U.S. Securities and Exchange Commission's (SEC) Office of Compliance Inspections and Examinations (OCIE)

Cybersecurity Initiative Audit Guide

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

Executive Summary

This AWS U.S. Securities and Exchange Commission's (SEC) Office of Compliance Inspections and Examinations (OCIE) Cybersecurity Initiative audit guide has been designed by AWS to guide financial institutions, which are subject to SEC audits on the use and security architecture of AWS services. This document is intended for use by AWS financial institution customers, their examiners, and audit advisors to understand the scope of the AWS services, provide guidance for implementation, and discuss examination when using AWS services as part of the financial institutions environment for customer data.

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 similar to on-premise infrastructure services that have been traditionally used by customers for their operating services and applications. Policies and processes that apply to devices and servers should also apply when those functions are supplied by AWS services. Controls pertaining solely to policy or procedure generally are entirely the responsibility of the customer. Similarly, management of access to AWS services, 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

AWS services are regularly assessed against industry standards and requirements. In an attempt to support a variety of industries including federal agencies, retailers, international organizations, health care providers and financial institutions, AWS elects to have a variety of assessments performed

against the services and infrastructure. For a complete list and information on assessment performed by third parties please refer to AWS Compliance web site.

OCIE Cybersecurity Audit Checklist for AWS

The AWS compliance program ensures that AWS services are regularly audited against applicable standards. Some control statements may be satisfied by the customer's use of AWS (for instance Physical access to sensitive data). However, most controls have either shared responsibilities between AWS and the customer, or are entirely the customer's responsibility. This audit checklist describes the customer responsibilities specific to the OCIE Cybersecurity Initiative when utilizing AWS services.

1. Governance

Definition: Governance includes the elements required to provide senior management assurance that its 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 the customer has purchased, what kinds of systems and information the customer plans 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 by the customer and ensure that the customer's security or risk management program has taken into account their use of the public cloud environment.

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

Governance Checklist

	Checklist Item
☐	**Documentation and Inventory.** Verify that the customer's 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 with a customer's application and/or customer data.

	Checklist Item
	• Review application architecture to identify data flows, planned connectivity between application components and resources that contain customer data. • Review all connectivity between the customer's network and 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)*
☐	**Risk Assessment.** Ensure the customer's risk assessment for AWS services includes potential cybersecurity threats, vulnerabilities and business consequences. • Verify that AWS services were included in the customer's risk assessment and privacy impact assessment. • Verify that system characterization was documented for AWS services as part of the risk assessment to identify and rank information assets.
☐	**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 the customer's information security policies and ensure that it includes AWS services and reflects the Identify Theft Red Flag Rules (17 CFR § 248—Subpart C—Regulation S-ID). • Confirm that the customer has assigned an employee(s) as an 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 the customer has used to model their information security architecture and processes. • Ensure the customer maintains documentation to support the audits conducted for their AWS services, including its review of AWS third-party certifications. • Verify that the customer's internal training records includes AWS security, such as Amazon IAM usage, Amazon EC2 Security Groups, and remote access to Amazon EC2 instances. • Confirm that the customer maintains a cybersecurity response policy and training for AWS services. • 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.

	Checklist Item
☐	**Service Provider Oversight.** Verify that the customer's 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 that their 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 customers AWS environment. • Review AWS Security Group implementation, AWS Direct Connect and Amazon VPN configuration for proper implementation of network segmentation and ACL and firewall settings on AWS services. (Example API Call, 5 - 8) • Verify that the customer has a procedure for granting remote, internet or VPN access to employees for AWS Console access and remote access to Amazon EC2 networks and systems.

	Checklist Item
	• Review the following to ensure the customer maintains 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. • VPC peering connectivity is between VPCs. This ensures network isolation is in place between VPCs • Subnet isolation is in place between business environment and environments used for test and development. • NACLs are associated with Subnets in which Business and Test/Development environments are located to ensure network isolation is in place subnets • Amazon EC2 instance isolation is in place between the business environment and environments used for test and development • Security Groups associated to 1 or more Instances within the Business, Test or Development environments ensure network isolation between Amazon EC2 instances Review the customer's DDoS layered defense solution running that operates directly on AWS which are leveraged as part of a DDoS solution such as: • Amazon CloudFront configuration • Amazon S3 configuration • Amazon Route 53 • ELB configuration • 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 they install on or connect to their AWS resources. Secure management of the customers' AWS resources means knowing what resources the customer is using (asset inventory), securely configuring the guest OS and applications on the customers resources (secure configuration settings, patching, and anti-malware), and controlling changes to the customers resources (change management).

Major audit focus: Customers must manage their operating system and application security vulnerabilities to protect the security, stability, and integrity of the asset.

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

4. Logical Access Control

Definition: Logical access controls determine not only who or what can have access to a specific system resource but 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 IAM enables a customer's users to securely control access to AWS services and resources. Using IAM, a customer can create and manage AWS users and groups and use permissions to allow and deny their permissions to AWS resources.

Major audit focus: This portion of the audit focuses on identifying how users and permissions are set up in AWS for the services being used by the customer. It is also important to ensure that the credentials associated with all of the customer's AWS accounts are being managed securely by the customer.

Audit approach: Validate that 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 the customer documents, their 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 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.

	Checklist Item
☐	**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 the customer's 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 the customer's connectivity between the customer's network and AWS: • VPN Connection between VPC and Firms network. • Direct Connect (cross connect and private interfaces) between customer and AWS. • Defined Security Groups, Network Access Control Lists and Routing tables in order to control access between AWS and the customer's network.
☐	**Personnel Control.** Ensure that the customer restricts users to those AWS services strictly required for their business function. (Example API Call, 12) • Review the type of access control the customer has 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 the customer IAM (LDAP solution) to manage access to resources which exist in networks at the Operating System / Application layers • 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, some customers who have sensitive data may require additional protection by encrypting the data when it is stored on AWS. Only 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 the customer protects on-premise data. Also, many security policies consider the Internet an insecure communications medium and would require the encryption of data in transit. Improper protection of customers' data could create a security exposure for the customer.

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 customer 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 customer PINs at Rest – AWS offers a number of key management services such as KMS, AWS CloudHSM and Server Side 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 a customer's 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 the customers Amazon EC2 instances and that implementation is in alignment with the customer's 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 within AWS services. • Review the customer's logging and monitoring policies and procedures and ensure their 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 customer's process and record of their use of network monitoring. • Ensure the customer utilizes analytics of events to improve their defensive measures and policies. • Review AWS IAM Credential report for unauthorized users, AWS Config and resource tagging for unauthorized devices. (Example API Call, 16) • Confirm the customer aggregates and correlates event data from multiple sources. The customer may use AWS services such as: a) VPC Flow logs to identify accepted/rejected network packets entering VPC. b) AWS CloudTrail to identify authenticated and unauthenticated API calls to AWS services c) ELB Logging – Load balancer logging. d) 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 be monitored by the interaction of both AWS and AWS customers. 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. The customer 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 that the customer's incident response plan and policy for cybersecurity incidents includes AWS services and addresses controls that mitigate cybersecurity incidents and recovery. • Ensure the customer is leveraging 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 that changes related to AWS are made as needed. • Note if the Incident Response Plan has customer notification procedures and how the customer addresses responsibility for losses associated with attacks or instructions impacting customers.

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 to the customer. 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 would often utilize multiple components in different AWS availability zones and involve data replication.

Audit approach: Understand the DR strategy for the customer's environment and determine the fault-tolerant architecture employed for the customer's 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 recovery from such an incident. • Within the Plan, ensure that AWS is included in the customer's 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) • 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 they continue 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 that the customer conducted the appropriate due diligence in selecting service providers.

Audit approach: Understand how the customer 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.

Appendix A: References and Further Reading

1. Amazon Web Services: Introduction to AWS Security https://d0.awsstatic.com/whitepapers/Security/Intro_to_AWS_Security.pdf
2. Amazon Web Services Risk and Compliance Whitepaper – https://d0.awsstatic.com/whitepapers/compliance/AWS_Risk_and_Compliance_Whitepaper.pdf
3. Using Amazon Web Services for Disaster Recovery - http://d36cz9buwru1tt.cloudfront.net/AWS_Disaster_Recovery.pdf
4. Identity federation sample application for an Active Directory use case - http://aws.amazon.com/code/1288653099190193
5. 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
6. 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
7. Client-Side Data Encryption with the AWS SDK for Java and Amazon S3 - http://aws.amazon.com/articles/2850096021478074
8. AWS Command Line Interface – http://docs.aws.amazon.com/cli/latest/userguide/cli-chap-welcome.html
9. Amazon Web Services Acceptable Use Policy - http://aws.amazon.com/aup/

Appendix B: Glossary of Terms

API: Application Programming Interface (API), in the context of AWS, These customer access points are called API endpoints, and they allow secure HTTP access (HTTPS), which allows you to establish a secure communication session with your storage or compute instances within AWS. AWS provides SDKs and CLI reference which allows customers to programmatically manage AWS services via API.

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.

Read more: http://docs.aws.amazon.com/cli/latest/reference/index.html#cli-aws and http://docs.aws.amazon.com/cli/latest/userguide/cli-chap-welcome.html

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)