Kion

Governance for the Public Sector Cloud

Managing Cost and Ensuring Compliance

Paving the Way to the Cloud

Forecasting a potential 30% reduction in data infrastructure spend, the U.S. Government embarked on a "cloud-first" policy beginning with the 2012 budget cycle. When evaluating new IT deployments, agencies were directed to default to cloud-based solutions in lieu of building additional in-house capabilities provided secure, reliable, and cost-effective options were available. The cloud promised less duplication of systems, more easily managed environments, and shorter procurement cycles. The overall goal was to deliver greater impact from IT spend to citizens.

The need to enable efficient and scalable technology development, deliver stellar customer experience to employees and the public, and reap economic efficiencies has helped pave the way for increased cloud consumption. In addition, the Federal Risk and Authorization Management Program (FedRAMP) has aided adoption by standardizing security services and streamlining the assessment process.

Six years after the cloud-first mandate, cloud use is steadily increasing across the government. In the intelligence community (IC) alone, cloud use has increased more than 200% year over year1. 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.

Challenges on the Road to Cloud Value

Cloud adoption has largely come from the bottom up, with small groups of early adopters migrating project workloads to the cloud and seeing initial success. These groups help transform organizational thinking and challenge the status quo. Seeing success, additional teams begin to express interest.

What happens next is somewhat predictable: agencies end up with numerous systems engineered for the cloud but still reliant on manual IT governance to control access, budget, and compliance.

Soon, it's impossible to answer basic questions about cloud use and operations:

- How do we determine the state of all cloud users and their access rights across the enterprise?

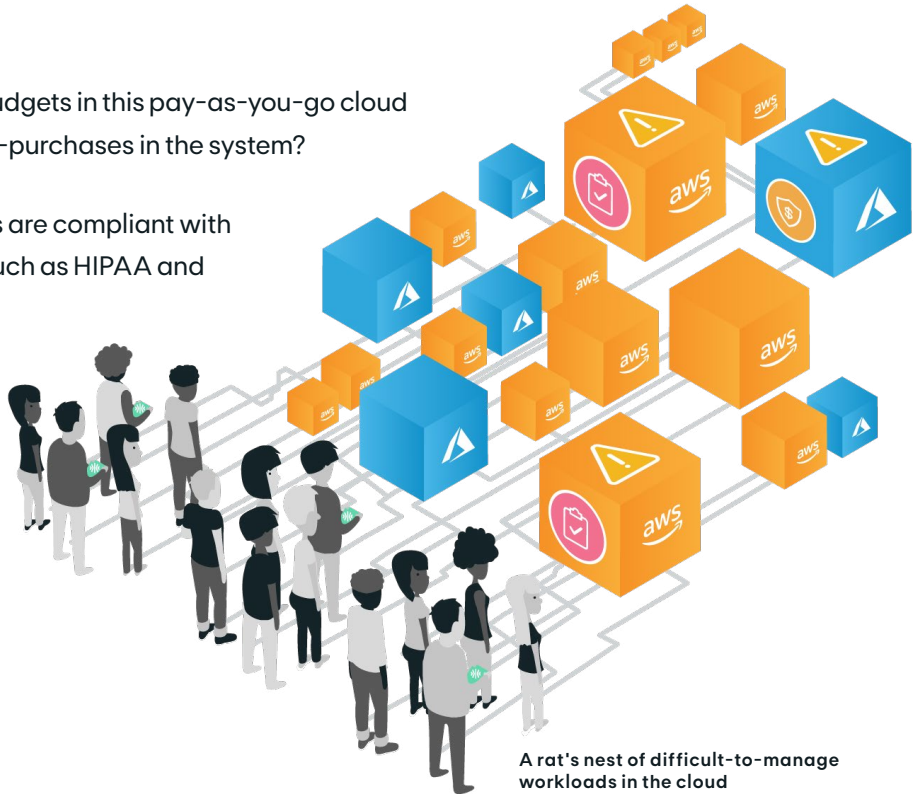
In the intelligence community (IC) alone, cloud use has increased more than

200%

year over year.[1]

- How can we ensure adherence to IT budgets in this pay-as-you-go cloud model, where every user makes micro-purchases in the system?
- How can we ensure all cloud accounts are compliant with relevant legal or regulatory policies such as HIPAA and FedRAMP?

Like most tales of technology adoption, there's a rush to take advantage of features and capabilities, followed by the struggle to manage the technology to achieve full adoption and value.



A rat's nest of difficult-to-manage workloads in the cloud

Here's how agencies try to 'tame the cloud' today:

Potential Solution	...And the Result
Apply traditional IT management processes to manage cloud resources.	• A central group is established to control cloud access through inefficient approval chains, help desk tickets, and manual processes. • Staff expend countless labor hours to create and update spreadsheets every month to track cloud access, monitor spend, and audit compliance. • Technical staff become frustrated with the amount of time it takes to get cloud resources — a conflict with the on-demand nature of the cloud. • Leadership question the true ROI of the cloud because of the increasing amount of labor required to manage the environment.
Allow unfettered, decentralized access to cloud service providers across multiple unconnected accounts.	• Cloud accounts and resources are set up inconsistently across the enterprise. • Technical staff have elevated permissions with no enforceable accountability for their actions. • Leadership has very little visibility into and control over cloud use and security practices across the enterprise
Use cloud broker technology to enable visibility and accountability.	• The number of cloud services available to the organization is greatly diluted by the broker's ability to keep pace with new services offered by CSPs like AWS and Microsoft. • Technical staff become discouraged when they must learn another new technology to use the cloud. • Leadership gains control and consistency, but sacrifices the innovation potential of the organization.

Cloud Governance Ensures Cloud Value

Technology makes up just one small part of cloud adoption: processes, operations, and people are critical elements of successful adoption. Agencies struggle to move from initial, project-based cloud use to organization-wide cloud adoption and value due to a lack of governance over these non-technology elements.

Cloud governance is the process of establishing, monitoring, and ensuring adherence to the rules, guidelines, and policies meant to control an organization's cloud resources and actions. Ideally, the governance process is largely automated to ensure agility and responsiveness to the organization's evolving needs.

A robust governance approach requires the following:

- Account management to centralize control of resources and allow for secure self-service account creation.
- Budget enforcement that is aligned to spending policies and provides the ability to alert, freeze, and terminate spend.
- Compliance automation that is supported with access policies and verification via reporting.

Teams Acknowledge a Lack of Governance

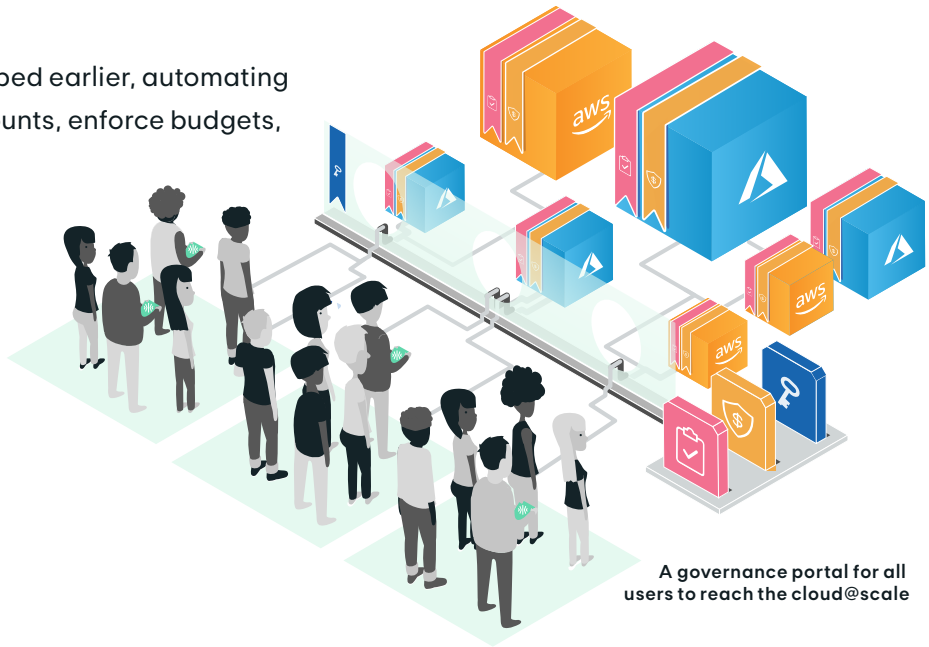
A study of over 550 senior leaders in government found that:

- 47% of respondents feel that cloud governance is non-existent, and 71% report using an application on at least one occasion which fell outside the agency-approved IT toolkit.
- 42% of respondents say cloud adoption has occurred entirely or partially outside of governance.[2]

Automating Cloud Governance with Kion

Automating cloud governance is a prerequisite to achieving organization-wide cloud value in an efficient and cost-effective manner.

Kion tackles the challenges described earlier, automating much of the effort to manage accounts, enforce budgets, and ensure compliance.



A governance portal for all users to reach the cloud@scale

> **"The current mechanisms of Federal funds systems work directly against the intended business advantages of cloud computing. This is the most impactful issue facing the Federal Government with cloud computing. While there are other disadvantages in the current Federal structures, they generally have a much lower impact than funding constraints."[3]**

Challenge	Kion helps you...
How do you determine the state of all cloud users and their access rights across the enterprise?	• Know 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.
How can you ensure adherence to IT budgets in the pay-as-you go cloud model, where every user makes micro-purchases in the system?	• Get a real-time view into budget and centralize cost management. • Enforce (not just report) cloud spending across many accounts and workloads to ensure compliance with the Antideficiency Act (ADA). • Get near real-time cloud spending reports for projects.
How do you ensure your cloud presence is compliant with relevant legal or regulatory policies such as HIPAA and FedRAMP?	• Automate staff adherence to defined compliance standards. • Maintain organizational security practices when many users are requesting cloud resources across many accounts.

"Easy scalability without proper governance can lead to the government committing to a large sum of money. There can be instances where scaling up for resources are outside the IT security boundaries ...These risks can all be mitigated by having the proper governance structure with the responsibility to enable IT cloud solutions and cloud related programs within the acquisition and contracting policies."[4]

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

2 Mastering the Migration to Cloud Computing, survey of federal leaders; https://www2.deloitte.com/us/en/pages/public-sector/articles/federal-cloud-migrationsurvey.html?id=us:2el:3pr:fed1253:eng:fed:030117

3 Acquisition Professional's C.A.S.T.L.E. Guide, draft; https://1yxsm73j7aop3quc9y5i-faw3-wpengine.netdna-ssl.com/wp-content/uploads/2017/09/AcquisitionProfessionals-CASTLE-Guide-Draft.pdf

4 Acquisition Professional's C.A.S.T.L.E. Guide, draft; https://1yxsm73j7aop3quc9y5i-faw3-wpengine.netdna-ssl.com/wp-content/uploads/2017/09/AcquisitionProfessionals-CASTLE-Guide-Draft.pdf