AWS Governance at Scale

Using automation for oversight and control when implementing a multi-account strategy

July 2018

Notices

This document is provided for informational purposes only. It represents AWS's current product offerings and practices as of the date of issue of this document, which are subject to change without notice. Customers are responsible for making their own independent assessment of the information in this document and any use of AWS's products or services, each of which is provided "as is" without warranty of any kind, whether express or implied. This document does not create any warranties, representations, contractual commitments, conditions or assurances from AWS, its affiliates, suppliers or licensors. The responsibilities and liabilities of AWS to its customers are controlled by AWS agreements, and this document is not part of, nor does it modify, any agreement between AWS and its customers.

Contents

Abstract

Customers need to structure their governance to grow and scale as they grow the number of AWS accounts. AWS proposes a new approach to meet these challenges. Governance at scale addresses AWS account management, cost control, and security and compliance through automation; organized by a centralized management toolset. Governance at scale aligns the organization hierarchy with the AWS multi-account structure for complete management through an intuitive interface.

There are three areas of focus for governance at scale, with techniques for addressing them using a toolset for a typical organizational hierarchy. An example use case is provided; along with evaluation and selection criteria for either developing or procuring a toolset to instantiate governance at scale.

Introduction

A common theme across organizations, as operational footprints scale on AWS, is the need to maintain control over cloud resource usage, visibility, and policy enforcement. The ability to rapidly provision instances introduces the potential risk of overspending and inadvertent misconfigurations. This causes security concerns when strong governance and enforcement are not in place. An organization must address challenges to oversight so that risks are known and can be minimized. Identified stakeholders are responsible for budget alignment, governance, compliance, business objectives, and technical direction across an entire organization. To meet these needs, AWS has developed this governance-at-scale guidance to help identify and instantiate best practices.

Governance at scale helps organizations establish centrally managed budgets for cloud resources, oversight of cloud implementations, and a dashboard of the organization's cloud health. Cloud health is based on near-real-time compliance to governance policies and enforcement mechanisms. To enable this, the policies and mechanisms are separated into three governance-at-scale focal points:

- **Account Management** - Automate account provisioning and maintain good security when hundreds of users and business units are requesting cloud-based resources.
- **Budget & Cost Management** - Enforce and monitoring budgets across many accounts, workloads, and users.
- **Security & Compliance Automation** - Manage security, risk, and compliance at a scale and pace to ensure the organization maintains compliance, while minimizing impact to the business.

Traditional Approaches to Manage Scale

Organizations employ three basic approaches to manage large operations on AWS, provision multiple AWS accounts, control budgets, and address security, risk, and compliance. Each of these approaches have limitations.

- **Traditional IT management processes.** A central group controls access through approval chains, and manual or partially automated setup processes for accounts and resources. This approach is difficult to scale because it relies on people and processes that lack automated workflows for help desk tickets, and hand-offs between staff with different roles.
- **Unrestricted, decentralized access** to AWS across multiple disassociated accounts. This approach can cause resource sprawl that leadership cannot see.

While usage can scale, visibility and accountability are sacrificed. The lack of visibility within a self-service cloud model introduces compliance and financial risks that most organizations cannot tolerate.

- **Use a cloud broker**. This approach enables visibility and accountability, but may limit which AWS services are available to developers and applications, or require additional technology augmentation for organizations that require native access to AWS services.

Organizations that have large scale cloud adoption attempt to work around these limitations by using a combination of technologies to address agility and governance goals. They might use a specific account management application, or a specific cost enforcement system, or multiple toolsets for security and compliance. These separate technologies introduce additional layers of complexity and interoperability challenges.

Governance at scale

AWS governance at scale helps you to monitor and control costs, accounts, and compliance standards associated with operating large enterprises on AWS. It is derived from best practices at AWS and from customers who have successfully operated at scale. The components are designed to be flexible so that both technical users and project teams can self-serve on AWS, while leadership maintains control on spending decisions and automated policy enforcement. Organizations can implement governance at scale practices by developing their own solution, investing in a commercial solution aligned to the framework, or engaging AWS Professional Services for custom options. Mechanisms that align to governance at scale focus on control and reporting of budget, security and compliance, and enforcing AWS access, across all stakeholder teams. A core element is a centralized interface that provides hierarchical structure while preserving native access to the AWS API, the AWS Management Console, and the AWS SDK/CLI.

AWS guidance to achieve governance at scale is designed to conform with an organization's existing structure and business processes. Figure 1 shows a typical government or corporate organization. Each layer can have different technical, financial, reporting, and security requirements. Different departments and teams can have different success criteria, goals, and technical skill sets.

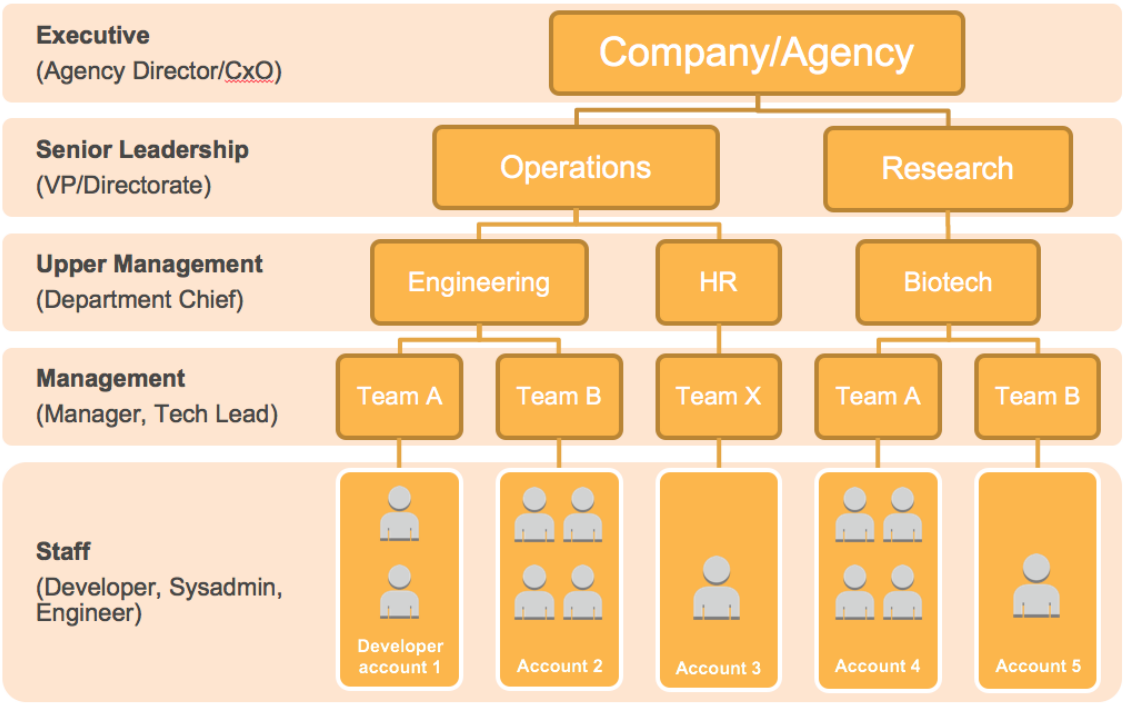

Figure 1: Sample organizational structure

An interface and subsystem that meets the governance at scale criteria allows leaders to allocate funding, assign budgets, and monitor near real time resource consumption. Each organizational level can institute policies or make adjustments to organization and project budgets based on mission priorities and usage patterns. They can then propagate these policies down through the organization. The interface provides the mechanisms for authorized staff to create new projects, request new AWS accounts (or access to existing accounts), restrict access to AWS resources, and obtain near-real time metrics on project budget consumption.

This hierarchy combined with security automation provides reliable near real-time reporting for each level of leadership and staff. The granular and transparent nature of the workflows and data assures leadership that cloud operations across the enterprise are visible and constrained as appropriate with the implemented governance policies.

Governance at scale focal points

Three focal points governance at scale implementations include are: **Account Management**, **Budget and Cost Management**, and **Security and Compliance Automation.**

Account Management

AWS guidance to achieve governance at scale streamlines account management across multiple AWS accounts and workloads within an organization (a Figure 2) through centralization, standardization, and automation of account maintenance tasks. It accomplishes this through policy automation, identity federation, and account automation. For example, instead of requiring a central group to manually manage the organization's master billing account, a self-service model with workflow automation is employed. It enables authorized staff to link multiple accounts to one or more master billing accounts, and attach appropriate, automatically enforced governance policies

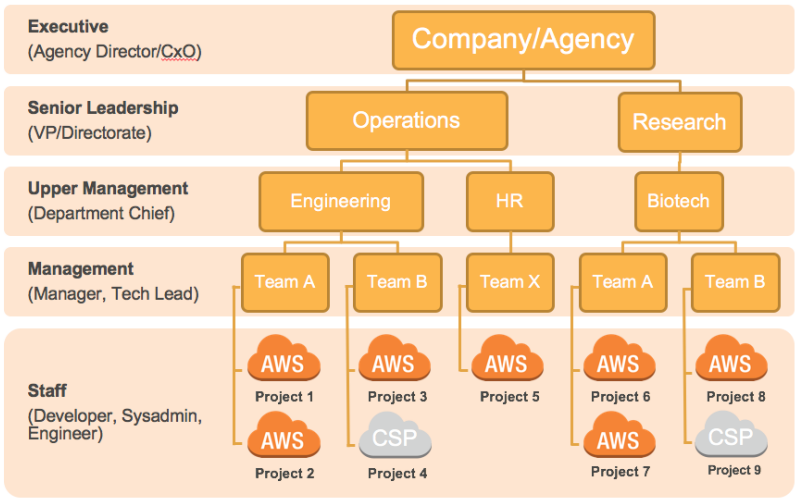

Figure 2: Automation can create and manage accounts at scale

Policy Automation

AWS guidance to achieve governance at scale automates the application of organizational policies, deploying accounts with standard specifications to ensure consistency across AWS accounts and resources. The policy engine is flexible to accommodate and enforce different types of security polices such as IAM, AWS CloudFormation, or custom scripts.

Identity Federation

AWS governance solutions employ single sign-on (SSO) through federated identity integration with external authentication providers such as OpenID, or Active Directory to centralize AWS account management and simplify user access to AWS accounts. When SSO is used in conjunction with AWS CloudTrail, user activity can be tracked across multiple AWS accounts.

Account Automation

Services like AWS Organizations, AWS CloudFormation, and AWS Service Catalog automate AWS account provisioning and network architecture baselining. They replace manual processes, and facilitate the use of pre-defined, standardized system deployment templates.

Users can create new AWS accounts for projects through self-service and leverage the AWS Management Console and APIs without the assistance of provisioning experts. Project or AWS account owners within an organization use a centralized interface to manage access to resources within their assigned area and configure cross-account access to AWS resources.

This automation of account management removes impediments such as ticketing or other out-of-band manual processes from the account provisioning process. This accelerates developers' access to AWS resources they need.

Budget and Cost Management

Automated methods define and enforce fiscal policies to achieve governance at scale. Budget planning and enforcement practices allow leaders and staff to allocate and manage budgets for multiple AWS accounts and define enforcement actions. This ensures spending is actively monitored and controlled in near real time. These mechanisms let leaders make proactive, well-informed decisions around budgetary controls and allocations across their organization. When budgets are aligned with projects and AWS accounts, automation ensures budgets are maintained in real time, and accounts can't exceed an approved budget.[1] Organizations are able to meet fiscal requirements, such as the Federal Anti-deficiency Act for U.S. Government agencies. Shared service providers or AWS resellers can implement governance at scale to provide chargeback capabilities across a diverse organization.

Budget Planning

It is important to align the organization's budget management process to an automated workflow. The workflow should be flexible so that different types of funding sources, such as investment, appropriation, and contract line items (CLINs), are managed as the funding is allocated across the organization. Financial owners define the timeframe for the funding source, set enforcement actions if budget limits

[1] For an example use case where budget enforcement is automated with a governance at scale solution, see Appendix A – Example Use Case.

are exceeded, and track utilization over time. For example, if AWS provides a customer a $10,000 credit, the financial owner has the ability to subdivide the funding amount across the organization. The automation will manage each allocation individually, while providing awareness and real-time financial dashboards to decision makers over the lifetime of the funding source.

Budget Enforcement

Enforcement of budget constraints is a key component of governance at scale. Each layer of the organization defines spending limits within accounts and projects, monitors account spending in near real-time, and triggers warning notifications or enforcement actions. Automated actions include:

- Restricting the use of AWS resources to those that cost less than a specified price.
- Throttle new resource provisioning.
- Shut down, terminate, or de-provision AWS resources after archiving configurations and data for future use.

Figure 3 illustrates how this could work. Red numbers indicate the current or projected spend exceeds the budget allocated to the project. Green numbers indicate that spend is within budget. When viewed on a governance dashboard, a decision maker has near real time awareness of usage and spend across the entire organization.

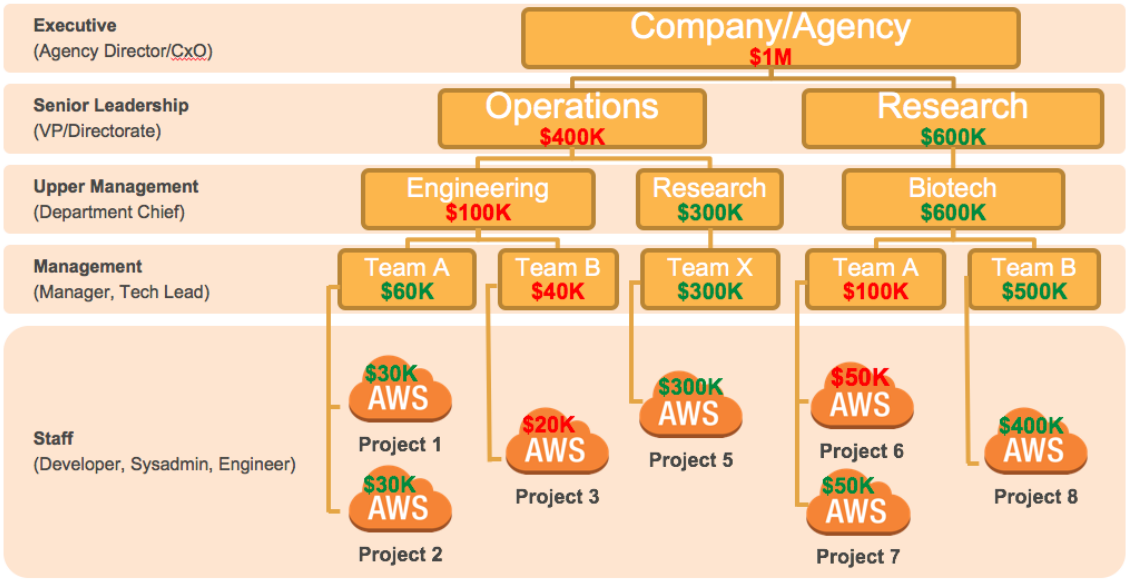

Figure 3: Budgets are allocated and enforced through the organization. Green indicates on-track spending and red indicates over spending.

Security and Compliance Automation

Governance at scale security and compliance practices employ automation to enforce security requirements, and help streamline activities across the organization's AWS accounts. These practices are made up of the following items: identity and access automation, security policy enforcement and security automation.

Identity & Access Automation

AWS guidance to achieve governance at scale is to offer Identity & Access Management (IAM) capabilities through a central portal. Users access the portal with an approved authentication scheme (Microsoft Active Directory, Lightweight Directory Access Protocol or similar). The system grants access based on roles defined by the organization. Once authorized, the system enforces a strict "policy of least privilege" by providing access to resources authorized by the appropriate authorities. The portal allows users and workload owners to request and approve access to projects, AWS accounts, and centralized resources by managing organizationally defined IAM policies applied at every level. For example, if a Chief Information Security Officer (CISO) wants to allow the organization to access a new AWS services that was previously not allowed, the developer can edit the IAM policy at the root OU level, and the system will implement the change across all cloud accounts.

Security Automation

Maintaining a secure posture when operating at scale requires automating security tasks and compliance assessments. Manual or semi-manual processes cannot keep pace with business growth. With automation, AWS services or Amazon Virtual Private Cloud (VPC) baseline configurations can be provisioned using standardized AWS configurations/AWS CloudFormation templates. These templates align with the organization's security and compliance requirements and have been pre-approved by organizations risk decision makers. The provisioning process interfaces with the organization's Governance, Risk, and Compliance (GRC) tools or systems of record[2]. Together they generate security documentation and implementation details for newly provisioned baseline architectures. These capabilities shorten the overall time required for a system or project to be assessed and approved for operations.

Well implemented security automation is responsive to security incidents. This includes processes to respond to policy violations by revoking AWS Identity and Access Management (IAM) user access, preventing new resource allocation, terminating resources, or isolating existing cloud resources for forensic analysis. Automation can be accomplished by collecting and storing AWS logging data into centralized data lakes and performing analytics, or basing responses on the output of other analytics tools.

Policy Enforcement

AWS guidance to achieve governance at scale helps you achieve policy enforcement on AWS Regions, services, and resource configurations. Enforcement is based on stakeholder roles and responsibilities, and in accordance with compliance regulations (eg. HIPAA, FedRAMP, PCI/DSS, etc.) At each level of the hierarchy the organization can specify which AWS services, features, and resources are approved for use on a per-department, per-user, or per-project basis. This ensures self-service requests can't provision unapproved items, as illustrated in Figure 4.

[2] Partner Solutions include Telos Xacta 360, RSA Archer

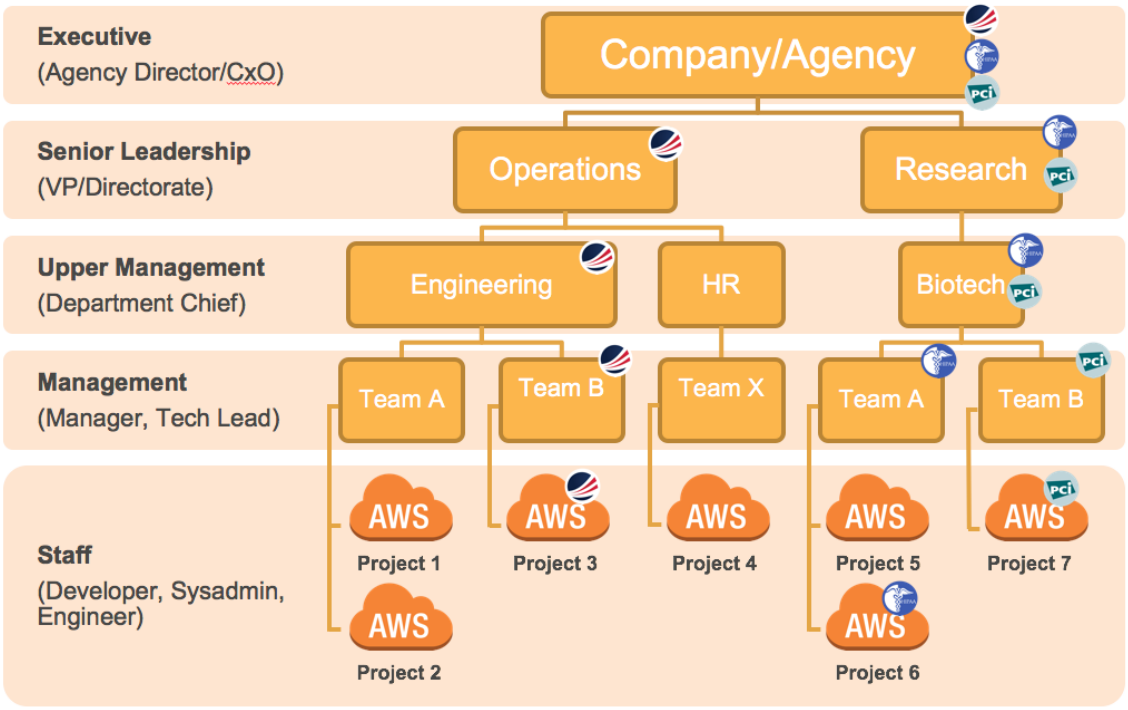

Figure 4: Security and compliance guardrails flow down through hierarchy. Circles indicates 3 party security requirements: Fedramp, HIPAA, and PCI.

Deciding on your solution

Designing a system to achieve governance at scale addresses key issues for organizations around account management, cost enforcement, and security and compliance. Organizations can build a governance at scale solution themselves, or the can build one in partnership with AWS Professional Services, or an AWS partner[3].

Decision Factor 1, Determine need

Does the organization's AWS footprint exceed or will it exceed the number of AWS accounts and resources that staff can manage using manual processes? For example, do you review account billing details, using spreadsheets for tracking, or, are you using the AWS Management Console to create and manage all accounts? If the answer to the top question is yes, then a governance at scale solution is needed.

[3] Partner offerings include Cloudtamer.io, Turbot, and Dome9 Security.

Decision Factor 2, Is it feasible to build versus buy?

In order to build a custom solution, your organization should be able to answer "yes" to the following questions.

- Does your organization have a robust AWS resource tagging or account management methodology for budget control and enforcement?
- Does your organization have an existing governance model with business processes that can be automated?
- Does your organization have the resources to build and maintain an enterprise software solution for managing governance at scale across the enterprise? Including: engineers and developers with advanced understanding of the AWS Cloud, APIs, security features and services, and sufficient staff to maintain the enterprise solution over time?

Refer to Appendix B: Governance at scale Capability Checklist to determine if your organization can develop a solution that meets all of the governance at scale requirements.

Decision Factor 3, Criteria selection for buying a commercial solution

A commercial solution may include one or more products, and/or professional services assistance with integration or to build key components. If you decide to purchase a 3rd party solution to achieve governance at scale, please refer to the Appendix B: Governance at scale Capability Checklist to determine if partner products or professional services meet all of your requirements

What does a Governance at scale solution look like to an organizational stakeholder?

Figure 5 illustrates how a finalized governance at scale implementation dashboard overlays cost and compliance indicators in the organization.

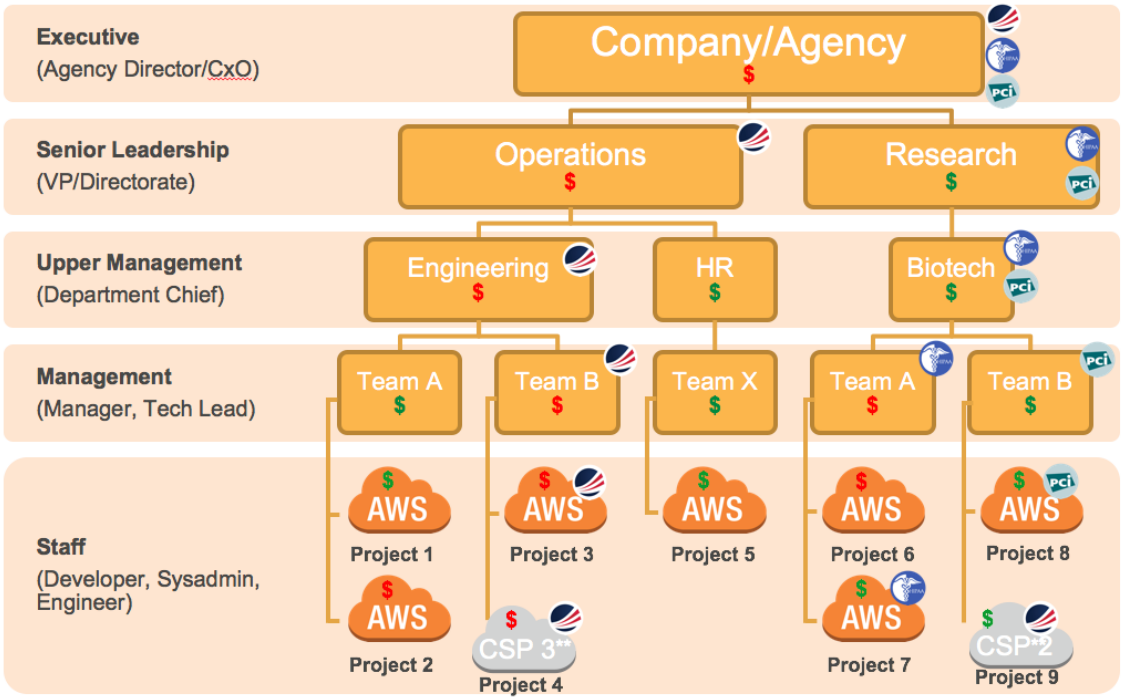

Figure 5: Example organization's cloud environment now viewed through a view, showing account, budget, and compliance status.

Decision makers at each layer of the hierarchy are provided real-time data and metrics that are tailored to their organizational role and/or business units.

- Executive – Executives can assign budgets and security policies any segment of the organization. Data is collected from the all segments and is presented in a summary view to include overall compliance status and financial health.
- Senior Leadership – Senior leaders can view their respective financial health within their sub-organization. They are responsible for assigning budgets to their respective subordinates and applying additional security policies as needed.
- Upper Management/Management – Management monitors budgets, grants personnel access to projects, and assigns focused security policies. This is achieved by assigning specific budget and security policies to business units and teams responsible for applications.

- Staff – Staff interact directly with cloud accounts and have operational awareness of current spend vs assigned budget. They can request access to other projects and exceptions to security and financial policies as appropriate.

Conclusion

Governance at scale is a new concept for automating cloud governance that can help your organization retire manual processes in account management, budget enforcement, and security and compliance. By automating these common challenges, the organization can scale without inhibiting agility, speed, and innovation, while providing decision makers with the visibility, control, and governance that is necessary to protect sensitive data and systems.

Carefully consider which solution you chose for your organization. The decision whether to build or buy can have critical implications on your AWS migration strategy. Discuss the potential impact with your AWS Solution Architect and/or Professional Services consultant. They can help ensure your solution meets your specific requirements. The use case example in Appendix A offers one way to formalize implementation. This real-world example shows the challenge organizations face and the effect a governance at scale implementation can have. Appendix B provides you with a list of the key capabilities for each governance at scale focal point.

The Governance at scale framework provides a “compass and map” to help enterprises build or buy solutions that can help them scale with confidence, by replacing human based governance processes with automation that is familiar and easy to use for all stakeholders.

Appendix A – Example Use Case

Implementing governance at scale to manage AWS accounts within an organization

ACME organization has outgrown their manual and spreadsheet-based governance process. The organization is large and profitable (1B yearly revenue) but have diverse business units that require autonomy and flexibility. They have a small governance team and a limited budget for a custom home-grown solution. Because of their organizational and financial constraints, they decided to purchase a solution from the AWS partner.[4] Once deployed and configured to align with organization specific processes and requirements, the solution is available for developers and decision makers to centrally manage their cloud resources. The workflow below describes how a new developer would access and manages their resources within a governance at scale solution.

John is a developer joining a team that designs application environments for deployment in the AWS Cloud. Therefore, he needs an AWS development environment so that he can manipulate infrastructure components using code without affecting other developers or systems. Each developer within the team is approved for individual monthly billing budgets for the use of AWS.

A governance at scale implementation and workflow for this scenario is:

1. John navigates to a portal to submit a request for an AWS account for developers. From a list, he chooses from a set of standard corporate AWS account types, and then specifies that he needs a monthly billing budget of $5,000.
2. His request triggers a notification that is sent to his manager. His manager uses the portal to confirm or change the monthly billing budget that John specified and selects any preapproved/assessed system boundary that John's environment is allowed to operate within.
3. An automated process creates a new AWS account for John, and then uses CloudFormation to build a baseline architecture and apply predefined IAM policies and AWS service configurations within John's new AWS account.

[4] Partner offerings include Cloudtamer.io, Turbot, and Dome9 Security.

- IAM policies include what services and resources that John is allowed to access, and the AWS service API calls he is allowed to perform. See https://aws.amazon.com/iam for details.
- AWS service configurations include such things as an Amazon Virtual Private Cloud (VPC) architecture that includes predefined AWS security groups to be assigned to Amazon Elastic Compute Cloud (EC2) instances, Amazon Simple Storage Service (Amazon S3) buckets provisioned with predefined access control policies, and network connectivity to access functional and security-enabling shared services (for example, code repositories, patch repositories, security scanning tools, anti-malware services, authentication services, time synchronization services, directory services, backup and recovery services, etc.).

4. An automated process interfaces with the organization's governance, risk, and compliance (GRC) tool to link John's AWS account with the preapproved/assessed system boundary, so that the GRC tool can account for the system inventory and monitor for compliance violations as part of automated IT auditing and continuous monitoring.
5. An automated process begins tracking the AWS services and resources that John provisions to record the spending rate within John's AWS account.
6. As the monthly spend limit is approached, an automated series of notifications is sent to John so that John can take action to ensure he does not overspend his budget. It is escalated to his management If John fails to react appropriately, a series of automated predefined budget enforcement actions take place, including preventing new AWS resources from being provisioned, and then shutting down or de-provisioning AWS resources.

Appendix B: Governance at scale capability checklist

There are several Amazon Partner Network (APN) partner solutions that you can use to meet the governance at scale requirements. We encourage organizations to evaluate each solution and make a decision based on your specific requirements. AWS Professional Services and Solution Architects can assist in your evaluation process. If you want to discuss partner products, reach out to your AWS Sales teams, or send an email to compliance-accelerator@amazon.com.

Account Management

Capability	Fully implements (yes/no)	Partially implements (yes/no)	Comments
Programmatically provision and delete AWS accounts using AWS APIs to ensure uniformity			
Allow external IAM accounts to enable and disable users			
Provide single sign on to the AWS Management Console for AWS account users to manage cloud resources			
Integrate with external IAM providers such as Active Directory			
Support MFA token management			
Associate AWS accounts with one or more master billing accounts			
Associate users with IAM policies to control access			
Support multi-level organizational hierarchy			
Support use of Enterprise Accelerators to apply baseline configurations to accounts			
Provide self-service workflow that allows users to join projects			
Provide self-service workflow that allows users to create new projects			

Capability	Fully implements (yes/no)	Partially implements (yes/no)	Comments
Provide self-service workflow that allows users to connect one or more accounts			
Control access to custom Amazon Machine Images (AMIs)			
Allow user access to the AWS API, AWS Management Console, and SDKs			

Budget and Cost Management

Capability	Fully implements (yes/no)	Partially Implements (yes/no)	Comments
Manage funding sources used to pay for AWS usage			
Allocate funding sources to individuals and AWS accounts based on organizational hierarchy			
Set monthly and yearly budgets for AWS accounts			
View current spending accrual of AWS accounts			
Aggregate spending of AWS accounts based on organization structure and purpose			
Apply cost restrictions to AWS accounts (for example, force use of Reserved Instances, restrict Amazon EC2 instance usage to instances less than $x/hr, etc.)			
Set rules to define enforcement actions (including notification, limit creating new cloud resources, archiving cloud resources, and termination of cloud resources) when financial thresholds are reached for each AWS account			
Send alerts to financial stakeholders when predefined limits and thresholds are met			

Security and Compliance Automation

Capability	Fully implements (yes/no)	Partially implements (yes/no)	Comments
Programmatically apply access control policies to restrict user access to AWS services that do not meet regulatory compliance standards (such as HIPAA, FedRAMP, PCI/DSS)			
Programmatically apply access control policies to restrict user access to AWS Regions that do not meet regulatory compliance standards (for example, HIPAA, FedRAMP, and PCI/DSS)			
Programmatically apply access control policies to restrict user access to AWS resource configurations that do not meet regulatory compliance standards (for example, HIPAA, FedRAMP, and PCI/DSS)			
Support multi-level organizational hierarchy to apply and inherit access control policies			
Collect and store logs for all AWS accounts, resources, and API actions			
Programmatically verify that cloud resources are configured in alignment with best practices, organizational policies, and regulatory compliance standards			
Programmatically generate Authorization to Operate (ATO) artifacts, including system security plans (SSPs), based on current cloud resources within AWS accounts			
Schedule continuous monitoring tasks (for example, vulnerability scans within and across AWS accounts) to determine whether the system is compliant			
Set rules to define enforcement actions (including notification, limit creating new cloud resources, and isolation of cloud resources) when compliance violation thresholds are reached for each AWS account			

Contributors

The following individuals and organizations contributed to this document:

- Doug Vanderpool - Principal Consultant, Advisory, AWS Professional Services
- Brett Miller – Technical Program Manager, WWPS Security and Compliance Business Acceleration Team
- Lou Vecchioni – Senior Consultant, AWS Professional Services
- Colin Desa - Head, Envision Engineering Center
- Tim Anderson – Program Manager, WWPS Security and Compliance Business Acceleration Team
- Nathan Case, Senior Consultant, AWS Professional Services

Further Reading

For additional information, see the following:

- AWS Whitepapers
- AWS Documentation
- AWS Compliance Quick Starts

Document Revisions

Date	Description
May 2017	First DRAFT Version
August 2017	DRAFT Version 2.0
November 2017	DRAFT Version 2.1
July 2018	DRAFT Version 2.2