to three questions. What does a good multi-cloud architecture look like? How can you ensure that your organization realizes—and can quantify—value from cloud? Finally, what are the principles that underpin a trusted multi-cloud architecture and let you realize value at scale?

Taking a cue from city planners, who must find ways for diverse types of buildings and users to interact with as little friction as possible, KPMG is proposing a new multi-cloud model based on six organizational, technical, and operational principles.

Multi-cloud model principles

1 Zoned workload placement

A well-planned city features different zones for different types of properties—commercial, industrial, and residential—each with its own infrastructure and rules for development. This can minimize conflict between property owners, who may have highly different priorities, and helps to controls costs by ensuring that each zone gets the infrastructure it needs—but no more. The same holds true for a multi-cloud operating environment. But in this case we're not creating neighborhoods or industrial parks but rather zones or "domains" where like IT applications will be housed on each cloud platform—high-volume applications here, specialty applications there, general data storage in one place, and perhaps highly sensitive data storage somewhere else. This simplifies oversight and security.

2 Domain-centric control planes

As organizations have moved their IT systems to the cloud, they've recognized the need for a way to manage and orchestrate their cloud operations according to well-defined policies and controls. A multi-cloud environment requires not just one control plane but a federated set of planes, each dedicated to a specific domain and its idiosyncrasies. Control plane software specifies domain policies, security rules, and compliance rules—and enforces them automatically.

3 Goal-driven, self-service landing zones

Like visitors arriving at an airport, end users of a multi-cloud need a place to enter its various domains—a landing zone where they can begin to use, request and build services or applications without requiring extensive help from IT. A good landing zone will centralize identity and access management, control what each type of user is able to do in the cloud, and accurately log and audit activity.

Multi-cloud model principles

4 Built-in security-as-code

Most software applications, and the cloud platforms on which they run, exist in a constant state of evolution as developers continually introduce new features and capabilities—and potentially open the door to new security vulnerabilities. To support this ongoing evolution at speed and scale while minimizing the chances for security compromises, companies can look for opportunities to build security checks and tests into their code during its development, incorporating features such as automated security tests and built-in monitoring functions. The more complex an organization's multi-cloud environment, the more important this "security-as-code" model becomes.

5 Sustainable transparency

Observability—the ability to record everything that is happening in IT systems to know whether they are functioning properly and, if not, identify the culprit—has long been critical to IT success. In a multi-cloud environment, observability must be outcome-focused and purpose-driven so the IT organization has access to the information it needs without being overwhelmed by data.

6 Metrics-driven governance

Operating in a multi-cloud environment introduces new governance challenges around accountability, costs, benefit-versus-risk analysis, and security. To ensure maximum value from a multi-cloud strategy, organizations must identify and monitor a broad range of metrics to understand, among other things, the degree to which cloud platforms are being used across the enterprise, operational efficiency and cloud costs, the extent to which the organization's cloud strategy is aligned with business objectives, and compliance with security policies.

How KPMG can help

By applying these six principles, organizations can employ an efficient multi-cloud strategy with coordinated policies, disciplined development of new applications, and high levels of security and observability. Using the right cloud platforms for the right applications, minimizing redundancy, and facilitating self-service by end users can help with cost control and contribute to high levels of realized value.

KPMG offers a suite of automation tools and software to help organizations optimize their capabilities in a multi-cloud environment. To learn more about how KPMG can help your organization create a multi-cloud environment, please contact:

Kevin Martelli
Principal, Advisory
kevinmartelli@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