WHITEPAPER

Running (Non-Banking Financial Services) NBFC Workload on AWS

ABOUT AXCESS.IO

AXCESS.IO is a niche provider of Managed Cloud Services to the businesses worldwide and has served an ever-growing number of clients since its inception. In a relatively short period of time, AXCESS.IO has quickly become a niche consulting firm specializing in Cloud Advisory, Cloud Managed Services, and DevOps Automation.

www.axcess.io
+91- 80 889 20295 / +1 866 CLOUD
sales@axcess.io

NBFC IN INDIA

The Indian economy is one of the major global economies. As such, financial services in India are going through striking changes in financial service delivery; and stories in NBFCs and Fintech companies are not different. Now, you have to ask yourself why this transformation is essential to you or how it will impact you. In this article, you will understand:

- How to conduct and manage risks in outsourcing financial services by financial institutions
- How financial organizations can secure information, manage risks, and handle cyber frauds.

Keep reading this article to find out how banks can assess and implement a secure system.

OUTSOURCING FINANCIAL SERVICES BY BANKS IN INDIA

For AWS to work out for your business, you first have to understand how responsibilities are shared. Both the customer and AWS have to share responsibilities. The first responsibility they have to share is the security of their information. As depicted, the client is responsible for security **in** the cloud service. How so?

SECURITY IN THE CLOUD BY THE CUSTOMER

Customers maintain security in the cloud by choosing what content to store on AWS, the appropriate AWS service that fits the environment of a given content, the structure, and format, how customer data should be encrypted.

Also, the customer manages content access by granting or denying access to data. Amazon provides more profound information on how you can correctly manage security in the cloud. Also, more information on the clients' side of the Shared Responsibility model has been provided by AWS.

SECURITY OF THE CLOUD BY AWS

AWS is responsible for the safety **of** the cloud, as depicted in the Shared Responsibility Model. You may wonder to yourself how AWS maintains such a remarkable record in securing customer data. AWS continually audits its infrastructure, and then services are approved to operate under their compliance standards and industry certifications. Then, customers use those certifications to authenticate the effectiveness of these AWS security control measures. AWS has got more than 2,500 security controls in which a customer can download detailed reports on AWS Artifact. The AWS Artifact is an automated portal, which generates compliance reports available on the AWS Management Console.

In addition to that, Amazon Regions helps customers choose their zones or geographic specifics where the servers storing their content will be located. For the case of financial institutions in India, selecting Asia Pacific (Mumbai) will be an excellent idea. AWS Asia Pacific (Mumbai) region offers detailed compliance standards by providing high levels of security to its global customers. The Asia Pacific (Mumbai) region is very compliant, and not only does it apply national data protection laws, but it also applies the global data protection laws.

GUIDELINES ON OUTSOURCING FROM THE RESERVE BANK OF INDIA

The Reserve Bank of India (RBI) has set some guidelines on outsourcing to help Non banking Financial Companies (NBFCs) manage risks and also provide guidance on the evaluation of a service provider, identify risks associated with outsourcing to that provider and enter into written agreements that address those risks.

Then, these guidelines provide steps to protect and preserve customer data. The RBI guidelines for NBFCs can be found here:

https://www.rbi.org.in/scripts/FS_Notification.aspx?Id=11160&fn=14&Mode=0

We have reviewed the compliance of the RBI guidelines and prepared a detailed report.

ASSESSMENT OF SERVICE PROVIDERS

REFERENCE

RBI Guideline Section 5.4.2

COMPLIANCE REPORT

Due Diligence Requirement	**Responsibility**	**AWS Compliance**
Past experience and competence to implement and support the proposed activity over the contracted period.	Service Provider	Fully complied Gartner has consistently named AWS as leader in it's vision and ability to deliver services.
Financial soundness and ability to service commitments even under adverse conditions.	Service Provider	Fully complied AWS is one of the biggest companies by market capitalization in the world. This is ranked No 5 in Fortune 500 list.
Business reputation and culture, compliance, complaints and outstanding or potential litigation.	Service Provider	Fully complied AWS is ISO 27017 certified.
Security and internal control, audit coverage, reporting and monitoring environment, business continuity management.	Service Provider	Fully complied AWS is ISO 27017 certified.
Ensuring due diligence by service provider of its employees.	Service Provider	Fully complied AWS is ISO 27017 certified.

CONFIDENTIALITY AND SECURITY

REFERENCE

RBI Guideline Section 5.6

COMPLIANCE REPORT

Due Diligence Requirement	**Responsibility**	**AWS Compliance**
5.6.1 Public confidence and customer trust in the NBFC is a prerequisite for the stability and reputation of the NBFC. Hence the NBFC shall seek to ensure the preservation and protection of the security and confidentiality of customer information in the custody or possession of the service provider.	NBFC	NA

5.6.2 Access to customer information by staff of the service provider shall be on 'need to know' basis i.e., limited to those areas where the information is required in order to perform the outsourced function.	Shared	Fully Complied **Tools** AWS IAM provides mechanism to manage user, role and access policy
5.6.3 The NBFC shall ensure that the service provider is able to isolate and clearly identify the NBFC'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 NBFCs, care shall be taken to build strong safeguards so that there is no comingling of information / documents, records and assets.	Shared	Fully Complied **Tools** AWS VPC is a logically isolated network
5.6.4 The NBFC shall 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.	Shared	Fully Complied **Tools** AWS provides a number of tools like CloudTrail, GuardDuty and Security Hub to manage all controls.
5.6.5 The NBFC shall immediately notify RBI in the event of any breach of security and leakage of confidential customer related information. In these eventualities, the NBFC would be liable to its customers for any damages.	Shared	Fully Complied **Process** AWS is ISO 27001 certified company.

CONTINUITY IN BUSINESSES AND MANAGEMENT OF DISASTER RECOVERY

REFERENCE

RBI Guideline Section 5.6

COMPLIANCE REPORT

Due Diligence Requirement	Responsibility	AWS Compliance
5.8.1 An NBFC shall require its service providers to develop and establish a robust framework for documenting, maintaining and testing business continuity and recovery procedures. NBFCs need to ensure that the service provider periodically tests the Business Continuity and Recovery Plan and may also consider occasional joint testing and recovery exercises with its service provider.	Shared	AWS has a well document business continuity and recovery plan. This is well documented in their SOC2 compliance report.
5.8.2 In order to mitigate the risk of unexpected termination of the outsourcing agreement or liquidation of the service provider, NBFCs shall retain an appropriate level of control over their	NBFC	

outsourcing and the right to intervene with appropriate measures to continue its business operations in such cases without incurring prohibitive expenses and without any break in the operations of the NBFC and its services to the customers.		
5.8.3 In establishing a viable contingency plan, NBFCs shall consider the availability of alternative service providers or the possibility of bringing the outsourced activity back in-house in an emergency and the costs, time and resources that would be involved.	NBFC	
5.8.4 Outsourcing often leads to the sharing of facilities operated by the service provider. The NBFC shall ensure that service providers are able to isolate the NBFC's information, documents and records, and other assets. This is to ensure that in appropriate situations, all documents, records of transactions and information given to the service provider, and assets of the NBFC, can be removed from the possession of the service provider in order to continue its business operations, or deleted, destroyed or rendered unusable.	Shared	AWS has services and tools to isolate customer's compute, storage and network instances within AWS public cloud. However, customer needs to protect it's information within it's own account.

OFFSHORE OUTSOURCING OF FINANCIAL SERVICES

RBI has a detailed guideline to de-risk the NBFC operation arising out of issues created by any geo-political situation.

AWS fully complies to all the requirement mandated in this section. AWS offers it's services in India through an entity named Amazon Internet Services Private Limited (AISPL). Customers also have option to provision their resources completely in AWS Mumbai region.

CONCLUSION

As the Indian economy is transforming to be a digital economy that provides financial services to people, financial institutions in India have to consider the changes that this transformation will bring. Factors that have to be considered are compliance regulations provided by the Reserve Bank of India for implementing security and business continuity to preserve and protect customer information.

All this can be executed well by thoughtfully examining the Shared Responsibility Model, where both the customer and AWS share responsibilities. The customer has responsibilities that entail security **in** the cloud. AWS, on the other hand, has responsibilities for the safety **of** the cloud.

Customers should be careful of what services they opt to use on AWS as these services directly affect them legally.