AWS User Guide to Banking Regulations & Guidelines in India

December 2017

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 AWS's current product offerings and practices as of the date of issue of this document, which are subject to change without notice. Customers are responsible for making their own independent assessment of the information in this document and any use of products or services, each of which is provided "as is" without warranty of any kind, whether express or implied. This document does not create any warranties, representations, contractual commitments, conditions or assurances from AWS, its affiliates, suppliers or licensors. The responsibilities and liabilities of AWS or its affiliates to its customers are controlled by agreements, and this document is not part of, nor does it modify, any agreement between AWS or its affiliates and its customers.

Contents

Abstract

This document provides information to assist banks operating in India as they accelerate their use of Amazon Web Services (AWS) cloud services.

Introduction

The Indian Financial Services industry is going through unprecedented transformation as government, regulators, financial institutions, and technology companies collaborate to realize the vision of Digital India. As banks in India transform their businesses, they are building solutions designed to operate at massive scale, keep their systems secure against global security threats, and comply with industry-specific regulations.

In September 2017, the Institute for Development and Research in Banking Technology (IDRBT) published FAQs on Cloud Adoption for Indian Banks. The FAQs recognize that Indian banks using cloud services can:

- Trade capital expense for variable expense
- Benefit from massive economies of scale
- Scale resources up or down based on actual demand
- Increase speed and agility
- Go global quickly and with minimal cost
- Enhance their business continuity plans
- Adopt enhanced security postures in the cloud

> "*Banks can benefit from far greater security postures in the cloud than they can achieve in traditional datacenters.*"
>
> "*The ultimate benefit of the cloud is that banks can spend less time on undifferentiated tasks and more time focusing on the core competencies that add value to their organisations.*"
>
> IDRBT FAQs on Cloud Adoption for Indian Banks, September 2017

The Reserve Bank of India (RBI) has previously issued guidelines to help Indian Banks manage risks associated with outsourcing, information security and technology. This white paper provides introductory information for banks using AWS as they assess their responsibilities with regards to the following guidelines from the RBI:

- **Guidelines on Managing Risks and Code of Conduct in Outsourcing of Financial Services by Banks** (Guidelines on Outsourcing). These provide guidance on prudent risk management practices for outsourcing arrangements.
- **Guidelines on Information Security, Electronic Banking, Technology Risk Management and Cyber Frauds.** These guidelines help banks identify and manage

risks associated with IT Governance, Information Security, Audit, IT Operations, IT Services Outsourcing, Cyber Fraud, Business Continuity Planning, Customer Awareness programs and legal issues.

Banks can use the information in this document to commence their due diligence and assess how to implement an appropriate information security, risk management and governance program for their use of AWS.

The Shared Responsibility Model

Before exploring the requirements contained in the guidelines, it is important that banks understand the AWS Shared Responsibility Model shown in Figure 1.

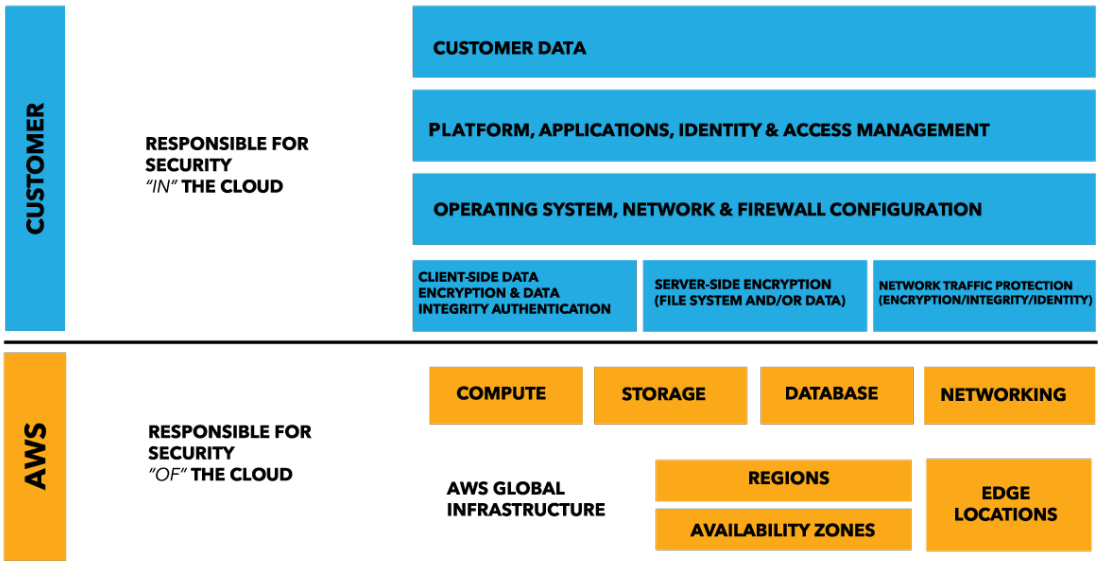

Figure 1: AWS Shared Security Responsibility Model

The Shared Responsibility Model is fundamental to understanding the respective roles of the customer and AWS in the context of the cloud security principles.

AWS operates, manages, and controls the IT components from the host operating system and virtualization layer down to the physical security of the facilities in which the services operate. Much like a traditional data center, the customer is responsible for managing the guest operating system (including installing updates and security patches) and other associated application software, as well as the configuration of the AWS-provided security group firewall. Customers should carefully consider the services they choose, as their responsibilities vary depending on the services they use, the integration of those services into their IT environments, and applicable laws and regulations.

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

- The content that they choose to store on AWS
- 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 technology such as host-based firewalls, host-based intrusion detection/ prevention, and encryption. AWS 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 webpage[1].

For more information about the Shared Responsibility Model and its implications for the storage and processing of personal data using AWS, see the whitepaper on Using AWS in the context of Common Privacy & Data Protection Considerations[2].

Security of the Cloud

In order to provide Security *of* the Cloud, AWS environments are continuously audited, and the infrastructure and services are approved to operate under several compliance standards and industry certifications across geographies and verticals. Customers can use these certifications to validate the implementation and effectiveness of AWS security controls, including internationally recognized security best practices and certifications. The AWS compliance program is based on the following actions:

- **Validate** that AWS services and facilities 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 maintains compliance with global standards and best practices.

AWS Compliance Assurance Programs

AWS has obtained certifications and independent third-party attestations for a variety of industry specific workloads, however the following are of particular importance to banks 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[3] 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[4] 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[5] 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[6] 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[7] 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[8] 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

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.

Further, Amazon Internet Services Private Limited, an Indian subsidiary of the Amazon Group which undertakes the resale and marketing of AWS services in India, has achieved full Cloud Service Provider (CSP) empanelment, and successfully completed the STQC (Standardization Testing and Quality Certification) audit from the Indian Ministry of Electronics and Information Technology (MeitY) for cloud services delivered from the AWS Asia Pacific (Mumbai) Region.

For more information about AWS certifications and attestations, see the AWS Assurance Programs[9] webpage. For information about general AWS security controls and service-specific security, see the Amazon Web Services: Overview of Security Processes[10] whitepaper.

> *"Cloud accreditation certifications and evaluations provide banks with assurance that cloud providers have effective physical and logical security controls in place. When banks leverage these reports, they avoid subjecting themselves to overly burdensome processes or approval workflows that may not be required for a cloud environment."*
>
> Institute for Development and Research in Banking Technology (IDRBT) FAQs on Cloud Adoption for Indian Banks, September 2017

AWS Artifact

Customers can use AWS Artifact[11] to review and download reports and details about more than 2,500 security controls. AWS Artifact is an automated compliance reporting portal available in the AWS Management Console that provides on-demand access to AWS security and compliance documents, including System & Organization Control (SOC) reports, Payment Card Industry (PCI) reports, and certifications from accreditation bodies across geographies and compliance verticals.

AWS Regions

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 Availability Zones. Availability Zones consist 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.

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. As with every AWS

Region, the Asia Pacific (Mumbai) Region is compliant with applicable national and global data protection laws.

For current information on AWS Regions and AZs, see the AWS Global Infrastructure[12] webpage.

RBI Guidelines on Outsourcing

The Guidelines on Outsourcing lay down a framework for banks to assess and manage risks when outsourcing activities to service providers. Banks are expected to carry out due diligence to evaluate the capabilities of the service provider and identify risks associated with the outsourcing arrangement, enter into written agreements addressing those risks, take appropriate steps to preserve and protect customer information and the bank's own business continuity, and monitor and control the outsourced activity on an ongoing basis. The Guidelines on Outsourcing state that the underlying principle is that banks should ensure that outsourcing arrangements do not diminish their ability to fulfil their obligations to customers or impede effective supervision by the RBI. Banks do not require prior approval from RBI for outsourcing activities, irrespective of whether the service provider is located inside or outside India.

A full analysis of Guidelines on Outsourcing is beyond the scope of this document. However, the following sections address the considerations in the Guidelines that most frequently arise in interactions with banks in India.

Assessment of Service Providers

Section 5.4.2 of the Guidelines on Outsourcing lists topics that should be evaluated in the course of due diligence when a bank is considering an outsourcing arrangement. The following table includes considerations for each component of Section 5.4.2.

Due Diligence Requirement	Customer Considerations
Past experience and competence to implement and support the proposed activity over the contracted period	Since 2006, AWS has provided flexible, scalable and secure IT infrastructure to businesses of all sizes around the world. AWS continues to grow and scale, allowing it to provide new services that help millions of active customers worldwide.
Financial soundness and ability to service commitments even under adverse conditions	The financial statements of Amazon.com Inc. include AWS sales and income, permitting assessment of its financial position and ability to service its debts and/or liabilities. These financial statements are available from the SEC or at Amazon's Investor Relations[13] website.
Business reputation and culture, compliance,	AWS has established formal policies and procedures to provide employees a common baseline for information security standards and guidance. The AWS Information Security Management

complaints and outstanding or potential litigation	System policy establishes guidelines for protecting the confidentiality, integrity, and availability of customers' systems and content. Maintaining customer trust and confidence is of the utmost importance to AWS. AWS performs a continuous risk assessment process to identify, evaluate and mitigate risks across the company. The process involves developing and implementing risk treatment plans to mitigate risks as necessary. The AWS Risk Management team monitors and escalates risks on a continuous basis, performing risk assessments on newly implemented controls at least every six months. Please refer to the following AWS Audit Reports for additional details: SOC 2, PCI DSS, ISO 27001, ISO 27017. Amazon.com has a Code of Business Conduct and Ethics, available at the Amazon Investor Relations website, which covers issues including, among other things, compliance with laws, conflicts of interest, bribery, discrimination and harassment, health and safety, recordkeeping and financial integrity. Amazon.com Inc's Form 10-K filing is available at the Amazon Investor Relations website or the website of the US Securities and Exchange Commission, and includes details of legal proceedings involving Amazon.com, Inc., Amazon Web Services, Inc., and other affiliates.
Security and internal control, audit coverage, reporting and monitoring environment, business continuity management	An AWS Chief Information Security Officer (CISO) is responsible for coordinating, developing, implementing, and maintaining an organization-wide information security program. AWS management re-evaluates the security program at least biannually. This process requires management to identify risks within its areas of responsibility and to implement appropriate measures designed to address those risks. AWS has established a formal audit program that includes continual, independent internal and external assessments to validate the implementation and operating effectiveness of the AWS control environment. To learn more about each of the audit programs leveraged by AWS, see the AWS Compliance Center. Compliance reports from these assessments are made available via AWS Artifact to customers to enable them to evaluate AWS. The AWS Compliance reports identify the scope of AWS services and Regions assessed, as well the assessor's attestation of compliance. A vendor or supplier evaluation can be performed by leveraging these reports and certifications.
External factors like political, economic, social and legal environment of the jurisdiction in which the service provider operates and other events that may	AWS works to comply with applicable central and state laws, statutes, ordinances, and regulations concerning IT security, privacy and data protection in order to minimize the risk of accidental or unauthorized access or disclosure of customer content.

impact service performance.	AWS formally tracks and monitors its regulatory and contractual agreements and obligations. In order to do so, AWS has performed and maintains the following activities: 1) Identified applicable laws and regulations for each of the jurisdictions in which AWS operates. 2) Documented and maintains all statutory, regulatory and contractual requirements relevant to AWS.
Ensuring due diligence by service provider of its employees	AWS Human Resources team is responsible for screening AWS new hires as per the Corporate Policy. Employees are required to review and sign-off on an employment contract, which acknowledges their responsibilities to overall Company standards and information security. Background checks are performed as part of the Company's hiring verification processes and include education, previous employment, and, in some cases, criminal and other background checks as permitted by law and regulation for employees commensurate with the employee's position and level of access to AWS facilities.

Confidentiality and Security

Section 5.6 of the Guidelines on Outsourcing states that banks should ensure the preservation and protection of the confidentiality and security of customer information in the custody or possession of the service provider. The following table includes considerations for key components of Section 5.6.

Requirement	Customer Considerations
5.6.2 Access to customer information by staff of the service provider should be on 'need to know' basis i.e., limited to those areas where the information is required in order to perform the outsourced function.	**Data Protection:** Customers choose how their data is secured. AWS offers customers strong encryption for their data in transit or at rest, and AWS provides customers with the option to manage their encryption keys. Where tokenization of data is desired before leaving the organization this can be achieved through offerings from a number of AWS partners. AWS only uses customer content to provide the services selected by each customer to that customer or as legally required, and does not use customer content for other purposes. **Access Rights**: AWS provides a number of ways for customers to identify users and securely access their AWS Account. A complete list of credentials supported by AWS can be found on the "My Security Credentials" page under "My Account". AWS also provides additional security options that enable customers to further protect their AWS Account and control access, including AWS Identity and Access Management (AWS IAM), key management and rotation, temporary security credentials, and multi-factor authentication (MFA).
5.6.3 The bank should ensure that the service provider	Amazon Virtual Private Cloud (Amazon VPC) lets customers provision a logically isolated section of the Amazon Web Services (AWS) cloud where they can launch AWS resources in a virtual network that they define.

is able to isolate and clearly identify the bank's customer information, documents, records and assets to protect the confidentiality of the information. In instances, where service provider acts as an outsourcing agent for multiple banks, care should be taken to build strong safeguards so that there is no comingling of information / documents, records and assets.	Customers have complete control over their virtual networking environment, including selection of their own IP address range, creation of subnets, and configuration of route tables and network gateways. Details of customer isolation and data segregation can be found within the AWS SOC2 report.
5.6.4 The bank should review and monitor the security practices and control processes of the service provider on a regular basis and require the service provider to disclose security breaches.	Please refer to the considerations in the preceding table in relation to "security and internal control, audit coverage, reporting and monitoring environment, business continuity management". Further, AWS has implemented a formal, documented incident response policy and program. This can be reviewed in the SOC 2 report via AWS Artifact. Customers can also see security notifications on the AWS Security Bulletins[14] website. AWS provides customers with various tools they can use to monitor their services, including those already noted and from the AWS Marketplace.[15]

Business Continuity and Management of Disaster Recovery Plan

Section 5.8 of the Guidelines on Outsourcing recommends that banks require service providers to establish a robust framework for documenting, maintaining and testing business continuity and recovery procedures.

The AWS Business Continuity plan details the process that AWS follows in the case of an outage, from detection to deactivation. This plan has been developed to recover and reconstitute AWS using a three-phased approach: Activation and Notification Phase, Recovery Phase, and Reconstitution Phase. This approach ensures that AWS performs system recovery and reconstitution efforts in a methodical sequence, maximizing the effectiveness of the recovery and reconstitution efforts and minimizing system outage time due to errors and

omissions. For more information, see the Amazon Web Services: Overview of Security Processes whitepaper and the SOC 2 report available via the AWS Artifact console.

AWS 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 as well as across multiple Availability Zones within each Region. To learn more about disaster recovery approaches, see the AWS Disaster Recovery[16] webpage.

> "*With readily deployable and scalable infrastructure, business continuity is always built into the business model. Banks can initiate business continuity plan of IT infrastructure with minimal effort and do not have to invest upfront.*"
>
> IDRBT FAQs on Cloud Adoption for Indian Banks, September 2017

If a customer decides to leave AWS, 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 using physical storage appliances. For more information, see the Cloud Storage with AWS[17] webpage.

Additionally, AWS 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. AWS also 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.

Monitoring and Control of Outsourced Activities

Section 5.9.1 of the Guidelines on Outsourcing recommends that banks implement a management structure to monitor and control its outsourcing activities.

The AWS Service Health Dashboard[18] provides up-to-the-minute information on the general availability of the services. The AWS Personal Health Dashboard gives customers a personalized view into the performance and availability of the services. It displays relevant and timely information to help customers manage events in progress, and provides proactive notification to help customers plan for scheduled actitivies.

AWS has implemented a formal, documented incident response policy and program, which can be reviewed in the SOC 2 report available via AWS Artifact. Customers can also see security notifications on the AWS Security Bulletins website. AWS provides customers with various additional tools they can use to monitor their services, including those already noted and from the AWS Marketplace.

> "*A CSP partner ecosystem includes access to a marketplace with software offerings for banks at a lower cost. A marketplace would typically feature software categories including Security, Networking, BI, Storage, Databases, Operating Systems, and Business Software.*"
>
> IDRBT FAQs on Cloud Adoption for Indian Banks, September 2017

Section 5.9.3 of the Guidelines on Outsourcing recommends that banks assess the adequacy of the risk management practices adopted in overseeing and managing the outsourcing arrangement, the bank's compliance with its risk management framework and the requirements of the Guidelines, via regular audit.

AWS has established a formal audit program to validate the implementation and effectiveness of the AWS control environment. The AWS audit program includes internal audits and third party accreditation audits. The objectives of these audits are to evaluate the operating effectiveness of the AWS control environment. Internal audits are planned and performed periodically. Audits by third party accreditation are conducted to review the continued performance of AWS against standards-based criteria and to identify general improvement opportunities.

Compliance reports from these assessments are made available to customers to enable them to evaluate AWS. The AWS Compliance reports identify the scope of AWS services and Regions assessed, as well the assessor's attestation of compliance. A vendor or supplier evaluation can be performed by leveraging these reports and certifications. Some key audit programs and certifications are described in the section entitled "AWS Compliance Assurance Programs". For a full list of audits, certifications and attestations, see the AWS Assurance Programs webpage.

> "*Banks should evaluate Cloud Service Providers (CSP) based on regulatory and compliance requirements of the bank and the related accreditations provided by CSP. Bank should validate CSP audit reports and meet the certification requirements including but not limited to ISO 27001, PCI-DSS & PA-DSS, Gopalakrishna Committee Recommendations of RBI, IDRBT Cloud Security Framework, SOC 1 and SOC2. "*
>
> IDRBT FAQs on Cloud Adoption for Indian Banks, September 2017

Off-shore outsourcing of Financial Services

Customers who provide an Indian contact address during the account creation process open an account with Amazon Internet Services Private Limited, an Indian entity that acts as a reseller of AWS services in India. Customers can choose the AWS Region or Regions in which their content and servers will be located, including the AWS Asia Pacific (Mumbai) Region. If

the customer makes this choice, their content will be located in India unless the customer chooses to move that content.

In any event, sections 1.4 and 7 of the Guidelines on Outsourcing explicitly contemplate off-shore outsourcing arrangements. The following table includes considerations for key components of Section 7.

Requirement	Customer Considerations
7.1 The engagement of service providers in a foreign country exposes a bank to country risk - economic, social and political conditions and events in a foreign country that may adversely affect the bank. Such conditions and events could prevent the service provider from carrying out the terms of its agreement with the bank. To manage the country risk involved in such outsourcing activities, the bank should take into account and closely monitor government policies and political, social, economic and legal conditions in countries where the service provider is based, during the risk assessment process and on a continuous basis, and establish sound procedures for dealing with country risk problems.	AWS customers choose the AWS Region in which their content will be stored, and can monitor and manage risk as appropriate. Please refer to the section entitled “AWS Regions”.
7.1 (continued) This includes having	Customers manage access to their content and AWS services and resources, including the ability to import and export data. AWS provides

appropriate contingency and exit strategies.	services such as AWS Import/Export and AWS Snowball to transfer large amounts of data into and out of AWS using physical storage appliances. For more information, see the Cloud Storage with AWS webpage. Additionally, AWS offers AWS Database Migration Service, a web service customers can use to migrate a database from an AWS service to an on-premises database. AWS provides customers with the ability to delete their data. Because customers retain control and ownership of their data, it is their responsibility to manage their own data retention requirements. In alignment with ISO 27001 standards, when a storage device has reached the end of its useful life, AWS procedures include a decommissioning process that is designed to prevent customer's data from being exposed to unauthorized individuals. AWS uses the techniques detailed in DoD 5220.22-M ("National Industrial Security Program Operating Manual") or NIST 800-88 ("Guidelines for Media Sanitization") to destroy data as part of the decommissioning process. If a hardware device is unable to be decommissioned using these procedures, the device will be degaussed or physically destroyed in accordance with industry-standard practices. For more information, see ISO 27001 standards, Annex A, domain 8. AWS has been validated and certified by an independent auditor to confirm alignment with the ISO 27001 certification standard.
7.2 The activities outsourced outside India should be conducted in a manner so as not to hinder efforts to supervise or reconstruct the India activities of the bank in a timely manner.	Customers retain ownership and control of their content when using AWS services, and do not cede that ownership and control of their content to AWS. 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. AWS provides customers with various tools they can use to monitor their services, including those already noted and from the AWS Marketplace. 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. AWS CloudTrail is a service that enables governance, compliance, operational auditing and risk auditing of a customer's account. With CloudTrail, customers can log, continuously monitor, and retain account activity.

Outsourcing Agreements

Section 5.5.1 of the Guidelines on Outsourcing clarifies that the type and level of services to be provided and the contractual liabilities and obligations of the parties should be clearly set out in a written agreement between the bank and its service provider.

AWS customers 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. AWS also provides an introductory guide to help Indian banks assess the Enterprise Agreement against the Guidelines on Outsourcing. For more information about Enterprise Agreements, contact your AWS representative.

Guidelines on Information Security, Electronic Banking, Technology Risk Management and Cyber Frauds

The Guidelines on Information Security, Electronic Banking, Technology Risk Management and Cyber Frauds help banks identify and manage risks arising from the use of information technology. These Guidelines are based on the Report and Recommendations of the Working Group on Information Security, Electronic Banking, Technology Risk Management and Cyber Frauds chaired by Mr Shri. G. Gopalakrishna. While a full analysis of the Guidelines is beyond the scope of this document, the following table includes considerations for key components of Chapter 2 of the Guidelines.

Chapter 2 – Information Security

No	RBI Guideline Reference	Key consideration / Recommendations	Customer Considerations
1	Policy and Procedure	Board approved information security policy.	**This is a customer responsibility.**
2	Risk assessment	ISO 27001 and 27002 based risk assessment, with quantitative and qualitative analysis.	**This is a shared responsibility when using AWS, as customers and AWS have different roles relevant to this topic.** AWS performs a continuous risk assessment process to identify, evaluate and mitigate risks across the company. The process involves developing and implementing risk treatment plans to mitigate risks as necessary. The AWS risk management team monitors and escalates risks on a continuous basis, performing risk assessments on newly implemented controls at least every six months. AWS has established a formal audit program that includes continual, independent internal and external assessments to validate the implementation and operating effectiveness of the AWS control environment. Internal and external audits are planned and performed according to the documented audit scheduled to review the continued performance of AWS against standards-based criteria and to identify general improvement opportunities. Standards-based criteria includes but is not limited to the ISO/IEC 27001, Federal Risk and Authorization Management Program (FedRAMP), the American Institute of Certified Public Accountants (AICPA): AT 801 (formerly Statement on Standards for Attestation Engagements [SSAE] 16), and the International Standards for Assurance Engagements No.3402 (ISAE 3402) professional standards. Compliance reports from these assessments are made available to customers to enable them to evaluate AWS. The AWS Compliance reports identify the scope of AWS services and Regions assessed, as well the assessor's attestation of compliance. A vendor or supplier evaluation can be performed by leveraging these reports and certifications.
3	Inventory and information classification	Detailed inventory of information and assets and ISO 27001 based asset management, labeling and classification.	**This is a shared responsibility when using AWS, as customers and AWS have different roles relevant to this topic.** Customers retain control and ownership of their data and may implement a labeling and handling policy and procedures to meet their requirements. Customers determine what data

No	RBI Guideline Reference	Key consideration / Recommendations	Customer Considerations
			will be used for, who it can be used by, the format and structure of the data and how it is protected from disclosure to unauthorized parties including whether it is encrypted. AWS treats all Customer content and associated assets as critical information. AWS services are content agnostic, in that they offer the same high level of security to all customers, regardless of the type of content being stored. AWS is vigilant about its customers' security and has implemented sophisticated technical and physical measures against unauthorized access.
4	Define roles and responsibility	Define roles and responsibility like Information owner, custodian, application owner, end user, security administrator.	**This is a customer responsibility.**
5	Access control	Effective access control process, Granular and “need-to-have” “need-to-do” based access. Access control automation, segregation of duty, two factor authentication.	**This is a shared responsibility when using AWS, as customers and AWS have different roles relevant to this topic.** AWS has a formal access control policy that is reviewed and updated on an annual basis (or when any major change to the system occurs that impacts the policy). The policy addresses purpose, scope, roles, responsibilities and management commitment. Access control procedures are systematically enforced through proprietary tools. Procedures exist so that Amazon employee and contractor user accounts are added, modified, or disabled in a timely manner and are reviewed on a periodic basis. In addition, password complexity settings for user authentication to AWS systems are managed in compliance with Amazon’s Corporate Password Policy. AWS has established formal policies and procedures to delineate standards for logical access to AWS platform and infrastructure hosts. Where permitted by law, AWS requires that all employees undergo a background investigation commensurate with their position and level of access. The policies also identify functional responsibilities for the administration of logical access and security. AWS controls access to systems through authentication that requires a unique user ID and password. AWS systems do not allow actions to be performed on the information system without identification or authentication. Upon approval and ID confirmation by their manager or a designee, an AWS employee can report to Amazon IT support to receive a hardware multi-factor authenticator.

No	RBI Guideline Reference	Key consideration / Recommendations	Customer Considerations
			Remote access requires multi-factor authentication and the number of unsuccessful log-on attempts is limited. All remote administrative access attempts are logged, and the logs are reviewed by the Security team for unauthorized attempts or suspicious activity. If suspicious activity is detected, the incident response procedures are initiated. AWS has implemented a session lock out policy that is systematically enforced. The information systems implements a session lock after a period of inactivity, as well as in the case of multiple log-in attempts, and limits the number of concurrent sessions that may exist. The session lock is retained until established identification and authentication procedures are performed.
6	Information security and information asset life-cycle	Information security across asset lifecycle. Ongoing support and maintenance of controls, configuration management. Segregation of test and dev environment.	**This is a shared responsibility when using AWS, as customers and AWS have different roles relevant to this topic.** AWS has established and maintains a company-wide policy that defines roles, responsibilities and classifications for managing changes to the production environment. Changes to AWS services and features follow secure software development practices, which include a security risk review prior to launch. In order to reduce the risk of unauthorized access or changes to the production environment, development, test and production environments are logically separated. Because the development, test and production environments emulate the production system, AWS can properly assess and prepare for the change impact. AWS developers that require access to production environments must explicitly request access through the AWS access management system, have the access reviewed and approved by the appropriate owner, and upon approval obtain authentication. AWS service teams maintain service specific change management standards that inherit and build on the AWS Change Management guidelines. When a storage device has reached the end of its useful life, AWS procedures include a decommissioning process that is designed to prevent customer data from being exposed to unauthorized individuals. AWS uses the techniques detailed in DoD 5220.22-M (“National Industrial Security Program Operating Manual “) or NIST 800-88 (“Guidelines for Media Sanitization”) to destroy data as part of the decommissioning process. If a hardware device is unable to be decommissioned using these procedures, the device will be degaussed or physically destroyed in accordance with industry-standard practices.

No	RBI Guideline Reference	Key consideration / Recommendations	Customer Considerations
7	Personnel security	Manage reduce risk exposure from internal users. Background and check, character reference and verify prior experience.	**This is a shared responsibility when using AWS, as customers and AWS have different roles relevant to this topic.** Background checks are performed as part of hiring verification processes and include education, previous employment, and, in some cases, criminal and other background checks as permitted by law and regulation for employees commensurate with the employee's position and level of access to AWS facilities. The AWS Risk Assessment process is responsible for identifying, correcting, or mitigating any opportunity for unauthorized access as it relates to nature or man-made disaster scenarios. AWS data centers have been specifically designed to be accessible under a variety of natural and man-made disaster scenarios.
8	Physical Security	Secure location and critical asset from manmade threats, Restrict access to datacenter. Monitoring of compromised environment controls and mitigation.	**This is primarily managed by AWS.** AWS has implemented a formal, documented physical and environmental protection policy that is updated and reviewed annually. Physical access to all AWS data centers housing IT infrastructure components is restricted to authorized data center employees, vendors, and contractors who require access in order to execute their jobs. Access to facilities is only permitted at controlled access points requiring multi-factor authentication designed to prevent tailgating and ensure that only authorized individuals enter an AWS data center. On a quarterly basis, access lists and authorization credentials of personnel with access to data centers housing systems and devices within the system boundary are reviewed by the respective data center Area Access Managers (AAM). All entrances to AWS data centers, including the main entrance, the loading dock, and any roof doors/hatches, are secured with intrusion detection devices that sound alarms if the door is forced open or held open. Trained security guards are stationed at the building entrance 24/7. If a door or cage within a data center has a malfunctioning card reader or PIN pad and cannot be secured electronically, a security guard is posted at the door until it can be repaired. Physical access is controlled both at the perimeter and at building ingress points by professional security staff utilizing video surveillance, intrusion detection systems, and other electronic means. Physical access points to server locations are managed by electronic access control devices, requiring proper multi-factor authorization to access them. All access

No	RBI Guideline Reference	Key consideration / Recommendations	Customer Considerations
			records are tracked in the AWS access management and request system, and are available for review. Periodic reviews are automatically triggered and enforced. AWS provides data center physical access to approved employees and contractors who have a legitimate business need for such privileges. All visitors are required to present identification and are signed in and escorted by authorized staff. When an employee or contractor no longer requires these privileges, his or her access is promptly revoked, even if he or she continues to be an employee of AWS. In addition, access is automatically revoked when an employee's record is terminated in the AWS HR system. Cardholder access to data centers is reviewed quarterly. Cardholders marked for removal have their access revoked as part of the quarterly review. Each AWS data center is evaluated to determine the controls that must be implemented to mitigate, prepare, monitor, and respond to natural disasters or malicious acts that may occur. Controls implemented to address environmental risks can include but are not limited to the following: • AWS data centers are equipped with sensors and master shutoff-valves to detect the presence of water. Mechanisms are in place to remove water in order to prevent any additional water damage. • Automatic fire detection and suppression equipment has been installed to reduce risk and notify AWS Security Operations Center, and emergency responders in the event of a fire. The fire detection system utilizes smoke detection sensors in all data center environments (e.g., VESDA, point source detection), mechanical and electrical infrastructure spaces, chiller rooms, and generator equipment rooms. These areas are protected by either wet-pipe, double-interlocked pre-action, or gaseous sprinkler systems. • The data center electrical power systems are designed to be fully redundant and maintainable without impact to operations, 24 hours a day, and Uninterruptible Power Supply (UPS) units provide back-up power in the event of an electrical failure for critical and essential loads in the facility. Data centers use generators to provide back-up power for the entire facility. • Climate control is required to maintain a constant operating temperature for servers and other hardware, which prevents overheating and reduces the possibility of

No	RBI Guideline Reference	Key consideration / Recommendations	Customer Considerations
			service outages. Data centers are conditioned to maintain atmospheric conditions at specified levels. Personnel and systems monitor and control temperature and humidity at appropriate levels. This is provided at N+1 and also utilizes free cooling as primary source of cooling when and where it is available based on local environmental conditions. • Availability Zones are physically separated within a metropolitan region and are in different flood plains. • Each Availability Zone is designed as an independent failure zone and automated processes move customer traffic away from the affected area in the case of a failure. The physical security and environmental controls that AWS implements are documented within its compliance reports. These controls are independently verified by reputable third-party auditors as part of the SOC1/2 and ISO27001 compliance programs.
9	User Training and Awareness	User awareness program to cover Information Security policy and process, acceptable use of assets. Reporting of security concern and incident.	**This is a shared responsibility when using AWS, as customers and AWS have different roles relevant to this topic.** AWS has implemented formal, documented security awareness and training policy and procedures that address purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance. The security awareness and training policy and procedures are reviewed and updated at least annually, or sooner if required due to information system changes. The policy is disseminated through the internal Amazon communication portal to all employees, vendors, and contractors prior to receiving authorized access to the information system or performing assigned duties. AWS has developed, documented and disseminated role based security awareness training for personnel responsible for designing, developing, implementing, operating, maintaining, and monitoring the system affecting security and availability and provides resources necessary for personnel to fulfill their responsibilities. Training includes, but is not limited to the following information (when relevant to the employee's role): • Workforce conduct standards • Candidate background screening procedures • Clear desk policy and procedures

No	RBI Guideline Reference	Key consideration / Recommendations	Customer Considerations
			• Social engineering, phishing, and malware • Data handling and protection • Compliance commitments • Use of AWS security tools • Security precautions while traveling • How to report security and availability failures, incidents, concerns, and other complaints to appropriate personnel • How to recognize suspicious communications and anomalous behavior in organizational information systems • Practical exercises that reinforce training objectives • ITAR responsibilities
10	Incident Management	Documented incident management process with escalation and communication. Response plan and periodic testing of process and plan.	**This is a shared responsibility when using AWS, as customers and AWS have different roles relevant to this topic.** Customers are responsible for identifying and managing incidents including incidents involving customer storage, virtual machines, and applications, unless the incident is caused by AWS. AWS employees are trained on how to recognize suspected security incidents and where to report them. When appropriate, incidents are reported to relevant authorities. AWS maintains the Latest Bulletins webpage to notify customers of security and privacy events affecting. AWS has implemented a formal, documented incident response policy and program. The policy addresses purpose, scope, roles, responsibilities, and management commitment. AWS utilizes a three-phased approach to manage incidents: 1. Activation and Notification Phase: Incidents for AWS begin with the detection of an event. Events originate from several sources such as: • Metrics and alarms - AWS maintains an exceptional situational awareness capability, most issues are rapidly detected from 24x7x365 monitoring and alarming of real time metrics and service dashboards. The majority of incidents are detected

No	RBI Guideline Reference	Key consideration / Recommendations	Customer Considerations
			in this manner. AWS utilizes early indicator alarms to proactively identify issues that may ultimately impact Customers. • Trouble tickets entered by an AWS employee. • Calls to the 24x7x365 technical support hotline. If the event meets incident criteria, the relevant on-call support engineer use Event Management Tool system to start an engagement and page relevant program resolvers (for example, Security team). The resolvers will perform an analysis of the incident to determine if additional resolvers should be engaged and to determine the approximate root cause. 2. Recovery Phase - The relevant resolvers will perform break fix to address the incident. After addressing troubleshooting, break fix and affected components, the call leader will assign follow-up documentation and follow-up actions and end the call engagement. 3. Reconstitution Phase – The call leader will declare the recovery phase complete after the relevant fix activities have been addressed. The post mortem and deep root cause analysis of the incident will be assigned to the relevant team. The results of the post mortem will be reviewed by relevant senior management and actions, such as design changes, will be captured in a Correction of Errors (COE) document and tracked to completion. AWS Incident Management planning, testing and test results are reviewed by third party auditors.
11	Application Control and Security	Application control and risk mitigation measures. “Need-to-know” privileges for application. Maintain application and log and audit trail.	**This is a customer responsibility.**
12	Migration controls	Documented Migration policy. requirement of roadmap / migration plan / methodology for data migration.	**This is a customer responsibility.**
13	Implementation of new technologies	Carry out due diligence with regard to new technologies. Formal product approval process including inter-alia, security aspects legal and regulatory.	**This is a customer responsibility.**

No	RBI Guideline Reference	Key consideration / Recommendations	Customer Considerations
14	Encryption	Bank should select encryption algorithms which are well established international standards. Secure and fully automated key management.	**This is a shared responsibility when using AWS, as customers and AWS have different roles relevant to this topic.** Customers may open a secure, encrypted channel to AWS servers using HTTPS (TLS/SSL). Customers retain 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 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, AWS provides APIs for customers to integrate encryption and data protection with any of the services customers develop or deploy in an AWS environment. Access to Customer Master Keys (CMKs), including by AWS employees, is secured by both technical and operational controls. By design, no individual AWS employee can gain access to the physical CMK 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 CMKs in memory. Audit records captured in the AWS central audit system are encrypted at rest and in transit.
15	Data Security	Define and implement procedures to ensure the integrity and consistency of all data stored in electronic form. Data Classification. Monitor and control movement of sensitive data. Secure	**This is a shared responsibility when using AWS, as customers and AWS have different roles relevant to this topic.** Customers retain control and ownership of their data and may implement a structured data-classification program to meet their requirements.

No	RBI Guideline Reference	Key consideration / Recommendations	Customer Considerations
		disposal of electronic and paper based media.	Customers retain ownership and control over their content by design through simple, but powerful tools that allow customers to determine where their content will be stored, how it will be secured in transit or at rest, and how access to their AWS environment will be managed. AWS has implemented global privacy and data protection best practices in order to helping customers establish, operate and leverage the security control environment. These security protections and control processes are independently validated by multiple third-party independent assessments. AWS classifies all media entering AWS facilities 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 equipment use procedures are followed: • Every AWS 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.
16	Vulnerability Assessment	Perform vulnerability scan, automate vulnerability scan, act on results of	**This is a shared responsibility when using AWS, as customers and AWS have different roles relevant to this topic.**

No	RBI Guideline Reference	Key consideration / Recommendations	Customer Considerations
		Vulnerability Assessment scan for mitigation and remediation.	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. AWS customers also have the ability to report issues to AWS via the AWS Vulnerability Reporting website at: http://aws.amazon.com/security/vulnerability-reporting/.
17	Establishing on-going security monitoring processes	Banks to have robust monitoring process to identify event and unusual activity. Enable audit log, record events for monitoring. Effective attack detection and Analysis using SIEM, IDS/IPS, NBA, MSSP (Managed Security Service Provider)	**This is a shared responsibility when using AWS, as customers and AWS have different roles relevant to this topic.** Customers manage access to their customer content and AWS services and resources. AWS provides an advanced set of access, encryption, and logging features to help customers do this effectively (such as AWS CloudTrail). AWS deploys monitoring devices throughout the environment to collect critical information on unauthorized intrusion attempts, usage abuse, and network and application bandwidth usage. These monitoring devices are designed to trigger alarms in the case of validation errors while capturing audit logs. Monitoring devices detect and monitor for: • Port scanning attacks • Usage (CPU, Processes, disk utilization, swap rates, and errors in software generated loss) • Application performance metrics • Unauthorized connection attempts Authentication logging aggregates sensitive logs from EC2 hosts and stores them on S3. The log integry checker inspects logs to ensure they were uploaded to S3 unchanged by

No	RBI Guideline Reference	Key consideration / Recommendations	Customer Considerations
			comparing them with local manifest files. Access and privileged command auditing logs record every automated and interactive login to the systems as well as every privileged command executed
18	Security measures against Malware	Malware protection at host and network level. Email attachment and Proxy/content filtering. User education and awareness.	**This is a customer responsibility.**
19	Patch Management	Application and OS patch management process.	**This is a shared responsibility when using AWS, as customers and AWS have different roles relevant to this topic.** Customers retain control of their own guest operating systems, software and applications and are responsible for performing vulnerability scans and patching of their own systems. AWS is responsible for patching systems supporting the delivery of service to customers, such as the hypervisor and networking services. This is done as required per AWS policy and in accordance with ISO 27001, NIST, and PCI requirements. AWS Security teams also subscribe to newsfeeds for applicable vendor flaws and proactively monitor vendors' websites and other relevant outlets for new patches.
20	Change management	Documented change management process covering upgrades and modifications to application and software, modifications to business information, emergency 'fixes', and changes to the computers / networks that support the application.	**This is a shared responsibility when using AWS, as customers and AWS have different roles relevant to this topic.** 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-provided security group firewalls and other security, change management, and logging features. AWS applies a systematic approach to managing change to ensure that all changes to a production environment are reviewed, tested, and approved. Facilities, equipment, and software components of production operations are identified throughout their lifecycle to ensure that only acceptable components are used in production. The development, test and production environments emulate the production system environment and are used to properly assess and prepare for the impact of a change to the production system environment. In order to reduce the risks of unauthorized access or change to the production environment, the development, test and production environments

No	RBI Guideline Reference	Key consideration / Recommendations	Customer Considerations
			are logically separated. In order to apply changes to the AWS production environments, AWS service teams must first run a full set of tests in the test environment, and the testing methodology must be documented. The AWS service, including application programming interfaces (APIs), are labeled and marked by identifiers. Facilities, equipment, and software components are tracked such that quality-impacting issues and errors are traceable to related components.
21	Audit trails	Audit trail for existing IT assets. Encryption of log file. Enough storage capacity for log retention, prevent modification to log data. Use of SIEM for log aggregation.	**This is a shared responsibility when using AWS, as customers and AWS have different roles relevant to this topic.** Customers retain control of their own guest operating systems, software and applications and are responsible for developing logical monitoring of the conditions of these systems. Please refer to rows 2, 17, 20 and 27.
22	Information security reporting and metrics.	Security monitoring to provide an informed view of aspects like the effectiveness and efficiency of information security arrangements. Analyze and report security incident. Fraud analysis.	**This is a shared responsibility when using AWS, as customers and AWS have different roles relevant to this topic.** Customers retain control of their own guest operating systems, software and applications and are responsible for developing logical monitoring, analysis and incident response for these systems. AWS provides near real-time alerts when the AWS monitoring tools show indications of compromise or potential compromise, based upon threshold alarming mechanisms determined by AWS service and Security teams. AWS correlates information gained from logical and physical monitoring systems to enhance security on an as-needed basis. Upon assessment and discovery of risk, Amazon disables accounts that display atypical usage matching the characteristics of bad actors.
23	Information security and Critical service providers/vendors.	Evaluate the role that the third party performs in relation to the IT environment. Relationship between the enterprise and a third-party provider should be documented as contract.	**This is a customer responsibility.**
24	Network Security	Adopt defense in depth approach. Network segmentation and logical security	**This is a shared responsibility when using AWS, as customers and AWS have different roles relevant to this topic.**

No	RBI Guideline Reference	Key consideration / Recommendations	Customer Considerations
		domain. Network and application firewall. IDS and IPS.	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-provided security group firewalls and other security, change management, and logging features. The AWS Network consists of the internal data center facilities, servers, networking equipment and host software systems that are within AWS control and are used to provide the services. The AWS network provides significant protection against traditional network security issues. For example: • Distributed Denial Of Service (DDoS) Attacks. AWS API endpoints are hosted on large, Internet-scale infrastructure and use proprietary DDoS mitigation techniques. Additionally, AWS networks are multi-homed across a number of providers to achieve Internet access diversity. • Man in the Middle (MITM) Attacks. All of the AWS APIs are available via TLS/SSL-protected endpoints, which provide server authentication. Amazon EC2 AMIs automatically generates new SSH host certificates on first boot and logs them to the instance's console. Customers can then use the secure APIs to call the console and access the host certificates before logging into the instance for the first time. Customers can use TLS/SSL for all of their interactions with AWS. • IP Spoofing. The AWS-controlled, host-based firewall infrastructure will not permit an instance to send traffic with a source IP or MAC address other than its own. • Port Scanning. Unauthorized port scans by Amazon EC2 customers are a violation of the AWS Acceptable Use Policy. Violations of the AWS Acceptable Use Policy are taken seriously, and every reported violation is investigated. Customers can report suspected abuse using the contacts available on the AWS website at: http://aws.amazon.com/contact-us/report-abuse/. When unauthorized port scanning is detected by AWS, it is stopped and blocked. Port scans of Amazon EC2 instances are generally ineffective because, by default, all inbound ports on Amazon EC2 instances are closed and are only opened by the customer. Customers' strict management of security groups can further mitigate the threat of port scans. Customers may request permission to conduct vulnerability scans as required to

No	RBI Guideline Reference	Key consideration / Recommendations	Customer Considerations
			meet specific compliance requirements. These scans must be limited to customers' own instances and must not violate the AWS Acceptable Use Policy. Advanced approval for these types of scans can be initiated by submitting a request via the website at: http://aws.amazon.com/security/penetration-testing/. • Packet sniffing by other tenants. Virtual instances are designed to prevent other instances running in promiscuous mode to receive or "sniff" traffic that is intended for a different virtual instance. While customers can place interfaces into promiscuous mode, the hypervisor will not deliver any traffic to them that is not addressed to them. Even two virtual instances that are owned by the same customer located on the same physical host cannot listen to each other's traffic. While Amazon EC2 does provide protection against one customer inadvertently or maliciously attempting to view another's data, as a standard practice customers can encrypt sensitive traffic. In addition, firewall devices are configured to restrict access to Amazon's corporate and production networks. The configurations of these firewall policies are maintained using an automatic push from a parent server every 24 hours. All changes to the firewall policies are reviewed and approved. Network devices, including firewall and other system boundary devices are configured to fail securely in the event of an operational failure. Boundary firewalls and load balancer devices are set to fail to deny all until the device's functionality is restored.
25	Remote Access	No remote access except compelling business Need. Parodic review of remote access approvals and configurations. Encrypted communication for remote access.	**This is a customer responsibility.**
26	Distributed Denial of service attacks(DDoS/DoS)	DDoS defense strategy with detective/preventive capability. Conduct code review, network design analysis and configuration testing.	**This is a shared responsibility when using AWS, as customers and AWS have different roles relevant to this topic.** The AWS Network consists of the internal data center facilities, servers, networking equipment and host software systems that are within AWS control and are used to provide the services.

No	RBI Guideline Reference	Key consideration / Recommendations	Customer Considerations
			The AWS Network provides significant protection against traditional network security issues. Please refer to row 24 above.
27	Implementation of ISO 27001 ISMS	Implement Information Security Management System (ISMS) best practices for their critical functions/processes.	**This is a shared responsibility when using AWS, as customers and AWS have different roles relevant to this topic.** The AWS implementation of and alignment with ISO 27001 demonstrates a commitment to information security at every level of the organization. AWS is assessed by an independent third-party auditor to validate alignment with the ISO 27001 standard. Compliance with these internationally-recognized standards and code of practice is evidence that the AWS security program is comprehensive and in accordance with industry leading best practices.
28	Wireless Security	Wireless Access devices connected to the corporate network must be registered and approved by Info Sec function of a bank. Implement authenticated access and prevent unauthorized device/access.	**This is a customer responsibility.**
29.	Business Continuity Considerations	Business continuity planning. Risk assessments for changing risks in business continuity scenarios	**This is a shared responsibility when using AWS, as customers and AWS have different roles relevant to this topic.** The AWS Business Continuity policy lays out the guidelines used to implement procedures to respond to a serious outage or degradation of AWS services, including the recovery model and its implications on the business continuity plan. Customers have the capability to implement a robust continuity plan, including the utilization of frequent server instance back-ups, data redundancy replication, and the flexibility to place instances and store data within multiple geographic AWS Regions as well as across multiple Availability Zones within each Region. Customers are responsible for properly implementing contingency planning, training and testing for their systems hosted on AWS.
30	Information security assurance	Penetration testing, audit and assessment.	**This is a shared responsibility when using AWS, as customers and AWS have different roles relevant to this topic.**

No	RBI Guideline Reference	Key consideration / Recommendations	Customer Considerations
			AWS has established a formal audit program that includes continual, independent internal and external assessments to validate the implementation and operating effectiveness of the AWS control environment. Internal and external audits are planned and performed according to the documented audit scheduled to review the continued performance of AWS against standards-based criteria and to identify general improvement opportunities. Standards-based criteria includes but is not limited to the ISO/IEC 27001,the American Institute of Certified Public Accountants (AICPA): AT 801 (formerly Statement on Standards for Attestation Engagements [SSAE] 16), and the International Standards for Assurance Engagements No.3402 (ISAE 3402) professional standards. Compliance reports from these assessments are made available to customers to enable them to evaluate AWS. The AWS Compliance reports identify the scope of AWS services and Regions assessed, as well the assessor's attestation of compliance. A vendor or supplier evaluation can be performed by leveraging these reports and certifications.
31	General information regarding delivery channels	Provision for various banking channels, periodic re-evaluation of past risk controls, raise security awareness. Securing internet banking.	**This is a customer responsibility.**

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[19] webpage.

For banks in India assessing use of AWS, next steps typically include the following:

- 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[20].
- Obtain and review a copy of the latest AWS System & Organization Control 1 & 2 reports, PCI-DSS Attestation of Compliance and Responsibility Summary, and ISO 27001 certification, from the AWS Artifact portal (accessible via the AWS Management Console).
- Consider the relevance and application of the CIS AWS Foundations Benchmark available at CIS Amazon Web Services Foundations[21], as appropriate for your cloud adoption and use cases. These industry-accepted best practices published by the Center for Internet Security go beyond the high-level security guidance already available, providing AWS users with clear, step-by-step implementation and assessment recommendations.
- Learn more about other governance and risk management practices as necessary as part of your due diligence and risk assessment, using the tools and resources referenced throughout this document and in the following Further Reading section.
- Speak to your AWS representative about an Enterprise Agreement, and the introductory guide designed to help Indian banks assess the Enterprise Agreement against the Guidelines on Outsourcing.

Further Reading

For additional help, see the following sources:

- AWS Best Practices for DDoS Resiliency[22]
- AWS Security Checklist[23]
- Cloud Adoption Framework - Security Perspective[24]
- Introduction to AWS Security Processes[25]
- AWS Security Best Practices[26]
- Encrypting Data at Rest[27]
- AWS Risk & Compliance[28]
- Using AWS in the Context of Common Privacy and Data Protection Considerations[29]
- Security at Scale: Logging in AWS[30]
- Security at Scale: Governance in AWS[31]
- Securing Data Centers by Design[32]
- Secure Content Delivery with CloudFront[33]

Document Revisions

Date	Description
December 2017	First publication

Notes

[1] http://aws.amazon.com/compliance

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

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

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

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

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

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

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

[9] https://aws.amazon.com/compliance/pci-data-privacy-protection-hipaa-soc-fedramp-faqs/

[10] https://d0.awsstatic.com/whitepapers/Security/AWS_Security_ Whitepaper.pdf

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

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

[13] http://phx.corporate-ir.net/phoenix.zhtml?c=97664&p=irol-irhome

[14] https://aws.amazon.com/security/security-bulletins/

[15] https://aws.amazon.com/marketplace

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

[17] https://aws.amazon.com/products/storage/

[18] https://status.aws.amazon.com/

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

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

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

[22] https://d0.awsstatic.com/whitepapers/Security/DDoS_White_Paper.pdf

[23] https://d0.awsstatic.com/whitepapers/Security/AWS_Security_Checklist.pdf

[24] https://d0.awsstatic.com/whitepapers/AWS_CAF_Security_Perspective.pdf

[25] https://d0.awsstatic.com/whitepapers/Security/Intro_Security_Practices.pdf

[26] https://d0.awsstatic.com/whitepapers/Security/AWS_Security_Best_Practices.pdf

[27] https://d0.awsstatic.com/whitepapers/AWS_Securing_Data_at_Rest_ with_Encryption. pdf

[28] https://d0.awsstatic.com/whitepapers/compliance/AWS_Risk_and_ Compliance_ Whitepaper.pdf

[29] https://d0.awsstatic.com/whitepapers/compliance/Using_AWS_in_the_ context_of_ Singapore_Privacy_Considerations.pdf

[30] http://d0.awsstatic.com/whitepapers/compliance/AWS_Security_at_ Scale_Logging_in_ AWS_Whitepaper.pdf

[31] http://d0.awsstatic.com/whitepapers/compliance/AWS_Security_at_ Scale_Governance _in_AWS_Whitepaper.pdf

[32] https://aws.amazon.com/compliance/data-center/

[33] https://d0.awsstatic.com/whitepapers/Security/Secure_content_ delivery_with _CloudFront_whitepaper.pdf