Kion

Achieving Multi-Cloud Governance Across Providers and Regions

Across government missions, it makes sense to be cloud-smart today

Six years after the cloud-first mandate, cloud use is steadily increasing across government agencies. In the US intelligence community (IC) alone, cloud use has increased more than 200% year over year[1]. An ever-growing number of missions are now being executed with greater agility, cost savings, and speed because the government is taking advantage of commercial cloud services.

Commercial cloud technology is a safer bet to run your workloads, regardless of the mission being supported. Whether you are running sensitive workloads that must satisfy Department of Defense (DoD) Impact Level 6 or you must meet Intelligence Community Directive (ICD) 503 regulatory requirements, both AWS and Azure now provide regions to bring the cloud to customers across the DoD and IC.

Today, the new mandate is cloud smart, and the DoD has indicated it "is driving toward an enterprise cloud environment that is composed of a General Purpose cloud and multiple Fit For Purpose clouds"[2]. This means your approach to governing your cloud must be provider-agnostic and region-spanning. How do you get quick access, a consistent user experience, and compliance and financial control across public cloud providers and classification domains?

Streamlining provisioning across providers & classifications

If you must rely on a central group – with cumbersome approval chains, help desk tickets, and manual processes — to enable your teams to operate in the cloud, you'll soon question the ROI of the cloud.

In this scenario, cloud becomes the enabler for a new type of "shadow IT" where team members circumvent established policies and procure their own cloud accounts because the central group can't move quickly enough to provision cloud accounts.

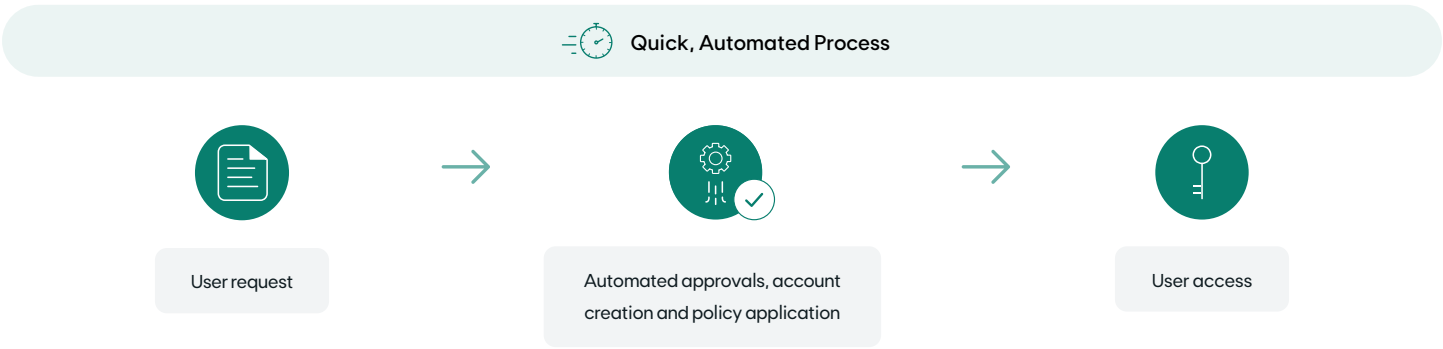
1: CIA's Cloud is 'Pretty Close' to Invincible, CIO Says
https://www.nextgov.com/it-modernization/2017/06/cias-cloud-pretty-close-invincible-cio-says/138679

2: Department of Defense, DoD Cloud Strategy, December 2018
https://media.defense.gov/2019/Feb/04/2002085866/-1/-1/1/DOD-CLOUD-STRATEGY.PDF

Traditional cloud provisioning typically looks like:

It shouldn't matter what cloud provider a developer wants access to – or the classification domain. An authorized user should be able to get access in less than 48 hours and leadership should have visibility into who's in their cloud.

Cloud provisioning should look like:



Kion is available in AWS and Azure, in the commercial, government, and isolated air-gapped regions including AWS C2S and AWS SC2S. With Kion as your cloud governance solution, you can:

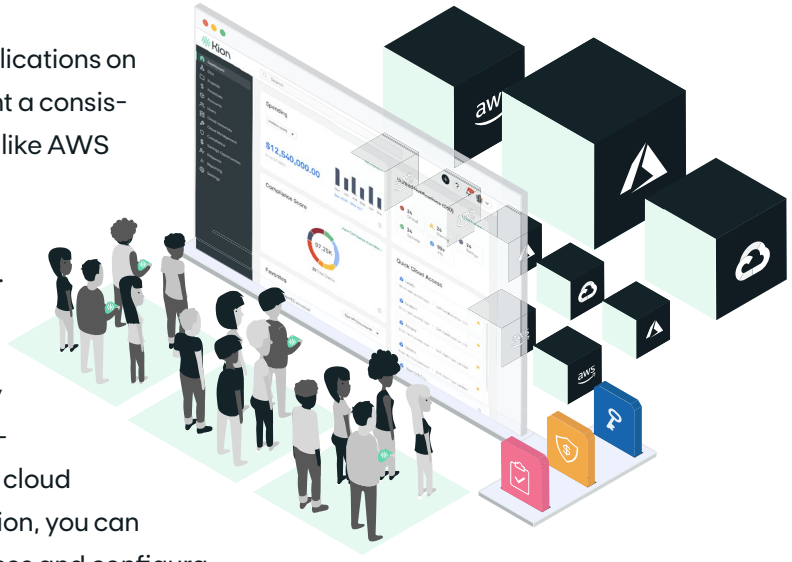
- Easily see what accounts you manage and who has access to accounts.
- Quickly create projects or add users to meet project and customer needs.
- Control available services upon access attempt.

Getting a consistent user experience across providers and classifications

With secure regions available from the leading cloud providers, you can now move applications from legacy IT environments to secure cloud environments. But the reality is that there are use cases and needs that require your teams to use more than one cloud provider and operate in more than one classification domain.

For example, you will probably want to build applications in a lower environment with richer access to resources and migrate these applications to higher classification environments without fear of re-architecture. In addition,

you likely have some team members developing applications on the low side and some on the high side. So, you'll want a consistent user experience between commercial providers like AWS and Azure and across different regions such as Azure Commercial, Azure Government, AWS Commercial, AWS GovCloud, AWS SC2S, and AWS C2S.



Kion is a proven solution that works across cloud providers and classification domains to help simplify governance and ensure a consistent end user experience in accessing and managing the cloud using the cloud service provider's native interfaces and APIs. With Kion, you can set and enforce policies to ensure that specific services and configurations are used to consistently meet compliance requirements.

Controlling cost across providers and classifications

The hallmarks of the cloud – decentralized account creation, variable and pay-as-you-go usage, and quick pay cycles — create financial spending risk and budget challenges. Each cloud resource ordered commits you to paying for the resource, and costs accrue upon request and deployment. In addition, it's extremely difficult to determine the full amount and impact of an overrun until it's typically too late because actual costs accrued can take anywhere from 24 to 48 hours before they show up on the cloud service provider's billing reports. And cloud providers don't support stopping spend when budgets are reached.

Kion provides the financial controls needed to help satisfy federal government financial requirements. With Kion, you can track, manage, and enforce cloud spending across providers and regions.

1 **Set Up**

Set up funding sources based on time period & amount authorized

2 **Allocate**

Allocate funding to divisions & directorates to set spend plan for cloud project

3 **Specify**

Specify enforcement actions to notify, slow, & stop spending based on near-real-time cloud costs

4 **Sit Back**

Sit back & relax while enforcement actions notify, slow, and stop spending based on near-real-time cloud costs

Kion: the comprehensive cloud governance solution that works across your cloud environments and classification domains.