Introduction to Auditing the Use of AWS

October 2015

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 4

Introduction 5

Approaches for using AWS Audit Guides 6

Examiners 6

AWS Provided Evidence 6

Auditing Use of AWS Concepts 8

Identifying assets in AWS 9

AWS Account Identifiers 9

1. Governance 10
2. Network Configuration and Management 14
3. Asset Configuration and Management 15
4. Logical Access Control 17
5. Data Encryption 19
6. Security Logging and Monitoring 20
7. Security Incident Response 21
8. Disaster Recovery 22
9. Inherited Controls 23

Appendix A: References and Further Reading 25

Appendix B: Glossary of Terms 26

Appendix C: API Calls 27

Abstract

Security at AWS is job zero. All AWS customers benefit from a data center and network architecture built to satisfy the needs of the most security-sensitive organizations. In order to satisfy these needs, AWS compliance enables customers to understand the robust controls in place at AWS to maintain security and data protection in the cloud.

As systems are built on top of AWS cloud infrastructure, compliance responsibilities will be shared. By tying together governance-focused, audit-friendly service features with applicable compliance or audit standards, AWS Compliance enablers build on traditional programs, helping customers to establish and operate in an AWS security control environment

AWS manages the underlying infrastructure, and you manage the security of anything you deploy in AWS. AWS as a modern platform allows you to formalize the design of security, as well as audit controls, through reliable, automated and verifiable technical and operational processes built into every AWS customer account. The cloud simplifies system use for administrators and those running IT, and makes your AWS environment much simpler to audit sample testing, as AWS can shift audits towards a 100% verification verses traditional sample testing.

Additionally, AWS' purpose-built tools can be tailored to customer requirements and scaling and audit objectives, in addition to supporting real-time verification and reporting through the use of internal tools such as AWS CloudTrail, Config and CloudWatch. These tools are built to help you maximize the protection of your services, data and applications. This means AWS customers can spend less time on routine security and audit tasks, and are able to focus more on proactive measures which can continue to enhance security and audit capabilities of the AWS customer environment.

Introduction

As more and more customers deploy workloads into the cloud, auditors increasingly need not only to understand how the cloud works, but additionally how to leverage the power of cloud computing to their advantage when conducting audits. The AWS cloud enables auditors to shift from percentage-based sample testing toward a comprehensive real-time audit view, which enables 100% auditability of the customer environment, as well as real-time risk management.

The AWS management console, along with the Command Line Interface (CLI), can produce powerful results for auditors across multiple regulatory, standards and industry authorities. This is due to AWS supporting a multitude of security configurations to establish security, compliance by design, and real-time audit capabilities through the use of:

- **Automation** - Scriptable infrastructure (e.g. Infrastructure as Code) allows you to create repeatable, reliable and secure deployment systems by leveraging programmable (API-driven) deployments of services.

- **Scriptable Architectures** – "Golden" environments and Amazon Machine Images (AMIs) can be deployed for reliable and auditable services, and they can be constrained to ensure real-time risk management.

- **Distribution** - Capabilities provided by AWS CloudFormation give systems administrators an easy way to create a collection of related AWS resources and provision them in an orderly and predictable fashion.

- **Verifiable-** Using AWS CloudTrail, Amazon CloudWatch, AWS OpsWorks and AWS CloudHSM enables evidence gathering capability.

Approaches for using AWS Audit Guides

Examiners

When assessing organizations that use AWS services, it is critical to understand the "Shared Responsibility" model between AWS and the customer. The audit guide organizes the requirements into common security program controls and control areas. Each control references the applicable audit requirements.

In general, AWS services should be treated similarly to on-premise infrastructure services that have been traditionally used by customers for operating services and applications. Policies and processes that apply to devices and servers should also apply when those functions are supplied by AWS. Controls pertaining solely to policy or procedure are generally entirely the responsibility of the customer. Similarly, AWS management, either via the AWS Console or Command Line API, should be treated like other privileged administrator access. See the appendix and referenced points for more information.

AWS Provided Evidence

Amazon Web Services Cloud Compliance enables customers to understand the robust controls in place at AWS to maintain security and data protection in the cloud. As systems are built on top of AWS cloud infrastructure, compliance responsibilities will be shared**.** Each certification means that an auditor has verified that specific security controls are in place and operating as intended. You can view the applicable compliance reports by contacting your AWS account representative. For more information about the security regulations and standards with which AWS complies visit the AWS Compliance webpage. To help you meet specific government, industry, and company security standards and regulations, AWS provides certification reports that describe how the AWS Cloud infrastructure meets the requirements of an extensive list of global security standards, including: ISO 27001, SOC, the PCI Data Security Standard, FedRAMP, the Australian Signals Directorate (ASD) Information Security Manual, and the Singapore Multi-Tier Cloud Security Standard (MTCS SS 584).

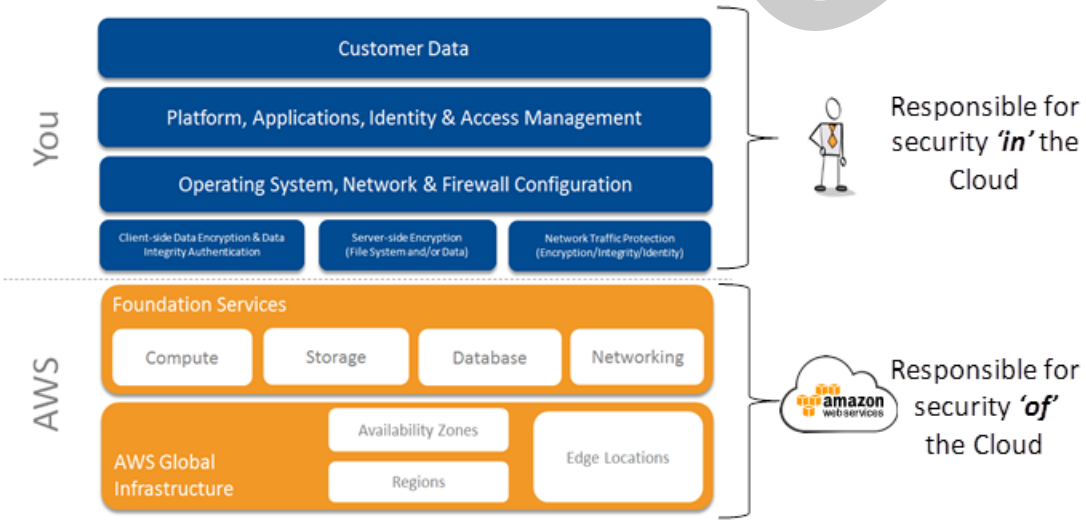
For more information about the security regulations and standards with which AWS complies, see the AWS Compliance webpage.

Auditing Use of AWS Concepts

The following concepts should be considered during a security audit of an organization's systems and data on AWS:

- Security measures that the cloud service provider (AWS) implements and operates – "security of the cloud"
- Security measures that the customer implements and operates, related to the security of customer content and applications that make use of AWS services – "security in the cloud"

While AWS manages security **of** the cloud, security **in** the cloud is the responsibility of the customer. Customers retain control of what security they choose to implement to protect their own content, platform, applications, systems and networks, no differently than they would for applications in an on-site datacenter.



Additional detail can be found at the AWS Security Center, at AWS Compliance, and in the publically available AWS whitepapers found at: AWS Whitepapers

Identifying assets in AWS

A customer's AWS assets can be instances, data stores, applications, and the data itself. Auditing the use of AWS generally starts with asset identification. Assets on a public cloud infrastructure are *not* categorically different than in-house environments, and in some situations can be less complex to inventory because AWS provides visibility into the assets under management.

AWS Account Identifiers

AWS assigns two unique IDs to each AWS account: an AWS account ID and a canonical user ID. The AWS account ID is a 12-digit number, such as 123456789012, that you use to construct Amazon Resource Names (ARNs). When you refer to resources, like an IAM user or an Amazon Glacier vault, the account ID distinguishes your resources from resources in other AWS accounts.

Amazon Resource Names (ARNs) and AWS Service Namespaces

Amazon Resource Names (ARNs) uniquely identify AWS resources. We require an ARN when you need to specify a resource unambiguously across all of AWS, such as in IAM policies, Amazon Relational Database Service (Amazon RDS) tags, and API calls.

ARN Format example:

```
    <!-- Elastic Beanstalk application version -->
arn:aws:elasticbeanstalk:us-east-1:123456789012:environment/My App/MyEnvironment

<!-- IAM user name -->
arn:aws:iam::123456789012:user/David

<!-- Amazon RDS tag -->
arn:aws:rds:eu-west-1:001234567890:db:mysql-db

<!-- Amazon S3 bucket (and all objects in it)-->
arn:aws:s3:::my_corporate_bucket/*
```

In addition to Account Identifiers, Amazon Resource Names (ARNs) and AWS Service Namespaces, each AWS service creates a unique service identifier (e.g. Amazon Elastic Compute Cloud (Amazon EC2) instance ID: i-3d68c5cb or Amazon Elastic Block Store (Amazon EBS) Volume ID vol-ecd8c122) which can be used to create an environmental asset inventory and used within work papers for scope of audit and inventory.

Each certification means that an auditor has verified that specific security controls are in place and operating as intended.

1. Governance

Definition: Governance provides assurance that customer direction and intent are reflected in the security posture of the customer. This is achieved by utilizing a structured approach to implementing an information security program. For the purposes of this audit plan, it means understanding which AWS services have been purchased, what kinds of systems and information you plan to use with the AWS service, and what policies, procedures, and plans apply to these services.

Major audit focus: Understand what AWS services and resources are being used and ensure your security or risk management program has taken into account the use of the public cloud environment.

Audit approach: As part of this audit, determine who within your organization is an AWS account and resource owner, as well as the AWS services and resources they are using. Verify policies, plans, and procedures include cloud concepts, and that cloud is included in the scope of the customer's audit program.

Governance Checklist

	Checklist Item
☐	Understand use of AWS within your organization. Approaches might include: • Polling or interviewing your IT and development teams. • Performing network scans, or a more in-depth penetration test. ▪ Review expense reports and/or Purchase Orders (PO's) payments related to Amazon.com or AWS to understand what services are being used. Credit card charges appear as "AMAZON WEB SERVICES AWS.AMAZON.CO WA" or similar. Note: Some individuals within your organization may have signed up for an AWS account under their personal accounts, as such, consider asking if this is the case when polling or interviewing your IT and development teams.
☐	**Identify assets.** Each AWS account has a contact email address associated with it and can be used to identify account owners. It is important to understand that this e-mail address may be from a public e-mail service provider, depending on what the user specified when registering. • A formal meeting can be conducted with each AWS account or asset owner to

	Checklist Item
	understand what is being deployed on AWS, how it is managed, and how it has been integrated with your organization's security policies, procedures, and standards. **Note**: The AWS Account owner may be someone in the finance or procurement department, but the individual who *implements* the organization's use of the AWS resources may reside in the IT department. You may need to interview both.
☐	**Define your AWS boundaries for review.** The review should have a defined scope. Understand your organization's core business processes and their alignment with IT, in its non-cloud form as well as current or future cloud implementations. • Obtain a description of the AWS services being used and/or being considered for use. • After identifying the types of AWS services in use or under consideration, determine the services and business solutions to be included in the review. • Obtain and review any previous audit reports with remediation plans. • Identify open issues in previous audit reports and assess updates to the documents with respect to these issues.
☐	**Assess policies.** Assess and review your organization's security, privacy, and data classification policies to determine which policies apply to the AWS service environment. • Verify if a formal policy and/or process exists around the acquisition of AWS services to determine how purchase of AWS services is authorized. • Verify if your organization's change management processes and policies include consideration of AWS services
☐	**Identify risks.** Determine whether a risk assessment for the applicable assets has been performed.
☐	**Review risks.** Obtain a copy of any risk assessment reports and determine if they reflect the current environment and accurately describe the residual risk environment.
☐	**Review risks documentation.** After each element of your review, review risk treatment plans and timelines/milestones against your risk management policies and

	Checklist Item
	procedures.
☐	**Documentation and Inventory.** Verify your AWS network is fully documented and all AWS critical systems are included in their inventory documentation, with limited access to this documentation. • Review AWS Config for AWS resource inventory and configuration history of resources *(Example API Call, 1)*. • Ensure that resources are appropriately tagged and associated with application data. • Review application architecture to identify data flows, planned connectivity between application components and resources that contain data. • Review all connectivity between your network and the AWS Platform by reviewing the following: ▪ VPN connections where the customers on-premise Public IPs are mapped to customer gateways in any VPCs owned by the Customer. *(Example API Call, 2 & 3)*. Direct Connect Private Connections, which may be mapped to 1 or more VPCs owned by the customer. *(Example API Call, 4)*
☐	**Evaluate risks.** Evaluate the significance of the AWS-deployed data to the organization's overall risk profile and risk tolerance. Ensure that these AWS assets are integrated into the organization's formal risk assessment program. • AWS assets should be identified and have protection objectives associated with them, depending on their risk profiles.
☐	**Incorporate use of AWS into risk assessment.** Conduct and/or incorporate AWS service elements into your organizational risk assessment processes. Key risks could include: • Identify the business risk associated with your use of AWS and identify business owners and key stakeholders. • Verify that the business risks are aligned, rated, or classified within your use of AWS services and your organizational security criteria for protecting confidentiality,

	Checklist Item
	integrity, and availability. • Review previous audits related to AWS services (SOC, PCI, NIST 800-53 related audits, etc.). • Determine if the risks identified previously have been appropriately addressed. • Evaluate the overall risk factor for performing your AWS review. • Based on the risk assessment, identify changes to your audit scope. • Discuss the risks with IT management, and adjust the risk assessment.
☐	**IT Security Program and Policy.** Verify that the customer includes AWS services in its security policies and procedures, including AWS account level best practices as highlighted within the AWS service Trusted Advisor which provides best practice and guidance across 4 topics – Security, Cost, Performance and Fault Tolerance. • Review your information security policies and ensure that it includes AWS services. • Confirm you have has assigned an employee(s) as authority for the use and security of AWS services and there are defined roles for those noted key roles, including a Chief Information Security Officer. **Note:** any published cybersecurity risk management process standards you have used to model information security architecture and processes. • Ensure you maintain documentation to support the audits conducted for AWS services, including its review of AWS third-party certifications. • Verify internal training records include AWS security, such as Amazon IAM usage, Amazon EC2 Security Groups, and remote access to Amazon EC2 instances. • Confirm a cybersecurity response policy and training for AWS services is maintained. **Note**: any insurance specifically related to the customers use of AWS services and any claims related to losses and expenses attributed to cybersecurity events as a result.
☐	**Service Provider Oversight.** Verify the contract with AWS includes a requirement to implement and maintain privacy and security safeguards for cybersecurity requirements.

2. Network Configuration and Management

Definition: Network management in AWS is very similar to network management on-premises, except that network components such as firewalls and routers are virtual. Customers must ensure network architecture follows the security requirements of their organization, including the use of DMZs to separate public and private (untrusted and trusted) resources, the segregation of resources using subnets and routing tables, the secure configuration of DNS, whether additional transmission protection is needed in the form of a VPN, and whether to limit inbound and outbound traffic. Customers who must perform monitoring of their network can do so using host-based intrusion detection and monitoring systems.

Major audit focus: Missing or inappropriately configured security controls related to external access/network security that could result in a security exposure.

Audit approach: Understand the network architecture of the customer's AWS resources, and how the resources are configured to allow external access from the public Internet and the customer's private networks. Note: AWS Trusted Advisor can be leveraged to validate and verify AWS configurations settings.

Network Configuration and Management Checklist

	Checklist Item
☐	**Network Controls.** Identify how network segmentation is applied within the AWS environment. • Review AWS Security Group implementation, AWS Direct Connect and Amazon VPN configuration for proper implementation of network segmentation and ACL and firewall setting or AWS services *(Example API Call, 5 - 8)*. • Verify you have a procedure for granting remote, Internet or VPN access to employees for AWS Console access and remote access to Amazon EC2 networks and systems. • Review the following to maintain an environment for testing and development of software and applications that is separate from its business environment: ▪ VPC isolation is in place between business environment and environments used for test and development. ▪ By reviewing VPC peering connectivity between VPCs to ensure network

	Checklist Item
	isolation is in place between VPCs ▪ Subnet isolation is in place between business environment and environments used for test and development. ▪ By reviewing NACLs associated to Subnets in which Business and Test/Development environments are located to ensure network isolation is in place. ▪ Amazon EC2 instance isolation is in place between business environment and environments used for test and development. ▪ By reviewing Security Groups associated to 1 or more Instances which are associated with Business, Test or Development environments to ensure network isolation is in place between Amazon EC2 instances ▪ Review DDoS layered defense solution running which operates directly on AWS reviewing components which are leveraged as part of a DDoS solution such as: ▪ Amazon CloudFront configuration ▪ Amazon S3 configuration ▪ Amazon Route 53 ▪ ELB configuration ▪ Note: The above services do not use Customer owned Public IP addresses and offer DoS AWS inherited DoS mitigation features. ▪ Usage of Amazon EC2 for Proxy or WAF Further guidance can be found within the "AWS Best Practices for DDoS Resiliency Whitepaper"
☐	**Malicious Code Controls.** Assess the implementation and management of anti-malware for Amazon EC2 instances in a similar manner as with physical systems.

3. Asset Configuration and Management

Definition: AWS customers are responsible for maintaining the security of anything installed on AWS resources or connect to AWS resources. Secure management of the customer's AWS resources means knowing what resources you are using (asset inventory), securely configuring the guest OS and applications on your resources (secure configuration settings, patching, and anti-malware), and controlling changes to the resources (change management).

Major audit focus: Manage your operating system and application security vulnerabilities to protect the security, stability, and integrity of the asset.

Audit approach: Validate the OS and applications are designed, configured, patched and hardened in accordance with your policies, procedures, and standards. All OS and application management practices can be common between on-premise and AWS systems and services.

Asset Configuration and Management Checklist

	Checklist Item
☐	**Assess configuration management.** Verify the use of your configuration management practices for all AWS system components and validate that these standards meet baseline configurations. • Review the procedure for conducting a specialized wipe procedure prior to deleting the volume for compliance with established requirements. • Review your Identity Access Management system (which may be used to allow authenticated access to the applications hosted on top of AWS services). • Confirm penetration testing has been completed.
☐	**Change Management Controls.** Ensure use of AWS services follows the same change control processes as internal series. • Verify AWS services are included within an internal patch management process. Review documented process for configuration and patching of Amazon EC2 instances: ▪ Amazon Machine Images (AMIs) *(Example API Call, 9 - 10)* ▪ Operating systems ▪ Applications • Review API calls for in-scope services for delete calls to ensure IT assets have been properly disposed of.

4. Logical Access Control

Definition: Logical access controls determine not only who or what can have access to a specific system resource, but also the type of actions that can be performed on the resource (read, write, etc.). As part of controlling access to AWS resources, users and processes must present credentials to confirm that they are authorized to perform specific functions or have access to specific resources. The credentials required by AWS vary depending on the type of service and the access method, and include passwords, cryptographic keys, and certificates. Access to AWS resources can be enabled through the AWS account, individual AWS Identify and Access Management (IAM) user accounts created under the AWS account, or identity federation with the customer's corporate directory (single sign-on). AWS Identity and Access Management (IAM) enables users to securely control access to AWS services and resources. Using IAM you can create and manage AWS users and groups and use permissions to allow and deny permissions to AWS resources.

Major audit focus: This portion of the audit focuses on identifying how users and permissions are set up for the services in AWS. It is also important to ensure you are securely managing the credentials associated with all AWS accounts.

Audit approach: Validate permissions for AWS assets are being managed in accordance with organizational policies, procedures, and processes. Note: AWS Trusted Advisor can be leveraged to validate and verify IAM Users, Groups, and Role configurations.

Logical Access Control Checklist

	Checklist Item
☐	**Access Management, Authentication and Authorization.** Ensure there are internal policies and procedures for managing access to AWS services and Amazon EC2 instances. • Ensure documentation of use and configuration of AWS access controls, examples and options outlined below: ▪ Description of how Amazon IAM is used for access management. ▪ List of controls that Amazon IAM is used to manage – Resource management, Security Groups, VPN, object permissions, etc. ▪ Use of native AWS access controls, or if access is managed through

	Checklist Item
	federated authentication, which leverages the open standard Security Assertion Markup Language (SAML) 2.0. ▪ List of AWS Accounts, Roles, Groups and Users, Policies and policy attachments to users, groups, and roles *(Example API Call, 11)*. ▪ A description of Amazon IAM accounts and roles, and monitoring methods. ▪ A description and configuration of systems within EC2.
☐	**Remote Access.** Ensure there is an approval process, logging process, or controls to prevent unauthorized remote access. Note: All access to AWS and Amazon EC2 instances is "remote access" by definition unless Direct Connect has been configured. • Review process for preventing unauthorized access, which may include: ▪ AWS CloudTrail for logging of Service level API calls. ▪ AWS CloudWatch logs to meet logging objectives. ▪ IAM Policies, S3 Bucket Policies, Security Groups for controls to prevent unauthorized access. ▪ Review connectivity between firm network and AWS: ▪ VPN Connection between VPC and firm's network. ▪ Direct Connect (cross connect and private interfaces) between firm and AWS. ▪ Defined Security Groups, Network Access Control Lists and Routing tables in order to control access between AWS and the network.
☐	**Personnel Control.** Ensure restriction of users to those AWS services strictly for their business function *(Example API Call, 12)*. • Review the type of access control in place as it relates to AWS services. ▪ AWS access control at an AWS level – using IAM with Tagging to control management of Amazon EC2 instances (start/stop/terminate) within networks ▪ Customer Access Control – using IAM (LDAP solution) to manage access to resources which exist in networks at the Operating System / Application layers

	Checklist Item
	▪ Network Access control – using AWS Security Groups (SGs) , Network Access Control Lists (NACLs), Routing Tables, VPN Connections, VPC Peering to control network access to resources within customer owned VPCs.

5. Data Encryption

Definition: Data stored in AWS is secure by default; only AWS owners have access to the AWS resources they create. However, customers who have sensitive data may require additional protection by encrypting the data when it is stored on AWS. Only the Amazon S3 service currently provides an automated, server-side encryption function in addition to allowing customers to encrypt on the customer side before the data is stored. For other AWS data storage options, the customer must perform encryption of the data.

Major audit focus: Data at rest should be encrypted in the same way as on-premise data is protected. Also, many security policies consider the Internet an insecure communications medium and would require the encryption of data in transit. Improper protection of data could create a security exposure.

Audit approach: Understand where the data resides, and validate the methods used to protect the data at rest and in transit (also referred to as "data in flight"). Note: AWS Trusted Advisor can be leveraged to validate and verify permissions and access to data assets.

Data Encryption Checklist

	Checklist Item
☐	**Encryption Controls.** Ensure there are appropriate controls in place to protect confidential information in transport while using AWS services. ▪ Review methods for connection to AWS Console, management API, S3, RDS and Amazon EC2 VPN for enforcement of encryption. ▪ Review internal policies and procedures for key management including AWS services and Amazon EC2 instances. ▪ Review encryption methods used, if any, to protect PINs at rest – AWS offers a number of key management services such as KMS, CloudHSM and Server Side

	Checklist Item
	Encryption for S3 which could be used to assist with data at rest encryption *(Example API Call, 13-15)*.

6. Security Logging and Monitoring

Definition: Audit logs record a variety of events occurring within your information systems and networks. Audit logs are used to identify activity that may impact the security of those systems, whether in real-time or after the fact, so the proper configuration and protection of the logs is important.

Major audit focus: Systems must be logged and monitored, just as they are for on-premise systems. If AWS systems are not included in the overall company security plan, critical systems may be omitted from scope for monitoring efforts.

Audit approach: Validate that audit logging is being performed on the guest OS and critical applications installed on Amazon EC2 instances and that implementation is in alignment with your policies and procedures, especially as it relates to the storage, protection, and analysis of the logs.

Security Logging and Monitoring Checklist:

	Checklist Item
☐	**Logging Assessment Trails and Monitoring.** Review logging and monitoring policies and procedures for adequacy, retention, defined thresholds and secure maintenance, specifically for detecting unauthorized activity for AWS services. • Review logging and monitoring policies and procedures and ensure the inclusion of AWS services, including Amazon EC2 instances for security related events. • Verify that logging mechanisms are configured to send logs to a centralized server, and ensure that for Amazon EC2 instances the proper type and format of logs are retained in a similar manner as with physical systems. • For customers using AWS CloudWatch, review the process and record of the use of network monitoring. • Ensure analytics of events are utilized to improve defensive measures and policies. • Review AWS IAM Credential report for unauthorized users, AWS Config and resource tagging for unauthorized devices *(Example API Call, 16)*.

	Checklist Item
	• Confirm aggregation and correlation of event data from multiple sources using AWS services such as: ▪ VPC Flow logs to identify accepted/rejected network packets entering VPC. ▪ AWS CloudTrail to identify authenticated and unauthenticated API calls to AWS services ▪ ELB Logging – Load balancer logging. ▪ AWS CloudFront Logging – Logging of CDN distributions.
☐	**Intrusion Detection and Response.** Review host-based IDS on Amazon EC2 instances in a similar manner as with physical systems. • Review AWS provided evidence on where information on intrusion detection processes can be reviewed.

7. Security Incident Response

Definition: Under a Shared Responsibility Model, security events may by monitored by the interaction of both AWS and the AWS customer. AWS detects and responds to events impacting the hypervisor and the underlying infrastructure. Customers manage events from the guest operating system up through the application. You should understand incident response responsibilities and adapt existing security monitoring/alerting/audit tools and processes for their AWS resources.

Major audit focus: Security events should be monitored regardless of where the assets reside. The auditor can assess consistency of deploying incident management controls across all environments, and validate full coverage through testing.

Audit approach: Assess existence and operational effectiveness of the incident management controls for systems in the AWS environment.

Security Incident Response Checklist:

	Checklist Item
☐	**Incident Reporting.** Ensure the incident response plan and policy for cybersecurity incidents includes AWS services and addresses controls that mitigate cybersecurity

	incidents and aid recovery. • Ensure leveraging of existing incident monitoring tools, as well as AWS available tools to monitor the use of AWS services. • Verify that the Incident Response Plan undergoes a periodic review and changes related to AWS are made as needed. • Note if the Incident Response Plan has notification procedures and how the customer addresses responsibility for losses associated with attacks or impacting instructions.

8. Disaster Recovery

Definition: AWS provides a highly available infrastructure that allows customers to architect resilient applications and quickly respond to major incidents or disaster scenarios. However, customers must ensure that they configure systems that require high availability or quick recovery times to take advantage of the multiple Regions and Availability Zones that AWS offers.

Major audit focus: An unidentified single point of failure and/or inadequate planning to address disaster recovery scenarios could result in a significant impact. While AWS provides service level agreements (SLAs) at the individual instance/service level, these should not be confused with a customer's business continuity (BC) and disaster recovery (DR) objectives, such as Recovery Time Objective (RTO) Recovery Point Objective (RPO). The BC/DR parameters are associated with solution design. A more resilient design often utilizes multiple components in different AWS availability zones and involve data replication.

Audit approach: Understand the DR and determine the fault-tolerant architecture employed for critical assets. Note: AWS Trusted Advisor can be leveraged to validate and verify some aspects of the customer's resiliency capabilities.

Disaster Recovery Checklist:

	Checklist Item
☐	**Business Continuity Plan (BCP).** Ensure there is a comprehensive BCP, for AWS services utilized, that addresses mitigation of the effects of a cybersecurity incident and/or recover from such an incident. • Within the Plan, ensure that AWS is included in the emergency preparedness and crisis management elements, senior manager oversight responsibilities, and the testing plan.
☐	**Backup and Storage Controls.** Review the customer's periodic test of their backup system for AWS services *(Example API Call, 17-18)*. 1. Review inventory of data backed up to AWS services as off-site backup.

9. Inherited Controls

Definition: Amazon has many years of experience in designing, constructing, and operating large-scale datacenters. This experience has been applied to the AWS platform and infrastructure. AWS datacenters are housed in nondescript facilities. Physical access is strictly controlled both at the perimeter and at building ingress points by professional security staff utilizing video surveillance, intrusion detection systems, and other electronic means. Authorized staff must pass two-factor authentication a minimum of two times to access datacenter floors. All visitors and contractors are required to present identification and are signed in and continually escorted by authorized staff.

AWS only provides datacenter access and information to employees and contractors who have a legitimate business need for such privileges. When an employee no longer has a business need for these privileges, his or her access is immediately revoked, even if he or she continues to be an employee of Amazon or Amazon Web Services. All physical access to datacenters by AWS employees is logged and audited routinely.

Major audit focus: The purpose of this audit section is to demonstrate appropriate due diligence in selecting service providers.

Audit approach: Understand how you can request and evaluate third-party attestations and certifications in order to gain reasonable assurance of the design and operating effectiveness of control objectives and controls.

Inherited Controls Checklist

	Checklist Item
☐	**Physical Security & Environmental Controls.** Review the AWS provided evidence for details on where information on intrusion detection processes can be reviewed that are managed by AWS for physical security controls.

Conclusion

There are many third-party tools that can assist you with your assessment. Since AWS customers have full control of their operating systems, network settings, and traffic routing, a majority of tools used in-house can be used to assess and audit the assets in AWS.

A useful tool provided by AWS is the AWS Trusted Advisor tool. AWS Trusted Advisor draws upon best practices learned from AWS' aggregated operational history of serving hundreds of thousands of AWS customers. The AWS Trusted Advisor performs several fundamental checks of your AWS environment and makes recommendations when opportunities exist to save money, improve system performance, or close security gaps.

This tool may be leveraged to perform some of the audit checklist items to enhance and support your organizations auditing and assessment processes.

Appendix A: References and Further Reading

1. Amazon Web Services: Overview of Security Processes - https://d0.awsstatic.com/whitepapers/Security/AWS%20Security%20Whitepaper.pdf
2. Amazon Web Services Risk and Compliance Whitepaper – https://d0.awsstatic.com/whitepapers/compliance/AWS_Risk_and_Compliance_Whitepaper.pdf
3. AWS OCIE Cybersecurity Workbook - https://d0.awsstatic.com/whitepapers/compliance/AWS_SEC_Workbook.pdf
4. Using Amazon Web Services for Disaster Recovery - http://media.amazonwebservices.com/AWS_Disaster_Recovery.pdf
5. Identity federation sample application for an Active Directory use case - http://aws.amazon.com/code/1288653099190193
6. Single Sign-on with Windows ADFS to Amazon EC2 .NET Applications - http://aws.amazon.com/articles/3698?_encoding=UTF8&queryArg=searchQuery&x=20&y=25&fromSearch=1&searchPath=all&searchQuery=identity%20federation
7. Authenticating Users of AWS Mobile Applications with a Token Vending Machine http://aws.amazon.com/articles/4611615499399490?_encoding=UTF8&queryArg=searchQuery&fromSearch=1&searchQuery=Token%20Vending%20machine
8. Client-Side Data Encryption with the AWS SDK for Java and Amazon S3 - http://aws.amazon.com/articles/2850096021478074
9. AWS Command Line Interface – http://docs.aws.amazon.com/cli/latest/userguide/cli-chap-welcome.html
10. Amazon Web Services Acceptable Use Policy - http://aws.amazon.com/aup/

Appendix B: Glossary of Terms

Authentication: Authentication is the process of determining whether someone or something is, in fact, who or what it is declared to be.

Availability Zone: Amazon EC2 locations are composed of regions and Availability Zones. Availability Zones are distinct locations that are engineered to be insulated from failures in other Availability Zones and provide inexpensive, low latency network connectivity to other Availability Zones in the same region.

EC2: Amazon Elastic Compute Cloud (Amazon EC2) is a web service that provides resizable compute capacity in the cloud. It is designed to make web-scale cloud computing easier for developers.

Hypervisor: A hypervisor, also called Virtual Machine Monitor (VMM), is software/hardware platform virtualization software that allows multiple operating systems to run on a host computer concurrently.

IAM: AWS Identity and Access Management (IAM) enables a customer to create multiple Users and manage the permissions for each of these Users within their AWS Account.

Object: The fundamental entities stored in Amazon S3. Objects consist of object data and metadata. The data portion is opaque to Amazon S3. The metadata is a set of name-value pairs that describe the object. These include some default metadata such as the date last modified and standard HTTP metadata such as Content-Type. The developer can also specify custom metadata at the time the Object is stored.

Service: Software or computing ability provided across a network (e.g., EC2, S3, VPC, etc.).

Appendix C: API Calls

The AWS Command Line Interface is a unified tool to manage your AWS services. http://docs.aws.amazon.com/cli/latest/reference/index.html#cli-aws

1. List all resources with tags
    - aws ec2 describe-tags

http://docs.aws.amazon.com/cli/latest/reference/ec2/describe-tags.html

2. List all Customer Gateways on the customers AWS account:
    - aws ec2 describe-customer-gateways –output table
3. List all VPN connections on the customers AWS account
    - aws ec2 describe-vpn-connections
4. List all Customer Direct Connect connections
    - aws directconnect describe-connections
    - aws directconnect describe-interconnects
    - aws directconnect describe-connections-on-interconnect
    - aws directconnect describe-virtual-interfaces
5. List all Customer Gateways on the customers AWS account:
    - aws ec2 describe-customer-gateways –output table
6. List all VPN connections on the customers AWS account
    - aws ec2 describe-vpn-connections
7. List all Customer Direct Connect connections
    - aws directconnect describe-connections
    - aws directconnect describe-interconnects
    - aws directconnect describe-connections-on-interconnect
    - aws directconnect describe-virtual-interfaces
8. Alternatively use Security Group focused CLI:
    - aws ec2 describe-security-groups
9. List AMI currently owned/registered by the customer
    - aws ec2 describe-images –owners self
10. List all Instances launched with a specific AMI
    - aws ec2-describe-instances --filters “Name=image-id,Values=XXXXX” (where XXXX = image-id value e.g. ami-12345a12

11. List IAM Roles/Groups/Users
    - aws iam list-roles
    - aws iam list-groups
    - aws iam list-users
12. List Policies assigned to Groups/Roles/Users:
    - aws iam list-attached-role-policies --role-name XXXX
    - aws iam list-attached-group-policies --group-name XXXX
    - aws iam list-attached-user-policies --user-name XXXX

    where XXXX is a resource name within the Customers AWS Account
13. List KMS Keys
    - aws kms list-aliases
14. List Key Rotation Policy
    - aws kms get-key-rotation-status –key-id XXX (where XXX = key-id In AWS account
15. List EBS Volumes encrypted with KMS Keys
    - aws ec2 describe-volumes "Name=encrypted,Values=true"
    - targeted e.g. us-east-1)
16. Credential Report
    - aws iam generate-credential-report
    - aws iam get-credential-report
17. Create Snapshot/Backup of EBS volume
    - aws ec2 create-snapshot --volume-id XXXXXXX
    - (where XXXXXX = ID of volume within the AWS Account)
18. Confirm Snapshot/Backup completed
    - aws ec2 describe-snapshots --filters “Name=volume-id,Values=XXXXXX)