Auditing Security Checklist for Use of AWS

June 2013

(Please consult http://aws.amazon.com/compliance for the latest version of this paper)

Table of Contents

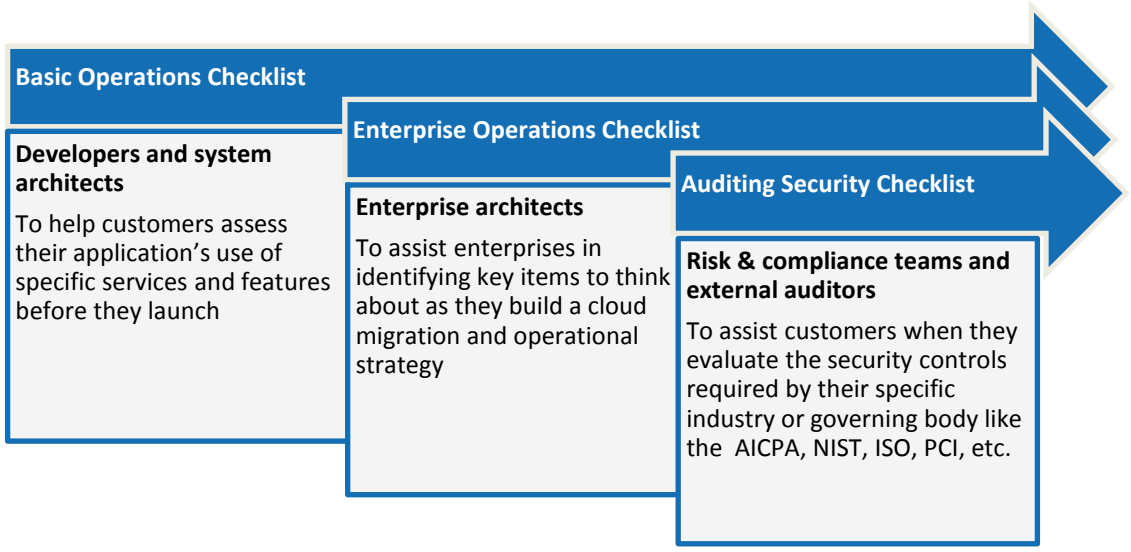
Abstract

Deploying an application on Amazon Web Services (AWS) is fast, easy, and cost-effective. In conjunction with deploying a cloud application in production, it is useful to have a checklist to assist in evaluating your use of AWS for the purposes of an internal review or external audit. This paper is targeted at AWS customers' internal compliance teams and their external auditors and who are evaluating or auditing the use of AWS for an internal review or external audit. It provides a checklist to help design and execute a security assessment of an organization's use of AWS, which may be required by industry or regulatory standards. This paper builds on top of Operational Checklist that provides operational and architectural guidance to help assess their application's operational readiness.

Introduction

Amazon Web Services is a flexible, cost-effective, and easy-to-use cloud computing platform. AWS provides a suite of infrastructure services that you can use to deploy your applications. This paper is targeted at customers' internal security, risk and compliance teams and their external auditors who may have a need to assess the use of AWS. However, it could also be useful to any organization for comparing its planned use of AWS against these auditing security best practices.

In addition, AWS provides Operational Checklists (including a Basic Operations Checklist and an Enterprise Operations Checklist) for developers, architects, and others who are looking for operational and architectural guidance from AWS to help assess their application's operational readiness.



How to Use the Checklists

Auditing Security Checklist - This checklist is intended to help AWS customers and their auditors assess the use of AWS, which may be required by industry or regulatory standards. Examples of such assessments are the need to:

- Evaluate the capability of AWS services to meet information security objectives and ensure future deployments within the AWS cloud is done in a secure and compliant way
- Assess the existing organizational use of AWS and to validate security leading practices
- Develop AWS usage policies and/or validate that existing policies are being followed

AWS complies with a wide variety of security standards relevant to these assessments. However, this paper does not advocate a specific standard or framework. Instead, this paper is written generically to allow any customer or auditor to use it to evaluate the security controls required by their industry or governing body, such as the American Institute of Certified Public Accountants (AICPA), International Organization for Standardization (ISO), National Institute of Standards and Technology (NIST), Payment Card Industry Security Standards Council (PCI SSC), Information Systems Audit and Control Association (ISACA), etc.

This paper provides a checklist to support assessments based on the following domains:

- Governance
- Asset Configuration and Management
- Logical Access Control
- Data Encryption
- Network Configuration and Management
- Security Logging and Monitoring
- Security Incident Response
- Disaster Recovery

This paper only includes security domains and topics that an auditor might perform *differently* than in an on-premises or hosted environment. Some of the audit tasks normally performed on IT systems or organizations, such as confirming that administrators use SSH to remotely access certain resources, are the same for cloud and on-premises environments and are not covered in this paper. Moreover, there are several security controls that customer systems inherit from AWS. For these controls, customers do not provide documentation and testing around those controls because they relate to AWS infrastructure. These controls include the physical and environmental protection measures for the AWS data centers housing the servers and equipment, as well as the maintenance of those servers and equipment. For organizations that require documentation and testing around those controls for their compliance efforts, the applicable AWS compliance report can be requested at https://aws.amazon.com/compliance/contact/.

Checklist	Intended Usage	Target Customer
Basic Operations Checklist	To help customers assess their application's use of specific services and features before they launch	Developers and system architects
Enterprise Operations Checklist	To assist enterprises identify key items to think about as they build a cloud migration and operational strategy	Enterprise architects
Auditing Security Checklist	To assist customers when they evaluate the security controls required by their specific industry or governing body like the AICPA, NIST, ISO, PCI SSC, etc.	Auditors or risk and compliance professional

Auditing Use of AWS Concepts

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

I. **Understand the AWS "Shared Responsibility" model** - To effectively evaluate assets residing in AWS, customers should understand which categories of assets they control versus which categories of assets AWS controls.

- AWS provides a secure global infrastructure and services for which AWS operates, manages, and controls the components from the host operating system and virtualization layer down to the physical security of the facilities in which the services operate. These parts of the system can be validated by the customer through the AWS certifications and reports (e.g., Service Organization Control (SOC) reports, ISO 27001 certification, PCI assessments, etc.). The applicable AWS compliance certifications and reports can be requested at https://aws.amazon.com/compliance/contact/.
- Customers are responsible for the security of anything their organization puts on their AWS assets or connect to their AWS assets, such as the guest operating system and applications on their virtual machine instance, the data and objects in their S3 buckets or RDS database, etc.

Understanding this separation of responsibility and control is needed to effectively direct an organization's validation efforts. See Figure 1 below.

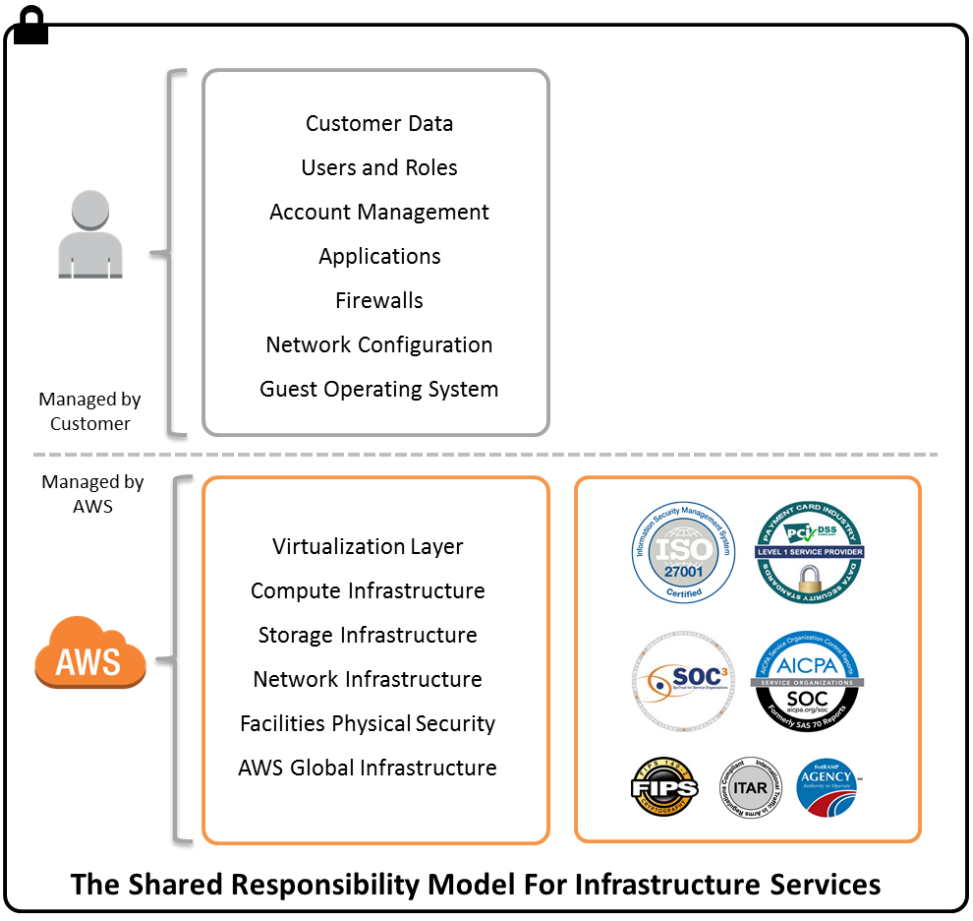


Figure 1: The Shared Responsibility Model

Additional detail can be found at the AWS Security Center, AWS Compliance, and in the publically available AWS whitepapers found at http://aws.amazon.com/whitepapers/.

II. **Define the organization's AWS assets** - A customer's AWS assets can be instances, data stores, applications, the data itself, etc. Auditing the use of AWS usually 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 complicated to inventory because AWS provides visibility into the assets under management.

III. **Manage security holistically** - The AWS infrastructure should be an integral part of an organization's information security management program. Security control objectives should remain consistent regardless of where the systems and data reside, however, controls and audit plans can be modified according to the guidelines in this paper.

The list of considerations is high-level and designed to provide limited technical details. Depending on your skill-set and familiarity with AWS, you may need to reference other AWS resources in order to fully assess the security elements. For example, to understand how Multi-Factor Authentication (MFA) for Application Programming Interface (API) calls can be enforced at the console, you may want to refer to the IAM section of the AWS website http://aws.amazon.com/iam/. For a more technical discussion of each of these security mechanisms and the service-specific considerations, please refer to the resources at http://aws.amazon.com/whitepapers/.

Auditing Security Checklist

For each checklist category in the table below, additional details are provided through internal references to subsequent sections of this document.

	Checklist Category	Description
☐	Pre-Audit Procedures	Is your organization prepared for an audit?
☐	Governance	Does your organization understand the AWS services and resources being used? Has your organization's risk management program taken into account use of AWS?
☐	Asset Configuration and Management	Does your organization manage operating system and application security vulnerabilities to protect the security, stability, and integrity of the asset?
☐	Logical Access Control	Does your organization understand how users and permissions are set-up in AWS? Does your organization securely manage the credentials associated with your AWS accounts?
☐	Data Encryption	Does your organization understand where your organization's data resides and how is it protected?
☐	Network Configuration and Management	Does your organization understand the network architecture of your AWS resources?
☐	Security Logging and Monitoring	Are your organization's systems residing on AWS logged and monitored?
☐	Security Incident Response	Does your organization's incident management plan and processes include systems in the AWS environment?
☐	Disaster Recovery	Does your organization's disaster recovery strategy include systems in the AWS environment?

Pre-Audit Procedures

Prior to conducting an audit, it is important to confirm the audit plan and scope, and identify known risks.

Pre-Audit Procedures 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 posing this question when polling or interviewing your IT and development teams.
☐	**Define your AWS audit objectives.** • Your audit objectives should be high-level and describe the overall audit goals. • Review your AWS audit objectives within your organization and align them with your audit program and schedule. • Modify your audit objectives to align with the organization's audit program, annual plan, and charter.
☐	**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.
☐	**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 procedures.
☐	**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, 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.

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 organization. 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 your organization has 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 by your organization and ensure that the organization's security or risk management program has taken into account your use of the public cloud environment.

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

Governance Checklist

	Checklist Item
☐	**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 used when registering. • A formal meeting can be conducted with each AWS account or asset owner to 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 understands the organization's use of the AWS resources may be someone in the IT department. You may need to interview both.
☐	**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.
☐	**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.
☐	**Modify audit plan.** Modify the audit plan to include the scope of the AWS systems, if not done previously. As needed, add AWS assets to applicable annual security assessment procedures and annual external audit initiatives. • Ensure that IT management and security policies are updated to accommodate deployment of IT resources into the AWS environment (this can be performed at the end of the audit).

2. Asset Configuration and Management

Definition: AWS customers are responsible for maintaining the security of anything they install on their AWS resources or connect to their AWS resources. Secure management of your AWS resources means knowing what resources your organization is using (asset inventory), securely configuring the guest OS and applications on your resources (secure configuration settings, patching, and anti-malware), and controlling changes to your 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 your guest OS and applications are designed, configured, patched and hardened in accordance to your organizational 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
☐	**Obtain asset inventory listing.** Verify AWS account and resource owner(s) understand the AWS resources their organization is using by creating and reconciling an asset inventory listing. • Verify the services installed on the resources in the asset inventory listing.
☐	**Assess patching.** Ensure all operating instances are included and classified in the asset identification exercise performed under the Governance review. Documenting the total population of all AWS accounts is critical to effectively identifying all operating assets in the AWS environment. • Validate that the processes in place to manage patches for software and system components (identification, testing, and deployment) include the assets in the AWS environment. The process should include identification of vulnerabilities, validation of system patch level, implementation of patching, etc.
☐	**Assess configuration management.** Verify the use of your organizational configuration management practices for all AWS system components and validate that these standards are appropriate to address known security vulnerabilities. • AWS provides the ability to start new instances based on a common (public) or an organizational-specific Amazon Machine Image (AMI). Evaluate the machine images used, and determine if an image has been approved for use that has been reviewed by your internal compliance and/or security teams. Establishing an approved machine image will help ensure new images are compliant with your policies and processes. • For each instance, follow your required security, audit and validation procedures. These procedures may include checking vendor supplied defaults are changed prior to deployment, default passwords are changed, unnecessary accounts are deleted, etc. • If mandated by your organizational policy, determine if only one primary function is assigned per server. • Determine if remote administrative access is performed securely (e.g. via SSH); this includes with the use of strong cryptography, if applicable. • Determine if all unnecessary functions and accounts are removed. • Validate there are no unnecessary scripts, drivers, features, subsystems, EBS volumes, or webservers running.
☐	**Assess privileged access.** Access to the operating systems and applications should be restricted. Validate access to the operating systems and applications to determine appropriateness of the access and whether it is managed in accordance with organizational policies and procedures. • Validate access logging is appropriately aligned with your organization's defined access standards commensurate with the level of access privilege. In general, logging for guest operating systems and applications can be done in the same way as with on-premise systems.

3. 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 your corporate directory (single sign-on). AWS Identity and Access Management (IAM) enables an organization's users to securely control access to AWS services and resources. Using IAM an organization 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 your organization. It is also important to ensure that the credentials associated with all of your AWS accounts are being managed securely by your organization.

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. See the AWS Trusted Advisor section of this whitepaper for additional information.

Internal Access Control Checklist

	Checklist Item
☐	**Assess AWS account management.** Document the ownership and management of the AWS account (known as the root account) for each information system or organization that you are auditing. • Evaluate whether the assignment of responsibility is appropriate. • Evaluate whether it is practical to have two AWS user accounts for individuals with full- or high-level of access to AWS services. • Consider the use of one AWS account for administrative level tasks and another AWS user account for user access activity. This can help limit the exposure of sensitive accounts to threats as well as the exposure to accidental deletion or compromise of information.
☐	**Assess Multi-Factor Authentication (MFA).** Determine whether multi-factor authentication of AWS accounts is required by your policies. Learn More… • If required, check the AWS Management Console to determine whether MFA is enforced on the AWS account and individual IAM user accounts. Learn More…
☐	**Review Identify and Access Management (IAM) user account(s).** Working with the AWS Account owners, log into the AWS Management Console to see what IAM user accounts exist. • Document the permissions and evaluate for appropriateness. Evaluate the use of temporary credentials in accordance with your organization's policies. This may be done by inquiry or by a review of the IAM user accounts active on the AWS account. Learn More…
☐	**Review group permissions.** Log into the AWS Management Console to review the use of AWS Groups within AWS IAM. These are collections of AWS users from the same AWS account and are used to facilitate user administration functions. • Review the access to AWS resources for each AWS Group and compare to the assignment of AWS IAM policies. • All permissions and policies assigned to an AWS Group cumulatively apply to the AWS IAM user accounts who are members of the group. Learn More…

	Checklist Item
☐	**Review organization system user accounts.** Determine whether your organization's authentication system is integrated with AWS to grant access to AWS resources. This can be validated by assigning an auditor user account with AWS permissions, and testing login or data access privileges. Tailor your testing to include all AWS assets identified as appropriate. • Identify AWS systems not subject to the organizational authentication system permissions; consider whether these can be brought in under the regular permission management system as appropriate.
☐	**Assess access credentials for application and system processes.** Determine which application or system processes access AWS services via APIs and AWS software development kits. If application or system processes require access to AWS resources, ensure access is provisioned securely and according to policy and document your understanding. The three types of access credentials are: • Signing symmetric encryption keys (for access via REST/Query APIs and third-party tools) • X.509 certificates and associated private keys (for access via SOAP APIs and command lines) • Multi-factor authentication (optional)
☐	**Assess IAM roles.** IAM roles allow AWS account administrators to delegate access to users or services that normally don't have access to your organization's AWS resources. IAM users or AWS services can assume a role to obtain temporary security credentials that can be used to make AWS API calls. If IAM roles are used with your organization's AWS account, review the roles to ensure a new AWS role is created for every type of access and specific privileges that operating system services and applications that require to AWS resources. Learn More… • Evaluate each IAM role and determine how access is provided to AWS resources Identity and Access Management policies RBAC (Role Based Access Control). • Analyze the applicability of the organizational policy related to this type of access and document any deviations. • Verify if MFA for API access is utilized. Note: Because the AWS Management Console calls AWS service APIs, you can enforce MFA on APIs regardless of access path.
☐	**Conduct access control testing.** Perform testing as appropriate based on the types of access utilized. Testing may include: • Access key rotation schedule (done frequently) • X.509 certificates PKI integration or use of AWS certificates • Secure certificate and key management (ensuring that private keys are securely stored and not uploaded to AWS) • Alternate authentication mechanism implementations, such as including Lightweight Directory Access Protocol (LDAP) or Active Directory (AD) authentication and disabling AWS EC2 key pair authentication, can also be considered
☐	**Document permission management over AWS resources.** Verify that the organization's information security management system includes permission management and control over AWS resources. AWS user accounts managed outside the organization's information security management system should be identified. Learn More…

4. 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 client side before the data is stored. For other AWS data storage options, encryption of the data must be performed by the customer.

Major audit focus: Data at rest should be encrypted in the same way as the organization 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 organizations' data could create a security exposure for the organization.

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. See the AWS Trusted Advisor section of this whitepaper for additional information.

Data Encryption Checklist

	Checklist Item
☐	**Identify data assets and requirements.** Ensure all enterprise data is included is classified in the asset identification exercise performed under the Governance review. Documenting the total population of all AWS accounts is critical to effectively identify all data assets within the AWS environment. • Determine data storage requirements for all applicable data elements.
☐	**Review encryption of data at rest.** Evaluate cryptographic algorithms and mechanisms used by your organization to encrypt AWS data at rest. • For Amazon S3, this includes determining whether client-side or server-side encryption is used. Learn More… • For all other AWS data storage services, this will involve identifying the client-side encryption mechanisms used.
☐	**Review encryption of data in transit.** • If encryption of data in transit is required, identify whether connections to all applicable AWS services are via secure endpoints for HTTPS transmission. Also determine the use of Windows X.509 certificates, SSH, SSL/TLS wrappers for native database protocols, and/or VPN solutions. • Understand and verify documentation around the protection of data in transit when managing AWS services. Note: Customers manage their AWS services, such as Amazon EC2 and Amazon S3 using either the AWS Web Console or AWS APIs. Because the security of these communication mechanisms are well documented, this documentation activity would help the risk assessment function and the due diligence needed to understand the protections in place for data in transit (e.g., when S3 data objects are uploaded via the AWS Console).

5. 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 your AWS resources, and how the resources are configured to allow external access from the public Internet and your organization's private networks. Note: AWS Trusted Advisor can be leveraged to validate and verify AWS configurations settings. See the AWS Trusted Advisor section of this whitepaper for additional information.

Network Configuration and Management Checklist

	Checklist Item
☐	**Review traffic to EC2 Instances.** AWS EC2 security groups act as a host-based firewall for instances. Verify that EC2 security groups are configured correctly by your organization to restrict inbound traffic to instances by port, protocol, or source IP address (individual IP or Classless Inter-Domain Routing (CIDR) block).
☐	**Review traffic to VPC Networks.** Identify how network segmentation is applied within your AWS environment. • Security zones. Determine whether your AWS resources should be divided into trusted and untrusted security zones using private and public subnetworks (DMZs) within AWS VPC. This may include evaluating the control and monitoring of: - Inter-zone communication - The use of per-zone access control rights - The management of zones using dedicated management channel/roles - The application of per-zone confidentiality and integrity rules • Network segmentation. If an AWS VPC is used to create private subnetworks, identify them and determine how they are used. For example, if they isolate organizational entities or specific workloads. • Determine if network access control lists (NACLs) are required to restrict access to services between subnets. Review the VPC NACLs and compare to your organization's NACL policy. • Evaluate the use of protection layers in traffic flow to enforce all traffic to traverse security zones. • Evaluate the consistency with which all network controls are implemented. One of the advantages of elastic cloud infrastructure and automated deployment is the ability to apply the same security controls across all AWS regions. Repeatable and uniform deployments can help improve overall security posture.
☐	**Review additional network controls.** Some organizations may also deploy a network-level security control appliance using an in-line approach, where traffic intercepted and analyzed prior to being forwarded to its final destination. • Confirm that external vulnerability assessments are performed regularly and per your policy or if a major system change has been implemented (e.g., scanning). • Confirm that your organization is conducting regular penetration testing. • Obtain and review a copy of the latest vulnerability assessment and review remediation efforts, tracking of issues and timeframe for closing out vulnerabilities. • Validate if the vulnerability and pen testing processes are in alignment with your organization's policies and procedures. • Confirm your organizational penetration testing conducted on AWS follows the AWS Acceptable Use Policy and the proper scheduling procedures. Please see https://aws.amazon.com/security/penetration-testing/ for more information on the AWS penetration testing process.

6. Security Logging and Monitoring

Definition: Audit logs record a variety of events occurring within an organization'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 your EC2 instances and that implementation is in alignment with your organizational policies and procedures, especially as it relates to the storage, protection, and analysis of the logs.

Security Logging and Monitoring Checklist:

	Checklist Item

☐	**Review logging requirements.** Understand what needs to be logged within your environment per your organization's policies, procedures and compliance requirements.
	• Take into consideration logging of all user activities, exceptions, and security events, possibly including:
	  - Actions taken by any individual with root or administrative privileges
	  - Accesses to all audit trails
	  - Invalid logical access attempts
	  - Uses of identification and authentication mechanisms
	  - Initializations of audit log processes
	  - Creation and deletion of system level objects
	• Review the inventory of the AWS assets you own to determine which policies and procedures apply to the AWS assets from a logging perspective. Focus your audit efforts on understanding the level of logging within the AWS systems. For critical applications, logs for all "change" "add" "modify" "delete" transactions may require a log entry. Each log entry could have the following:
	  - User identification
	  - Type of events
	  - Date and time stamps
	  - Success or failure indications
	  - Origination of events
	  - Identity or name of affected data, system components, or resources
	• Based on your organizational policies, validate you have logging enabled for all of your AWS system components and environments.
	• Review the extent of logging is commensurate with the needs of your organization.

☐	**Review user access logging.** For all impacted systems and users, validate access logging is in place and your logs include all relevant user activities, exceptions, and security events. Note many of the AWS services provide built in access control audit trail capabilities. • Validate access logs are retained for a time period which is in alignment with organization's policies to assist in future investigations.
☐	**Review change management logging.** Understand the scope of your change logging and validate it is appropriate based on your companies policies and procedures. Change management logs likely are not to be restricted to only infrastructure changes, add, and delete requests; they should also include changes in code repository, gold image/application inventory changes, processes /policies and documentations changes.

	Checklist Item
	• Review the procedures in place for protections of your AWS log repository. Validate they meet and/or align with your internal organizational policy requirements. • Validate the different roles assignments for modifying and deleting changes. • Validate alerting is in place to identify when users attempt to change log data. File-integrity monitoring or change-detection software on logs can assist with this objective. • Understand procedures in place for reviewing logs for all system components and validate the reviews are occurring on a timely basis. Log reviews must include those servers which perform security functions like intrusion-detection system (IDS) and authentication, authorization, and accounting protocols (AAA) servers (for example, RADIUS).
☐	**Review log protection.** Logging facilities and log information should be protected against tampering and unauthorized access. Administrator and operator logs are a sensitive target for unauthorized deletes. Checks for protecting AWS system log information may include: • Verify audit trails are enabled and active for system components. • Verify only individuals who have a job-related need can view audit trail files. • Verify current audit trail files are protected from unauthorized modifications via access control mechanisms, physical segregation, and/or network segregation. • Verify current audit trail files are backed up to a centralized log server or media that is difficult to alter. • Verify logs for external-facing technologies (for example, wireless, firewalls, DNS, mail) are offloaded or copied onto a secure centralized internal log server or media. • Verify the use of file-integrity monitoring or change-detection software for logs by examining system settings and monitored files and results from monitoring activities. • Examine security policies and procedures to verify they include procedures to review security logs at least daily and that follow-ups to exceptions are required. • Verify regular log reviews are performed for all system components. • Examine security policies and procedures and verify they include audit log retention policies and require audit log retention for the required duration.
☐	**Review monitoring mechanisms and/or procedures.** Validate that your organization's Security Information and Event Management (SIEM) mechanisms and/or procedures are extended to your AWS environments. • Further validate that alarming coming from your AWS environments is being identified and addressed in a timely manner and the response is in alignment with organizational policies and procedures.

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 organization 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
☐	**Assess current incident management process.** Assess the current state of your organization's information security event handling process. • Review if your incident management process has been extended to include your use of AWS services
☐	**Review incident management plan.** Review incident management plan along with appropriates roles and responsibilities internally for your organization.
☐	**Assess incident management plan communication.** Evaluate how incident management plans are disseminate throughout your organization.

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 your organization. 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 your environment and determine the fault-tolerant architecture employed for your organization's critical assets. Note: AWS Trusted Advisor can be leveraged to validate and verify some aspects of your resiliency capabilities. See the AWS Trusted Advisor section of this whitepaper for additional information.

Disaster Recovery Checklist:

	Checklist Item
☐	**Understand Current State.** Obtain and review your organization's DR plans that are specific to your AWS resources. • Identify the current AWS Regions and corresponding Availability Zones (AZs) utilized by your Organization assets. • Determine if a multi-AZ strategy deployment strategy was utilized for your organization's assets. An AZ is a distinct location that is designed to be insulated from failures in other AZ's. AWS recommends that customers launch instances in more than one AZ to prevent loss of service in the event of a failure that affects an entire AZ. • Identify each Region that your assets currently reside within. Determine if your organization's policies specify the Regions that your organization may not use due to legal or regulatory requirements. • Through review of your organization's AWS architecture documentation, DR plans, and discussions with key DR personnel, identify the proposed DR approach at time of disaster.

	Checklist Item
☐	**Review incident management plan.** Review incident management plan along with appropriates roles and responsibilities internally for your organization.
☐	**Assess incident management plan communication.** Evaluate how incident management plans are disseminate throughout your organization.
☐	**Evaluate Use of AWS Capabilities.** Identify if your organization's DR plan includes one or more of the following: • Utilize AWS for storage/backup and recovery – AWS EBS and S3 service can be utilized for storage/backup purposes and at time of disaster your data is recovered from the appropriate source. • Pilot light solution – Your organization's key systems are configured and running in AWS, and at time of disaster, you scale up the remainder of your environment. • Hot Standby solution – All your critical systems and relevant support systems are running in AWS in the smallest fleet • Multi-site solution – Your critical systems are deployed to AWS as well as on your own infrastructure running an active-active configuration • Automated deployment – all your critical infrastructure and supporting systems run on multi-AZ AWS solution. • Depending on your use case for DR purposes, you can consider the following: - For data backup processes, confirm the data that is being backed-up using AWS services and validate that your organization's data retention policies are applied in your organization's use of each service. - Identify and review the latest DR test that validated that your data can be successfully restored. • Additional areas of consideration include: - Validate the completeness of your Amazon Machine Image (AMI) library. Validate the AMI is complete and up to date with all relevant software updates, configuration changes and patches. - Identify if automated provisioning of AWS resources is utilized. If not, identify the process in place to regularly update and maintain these AMI's and ensure it is in alignment with your organization's patch management and configuration management policies. - Understand how your instances, data stores, and databases replicate. - Validate your organization's required changes to the Domain Name System (DNS) at time of disaster and validate this process is documented in the DR plan. - Review Single Point of Failure (SPOF) analysis with your IT and business team. - Ensure your IT and business teams have developed a specific process to identify the organization's critical assets on AWS as part of the DR plan.
☐	**Review DR Testing.** Understand the cadence and types of DR testing executed across your AWS infrastructure. • Identify if detailed component failure analysis reviews have been executed and review the results to determine if they consider the single or multi-AZ deployment approach to be taken by your organization.

AWS Trusted Advisor

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. Trusted Advisor currently checks for the following security recommendations:

- Verify that external access to common administrative ports is limited to only a small subset of addresses
- Verify external access to common database ports
- Verify that IAM is configured to ensure limited internal access to AWS resources
- Verify that MFA is enabled to provide two-factor authentication for the root AWS account

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 - http://media.amazonwebservices.com/pdf/AWS_Security_Whitepaper.pdf
2. Amazon Web Services Risk and Compliance Whitepaper – http://media.amazonwebservices.com/AWS_Risk_and_Compliance_Whitepaper.pdf
3. Using Amazon Web Services for Disaster Recovery - http://media.amazonwebservices.com/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. Amazon's Corporate IT Deploys SharePoint 2010 to the Amazon Web Services Cloud - http://media.amazonwebservices.com/AWS_Amazon_SharePoint_Deployment.pdf
9. 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.

EBS: Amazon Elastic Block Store (EBS) provides block level storage volumes for use with Amazon EC2 instances. Amazon EBS volumes are off-instance storage that persists independently from the life of an instance.

FISMA: Federal Information Security Management Act of 2002. In accordance with FISMA, the National Institute of Standards and Technology (NIST) is responsible for developing standards, guidelines, and associated methods and techniques for providing adequate information security for all agency operations and assets, excluding national security systems.

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.

ISAE 3402: The International Standards for Assurance Engagements No. 3402 (ISAE 3402) is the international standard on assurance engagements. It was put forth by the International Auditing and Assurance Standards Board (IAASB), a standard-setting board within the International Federation of Accountants (IFAC). ISAE 3402 is now the new globally recognized standard for assurance reporting on service organizations.

ISO 27001: ISO/IEC 27001 is an Information Security Management System (ISMS) standard published by the International Organization for Standardization (ISO) and the International Electrotechnical Commission (IEC). ISO 27001 formally specifies a management system that is intended to bring information security under explicit management control. Being a formal specification means that it mandates specific requirements. Organizations that claim to have adopted ISO/IEC 27001 can therefore be audited and certified compliant with the standard.

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.

PCI: Refers to the Payment Card Industry Security Standards Council, an independent council originally formed by American Express, Discover Financial Services, JCB, MasterCard Worldwide and Visa International, with the goal of managing the ongoing evolution of the Payment Card Industry Data Security Standard.

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

Service Level Agreement (SLA): A service level agreement is a part of a service contract where the level of service is formally defined. The SLA is used to refer to the contracted delivery time (of the service) or performance.

SOC 1: Service Organization Controls 1 (SOC 1) Type II report, formerly the Statement on Auditing Standards (SAS) No. 70, Service Organizations report (commonly referred to as the SSAE 16 report), is a widely recognized auditing standard developed by the American Institute of Certified Public Accountants (AICPA). The international standard is referenced as the International Standards for Assurance Engagements No. 3402 (ISAE 3402).

SSAE 16: The Statement on Standards for Attestation Engagements No. 16 (SSAE 16) is an attestation standard published by the Auditing Standards Board (ASB) of the American Institute of Certified Public Accountants (AICPA). The standard addresses engagements undertaken by a service auditor for reporting on controls at organizations that provide services to user entities, for which a service organization's controls are likely to be relevant to a user entities internal control over financial reporting (ICFR). SSAE 16 effectively replaces Statement on Auditing Standards No. 70 (SAS 70) for service auditor's reporting periods ending on or after June 15, 2011.

Virtual Instance: Once an AMI has been launched, the resulting running system is referred to as an instance. All instances based on the same AMI start out identical and any information on them is lost when the instances are terminated or fail.

Version History

June 2013 version - Initial release