This paper has been archived.

For the most recent security content, see
Best Practices for Security, Identity, and Compliance at
https://aws.amazon.com/architecture/security-identity-compliance

Security at Scale: Governance in AWS

Analysis of AWS features that can alleviate on-premise challenges

October 2015

Table of Contents

Abstract

You can run nearly anything on AWS that you would run on on-premise: websites, applications, databases, mobile apps, email campaigns, distributed data analysis, media storage, and private networks. The services AWS provides are designed to work together so that you can build complete solutions. An often overlooked benefit of migrating workloads to AWS is the ability to achieve a higher level of security, at scale, by utilizing the many governance-enabling features offered. For the same reasons that delivering infrastructure in the cloud has benefits over on-premise delivery, cloud-based governance offers a lower cost of entry, easier operations and improved agility by providing more oversight, security control, and central automation. This paper describes how you can achieve a high level of governance of your IT resources using AWS. In conjunction with the AWS Risk and Compliance whitepaper and the Auditing Security Checklist whitepaper, this paper can help you understand the security and governance features built in to AWS services so you can incorporate security benefits and best practices in building your integrated environment with AWS.

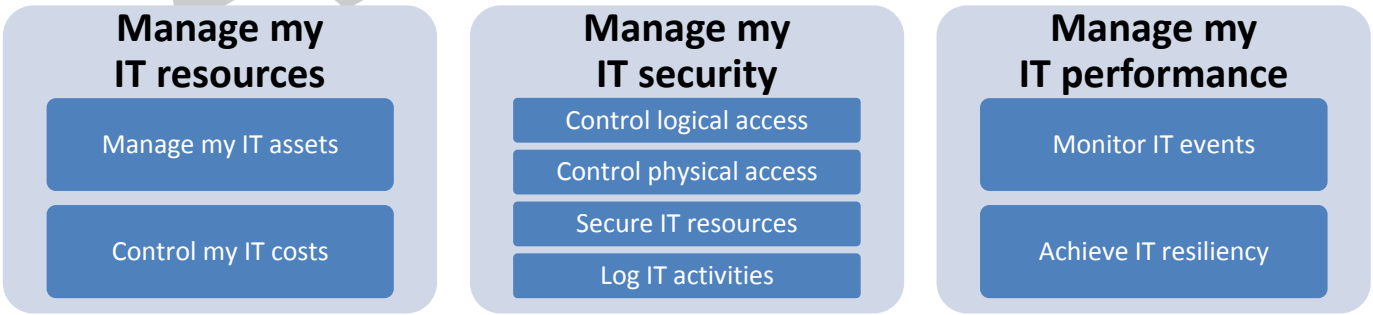
Introduction

Industry and regulatory bodies have created a complex array of new and legacy laws and regulations mandating a wide range of security and organizational governance measures. As such, research firms estimate that many companies are spending as much as 75% of their IT dollars to manage infrastructure and spending only 25% of their IT dollars on IT aspects that are directly related to the business their companies are providing. One of the key ways to improve this metric is to more efficiently address the back-end IT governance requirements. An easy and effective way to do that is by leveraging AWS's out-of-the-box governance features.

While AWS offers a variety of IT governance-enabling features, it can be hard to decide how to start and what to implement. This paper looks at the common IT governance domains by providing the use case (or the on-premise challenge), the AWS enabling features and the associated governance value propositions of using those features. This document is designed to help you achieve the objectives of each IT governance domain[1].

This paper follows the approach of the major domains of commonly-implemented IT governance frameworks (e.g. CoBIT, ITIL, COSO, CMMI, etc.); however, the IT governance domains through which the paper is organized are generic to allow any customer to use it to evaluate the governance features of using AWS versus what can be done with your on-premise resources and tools. The following IT governance domains are discussed through a "use-case" approach:

I want to better…



[1] While this paper features a robust list of the governance-enabling features, because new features are consistently being developed, it is not inclusive of all the features available. Additional tutorials, developer tools, documentation can be found at http://aws.amazon.com/resources/.

Manage IT resources

Manage IT assets

Identifying and managing your IT assets is the first step in effective IT governance. IT assets can range from the high-end routers, switches, servers, hosts and firewalls to the applications, services, operating systems and other software assets deployed in your network. An updated inventory of hardware and software assets is vital for decisions on upgrades and purchases, tracking warranty status, or for troubleshooting and security reasons. It is becoming a business imperative to have an accurate asset inventory listing to provide on-demand views and comprehensive reports. Moreover, comprehensive asset inventories are specifically required for certain compliance regulations. For example, FISMA, SOX, PCI DSS and HIPAA all mandate accurate asset inventories as a part of their requirements. However, the nature of pieced-together on-premise resources can make maintaining this listing arduous at best and impossible at worst. Often organizations have to employ third-party solutions to enable automation of the asset inventory listing, and even then, it is not always possible to see a detailed inventory of every type of asset on a single console.

Using AWS, there are multiple features available for you to quickly and easily obtain an accurate inventory of your AWS IT resources. Those features, associated 'how to' guidance, and links to learn more about the feature are provided below:

AWS governance-enabling feature	How you get security at scale
Account Activity page	Provides a summarized listing of IT resources by detailing usage of each service by region. Learn more.
Amazon Glacier vault inventory	Provides Glacier data inventory by showing all IT resources in Glacier. Learn more.
AWS CloudHSM	Provides virtual and physical control over encryption keys by providing customer-dedicated HSMs for key storage. Learn more.
AWS Data Pipeline Task Runner	Provides automated processing of tasks by polling the AWS Data Pipeline for tasks and then performing and reporting status on those tasks. Learn more.
AWS Management Console	Provides a real-time inventory of assets and data by showing all IT resources running in AWS, by service. Learn more.
AWS Storage Gateway APIs	Provide the capability to programmatically inventory assets and data by programming interfaces, tools, and scripts to manage resources. Learn more.

Control IT costs

You can better control your IT costs by obtaining resources in the most cost-effective way by understanding the costs of your IT services. However, managing and tracking the costs and ROI associated with IT resource spend on-premise can be difficult and inaccurate because the calculations are so complex; capacity planning, predictions of use, purchasing costs, depreciation, cost of capital and facilities costs are just a few aspects that make total cost of ownership difficult to calculate..

Using AWS, there are multiple features available for you to easily and accurately understand and control your IT resource costs. Using AWS you can achieve cost savings of up to 80%, compared to the equivalent on-premises deployments[2]. Those features, associated 'how to' guidance, and links to learn more about the feature are provided below:

AWS governance-enabling feature	How you get security at scale
Account Activity page	Provides an anytime view of spending on IT resources by showing resources used by service. Learn more.
Amazon EC2 idempotency instance launch	Helps prevent erroneous launch of resources and incurrence of additional costs by preventing timeouts or connection errors from launching additional instances. Learn more.
Amazon EC2 resource tagging	Provides association between resource expenditures and business units by applying custom searchable labels to compute resources. Learn more.
AWS Account Billing	Provides easy-to-use billing features that help you monitor and pay your bill by detailing resources used and associated actual compute costs incurred. Learn more.
AWS Management Console	Provides a one-stop-shop view for cost drivers by showing all IT resources running in AWS by service including actual costs and run rate. Learn more.
AWS service pricing	Provides definitive awareness of AWS IT resource rates by providing pricing for each AWS product and specific pricing characteristics. Learn more.
AWS Trusted Advisor	Helps optimize cost of IT resources by identifying unused and idle resources. Learn more.
Billing Alarms	Provides proactive alerts on IT resource spend by sending notifications of spending activity. Learn more.
Consolidated billing	Provides centralized cost control and cross-account cost visibility by combining multiple AWS accounts into one bill. Learn more.

[2] See the Total Cost of Ownership Whitepaper for more information on overall cost savings using AWS

Pay-as-you-go pricing	Provides computing resources and services that you can use to build applications within minutes at pay-as-you-go pricing with no up-front purchase costs or ongoing maintenance costs by automatically scaling into multiple servers when demand for your application increases. Learn more.

Manage IT security

Control physical access to IT resources

Physical access management is a key component of IT governance programs. In addition to the locks, security alarms, access controls, and surveillance videos that define the traditional components of physical security, the electronic controls over physical access are also paramount to effective physical security. The traditional physical security industry is in rapid transition, and areas of specialization are surfacing making physical security vastly more complex. As the on-premise physical security considerations and controls have become more complex, there is an increased need for uniquely qualified and specialized IT security professionals to manage the significant effort required to achieve effective physical control around access credentials for cards/card readers, controllers, and system servers for hosting data around physical security.

Using AWS, you can easily and effectively outsource controls related to physical security of your AWS infrastructure to AWS specialists with the skill-sets and resources needed to secure the physical environment. AWS has multiple different, independent auditors validate the data center physical security throughout the year, attesting to the design and detailed testing of the effectiveness of our physical security controls. Learn more about the AWS audit programs and associated physical security controls below:

AWS governance-enabling feature	How you get security at scale
AWS SOC 1 physical access controls	Provides transparency into the controls in place that prevent unauthorized access to data centers. Controls are properly designed, tested and audited by an independent audit firm. Learn more.
AWS SOC 2-Security physical access controls	Provides transparency into the controls in place that prevent unauthorized access to data centers. Controls are properly designed, tested and audited by an independent audit firm. Learn more.
AWS PCI DSS physical access controls	Provides transparency into the controls in place that prevent unauthorized access to data centers, relevant to the Payment Card Industry Data Security Standard. Controls are properly designed, tested and audited by an independent audit firm. Learn more.
AWS ISO 27001 physical access controls	Provides transparency into the controls and processes in place that prevent unauthorized access to data centers, relevant to the ISO 27002 security best practice standard. Controls are properly designed, tested and audited by an independent audit firm. Learn more.

AWS FedRAMP physical access controls	Provides transparency into the controls and processes in place that prevent unauthorized access to data centers, relevant to the NIST 800-53 best practice standard. Controls are properly designed, tested and audited by a government-accredited independent audit firm. Learn more.

Control logical access to IT resources

One of the primary objectives of IT governance is to effectively manage logical access to computer systems and data. However, many organizations are struggling to scale their on-premise solutions to meet the growing and continuously changing number of considerations and complexities around logical access, including the ability to establish a rule of least privilege, manage permissions to resources, address changes in roles and information needs, and the growth of sensitive data. Major, persistent challenges for managing logical access in an on-premise environment are providing users with access based on:

- Role (i.e. internal users, contractors, outsiders, partners, etc.)
- Data classification (i.e. confidential, internal use only, private, public, etc.)
- Data type (i.e. credentials, personal data, contact information, work-related data, digital certificates, cognitive passwords, etc.)

There are multiple control features AWS offers you effectively manage your logical access based on a matrix of use cases anchored in least-privilege. Those features, associated 'how to' guidance, and links to learn more about the feature are provided below:

AWS governance-enabling feature	How you get security at scale
Amazon S3 Access Control Lists (ACLs)	Provides central permissions and conditions by adding specific conditions to control how a user can use AWS, such as time of day, their originating IP address, whether they are using SSL, or whether they have authenticated with a Multi-Factor Authentication device. Learn more here and here.
Amazon S3 Bucket Policies	Provides the ability to create conditional rules for managing access to their buckets and objects by allowing you to restrict access based on account as well as request-based attributes, such as HTTP referrer and IP address. Learn more.
Amazon S3 Query String Authentication	Provides the ability to give HTTP or browser access to resources that would normally require authentication by using the signature in the query string to secure the request. Learn more.
AWS CloudTrail	Provides logging of API or console actions (e.g., log if someone changes a bucket policy, stops and instance, etc.), allowing advanced monitoring capabilities. Learn more.
AWS IAM Multi-Factor Authentication (MFA)	Provides enforcement of MFA across all resources by requiring a token to sign in and access resources. Learn more.

AWS IAM password policy	Provides the ability to manage the quality and controls around your users' passwords by allowing you to set a password policy for the passwords used by IAM users that specifies that passwords must be of a certain length, must include a selection of characters, etc. Learn more.
AWS IAM Permissions	Provides the ability to easily manage permissions by letting you specify who has access to AWS resources, and what actions they can perform on those resources. Learn more.
AWS IAM Policies	Enables you to achieve detailed, least-privilege access management by allowing you to create multiple users within your AWS account, assign them security credentials, and manage their permissions. Learn more.
AWS IAM Roles	Provides the ability to temporarily delegate access to users or services that normally don't have access to your AWS resources by defining a set of permissions to access the resources that a user or service needs. Learn more.
AWS Trusted Advisor	Provides automated security management assessment by identifying and escalating possible security and permission issues. Learn more.

Secure IT resources

Securing IT resources is the cornerstone of IT governance programs. However, for on-premise environments, there is a litany of security steps that must be taken when a new server is brought online. For example, firewall and access control policies must be updated, the newly created server image must be verified to be in compliance with security policy, and all software packages have to be up to date. Unless these security tasks are automated and delivered in a way that can keep up with the highly dynamic needs of the business, organizations working solely with traditional governance approaches will either cause users to work around the security controls, or will cause costly delays for the business.

AWS provides multiple security features that enable you to easily and effectively secure your IT resources. Those features, associated 'how to' guidance, and links to learn more about the feature are provided below:

AWS governance-enabling feature	How you get security at scale
Amazon Linux AMIs	Provides the ability to consistently deploy a "gold" (hardened) image by developing a private image to be used in all instance deployments. Learn more.
Amazon EC2 Dedicated Instances	Provides a private, isolated virtual network and ensures that your Amazon EC2 compute instances are be isolated at the hardware level and launching these instances into a VPC. Learn more.
Amazon EC2 instance launch wizard	Enables consistent launch process by providing restrictions around machine images available when launching instances. Learn more.

Amazon EC2 security groups	Provides granular control over inbound and outbound traffic by acting as a firewall that controls the traffic for one or more instances. Learn more.
Amazon Glacier archives	Provides inexpensive long term storage service for securing and durably storage for data archiving and backup using AES 256 bit encryption by default. Learn more.
Amazon S3 Client-Side Encryption	Provides the ability to encrypt your data before sending it to Amazon S3 by building your own library that encrypts your objects data on the client side before uploading it to Amazon S3. The AWS SDK for Java can also automatically encrypt your data before uploading it to Amazon S3. Learn more.
Amazon S3 Server-Side Encryption	Provides encryption of objects at rest and keys managed by AWS by using AES 256 bit encryption for Amazon S3 data. Learn more.
Amazon VPC	Provides a virtual network closely resembling a traditional network that is operated on-premise, but with benefits of using the scalable infrastructure of AWS. Allows you to create logically isolated sections of AWS where you can launch AWS resources in a virtual network that you define. Learn more.
Amazon VPC logical isolation	Provides virtual isolation of resources by allowing machine images to be isolated from other networked resources. Learn more.
Amazon VPC network ACLs	Provides 'firewall-type' isolation for associated subnets by controlling inbound and outbound traffic at the subnet level. Learn more.
Amazon VPC private IP addresses	Helps protect private IP addresses from internet exposure by routing their traffic through a Network Address Translation (NAT) instance in a public subnet. Learn more.
Amazon VPC security groups	Provides 'firewall-type' isolation for associated Amazon EC2 instances by controlling inbound and outbound traffic at the instance level. Learn more.
AWS CloudFormation templates	Provides the ability to consistently deploy a specific machine image along with other resources and configurations by provisioning infrastructure with scripts. Learn more.
AWS Direct Connect	Removes need for a public Internet connection to AWS by establishing a dedicated network connection from your premises to AWS' datacenter. Learn more.
On-premise hardware/software VPN connections	Provides granular control over network security by allowing secure connections from existing network to AWS. Learn more.

Virtual private gateways	Provides granular control over network security by providing a way to create a Hardware VPN Connection to your VPC. Learn more.

Manage logging around IT resources

A major enabler of securing IT is the logging around IT resources. Logging is critically important to IT governance for a variety of use cases, including but not limited to: detecting/tracking suspicious behavior, supporting forensic analysis, meeting compliance requirements, supporting IT/networking maintenance and operations, managing/reducing IT security costs, monitoring service levels, and supporting internal business processes. Organizations are increasingly dependent on effective log management to support core governance functions including cost management, service level and line-of-business application monitoring, and other IT-security and compliance focused activities. The SANS Log Management Survey consistently shows that organizations are continuously seeking more uses from their logs, but are encountering friction in their ability to achieve that use cases using on-premise resources to collect and analyze those logs. With more log types to collect and analyze from different IT resources, organizations are challenged by the manual overhead associated with normalizing log data that is in widely different formats, as well as with the searching, correlating and reporting functionalities. Log management is a key capability for security monitoring, compliance, and effective decision-making for the tens- or hundreds-of-thousands of activities each day.

Using AWS, there are multiple logging features that enable you to effectively log and track the use of your IT resources. Those features, associated 'how to' guidance, and links to learn more about the feature are provided below:

AWS governance-enabling feature	How you get security at scale
Amazon CloudFront access logs	Provides log files with information about end user access to your objects. Logs can be distributed directly to a specific Amazon S3 bucket. Learn more.
Amazon RDS database logs	Provides a way to monitor a number of log files generated by your Amazon RDS DB Instances. Used to diagnose, trouble shoot and fix database configuration or performance issues. Learn more.
Amazon S3 Object Expiration	Provides automated log expiration by scheduling removal of objects after a defined time period. Learn more.
Amazon S3 server access logs	Provides logs of access requests with details about the request such as the request type, the resource with which the request was made, and the time and date that the request was processed. Learn more.
AWS CloudTrail	Provides logs of security actions done via the AWS Management Console or APIs. Learn more.

Manage IT performance

Monitor and respond to events

IT performance management and monitoring has become a strategically important part of any IT governance program. IT monitoring is an essential element of governance that allows you to prevent, detect and correct IT issues that may impact performance and/or security. The key governance challenge in on-premise environments around IT performance management is that you are faced with multiple monitoring systems to manage every layer of your IT resources, and the mix of proprietary management tools and IT processes results in a systemic complexity that can at best slow response times and at worst, impact the effectiveness of your IT performance monitoring and management. Moreover, the increasing complexity and sophistication of security threats mean that event monitoring and response capabilities need to continuously and rapidly evolve to address emerging threats. As such, on-premise performance management is continuously faced with growing challenges around infrastructure procurement, scalability, ability to simulate test conditions across multiple geographies, etc.

Using AWS, there are multiple monitoring features that enable you to easily and effectively monitor and manage your IT resources. Those features, associated 'how to' guidance, and links to learn more about the feature are provided below:

AWS governance-enabling feature	How you get security at scale
Amazon CloudWatch	Provides statistical data you can use to view, analyze, and set alarms on the operational behavior of your instances. These metrics include CPU utilization, network traffic, I/O, and latency. Learn more.
Amazon CloudWatch alarms	Provides consistent alarming for critical events by providing custom metrics, alarms and notifications for events. Learn more.
Amazon EC2 instance status	Provides instance status checks that summarize results of automated tests and provides information about certain activities that are scheduled for your instances. Uses automated checks to detect whether specific issues are affecting your instances. Learn more.
Amazon Incident Management Team	Provides continuous incident detection, monitoring and management with 24-7-365 staff operators to support detection, diagnostics, and resolution of certain security events. Learn more.
Amazon S3 TCP selective acknowledgement	Provides the ability to improve recovery time after a large number of packet losses. Learn more.
Amazon Simple Notification Service	Provides consistent alarming for critical events by managing the delivery of messages to subscribing endpoints or clients. Learn more.
AWS Elastic Beanstalk	Provides ability to monitor application deployment details of capacity provisioning, load balancing, auto-scaling, and application health monitoring. Learn more.
Elastic Load Balancing	Provides the ability to automatically distribute your incoming application traffic across multiple Amazon EC2 instances by detecting

	over utilized instances and rerouting traffic to underutilized instances. Learn more.

Achieve resiliency

Data protection and disaster recovery planning should be a priority component of IT governance for all organizations. Arguably, the value of DR is not in question; every organization is concerned about its ability to get back up and running after an event or disaster. But implementing governance around IT resource resiliency can be expensive and complex, as well as tedious and time-consuming. Organizations are faced with a growing number of events that can cause unplanned downtime and operational blockers. These events can be caused by technical problems (e.g. viruses, data corruption, human error, etc.) or natural phenomena (e.g. fires, floods, power failures, weather-related outages, etc.). As such, organizations are faced with increasing costs and complexity in planning, testing and operating on-premise failover sites because of continual data growth.

In the face of these challenges, cloud computing's server virtualization enables the quality resiliency programs to be feasible and cost-effective. Using AWS, there are multiple features that enable you to easily and effectively achieve resiliency for your IT resources. Those features, associated 'how to' guidance, and links to learn more about the feature are provided below:

AWS governance-enabling feature	How you get security at scale
Amazon EBS snapshots	Provides highly available, highly reliable, predictable storage volumes with incremental point in time backup control of server data. Learn more.
Amazon RDS Multi-AZ Deployments	Provides the ability to safeguard your data in the event with automated availability controls, homogenous resilient architecture. Learn more.
AWS Import/Export	Provides the ability to move massive amounts of data locally by creating import and export jobs quickly using Amazon's high-speed internal network. Learn more.
AWS Storage Gateway	Provides seamless and secure integration between your on-premises IT environment and AWS's storage infrastructure by scheduling snapshots that the gateway stores in Amazon S3 in the form of Amazon EBS snapshots. Learn more.
AWS Trusted Advisor	Provides automated performance management and availability control by identifying options to increase the availability and redundancy of your AWS application. Learn more.
Extensive 3rd Party Solutions	Provides secure data storage and automated availability control by easily connecting you with a market of applications of tools. Learn more.
Managed AWS No-SQL/SQL Database Services	Provides secure and durable data storage automatically replicating data items across multiple Availability Zones in a Region to provide built-in high availability and data durability. Learn more: • Amazon Dynamo DB

	• Amazon RDS
Multi-region deployment	Provides geo-diversity in compute locations, power grids, fault lines, etc. providing a variety of locations. Learn more.
Route 53 health checks and DNS failover	Monitors availability of stored backup data by allowing you to configure DNS failover in active-active, active-passive, and mixed configurations to improve the availability of your application. Learn more.

Service-Governance Feature Index

The information above is presented by governance domain. For your reference, a summary of governance feature by major AWS services is described in the table below:

AWS Service	Governance Feature
Amazon EC2	Amazon EC2 idempotency instance launch Amazon EC2 resource tagging Amazon Linux AMIs Amazon EC2 Dedicated Instances Amazon EC2 instance launch wizard Amazon EC2 security groups
Elastic Load Balancing	Elastic Load Balancing traffic distribution
Amazon VPC	Amazon VPC Amazon VPC logical isolation Amazon VPC network ACLs Amazon VPC private IP addresses Amazon VPC security groups On-premise hardware/software VPN connections
Amazon Route 53	Amazon Route 53 latency resource record sets Route 53 health Checks and DNS failover
AWS Direct Connect	AWS Direct Connect
Amazon S3	Amazon S3 Access Control Lists (ACLs)

	Amazon S3 Bucket Policies Amazon S3 Query String Authentication Amazon S3 Client-Side Encryption Amazon S3 Server-Side Encryption Amazon S3 Object Expiration Amazon S3 server access logs Amazon S3 TCP selective acknowledgement Amazon S3 TCP window scaling
Amazon Glacier	Amazon Glacier vault inventory Amazon Glacier archives
Amazon EBS	Amazon EBS snapshots
AWS Import/Export	AWS Import/Export bulk datano…
AWS Storage Gateway	AWS Storage Gateway integration AWS Storage Gateway APIs
Amazon CloudFront	Amazon CloudFront Amazon CloudFront access logs
Amazon RDS	Amazon RDS database logs Amazon RDS Multi-AZ Deployments Managed AWS No-SQL/SQL Database Services
Amazon Dynamo DB	Managed AWS No-SQL/SQL Database Services
AWS Management Console	Account Activity page AWS Account Billing AWS service pricing AWS Trusted Advisor Billing Alarms Consolidated billing Pay-as-you-go pricing

	AWS CloudTrail Amazon Incident Management Team Amazon Simple Notification Service Multi-region deployment
AWS Identity and Access Management (IAM)	AWS IAM Multi-Factor Authentication (MFA) AWS IAM password policy AWS IAM Permissions AWS IAM Policies AWS IAM Roles
Amazon CloudWatch	AWS CloudWatch Dashboard Amazon CloudWatch alarms
AWS Elastic Beanstalk	AWS Elastic Beanstalk monitoring
AWS CloudFormation	AWS CloudFormation templates
AWS Data Pipeline	AWS Data Pipeline Task Runner
AWS CloudHSM	CloudHSM key storage
AWS Marketplace	Extensive 3rd Party Solutions
Data Centers	AWS SOC 1 physical access controls AWS SOC 2-Security physical access controls AWS PCI DSS physical access controls AWS ISO 27001 physical access controls AWS FedRAMP physical access controls

Conclusion

The primary focus of IT Governance is around managing resources, security and performance in order to deliver value in strategic alignment with the goals of the business. Given the rate growth and increasing complexity in technology, it is increasingly challenging for on-premise environments to scale to provide the granular controls and features needed to deliver quality IT governance in a cost-efficient manner. For the same reasons that delivering infrastructure in the cloud has benefits over on-premise delivery, cloud-based governance offers a lower cost of entry, easier operations and improved agility by providing more oversight and automation that enables organizations to focus on their business.

References and Further Reading

What can I do with AWS? http://aws.amazon.com/solutions/aws-solutions/.

How can I get started with AWS? http://docs.aws.amazon.com/gettingstarted/latest/awsgsg-intro/gsg-aws-intro.html