Federal Financial Institutions Examination Council (FFIEC)

Audit Guide

October 2015

Please note: This whitepaper is currently being updated.

Check back later for the most up-to-date information.

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 4

Approaches for using AWS Audit Guides 4

Examiners 4

AWS Provided Evidence 4

FFIEC Audit Checklist for AWS 5

1. Governance 5

2. Network Configuration and Management 7

3. Asset Configuration and Management 9

4. Logical Access Control 10

5. Data Encryption 13

6. Security Logging and Monitoring 13

7. Security Incident Response 15

8. Disaster Recovery 15

9. Inherited Controls 17

Executive Summary

This AWS Federal Financial Institutions Examination Council (FFIEC) audit guide has been designed by AWS to guide financial institutions that are subject to audits by members of the FFIEC 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 AWS services and to provide guidance for implementation and 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. This audit guide organizes the requirements into common security program controls and control areas. Each control references the applicable audit requirements. For more detail on each control reference, the applicable regulatory requirements, examiner activities, and AWS evidence of compliance please refer to the Coalfire FFIEC Compliance on AWS whitepaper.

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 on-premise devices and servers should also apply when supplied by AWS services. Controls pertaining solely to policy or procedure are generally entirely a responsibility of the customer. Similarly, the management of access to AWS services, either via the AWS Console or Command Line API, should be treated like other privileged administrator access.

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 assessments performed by third parties, please refer to the AWS Compliance web site.

FFIEC 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's responsibilities for compliance with the FFIEC IT Handbook 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
☐	**IT Security Program and Policy.** Access the security policy and program related to the use of AWS services. Ensure that the program is properly documented for oversight, changes in service, IT security policies, incident reporting, and security roles. • Verify that there is appropriate approval for the use of AWS and the services are appropriately addressed within the information security program. • Confirm that an employee is assigned as authority for the use and security of AWS services and there are defined roles for those noted key roles. • Verify that any customer changes in AWS services are reflected in the security program. • Review the customer's IT security policies and ensure that they cover AWS services and take size and complexity into consideration. • Review management oversight and ensure that they assess and approve the use and configuration of AWS services. • Ensure the customer has integrated AWS services into their SIEM tools, and has a process for monitoring and addressing non-compliance. • Review the customer's use of any AWS reporting tools such as: ▪ Amazon CloudWatch ▪ AWS Trusted Advisor • Verify that there is a policy in place for the appropriate disclosure of client information within AWS.
▪	**Information Security Oversight.** Verify that the customer has conducted oversight and annual IT assessments, including any remediation(s) related to AWS services. • Include a review of management and Board of Directors (BOD) oversight.
☐	**Risk Assessment.** Assess and review the customer's risk assessment for AWS services, including: adherence to the customer's risks assessment policy and procedures, AWS-deployed data inclusion into the customer's risks assessment and BOD oversight. ▪ Verify that AWS services were included in risk assessment and privacy impact assessment.
☐	**Personnel Controls.** Verify that there are proper segregation of duties, background checks and training conducted for IT operations staff. ▪ Verify that the level of access for AWS services is comparable to the level of secure information and comprehensive screening, including signed statements of understanding for non-disclosure.

	Checklist Item
☐	**Systems Development Lifecycle.** Verify that the use of AWS development tools are documented and follow the customers SDLC process, including security requirements and configuration changes.
☐	**Service Provider Oversight.** Ensure that the customer documents and follows a defined process to evaluate, on-board and maintain security safeguards, including AWS. • Ensure that internal procedures include onboarding, shared security responsibility and communication process with AWS. • Verify that the customer's contract with AWS includes a requirement to implement and maintain privacy and security safeguards. • Verify adherence to appropriate due diligence standards, security program management and monitoring of service capabilities and reliability.
☐	**Documentation and Inventory.** Verify that the customer's AWS network is fully documented and all AWS critical systems are included in inventory documentation, with limited access to this documentation. ▪ Review AWS Config reports for AWS resource inventory, configuration history and configuration change notifications. (Example API Call 1)

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, additional transmission protection in the form of a VPN, and limits on 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 customer's AWS environment. (Example API Call 2-5) • Review the customer's overall infrastructure, including use of AWS services, to ensure there is no single point of failure. • Review AWS Security Group implementation, AWS Direct Connect and Amazon VPN configuration for proper implementation of network segmentation and ACL and firewall setting for AWS services. • Ensure that the customer's procedures for governing the daily activities of personnel include the administration of the AWS services. • Confirm the customer has established appropriate logging and monitoring for Amazon EC2 instances to ensure that any possible security related events are identified. • 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.
☐	**Malicious Code Controls.** Assess the customer's implementation and management of anti-malware for Amazon EC2 instances in a similar manner as with physical systems.
☐	**Firewall Controls.** Review the customer's defined process of firewall rules management within AWS and include Security Group configuration changes, VPN configuration and management approval along with maintenance of documentation of approvals. • Verify that the host-based or other firewall configuration is properly hardened. • Verify if AWS Security Groups are the primary firewall solution. If other firewall technologies are used, the examiner should review the technology to ensure that it is properly configured to hide internal addresses, block malicious code and has logging enabled. • Ensure AWS Security Group administration is performed from secure workstations and via HTTPS for either the AWS Console or command line API. Additionally,

	Checklist Item
	ensure that multi-factor authentication is enabled for any user that is assigned general administrative rights or rights to manage security groups within the AWS Console or through command line APIs. • Verify internal policies for restricting AWS Security Group management to select IT staff. • Verify that the customer's training records include AWS security, such as Amazon IAM usage, EC2 Security Groups, and remote access to EC2 instances.

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 customer's 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 that the customer's 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
☐	**Change Management Controls.** Ensure the customer's use of AWS services follows the same change control processes as internal services, including testing, back out procedures, training and logs related to changes. • Verify that AWS services are included within the customer's internal patch management process.

	Checklist Item
	• Ensure that patch management strategies include establishing version control of all operation systems, Amazon Machine Images and application software used within the AWS service environment. • Ensure that policies and procedures related to client information within AWS is secured in accordance with the customer's IT Security Policies.
☐	**Operating System Access.** Ensure the customer's internal policies and procedures call for restricting and monitoring privileged access to AWS services and Amazon EC2 instances to designated administrator. • Review the Amazon EC2 instances in use within the customer's organization. • If AWS monitoring tools are used, such as AWS CloudWatch, review its use for logical security.
☐	**Application Access Controls.** Review controls for applications implemented on Amazon EC2 instances to ensure they are appropriate for the risk of the application and the needs of the customer users. • Ensure that authentication and authorization methods, application access controls and assessment event logging for applications implemented on Amazon EC2 instances is conducted in a similar manner as with physical systems.
☐	**Database Security Controls.** Review access and data modification activity for Amazon RDS or customer databases in a similar manner as with internal systems. • Determine if production data is utilized in test environment using AWS database services and if so, ensure that the security policies and controls are configured to match production controls.

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 Identity and Access Management (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 access 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 customer's internal 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. • Federated Access Controls: Ensure that the mechanisms properly apply internal role assignment to AWS permission and understand the processes and methods to authorize access levels to ensure a least privilege model has been implemented. • Native AWS Access Controls: Compare Amazon IAM roles and user assignment to functional roles and responsibilities. Temporary credentials should also be considered to ensure that these credentials are only assigned limited privileges. (Example API Call 6-7) • Instant Access Controls: For Amazon EC2 instances, review implemented roles and assignments based on the local operating systems access controls mechanisms and/or any federation that the customer has established for managing access to the EC2 virtual machines. • Review the records for granting access, the type of access control in use within the customer's organization as it related to AWS services, and user account policy and password complexities and validate that they extend to AWS services.

	Checklist Item
	• Ensure that multi-factor identification is enabled for users and no shared accounts exist as it relates to AWS services.
☐	**Remote Access.** Ensure internal policies and procedures are followed for managing remote access to AWS services and Amazon EC2 instances. Note: All access to AWS and Amazon EC2 instances is "remote access" by definition unless Direct Connect has been configured. • Review access logging and Amazon IAM configuration. Amazon IAM accounts for network access should be configured for multi-factor authentication. (Example API Call 8) • Ensure that Security groups are configured to allow for direct access to common management ports for Amazon instances. (Example API Call 9) • Ensure that multi-factor authentication mechanisms and encryption configuration have been implemented on the system in a similar manner as with physical systems.
☐	**Personnel Control & Segregation of Duties.** Ensure that the IT staff are aware of the information security program, applicable to AWS services, and how it relates to their job functions. • Review the customer's type of access control in use within their organization as it relates to AWS services: ▪ Federated Access Controls: Review internal role assignments to AWS permissions and understand the processes and methods to authorize. ▪ Native AWS Access Controls: Compare Amazon IAM roles and user assignment to functional roles and responsibilities. (Example API Call 10) ▪ Instance Access Controls: Review implemented roles and assignments based on the local operating systems access controls mechanisms and/or any federation that the customer has established for managing access to the EC2 virtual machines. (Example API Call 11) • Verify internal policies and procedures for managing access to AWS services and Amazon EC2 instances. Individuals monitoring security administrator logs should function independently from individuals responsible for operations administrators. • Verify that information security awareness training includes AWS security, such as Amazon IAM usage, EC2 Security Groups and remote access to EC2 instances.

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, which they can enable 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 transit, 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. (Example API Call 12-14)

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 the customers logging and monitoring policies and procedures and ensure their inclusion of AWS services, and that they address segregation of duties, security and access authority. • Verify that there is a process to monitor service configuration changes. (Example API Call 15) • 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 Amazon CloudWatch, review the customer's process and record their use of network monitoring. Specifically, review VPC FlowLog events. (Example API Call 16)
☐	**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. • Review the customer's use and configuration of Amazon CloudWatch and how logs are stored and protected.

7. Security Incident Response

Definition: Under a Shared Responsibility Model, security events may by 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 the 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 includes appropriate AWS reporting processes, as well as communication procedures between the customer and AWS. • Ensure the customer is leveraging existing incident monitoring tools, as well as AWS available tools to monitor the use of AWS services. (Example API Call 17-18) • Verify that the customer's use of AWS services aligns with and can support their internally defined thresholds. • Verify that the Incident Response Plan undergoes an annual review and changes related to AWS are made as needed. • Note if the Incident Response Plan has a customer notification procedure.

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 Planning (BCP).** Ensure the customer has a comprehensive BCP that includes AWS services. • Within the Plan, ensure that AWS is included in the emergency preparedness and crisis management elements, senior manager oversight responsibilities, and the testing plan. • Ensure the customer has a recovery plan that includes the proper use of AWS availability zones. • Review the annual BCP test for AWS services.
☐	**Backup and Storage Controls.** Review the use of AWS services for off-site backup and ensure it is consistent with the customer's policy and procedures, as well as follows AWS best practices. • Review inventory of data backed up to AWS services as off-site backup. • Ensure policies and procedures address scalability as it relates to AWS services. • Conduct a test of backup data stored in AWS services. (Example API Call 19-21)

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 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.

Conclusion

There are many third-party tools that can assist you with your assessment. As 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 Risk and Compliance Whitepaper – https://d0.awsstatic.com/whitepapers/compliance/AWS_Risk_and_Compliance_Whitepaper.pdf
2. AWS OCIE Cybersecurity Workbook - https://d0.awsstatic.com/whitepapers/compliance/AWS_SEC_Workbook.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. Review VPNs
    - aws ec2 describe-customer-gateways
    - aws ec2 describe-vpn-connections
3. Review Direct Connect
    - aws directconnect describe-connections
    - aws directconnect describe-interconnects
    - aws directconnect describe-connections-on-interconnect
    - aws directconnect describe-virtual-interfaces
4. Review VPCs, Subnets and Routing Tables
    - aws ec2 describe-vpcs
    - aws ec2 describe-subnets
    - aws ec2 describe-route-tables
5. Review Security Groups and Network ACLs
    - aws ec2 describe-network-acls
    - aws ec2 describe-security-groups
6. List IAM Roles/Groups/Users
    - aws iam list-roles
    - aws iam list-groups
    - aws iam list-users
7. List all IAM Policies
    - aws iam list-policies
8. API to list IAM Users with MFA
    - aws iam list-mfa-devices
9. API to list Security Groups:

- aws ec2 describe-security-groups

10. 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
11. Review Amazon EC2 instances launched as roles:
    a. Identify Amazon EC2 Role ARN:
        - aws iam list-roles
    b. Filter Amazon EC2 instances by ARN:
        - aws ec2 describe-instances --filters "Name=iam-instance-profile.arn,Values=arn:aws:iam::accountid:instance-profile/rolename"
12. List KMS Keys
    - aws kms list-aliases
13. List Key Rotation Policy
    - aws kms get-key-rotation-status –key-id XXX (where XXX = key-id In AWS account
14. List EBS Volumes encrypted with KMS Keys
    - aws ec2 describe-volumes
15. Confirm AWS-Config Service is enabled within a region
    - aws configservice get-status –region XX-XXXX-X (where XX-XXXX-X = AWS region targeted e.g. us-east-1)
16. Examine FlowLog current status
    - aws ec2 describe-flow-logs

    a. View VPC Flow Log events in Cloudwatch taking output of log-group-name from above API call
        - aws logs describe-log-streams --log-group-name my-logs
        - aws logs get-log-events --log-group-name my-logs --log-stream-name 20150601
17. Review all Cloudwatch Alarms
    - aws-cloudwatch describe-alarms
18. Review alarms associated with a specific resource and metric
    - aws cloudwatch describe-alarms-for-metric --metric-name CPUUtilization --namespace AWS/EC2 --dimensions Name=InstanceId,Value=XXXXX
    - (Where XXXX = ec2 instance id)
19. Create Snapshot/Backup of EBS volume

- aws ec2 create-snapshot --volume-id XXXXXXX
- (where XXXXXX = ID of volume within the AWS Account)

20. Confirm Snapshot/Backup completed
    - aws ec2 describe-snapshots --filters “Name=volume-id,Values=XXXXXX)
21. Create volume from Snapshot (Restoring Backup)
    - aws ec2 create-volume --availability-zone XXXX --snapshot-id YYYY
    - (where XXX is the availability zone you want the new volume created)
    - (where YYY is the snapshot-id you want to restore from)