AISPL User Guide for Government Departments & Agencies in India

June 2018

Notices

This document is provided for informational purposes only. It is not legal or compliance advice, and should not be relied on as such. It represents AISPL'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 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 AISPL, its affiliates, suppliers or licensors. The responsibilities and liabilities of AISPL or its affiliates to its customers are controlled by agreements, and this document is not part of, nor does it modify, any agreement between AISPL or its affiliates and its customers.

Contents

Abstract

This document provides information to assist Indian Government departments and agencies operating at central, state, district and municipality levels understand the security and controls available, and assess how to implement an appropriate information security, risk management, and governance program in the AWS Cloud as they accelerate their use of AWS Services sold and offered by Amazon Internet Services Private Limited (AISPL).

Introduction

The Ministry of Electronics and Information Technology (MeitY) has launched the Government of India Cloud (GI Cloud) initiative, also known as MeghRaj[1], to provide strategic direction for the adoption of cloud services by the Government of India. The aim of the initiative is to realize a comprehensive vision to utilize and harness the benefits of the cloud and make it available for use by central and state government line departments, districts and municipalities to accelerate delivery of their Information and Communication Technology (ICT) enabled service projects.

Through this initiative, Amazon Internet Services Private Limited (AISPL)'s cloud service offerings have been empaneled by MeitY since December 2017.

In order to facilitate large scale adoption of GI Cloud within government, MeitY has issued a whitepaper, "Guidelines for Government Departments for Adoption/ Procurement of Cloud Services" or commonly known as "Guidelines for Procurement of Cloud Services", that provides guidelines for end user departments to procure and adopt cloud services. This whitepaper provides introductory information for Indian government departments for understanding AWS cloud services in relation to the MeitY Guidelines for Procurement of Cloud Services. The whitepaper references MeghRaj's policy which states "Government departments at the Centre and States to first evaluate the option of using the GI Cloud for implementation of all new projects funded by the government. Existing applications, services and projects may be evaluated to assess whether they should migrate to the GI Cloud."

In addition to the MeitY whitepaper, Government departments and agencies in India may also use the information in this document to conduct their due diligence and assess how to implement an appropriate information security risk management and governance program on their use of AWS services.

MeitY Guidelines for Procurement of Cloud Services

The Guidelines for Procurement of Cloud Services provides resources to Government departments on the procurement or adoption cloud services. Government departments should carry out due diligence to evaluate the capabilities of the service provider, determine the engagement models for procuring cloud services, identify security and operational risks associated with these models, enter into written agreements addressing those risks, and monitor and control their cloud services on an ongoing basis. The Guidelines for Procurement of Cloud Services state that the guidelines are provided general guidance and Departments should customize and formulate their specification of cloud resources and services according to the project specific requirements and their procurement strategy.

A full analysis of the Guidelines for Procurement of Cloud Services is beyond the scope of this document. However, the following sections address the considerations in the Guidelines that most frequently arise in interactions with Government departments in India.

The Shared Responsibility Model

Section 4.2 of the Guidelines for Procurement of Cloud Services acknowledges that the "CSP and the Departments share control over the Cloud environment and therefore both parties have responsibility for managing it. The CSP's part in this shared responsibility includes providing its services on a highly secure and controlled platform and providing a wide array of security features customers can use. The

[1] http://meity.gov.in/content/gi-cloud-meghraj

department's responsibility includes configuring their IT environments in a secure and controlled manner for their purposes."

Security and Compliance is a shared responsibility between AISPL and the customer. The Shared Responsibility Model shown in Figure 1 is fundamental to understanding the respective roles of the customer[2] and AISPL in the context of the cloud security principles. This shared model can help relieve customer's operational burden as AISPL or its affiliates 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 service operates. Customers should carefully consider the services they choose as their responsibilities vary depending on the services used, the integration of those services into their IT environment, and applicable laws and regulations. The nature of this shared responsibility also provides the flexibility and customer control that permits the deployment. As shown in the chart below, this differentiation of responsibility is commonly referred to as Security "of" the cloud versus Security "in" the cloud.

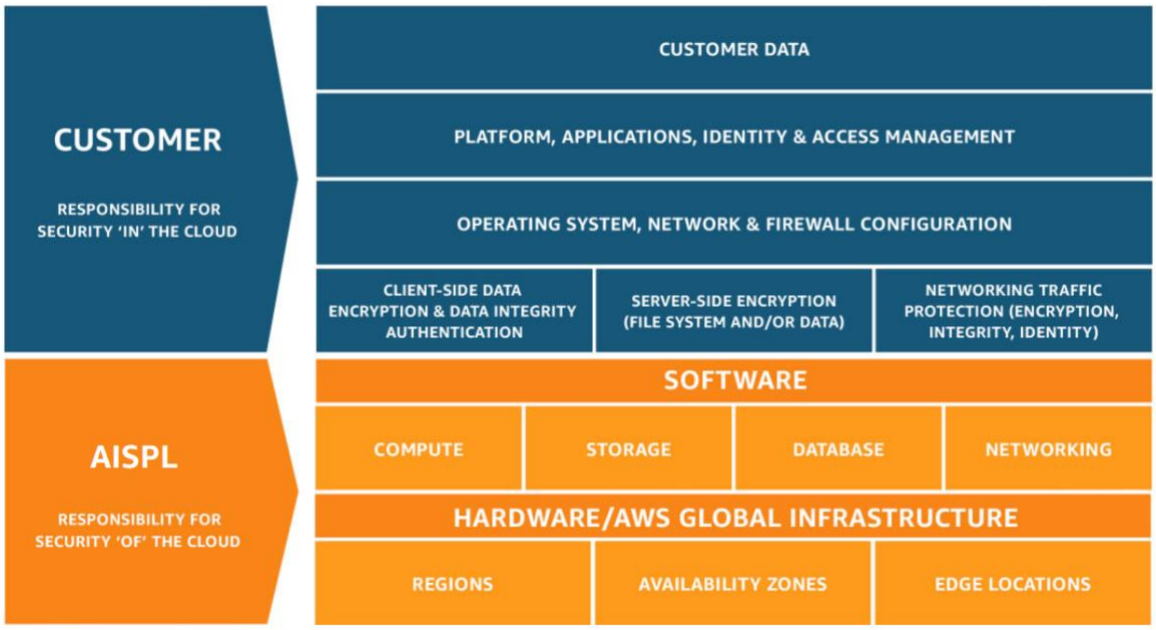

Figure 1: AISPL Shared Security Responsibility Model

AISPL responsibility "Security of the cloud" – AISPL is responsible for protecting the infrastructure that runs all of the services offered in the AWS loud. This infrastructure composes the hardware, software, networking, and facilities that run AWS cloud services.

Customer responsibility "Security in the cloud" – The AWS cloud services that a customer selects determine the scope of customer responsibility. This affects the amount of configuration work a customer must perform as part of their security responsibilities. For example, services such as Amazon Elastic Compute Cloud (Amazon EC2), Amazon Virtual Private Cloud (Amazon VPC), and Amazon S3 are categorized as Infrastructure as a Service (IaaS) and, as such, require the customer to perform all of the necessary security configuration and management tasks. If a customer deploys an Amazon EC2 instance, they are responsible for management of the guest operating system (including updates and security patches), any application software or utilities installed by the customer on the instances, and the configuration of the AWS-cloud provided firewall (called a security group) on each instance.

[2] Customer, in the context of this paper, refers to government departments that are using or planning to use AWS cloud services.

It is important to note that when using AWS services, customers maintain control over their content and are thus responsible for managing critical content security requirements, including:

- The content that they choose to store on AWS cloud
- The AWS services that are used with the content
- The country where the content is stored
- The format and structure of that content and whether it is masked, anonymized, or encrypted
- How the data is encrypted and where the keys are stored
- Who has access to that content and how those access rights are granted, managed and revoked

It is possible to enhance security and/or meet more stringent compliance requirements by leveraging technologies such as host-based firewalls, host-based intrusion detection and prevention, and encryption. AISPL provides tools and information to assist customers in their efforts to account for and validate that controls are operating effectively in their extended IT environment. For more information, see the AWS Cloud Compliance[i] webpage.

For more information about the Shared Responsibility Model and its implications for the storage and processing of personal data using AWS cloud, see the whitepaper on Using AWS cloud in the context of Common Privacy & Data Protection Considerations[ii].

Regions & Availability Zones

The AWS Cloud infrastructure is built around Regions and Availability Zones (AZs). An AWS Region is a physical location in the world where AWS has multiple AZs. Each AZ consists of one or more discrete data centers, each with redundant power, networking and connectivity, housed in separate facilities. These Availability Zones offer customers the ability to operate production applications and databases which are more highly available, fault tolerant and scalable than would be possible from a single data center.

AWS customers choose the AWS Region or Regions in which their content and servers will be located. This allows customers with geographic specific requirements to establish environments in a location or locations of their choice. For example, AWS customers in India can choose to deploy their AWS services exclusively in the Asia Pacific (Mumbai) Region and store their content on shore in India, if this is their preferred location. If the customer makes this choice, their content will be located in India unless the customer chooses to move that content.

Customers always retain control of which Region(s) are used to store and process content. AWS only stores and processes each customers' content in the Region(s), and using the services, chosen by the customer, and otherwise will not move customer content except as legally required. As with other AWS Regions, the AWS Asia Pacific (Mumbai) Region is designed and built to meet rigorous compliance standards globally, providing high levels of security for all AWS customers, and is compliant with applicable national and global data protection laws.

For current information on Regions and Availability Zones, see the AWS Global Infrastructure[iii] webpage.

Security of the Cloud

Cloud security is our highest priority. All our customers benefit from a data center and network architecture built to satisfy the needs of the most security sensitive organizations. Amazon Web Services Cloud Compliance enables customers to understand the robust controls in place to maintain security and data protection in the cloud. Each certification means that an auditor has verified that

specific security controls are in place and operating as intended. The compliance program is based on the following actions:

- **Validate** that AWS services across the globe maintain a ubiquitous control environment that is operating effectively. The AWS control environment includes policies, processes and control activities that leverage various aspects of the AWS overall control environment.

  The collective control environment encompasses the people, processes, and technology necessary to establish and maintain an environment that supports the operating effectiveness of the control framework. AWS has integrated applicable cloud-specific controls identified by leading cloud computing industry bodies into the AWS control framework. AWS monitors these industry groups to identify leading practices that can implement, and to better assist customers with managing their control environment.

- **Demonstrate** the AWS compliance posture to help customers verify compliance with industry and government requirements. AWS engages with external certifying bodies and independent auditors to provide customers with considerable information regarding the policies, processes, and controls established and operated by AWS. Customers can leverage this information to perform their control evaluation and verification procedures, as required under the applicable compliance standard.

- **Monitor** that, through the use of thousands of security control requirements, AWS cloud maintains compliance with global standards and best practices.

Security and Compliance Assurance

Section 4.2 states that Departments need to ensure that the CSPs facilities/services are certified for compliance to certain standards, which have been verified by MeitY, through the Standardization Testing and Quality Certification (STQC) authority, including internationally-recognized standards such as ISO/IEC 27001, ISO/IEC 27017, and ISO/IEC 27018.

Amazon Internet Services Private Limited (AISPL), the Amazon entity that sells AWS services in India, has achieved full Cloud Service Provider (CSP) empanelment, and successfully completed the MeitY STQC audit for AWS cloud services delivered from the Asia Pacific (Mumbai) Region.

To help you meet specific government, industry, and company security standards and regulations, we provide certification reports that describe how the AWS Cloud infrastructure meets the requirements of an extensive list of global security standards that include the following which are of relevance to Government departments in India:

ISO 27001 – ISO 27001 is a security management standard that specifies security management best practices and comprehensive security controls following the ISO 27002 best practice guidance. The basis of this certification is the development and implementation of a rigorous security program, which includes the development and implementation of an Information Security Management System which defines how AWS perpetually manages security in a holistic, comprehensive manner. For more information, or to download the AWS ISO 27001 certification, see the ISO 27001 Compliance[iv] webpage.

ISO 27017 – ISO 27017 provides guidance on the information security aspects of cloud computing, recommending the implementation of cloud-specific information security controls that supplement the guidance of the ISO 27002 and ISO 27001 standards. This code of practice provides additional information security controls implementation guidance specific to cloud service providers. For more information, or to download the AWS ISO 27017 certification, see the ISO 27017 Compliance[v] webpage.

ISO 27018 – ISO 27018 is a code of practice that focuses on protection of personal data in the cloud. It is based on ISO information security standard 27002 and provides implementation guidance on ISO 27002 controls applicable to public cloud Personally Identifiable Information (PII). It also provides a set of additional controls and associated guidance intended to address public cloud PII protection requirements not addressed by the existing ISO 27002 control set. For more information, or to download the AWS ISO 27018 certification, see the ISO 27018 Compliance[vi] webpage.

ISO 9001 - ISO 9001 outlines a process-oriented approach to documenting and reviewing the structure, responsibilities, and procedures required to achieve effective quality management within an organization. The key to the ongoing certification under this standard is establishing, maintaining and improving the organizational structure, responsibilities, procedures, processes, and resources in a manner where AWS products and services consistently satisfy ISO 9001 quality requirements. For more information, or to download the AWS ISO 9001 certification, see the ISO 9001 Compliance[vii] webpage.

PCI DSS Level 1 - The Payment Card Industry Data Security Standard (also known as PCI DSS) is a proprietary information security standard administered by the PCI Security Standards Council. PCI DSS applies to all entities that store, process or transmit cardholder data (CHD) and/or sensitive authentication data (SAD) including merchants, processors, acquirers, issuers, and service providers. The PCI DSS is mandated by the card brands and administered by the Payment Card Industry Security Standards Council. For more information, or to request the PCI DSS Attestation of Compliance and Responsibility Summary, see the PCI DSS Compliance[viii] webpage.

SOC – AWS System & Organization Control (SOC) Reports are independent third-party examination reports that demonstrate how AWS achieves key compliance controls and objectives. The purpose of these reports is to help customers and their auditors understand the AWS controls established to support operations and compliance. For more information, see the SOC Compliance[ix] webpage. There are three types of AWS SOC Reports:

- **SOC 1**: Provides information about AWS control environment that might be relevant to a customer's internal controls over financial reporting, and information for assessment and opinion of the effectiveness of internal controls over financial reporting (ICOFR).
- **SOC 2**: Provides customers and their service users with a business need with an independent assessment of AWS control environment relevant to system security, availability, and confidentiality.
- **SOC 3**: Provides customers and their service users with a business need with an independent assessment of AWS control environment relevant to system security, availability, and confidentiality without disclosing AWS internal information.

Customers can use AWS Artifact[x], an online compliance reporting portal, to review and download reports and details about more than 2,500 security controls. AWS Artifact is accessible from the AWS Management Console and provides on-demand access to security and compliance documents such as those listed above.

By tying together governance-focused, audit-friendly service features with such certifications, attestations and audit standards, AWS Compliance enablers build on traditional programs; helping customers to establish and operate in an AWS security control environment.

For more information about AWS certifications and attestations, see the AWS Assurance Programs[xi] webpage. For information about general AWS security controls and service-specific security, see the Amazon Web Services: Overview of Security Processes[xii] whitepaper.

Operation and Maintenance

Section 4.4 (b) of the Guidelines for Procurement of Cloud Services highlights that departments have the responsibility for applying secure user administration procedures in the cloud. The following table includes considerations for key components of Section 4.4 (b).

Requirement	Customer Considerations
i. Implement Identity and Access Management (IAM) that properly separates users by their identified roles and responsibilities, thereby establishing least privilege and ensuring that users have only the permissions necessary to perform their assigned tasks. *(Only relevant if IAM is getting implemented)*	Access Rights: AISPL provides a number of ways for customers to identify users and securely access their AWS Account. A complete list of credentials supported by AWS cloud can be found on the "My Security Credentials" page under "My Account". AWS cloud also provides additional security options that enable customers to further protect and control access to their AWS Accounts, including AWS Identity and Access Management (AWS IAM), key management and rotation, temporary security credentials, and multi-factor authentication (MFA).
ii. Administration of users, identities and authorizations, properly managing the root account, as well as any Identity and Access Management (IAM) users, groups and roles they associated with the user account.	AWS IAM allows customers the ability to create identities to provide authentication for people and processes in your AWS account. Identities represent the user and can be authenticated and then authorized to perform actions in AWS cloud. AWS IAM also allows creation of groups, which are collections of IAM users that customers can manage as a unit. Each of these can be associated with one or more policies to determine what actions a user, role, or member of a group can do with which AWS resources and under what conditions.
iii. Implement multi-factor authentication (MFA) for the root account, as well as any privileged Identity and Access Management accounts associated with it.	AWS Multi-factor authentication (MFA) provides an extra level of security for sign-in credentials. With MFA enabled, when users sign in to the website, they will be prompted for their user name and password (the first factor, i.e., what they know), as well as for an authentication code from their MFA device (the second factor, i.e., what they have). AISPL recommends customers activate MFA for their AWS account and their IAM users to prevent unauthorized access to their AWS environment. Currently AWS supports Gemalto hardware MFA devices as well as virtual MFA devices in the form of smartphone applications (i.e., Soft-Token/Authentication App).

Security Administration

Section 4.4 (c) of the Guidelines for Procurement of Cloud Services provides that Department and cloud service provider share the responsibility of operating the IT environment, including management, operation, and verification of IT controls. Departments are responsible for administering security and monitoring security incidents of their deployment in the cloud. The following table includes considerations for key components of Section 4.4 (c).

Requirement	Customer Considerations
i. Appropriately configure the security groups in accordance with the Government Department and Agency's networking policies.	Amazon Virtual Private Cloud (VPC) lets customers provision a logically isolated section of the AWS cloud where they can launch AWS resources in a virtual network that they define. A VPC may be private (not connected to the Internet), or public (connected to the Internet). Amazon VPC supports a virtual firewall solution, known as a Security Group, enabling filtering on both ingress and egress traffic from an instance. If

	customers don't specify a particular Security Group at launch time, the instance is automatically assigned to the default Security Group for the VPC. The default Security Group enables inbound communication from other members of the same group and outbound communication to any destination. Traffic can be restricted by any IP protocol, by service port, as well as source/destination IP address (individual IP or Classless Inter-Domain Routing (CIDR) block).
ii. Regularly review the security group configuration and instance assignment in order to maintain a secure baseline.	Customers can manually review security group configuration and instance assignment from the AWS Console. Alternatively, customers can receive notifications of a variety of important events related to security groups, such as when the security group was changed, using a variety of AWS services for auditing, logging and tracking configuration changes.
iii. Secure and appropriately segregate or isolate data traffic and application by functionality using DMZs, subnets etc.	Customers have complete control over their virtual networking environment. Customers can define subnets within their VPC, group similar kinds of instances based on IP address range, and then set up routing and security to control the flow of traffic in and out of the instances and subnets. To add a further layer of security within Amazon VPC, customers can configure network ACLs. These are stateless traffic filters that apply to all traffic inbound or outbound from a subnet within Amazon VPC. These ACLs can contain ordered rules to allow or deny traffic based upon IP protocol, by service port, as well as source/destination IP address.
iv. Ensure that the cloud infrastructure and all systems hosted on it, respectively, are properly monitored for unauthorized activity.	Customers manage access to their customer content and AWS services and resources. AWS cloud provides an advanced set of access, encryption, and logging features to help customers do this effectively (such as AWS CloudTrail). For details, please refer to the considerations in the section titled “Governance and Auditability”.
v. Properly implementing anti-malware and host-based intrusion detection systems on their instances, as well as any required network-based intrusion detection systems in accordance with the Government Department and Agency’s policies.	Customer can protect their systems in the cloud as they would protect a conventional infrastructure from threats such as viruses, worms, Trojans, rootkits, botnets, and spam. Customers assume responsibility and management of the guest operating system (including updates and security patches), other associated application software, as well as security, change management, and logging features such as anti-malware and host-based intrusion detection systems on their instances. Customers looking for defense in-depth can deploy a network- level security control appliance inline, where traffic is intercepted and analyzed prior to being forwarded to its final destination, such as an application server. Alternatively, if latency, complexity, and other architectural constraints rule out implementing an inline threat management layer, customers build an overlay network on top of their Amazon VPC using technologies such as GRE tunnels, virtual tunnel (vtun) interfaces, or by forwarding traffic on another ENI to a centralized network traffic analysis and intrusion detection system, which can provide active or passive threat response.
vi. Conducting regular vulnerability scanning and penetration testing of the systems, as mandated by their Government Department and Agency’s policies.	Customers are responsible for all scanning, penetration testing, file integrity monitoring and intrusion detection for their Amazon EC2 and Amazon ECS instances and applications. Scans should include customer IP addresses and not AWS endpoints. AWS endpoints are tested as part of AWS compliance vulnerability scans. AWS Security performs regular vulnerability scans on the underlying infrastructure, web application, and databases in the AWS environment using a variety of tools. External vulnerability assessments are conducted by an AWS approved third party vendor at least quarterly, and identified issues are investigated and tracked to resolution. Vulnerabilities that are identified

	are monitored and evaluated and countermeasures are designed, implemented, and operated to compensate for known and newly identified vulnerabilities. AWS Security teams also subscribe to newsfeeds for applicable vendor flaws and proactively monitor vendors' websites and other relevant outlets for new patches. AISPL customers also have the ability to report issues to AISPL via the AWS Vulnerability Reporting website at: http://aws.amazon.com/security/vulnerability-reporting/.
vii. Review the audit logs to identify any unauthorized access to the government agency's systems.	Customers manage access to their customer content and AWS services and resources. AWS cloud provides an advanced set of access, encryption, and logging features to help customers do this effectively (such as AWS CloudTrail). For details, please refer to the considerations in the section titled "Governance and Auditability".

Exit Management and Transition-Out Services

Section 4.5 of the Guidelines for Procurement of Cloud Services recommends that Departments shall evaluate the capabilities of the Cloud Service Provider to provide assistance during the exit management period including migration of virtual machines and data. The following table includes considerations for key components of Section 4.5.

Requirement	Customer Considerations
a. Migration of the VMs, data, content and any other assets to the new environment or on alternate cloud service provider's offerings and ensuring successful deployment and running of the Government Department's solution on the new infrastructure by suitably retrieving all data, scripts, software, virtual machine images, and so forth to enable mirroring or copying to Department supplied industry standard media.	**This is a shared responsibility when using AWS cloud, as customers and AISPL have different roles relevant to this topic.** If a customer decides to leave AWS cloud, they can manage access to their data and AWS services and resources, including the ability to import and export data. AWS provides services such as AWS Import/Export and AWS Snowball to transfer large amounts of data into and out of AWS cloud using physical storage appliances. AWS Snowball is a petabyte-scale data transport solution that uses secure appliances to transfer large amounts of data into and out of the AWS cloud. Using AWS Snowball addresses common challenges with large-scale data transfers including high network costs, long transfer times, and security concerns. Transferring data with Snowball is simple, fast, secure, and can be as little as one-fifth the cost of high-speed Internet. Additionally, AWS cloud offers AWS Database Migration Service, a web service that customers can use to migrate a database from an AWS service to an on-premises database.
b. The format of the data transmitted from the cloud service provider to the Department should leverage standard data formats (e.g., OVF, VHD…) whenever possible to ease and enhance portability.	**This is primarily managed by AWS.** AWS VM Import/Export enables customers to easily import virtual machine images from their existing environment to Amazon EC2 instances and export them back to their on-premises environment. Customers can import Windows and Linux VMs that use VMware ESX or Workstation, Microsoft Hyper-V, and Citrix Xen virtualization formats. Customers can also export previously imported EC2 instances back to on-premises virtualization infrastructure in VMware ESX, Microsoft Hyper-V or Citrix Xen formats. For a full list of supported operating systems, versions, and formats, please consult the VM Import section of the Amazon EC2 User Guide[xiii].
c. The ownership of the data generated upon usage of the system, at any point of time during the contract or expiry	**This is a customer responsibility.** Customers retain ownership and control of their content when using AWS services, and do not cede that ownership and control of their content to

or termination of the contract, shall rest absolutely with Government Department and Agency.	AWS cloud. Customers have complete control over which services they use and whom they empower to access their content and services, including what credentials will be required.
d. Ensure that all the documentation required for smooth transition including configuration documents are kept up to date	**This is a customer responsibility.** Customers assume responsibility and management of the guest operating system (including updates and security patches), other associated application software, as well as the configuration of the AWS cloud-provided security group firewalls and other security, change management, and logging features.
e. Ensure that the CSP does not delete any data at the end of the agreement (for a maximum of 45 days beyond the expiry of the Agreement) without the express approval of the Government Department and Agency. If data is to be retained the cost for retaining the data may be obtained in the commercial quote.	**This is a customer responsibility.** AWS cloud provides customers with the ability to delete their data. Because customers retain control and ownership of their data, it is their responsibility to manage data retention according to customer's own requirements.
f. Once the exit process is completed, remove the data, content and other assets from the cloud environment and destroy the VM, Content and data of the Government Department and Agency as per stipulations and shall ensure that the data cannot be forensically recovered.	**This is primarily managed by AWS cloud.** AWS cloud has implemented global privacy and data protection best practices that helps customers establish, operate and leverage the security control environment. These security protections and control processes are independently validated by multiple third-party independent assessments. In order to ensure that customer content is properly erased, block device-based storage volumes such as EBS and RDS are presented to customers as raw unformatted block devices that have been wiped prior to being made available for use. Wiping immediately before reuse ensures that customers do not have access to block devices or physical media that was previously used to store another customer's content. If you have procedures requiring that all data be wiped via a specific method, such as those detailed in NIST 800-88 ("Guidelines for Media Sanitization"), you have the ability to do so on Amazon EBS. You should conduct a specialized wipe procedure prior to deleting the volume for compliance with your established requirements. For non-block device services such as S3 or DynamoDB, customers never see an attached block device, only objects and the path to that object (for example a table or an item). When a customer deletes an asset in these services, the deletion of the mapping between an asset identifier or key and the underlying content begins immediately. Once the mapping is removed, the content is no longer accessible and cannot be processed by an application. AWS cloud classifies all media entering the cloud as critical and treats it accordingly, as high impact, throughout its life-cycle. To destroy data on storage devices as part of the decommissioning process in accordance with the AWS security standard, the following procedures are followed: • Every Amazon datacenter facility contains one approved degaussing device and one approved disk destruction device; • Equipment containing storage media is checked to ensure that any sensitive data and licensed software has been removed or securely overwritten prior to disposal or reuse;

	• The functionality of all media sanitation equipment is checked for operational readiness at regular intervals; • All Solid State Drives (SSD's) are wiped prior to crushing; • All hard drives and magnetic tapes are degaussed after being removed from a device and placed in a secure bin. • Degaussing and destruction device functionality is tested on a periodic basis to verify that the intended sanitization is being achieved. Portable storage devices (e.g. external hard drives, floppy disks, storage tapes, compact discs, digital video discs, USB flash/thumb drives, and diskettes except for those that are part of an approved device, such as a flash card that is part of a networking router) are not permitted for use within the system boundary.

Governance and Auditability

Section 4.8 of the Guidelines for Procurement of Cloud Services recommends that Departments should monitor their cloud environment to ensure appropriate application of identified risk mitigation controls (e.g., security configurations and audit trails). The following table includes considerations for key components of Section 4.8.:

Requirement	**Customer Considerations**
View into the performance and availability of the cloud services being used, as well as alerts that are automatically triggered by changes in the health of those services.	Amazon CloudWatch is a web service that provides monitoring for AWS cloud resources. It provides customers with visibility into resource utilization, operational performance, and overall demand patterns—including metrics such as CPU utilization, disk reads and writes, and network traffic. Customers can use CloudWatch to monitor their cloud resources such as compute and RDS database instances, as well as custom metrics generated by their applications and services and any log files their applications generate. Customers can set up CloudWatch alarms to receive alerts if certain thresholds are crossed, or to take other automated actions such as adding or removing EC2 instances if Auto-Scaling is enabled.
Receive alerts that provide proactive notifications of scheduled activities, such as any changes to the provisioned cloud resources.	Amazon Simple Notification Service (Amazon SNS) is a web service that makes it easy to set up, operate, and send notifications from the cloud. It provides developers with a highly scalable, flexible, and cost-effective capability to publish messages from an application and immediately deliver them to subscribers or other applications. The potential uses for Amazon SNS include monitoring applications, workflow systems, time-sensitive information updates, mobile applications, and many others.
System-wide visibility into resource utilization, application performance, and operational health through monitoring of the cloud resources.	As mentioned above, customers can use CloudWatch to gain system-wide visibility into resource utilization, application performance, and operational health, using these insights to react intelligently and keep applications running smoothly. Customers can also use CloudWatch dashboards to create customized views of the metrics and alarms for their AWS resources. Amazon CloudWatch dashboards are customizable home pages in the CloudWatch console that you can use to monitor your resources in a single view. Each dashboard can display multiple metrics, and customers can build multiple dashboards, each one focusing on providing a distinct view of their environment.

Review of auto-scaling rules and limits.	Customers can use the limits page of the Amazon EC2 console or the describe-account-limits (AWS CLI) command to view the current limits for their Auto Scaling resources.
Access to Logs of all user activity within an account. The recorded information should include API details. This is required to enable security analysis, resource change tracking, and compliance auditing.	AWS CloudTrail is a service that helps customers enable governance, compliance, and operational and risk auditing of their AWS account. With CloudTrail, customers can log, continuously monitor, and retain account activity. Actions taken by a user, role, or an AWS service are recorded as events in CloudTrail. Events include actions taken in the AWS Management Console, AWS Command Line Interface, and AWS SDKs and APIs. Customers can configure CloudTrail with CloudWatch logs to monitor their trail logs and be notified when specific activity occurs.
Ability to discover all of the provisioned resources and view the configuration of each. Notifications should be triggered on configuration changes, and departments should be given the ability to view the configuration history to perform incident analysis.	AISPL provides customers with various tools they can use to monitor their services. For access and system monitoring, AWS Config is a service that provides customers with an AWS resource inventory, configuration history, and configuration change notifications to enable security and governance. Config Rules enables customers to create rules that automatically check the configuration of AWS resources recorded by AWS Config. When customer's resources are created, updated, or deleted, AWS Config streams these configuration changes to Amazon Simple Notification Service (SNS), so that they are notified of all configuration changes. AWS Config represents relationships between resources, so that customers can assess how a change to one resource may impact other resources.
Monitoring of cloud resources with alerts to customers on any security configuration gaps.	AWS Trusted Advisor is an online resource to help customers reduce cost, increase performance, and improve security by optimizing their AWS environment. Trusted Advisor performs real-time monitoring of resources and alerts customers to security configuration gaps such as overly permissive access to certain instance ports and storage buckets, minimal use of role segregation using IAM, and weak password policies. Customers can stay up-to-date with their AWS resource deployment with weekly updates, plus create alerts and automate actions with Amazon CloudWatch.

Business Continuity and Disaster Recovery Management

Section 4.1 of the Guidelines for Procurement of Cloud Services recommends that departments configure a disaster recovery environment after undertaking a comprehensive analysis of the recovery time (RTO) and recovery point (RPO) objectives in relation to the project requirements.

Government departments in India can build highly available and fault tolerant applications on AWS's multiple Availability Zones (AZ) architecture. The AWS Mumbai Region has two AZs. Each AZ has one or more data centers and is designed as an independent failure zone. All Availability Zones are redundantly connected to multiple tier-1 transit providers. This means that Availability Zones are physically separated within a typical metropolitan region and are located in lower risk flood plains (specific flood zone categorization varies by Region). Each AZ runs on its own physically distinct and independent infrastructure, including discrete uninterruptable power supply (UPS) and onsite backup generation facilities. Common points of failure like generators and cooling equipment are not shared across Availability Zones, so that even extremely uncommon disasters such as fires, tornados, or flooding should not impact more than one AZ simultaneously. All AZs implement a similar set of security controls and compliance assurance programs.

Availability Zones are connected by low latency links for synchronous replication and all data centers are online and serving customers; no data center is "cold." AWS cloud provides customers the flexibility to place instances and store data across multiple Availability Zones within each Region. In

the unlikely event of failure of any AZ, automated processes move customer data traffic away from the affected area. Core applications are deployed in an N+1 configuration, so that in the event of a data center failure, there is sufficient capacity to enable traffic to be load balanced to the remaining sites.

While AISPL goes to great lengths to provide availability of the cloud, our customers share responsibility for ensuring availability within the cloud. Customers have succeeded by adopting best practices for high availability, such as taking advantage of multiple Availability Zones and configuring Auto Scaling groups to replace unhealthy instances. The Building Fault-Tolerant Applications on AWS cloud[xiv] whitepaper is a great introduction to achieving high availability in the cloud. In addition, the AWS Well-Architected Framework[xv] codifies the experiences of thousands of customers, helping customers assess and improve their cloud-based architectures and mitigate disruptions. Using AWS-cloud provided best practices and recommendations, customers should consider architecting the AWS usage to take advantage of multiple Availability Zones. Distributing applications across multiple Availability Zones provides the ability to remain resilient in the face of most failure modes, including natural disasters or system failures.

AWS cloud also provides customers with the capability to implement a robust continuity plan for their solutions, including the utilization of frequent server instance backups, data redundancy replication, and the flexibility to place instances and store data within multiple geographic AWS Regions. To learn more about disaster recovery approaches, see the AWS Disaster Recovery[xvi] webpage.

Contractual Terms

Section 4.10 of the Guidelines for Procurement of Cloud Services clarifies that Departments need to be aware of critical issues specific to cloud services, and the contractual relationship between the parties should be clearly set out in a written agreement between the Government department and its cloud service provider.

AISPL provides all its customers with a documented agreement that contains standardized terms and conditions that govern your access to and use of AWS service offerings including, but not limited to, security and data privacy. Customer agreements also include references to service level agreements that we offer with respect to the services and post on the Site, as they may be updated by us from time to time.

AISPL customers also have the option to enroll in an Enterprise Agreement with their service provider. Enterprise Agreements give customers the option to tailor agreements that best suit their needs. For more information about Enterprise Agreements, contact your AISPL representative.

Other Considerations

Identity and Access Management

A key aspect of cloud adoption is determining how identities will be managed. AWS Identity and Access Management (IAM) enables customers to manage access to AWS services and resources for their users securely.

Government departments may have existing identities managed by their Identity Management System (IDMS) such as an on-premises Active Directory. When using IAM, customers can create identities (user accounts) for AWS Console, API, or Command Line Interface (CLI) access based on access keys or username and password. Customers are generally required to manage identities and

credentials created outside of current IDMS. Similarly, if customers have multiple AWS accounts, they will end up with many identity stores and identities; one for each AWS account that represent a single user.

AISPL enables the customers to federate an agency IDMS with AWS IAM to control access to AWS resources. Using AWS IAM, customers can create and manage AWS cloud users and groups, and can federate their existing identities with IAM to implement role-based permissions that allow and deny access to AWS resources. This saves the customer from creating identities across AWS accounts. Additional benefits of federating IDMS with AWS IAM include: temporary security credentials, SSO or reduced sign-on for AWS Console, and CLI and API access. Additionally, identity lifecycle management remains within customer's IDMS, and customer can extend crypto-based two-factor authentication into AWS.

Federation enables customers to manage access to the AWS Cloud resources centrally. With federation, customers can use single sign-on (SSO) to access their AWS accounts using credentials from their corporate directory. Federation uses open standards, such as Security Assertion Markup Language 2.0 (SAML), to exchange identity and security information between an identity provider (IdP) and an application.

AISPL also offers non–SAML-based options for managing access to customer's AWS Cloud resources. AWS Directory Service for Microsoft Active Directory, also known as AWS Microsoft AD, uses secure Windows trusts to enable users to sign in to the AWS Management Console, AWS Command Line Interface (CLI), and Windows applications running on the AWS Cloud using Microsoft Active Directory credentials.

Data Encryption

Amazon Web Services (AWS) delivers a secure, scalable cloud computing platform with high availability, offering the flexibility for customers to build a wide range of applications. Customers may open a secure, encrypted channel to Amazon servers using HTTPS (TLS/SSL).

Organizational policies, or industry or government regulation requirements, might require the use of encryption for protecting data at rest. AWS cloud provides customers the ability to add an additional layer of security to data at rest in the cloud, providing scalable and efficient encryption features. This includes:

- Data encryption capabilities available in AWS storage and database services, such as Amazon Elastic Block Store, Amazon Simple Storage Service, Amazon Glacier, Amazon RDS for Oracle Database, Amazon RDS for SQL Server, and Amazon Redshift.
- Flexible key management options, including AWS Key Management Service, allowing customers to choose whether to have AWS cloud manage the encryption keys or enable customers to keep complete control over their keys.
- Dedicated, hardware-based cryptographic key storage using AWS CloudHSM, allowing customers to satisfy compliance requirements.

In addition, AISPL provides APIs for customers to integrate encryption and data protection with any of the services customers develop or deploy in an AWS cloud environment.

Audit records captured in the AWS central audit system are encrypted at rest and in transit.

Key Management

Where customers choose to encrypt their data as a security measure, the encryption requires keys. In the cloud, as in an on- premises system, it is essential that customers keep their keys secure. As

customers deploy encryption for various data classifications in AWS cloud, it is critical to adequately understand who has access to their encryption keys or data and under what conditions.

Customer controls the Key Management Infrastructure

Customers can choose to either use existing process to manage encryption keys in the cloud, or leverage server-side encryption with AWS key management and storage capabilities. When using own key management processes, customers are strongly recommended to store keys in tamper-proof storage, such as hardware security modules (HSM). Amazon Web Services provides an HSM service in the cloud, known as AWS CloudHSM. Alternatively, you can use HSMs that store keys on premises, and access them over secure links, such as IPSec virtual private networks (VPNs) to Amazon VPC, or AWS Direct Connect with IPSec.

The AWS CloudHSM service provides customers with dedicated access to a hardware security module (HSM) appliance designed to provide secure cryptographic key storage and operations within an intrusion-resistant, tamper-evident device. Customer can generate, store, and manage the cryptographic keys used for data encryption so that they are accessible only by customers. AWS CloudHSM appliances are designed to securely store and process cryptographic key material for a wide variety of uses such as database encryption, Digital Rights Management (DRM), Public Key Infrastructure (PKI), authentication and authorization, document signing, and transaction processing. They support some of the strongest cryptographic algorithms available, including AES, RSA, and ECC, and many others. Customer can implement CloudHSMs in multiple Availability Zones with replication between them to provide for high availability and storage resilience.

AWS cloud controls the Key Management Infrastructure

When customers take all responsibility for the encryption method and the Key Management Infrastructure (KMI), they have granular control over how their applications encrypt data. However, that granular control comes at a cost – both in terms of deployment effort and an inability to have AWS services tightly integrate with your applications' encryption methods. As an alternative, customers can choose a managed service that enables easier deployment and tighter integration with AWS cloud services. This option offers check box encryption for several services that store customer data, secured storage and control over their own keys, and auditability on all data access attempts. Choosing the right solutions depends on which AWS service customers are using and their requirements for key management.

AWS Key Management Service (KMS) is a managed service that makes it easy for customers to create and control the encryption keys used to encrypt your data, and uses FIPS 140-2 validated HSMs to protect the security of their keys. AWS KMS is integrated with most other AWS services to help customer protect the data stored with these services. AWS KMS is also integrated with AWS CloudTrail to provide customers with logs of all key usage to help meet their regulatory and compliance needs.

AWS KMS stores, tracks, and protects Customer Master Keys (master keys). When customers want to use a master key, they access it through AWS KMS. Master keys never leave AWS KMS unencrypted. There are two types of master keys in AWS accounts:

- Customer managed master keys are master keys that customers create, manage, and use. This includes enabling and disabling the master key, rotating its cryptographic material, and establishing the IAM policies and key policies that govern access to the master key, as well as using the master key in cryptographic operations. Customers can allow an AWS service to use a customer managed master key on their behalf, but they retain control of the master key.
- AWS managed master keys are master keys in customer's account that are created, managed, and used on their behalf by an AWS service that is integrated with AWS KMS. This master key is unique to their AWS account and region. Only the service that created the AWS managed master key can use it.

Access to master keys, including by AISPL employees, is secured by both technical and operational controls. By design, no individual AISPL employee can gain access to the physical master key material in the service due to hardening techniques such as never storing plaintext master keys on persistent disk, using but not persisting them in volatile memory, and limiting which users and systems can connect to service hosts. In addition, multi-party access controls are enforced for operations on the AWS KMS hardened security appliances that handle plaintext master keys in memory.

Auditing your AWS environment

With the increase in customers using cloud to deploy workloads, apart from understanding how the cloud works, it is becoming increasingly critical that auditors understand how best to leverage the power of cloud computing to their advantage when conducting audits. The AWS cloud enables auditors to shift from percentage-based sample testing towards a more comprehensive real-time audit view, which enables 100% auditability of the customer environment, as well as real-time risk management.

At the time of auditing organizations using AWS services, it is critical to for the auditor to understand the "Shared Responsibility" model between AISPL and the customer. The following table includes considerations for key audit domains of customer's AWS cloud environment.

Domain	Major audit focus	Audit Approach
Governance	Understand what AWS services and resources are being used and ensure your security or risk management program has taken into account the use of the public cloud environment.	As part of this audit, determine who within your organization is an AWS account and resource owner, as well as the AWS services and resources they are using. Verify policies, plans, and procedures include cloud concepts, and that cloud is included in the scope of the customer's audit program.
Network Configuration and Management	Missing or inappropriately configured security controls related to external access/network security that could result in a security exposure.	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 cloud configurations settings.
Asset Configuration and Management	Manage your operating system and application security vulnerabilities to protect the security, stability, and integrity of the asset.	Validate the OS and applications are designed, configured, patched and hardened in accordance with your policies, procedures, and standards. All OS and application management practices can be common between on-premise and AWS systems and services.
Logical Access Control	This portion of the audit focuses on identifying how users and permissions are set up for the services in AWS cloud. It is also important to ensure you are securely managing the credentials associated with all AWS accounts.	Validate permissions for AWS assets are being managed in accordance with organizational policies, procedures, and processes. Note: AWS Trusted Advisor can be leveraged to validate and verify IAM Users, Groups, and Role configurations.
Data Encryption	Data at rest should be encrypted in the same way as on-premise data is protected. Also, many security policies consider the Internet an insecure communications medium and would	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").

	require the encryption of data in transit. Improper protection of data could create a security exposure.	Note: AWS Trusted Advisor can be leveraged to validate and verify permissions and access to data assets.
Security Logging and Monitoring	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.	Validate that audit logging is being performed on the guest OS and critical applications installed on Amazon EC2 instances and that implementation is in alignment with your policies and procedures, especially as it relates to the storage, protection, and analysis of the logs.
Security Incident Response	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.	Assess existence and operational effectiveness of the incident management controls for systems in the AWS environment.
Disaster Recovery	An unidentified single point of failure and/or inadequate planning to address disaster recovery scenarios could result in a significant impact. While AISPL provides service level agreements (SLAs) at the individual instance/service level, these should not be confused with a customer's business continuity (BC) and disaster recovery (DR) objectives, such as Recovery Time Objective (RTO) Recovery Point Objective (RPO). The BC/DR parameters are associated with solution design. A more resilient design often utilizes multiple components in different AWS availability zones and involve data replication.	Understand the DR and determine the fault-tolerant architecture employed for critical assets. Note: AWS Trusted Advisor can be leveraged to validate and verify some aspects of the customer's resiliency capabilities.
Inherited Controls	The purpose of this audit section is to demonstrate appropriate due diligence in selecting service providers.	Understand how you can request and evaluate third-party attestations and certifications in order to gain reasonable assurance of the design and operating effectiveness of control objectives and controls.

For more information on how customers and their auditors can assess the security of their AWS environment in accordance with industry or regulatory standards, see the whitepaper on Auditing Security Checklist[xvii]. The audit guide organizes the requirements into common security program controls and control areas. Each control references the applicable audit requirements.

There are many third-party tools that can assist you with your assessment. Since AISPL 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 cloud.

A useful tool provided in AWS Services is the AWS Trusted Advisor tool. 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.

Further, to help make these audits more productive, AWS cloud has released the AWS Auditor Learning Path. This set of online and in-person classes provides foundational and advanced education about implementing security in the AWS Cloud and using AWS tools to gather the information necessary to audit an AWS environment.

Next Steps

Each organization's cloud adoption journey is unique. In order to successfully execute your adoption, you need to understand your current state, the target state, and the transition required to achieve the target state. Knowing this will help you set goals and create work streams that will enable you to thrive in the cloud.

The AWS Cloud Adoption Framework (AWS CAF) offers structure to help organizations develop an efficient and effective plan for cloud adoption. Guidance and best-practices prescribed within the framework can help you build a comprehensive approach to cloud computing across your organization, throughout your IT lifecycle. The AWS CAF breaks down the complicated process of planning into manageable areas of focus.

Many organizations choose to apply the AWS CAF methodology with a facilitator-led workshop. To find out more about workshops, contact your AWS representative. Alternatively, AWS provides access to tools and resources for self-service application of the AWS CAF methodology at the AWS Cloud Adoption Framework[xviii] webpage.

Contact your AWS representative to discuss how the AWS Partner Network, AWS Solution Architects, AWS Professional Services teams, and Training instructors can assist with your cloud adoption processes. If you don't have an AWS representative, Contact Us[xix].

Notes

[i] https://aws.amazon.com/compliance/

[ii] https://d1.awsstatic.com/whitepapers/compliance/Using_AWS_in_the_context_of_Common_Privacy_and_Data_Protection_Considerations.pdf

[iii] https://aws.amazon.com/about-aws/global-infrastructure/

[iv] https://aws.amazon.com/compliance/iso-27001-faqs/

[v] https://aws.amazon.com/compliance/iso-27017-faqs/

[vi] https://aws.amazon.com/compliance/iso-27018-faqs/

[vii] https://aws.amazon.com/compliance/iso-9001-faqs/

[viii] https://aws.amazon.com/compliance/pci-dss-level-1-faqs/

[ix] https://aws.amazon.com/compliance/soc-faqs/

[x] https://aws.amazon.com/artifact/

[xi] https://aws.amazon.com/compliance/programs/

[xii] https://d0.awsstatic.com/whitepapers/Security/AWS_Security_Whitepaper.pdf

[xiii] http://docs.aws.amazon.com/AWSEC2/latest/UserGuide/VMImportPrerequisites.html

[xiv] https://d0.awsstatic.com/whitepapers/aws-building-fault-tolerant-applications.pdf

[xv] https://d0.awsstatic.com/whitepapers/architecture/AWS_Well-Architected_Framework.pdf

[xvi] https://aws.amazon.com/disaster-recovery/

[xvii] https://d0.awsstatic.com/whitepapers/compliance/AWS_Auditing_Security_Checklist.pdf

[xviii] https://aws.amazon.com/professional-services/CAF/

[xix] https://aws.amazon.com/contact-us/