# Auditing Amazon Web Services

As organizations increase adoption of cloud services for running enterprise architecture and applications, auditors are required to step up their game and learn new in-depth audit skills. The previous Total Administrative Services Corporation (TASC) environment consisted of a conglomeration of disparate systems, infrastructure and spaghetti-string network connectivity, leading senior management to discover a better way to conduct business and transform the organization by leveraging cloud technologies. There are valuable insights, education and audit considerations to be gained from examining the cloud transformation, security and compliance journey one organization underwent through the period of May 2017 to May 2018.

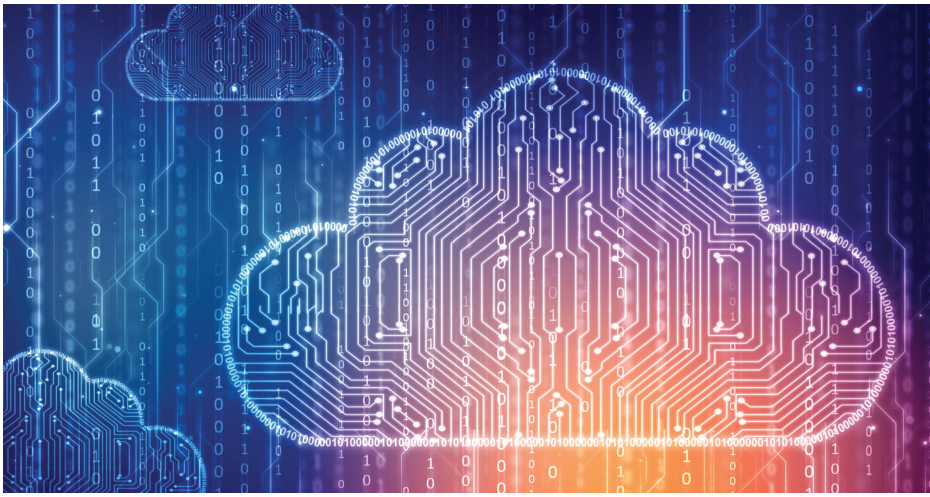
There are generalized audit approach considerations organizations can utilize to review operational, security and compliance aspects of their Amazon Web Services (AWS) offering. The generalized audit program presented here incorporates elements of the AWS Center for Internet Security (CIS) Foundation Benchmarks, published audit guidance and developer guides, which can be leveraged or tailored to other organizations needs when conducting an AWS assessment. The suggested audit topics and guidance are just that and are in no way a prescriptive set of tests an organization should or is directed to perform. The best place to start is with an overview of some of the general control considerations for AWS.

An important consideration before undertaking an AWS audit is understanding the specific AWS services the organization has purchased; the intended use of these services; the interrelationships between these services; how users, whether internal or external, are accessing the environment; and who is responsible for managing each service on a daily basis.

Documentation useful for auditing these services is available.[1] Developer guides, user guides and white papers providing information useful for developing an AWS audit universe and specific items of risk to consider are also available.

## Governance

Using elements of COBIT® 5, it is important to establish and determine whether a separation between a governance body and operational management is in place as a key risk of self-policing may be present, leading to an unruly cloud implementation, uncontrolled costs and failure to achieve stakeholder needs. Audit testing at this stage should determine whether coherent operational and/or compliance objectives formally exist in documents, whether they are communicated to operational management, and if regular meetings between the governance and management functions occur to measure achievement of these objectives. Further determinations should focus on whether and to what extent AWS services integrate into existing directives and processes such as the information security program; change management; incident



**Adam Kohnke,** CISA, CCNA:Security, ITIL v3, Security+
Is currently serving as the senior IT auditor for Total Administrative Services Corporation in Madison, Wisconsin, USA. Kohnke has more than two years of IT audit experience and more than six years in IT operations with various Fortune 500 companies as an incident, change and project manager.

**Do you have something to say about this article?**

Visit the *Journal* pages of the ISACA® website *(www.isaca.org/journal)*, find the article and click on the Comments link to share your thoughts.

***https://bit.ly/2FKDLJg***

## Enjoying this article?

- Read *AWS Audit Program.* *www.isaca.org/ www.isaca.org/aws-audit-program*
- Learn more about, discuss and collaborate on audit and assurance in ISACA's Online Forums. *https://engage.isaca.org/onlineforums*

response and disaster recovery; whether uniform asset inventory, tagging strategies and AWS service acquisition management processes are in effect to manage costs; and the use of AWS services and related resources. Additional focus areas in this portion of the review should revolve around the architecture of AWS services through the inspection of network diagrams, the level of integration with on-premise systems, vendor management processes, and other oversight functions such as routine execution of security and/or risk assessments.[2]

### Network Configuration and Management

This aspect of the review focuses primarily on determining and understanding whether the external virtual private cloud (VPC) provided by AWS meets organizational security and architecture requirements. Some considerations at this level include whether resources deployed to AWS regions, availability zones, AWS service access, and the implementation of VPCs, subnets and security groups (also known as firewall rules) are appropriate. A key risk to consider at this stage is whether VPC peering is active, between which resources or Amazon accounts, and the level of access granted through the VPC peering connection. VPC peering allows external access from other AWS root accounts to the organization's portion of the cloud and may serve as a potential data exfiltration vector. It should be adequately restricted and monitored when use is necessary. Further determinations should focus on whether network architecture comparisons occur on a routine basis against defined security requirements and the degree to which this architecture has properly segregated various environments such as test, stage and production. It is also important to review whether security groups and network access control lists (NACL) appropriately restrict inbound and outbound network traffic, default to deny traffic if allowed traffic patterns cannot be matched, and whether network baselining is occurring to understand standard network patterns and usage and facilitate the ability to identify and properly react to abnormal network traffic patterns.

### Asset Configuration and Management

AWS assets consist of the AWS services purchased from Amazon, the configurable settings associated with those service resources, and the data contained within or processed by those service resources. A simplified example is Amazon S3 (the service), the managed S3 buckets (the configurable service resource) and the data contained in those S3 buckets. This aspect of the review is concentrated on securely managing AWS service resources, controlling use of these service resources, ensuring secure configurations, controlling changes to these service resources and tracking changes to them over time.

> "ACCESS CONTROL INTRODUCES THE MOST RISK TO ORGANIZATIONS SIMPLY DUE TO THE NUMBER OF WAYS USERS CAN ACCESS AWS."

Audit testing should focus on determining whether AWS resources, such as Elastic Compute Cloud (EC2) instances or S3 buckets, are deployed in a baseline fashion across all AWS root accounts, regions and availability zones, further determining how nonconforming resources are identified and whether timely detection and correction of these resources' configurations are adequately facilitated. Further determinations should focus on whether modifications to critical AWS service resource configurations generate an audit trail, who can manipulate that audit trail, where and how those records are secured, and how long those records are retained in accordance with organizational directives.

### Logical Access Control

The access control setup in AWS is complex to say the least. Amazon provides numerous methods to organizations for accessing the data deployed through AWS service resources. Methods include HTTP access to the AWS root account, the AWS management console, the Identity and Access Management (IAM) service, application programming interface (API) Gateway, AWS Cognito, AWS CloudFront distributions, federated access via on-premise Active Directory, and others. Access control introduces the most risk to organizations simply due to the number of ways users can access AWS, which, in turn, introduces a more prevalent attack surface and increased activity with the management of each individual access vector listed previously.

Audit activity at this stage should focus on the AWS root accounts that exist, as there may be several. The AWS root account cannot be adequately restricted in the traditional sense, as a password policy cannot be applied to it and because the services or data it may access and manipulate cannot be restricted. It is important to note that a key concept regarding user accounts in AWS is access keys, which are separate from usernames or passwords and consist of two pieces of information necessary for programmatic use of AWS accounts. The first is the secret access key, which is only accessible at the time of account creation. The second is the access key ID. These two pieces of information are tokens used in tandem to programmatically access and sign API requests made within AWS. AWS allows generation of two separate access keys per account for the purposes of rotating access keys that should be an additional audit focus for administrative accounts.[3, 4]

Regarding the root account, it is strongly encouraged that use of the account is disabled by deleting the access keys or configuring the access keys to be inactive from the management console, and that administrative role-based accounts are created for everyday administrative tasks in the AWS environment. There are activities that require the use of the root account related to billing, support and ending AWS service use. If the decision to delete root access keys does not occur, one should ensure that the root account has multifactor authentication enabled against it and that registration with Amazon support has taken place in case there are any problems such as accessing the management console or other unforeseen scenarios.

After the root account, the review can advance by executing typical IT general control industry practices for access management such as how users' identities, roles and groups are structured; if they appropriately restrict access to AWS service resources; and whether other AWS accounts or Active Directory domains have administrative access to the services. Further audit focus should center on how cryptographic key management

> "EVERY AWS SERVICE THAT PROVIDES ACCESS TO THE ENVIRONMENT HAS DETAILED GUIDES EXPLAINING DEFAULT CONFIGURATION, POSSIBLE CONFIGURATIONS, ASSOCIATED ROLES, OR ACCESS AND CONTROLS."

access is restricted if used, whether key management activity is reviewed, and whether administration and standard user activity is segregated through use of different accounts or access groups. Every AWS service that provides access to the environment has detailed guides explaining default configuration, possible configurations, associated roles, or access and controls. Taking time to understand cross-service operations is also an important step to take early on, because some services work in tandem to provide users with access to the environment such as IAM and API Gateway.

## Data Encryption Controls

Amazon does a good job when it comes to providing organizations with strong (e.g., Advanced Encryption Standard [AES] AES-256) default encryption for AWS services for data at rest and limiting default access to certain service resources such as S3 storage buckets. This aspect of the review may seek to focus on whether a data classification scheme exists for information stored in specific AWS services, such as EC2, S3, Redshift, relational database service (RDS) or Lambda, and if appropriate encryption is actively protecting those service resources and their data. This part of the review may also focus on remote connectivity into the environment and ensuring strong encryption is required for remote access.

## Logging and Event Management

Amazon provides a variety of tools, such as CloudWatch and CloudTrail, that are useful for logging events occurring within AWS. Organizations are also able to integrate a security information and event management (SIEM) system for log correlation and centralized analysis. This part of the review seeks to validate whether an overall logging management strategy exists and whether the AWS environment reflects those requirements. The audit focus will overlap with the previous data encryption area to understand where sensitive data exist (i.e., S3 buckets, EC2 instances, Redshift clusters) and center on whether detailed logging is in place (date/time, success/failure indicators and source/destination IP address).

The audit's focus should also seek to determine whether log data are centrally managed for correlation analysis, whether access to logs is appropriately restricted, and whether modification attempts or logging failures can be promptly identified and addressed. Specific consideration to EC2 compute instances should occur, as well, to validate whether host intrusion detection mechanisms exist and are adequately configured to alert personnel to critical operating-system-level file changes. Finally, the audit should determine if the logging capability can adequately identify and alert personnel to unauthorized users or devices.

## Security Incident Response

This section of the audit will mostly focus on typical IT general control (ITGC) activities that mature organizations practice for internal security incident response, such as establishment of an incident response plan, routine exercising of the response and crisis communication aspects of the plan. A key risk this part of the review should focus on revolves around ensuring a support role exists under the AWS root account to manage security incidents with AWS support in the event a security breach occurs, impacting the organization. Additionally, a determination as to whether security contact information is registered with Amazon should be made to ensure that the organization is positioned to receive security advisory information in a timely manner.

Further audit focus should determine whether security questions have been established under the AWS root account. This helps ensure that interactions with AWS support require some level of authentication and may help limit unauthorized exposure of organizational information or resetting of root account credentials that give malicious users access to the AWS environment. Finally, the audit should determine whether an enterprisewide monitoring solution is deployed and the extent to which it is monitoring AWS service resources' availability and/or security states.

## Disaster Recovery

Disaster recovery in AWS covers a multitude of AWS services and resources. A good practice at this level of the review is to break disaster recovery testing points into several sections (e.g., network architecture, service configuration) to introduce some efficiency. Starting with the network architecture of AWS services, it is important to understand some AWS-specific concepts, namely regions and availability zones.

> “AWS TRUSTED ADVISOR OR OTHER TOOLS CAN BE LEVERAGED TO ASSIST WITH DETERMINING THE SUFFICIENCY OF AN ORGANIZATION'S AWS SERVICE FAULT TOLERANCE.”

AWS regions consist of geographical areas (i.e., Sao Paulo, US-East) that offer a collection of AWS services through availability zones (us-east-1a or us-east-1b). Availability zones are collections of fault-tolerant data centers that are physically isolated to a specific region but securely connect to each other over low-latency network links for fault tolerance. The services purchased through AWS can be configured to operate across multiple regions and availability zones. When replicating data between regions, the data traverse the public Internet, and some of the first audit checks are to determine whether this fault-tolerant condition exists, whether appropriate regions have been selected for fault tolerance and whether this connection is encrypted.

The audit's focus in this area should first determine whether the organization's disaster recovery processes and plans incorporate AWS services and the degree to which these recovery plans are reviewed, exercised and adjusted. Further, the audit should center on whether alternative workarounds for key processes are identified and incorporated into recovery plans, whether cross-training of staff occurs in the event that primary personnel are unavailable, and the extent to which the AWS services' resources themselves (i.e., S3 buckets, EC2 instances) are redundant. AWS Trusted Advisor or other tools can be leveraged to assist with determining the sufficiency of an organization's AWS service fault tolerance and may aid organizations with efficiently and effectively determining the overall security and compliance state of the AWS environment.

## The Current AWS Risk Universe

Each AWS service category (i.e., compute, storage) referenced in **figure 1** is a small subset of current AWS service offerings, and each can be thought of as galaxies with the individual service offerings listed in the service category as solar systems, each with their own configurations and risk considerations (planets).[5] The list is constantly growing as AWS develops new service offerings under the individual service categories. Effort should be taken by reading the developer guides for each service offering in use by the organization to understand potential configurations, applicable risk to the organization and potential mitigation strategies that should be taken.

A resource released by ISACA®, the *Amazon Web Services (AWS) Audit Program* [6], can assist practitioners in designing and implementing effective AWS audits.

## Endnotes

1. Amazon Web Services, AWS Documentation, https://*aws.amazon.com/documentation*
2. Amazon Web Services, *Introduction to Auditing the Use of AWS*, October 2015, *https://d1.awsstatic.com/whitepapers/compliance/AWS_Auditing_Security_Checklist.pdf*
3. Amazon Web Services, *AWS Security Best Practices*, August 2016, *https://d1.awsstatic.com/whitepapers/Security/AWS_Security_Best_Practices.pdf*
4. CIS Benchmarks, *CIS Amazon Web Services Foundations*, 23 May 2018, *https://d0.awsstatic.com/whitepapers/compliance/AWS_CIS_Foundations_Benchmark.pdf*
5. Amazon, "AWS Documentation," *https://docs.aws.amazon.com/index.html#lang/en_us*
6. ISACA®, *Amazon Web Services (AWS) Audit Program*, USA, 2019, *www.isaca.org/aws-audit-program*

**Figure 1—Current AWS Service Offerings**

| Subset of AWS Services by Category | Subset of Service Offerings per Category |
|---|---|
| Analytics | Amazon Athena, Amazon Cloud Search, AWS Data Pipeline, Amazon Glue, Amazon EMR, Amazon Kinesis, Amazon Redshift |
| Compute | Amazon EC2, AWS Batch, Amazon ECR, Amazon ECS, Amazon EKS, AWS Elastic Beanstalk, AWS Lambda |
| Database | Amazon Aurora, Amazon Dynamo DB, Amazon Elasti Cache Amazon Neptune, Amazon RDS, Amazon Redshift |
| Developer Tools | AWS Cloud9, AWS Code Build, AWS Code Commit AWS Code Deploy |
| Desktop & App Streaming | Amazon WAM, Amazon Workspaces, Amazon Appstream |
| Networking & Content Delivery | Amazon API Gateway, Amazon Cloud Front, Amazon VPC, Amazon Route 53 |
| Mobile Services | AWS AppSync, AWS Device Farm, Amazon Mobile Analytics, Amazon Mobile Hub, Amazon Pinpoint |
| Machine Learning | Amazon Comprehend, AWS Deep Lens, Amazon Lex |
| Management Tools | AWS Auto Scaling, AWS Cloud Formation, AWS Cloud Trail, AWS Cloud Watch, AWS Config, AWS Health |
| Security, Identity & Compliance | AWS Identity & Access Management, AWS Artifact, AWS Certificate Manager, AWS Cloud HSM, Amazon Cognito, Amazon Inspector, Amazon Guard Duty, AWS Shield |
| Storage | Amazon S3, Amazon EBS, Amazon EFS, Amazon Glacier Amazon Snowball |