BERAR FINANCE LIMITED

CLOUD ADOPTION POLICY

RECORD OF REVIEW:

Document Number	01
Version Number	02
Document Classification	External
Originally formulated	March 30,2023
Created by	IT Department
Reviewed by	IT Strategy Committee
Approved by	Board of Directors of the Berar Finance

Version No.	Created/Modified Date
1	March 30,2023
2	May 23, 2024

1. Purpose

Organizations are increasingly moving infrastructure and operations to hosted providers to provide data and tools to employees efficiently and cost-effectively. Berar Finance Limited has also moved towards deployment of the Cloud or usage of cloud-based applications (Software As a Service) platforms.

Cloud adoption and security policy aims to establish guidance and process framework to assess the operational and security capabilities of Cloud Service Providers ("CSP") to provide better service delivery and determine compliance with Berar Finance Limited's ("Berar Finance").

The Technology Team is responsible for and committed to managing the confidentiality, integrity, and availability of Berar Finance's networks, systems, and applications within the scope of its authority. This includes ensuring wherever possible that cloud environments hosting Berar Finance's infrastructure meet specified security controls and do not endanger the security requirements of Berar Finance.

2. Definitions

Cloud Service Provider ("CSP"): Any organization that offers some component of cloud computing — typically Infrastructure as a Service ("IaaS"), Software as a Service ("SaaS") or Platform as a Service ("PaaS") — to other businesses or individuals.

International Organization for Standardization ("ISO"): An international standard-setting body composed of representatives from various national standards organizations that promotes proprietary, industrial, and commercial standards.

Operating System ("OS"): System software that, after being initially loaded into the computer by a boot program, manages all the other programs in a computer.

Personally Identifiable Information ("PII"): Any information that can uniquely identify people as individuals, separate from all others is PII. It may include names, addresses, emails, birthdates, medical records, credit card numbers, etc.

XLAs: An Experience Level Agreement, or XLA, is an experience metric that measures the gap between the experience you are delivering now, to your employees or customers, and the experience you want to be providing.

SLA: A service-level agreement ("SLA") sets the expectations between the service provider and the customer and describes the products or services to be delivered, the single point of contact for end-user problems, and the metrics by which the effectiveness of the process is monitored and approved.

Infrastructure as a Service ("IaaS"): A cloud computing service where enterprises rent or lease servers for computing and storage in the cloud. Users can run any operating system or applications on the rented servers without the maintenance and operating costs of those servers.

Platform as a Service ("PaaS"): Complete cloud environment that includes everything developers need to build, run, and manage applications—from servers and operating systems to all the networking, storage, middleware, tools, and more.

Software as a service ("SaaS"): A way of delivering applications over the Internet—as a service. SaaS applications are also known as Web-based software, on-demand software, or hosted software.

3. Scope

This Policy applies to all of Berar Finance's managed IT Systems, Infrastructure, as well as Applications that are hosted in cloud infrastructure or Software-As-a-Service platforms delivered through public clouds. The technology department will be responsible for defining cloud adoption model and enforcing the security of cloud environments wherever possible by the requirements in this Policy.

4. Cloud Adoption Policy

4.1 Cloud Strategy

Berar Finance Limited's cloud strategy shall align with IT strategy and business strategy, which is to enable business growth on scale and create frictionless customer experience through open technologies that are flexible, secure, and faster.

Objectives of movement to the cloud will be to increase agility, provide faster service and newer technologies to customers and increase retention and revenues, operational efficiency by providing resources on-demand faster, being consistent in security compliance through automation, and reduce spending on capital expenditure.

4.2 Cloud Governance

Berar Finance shall establish and present a well-documented policy for cloud adoption. This policy should, among other things, specify the activities suitable for cloud migration, safeguard stakeholder interests, and ensure regulatory compliance, including privacy, security, data sovereignty, recoverability, and data storage requirements in line with data classification.

The policy shall also include provisions for thorough due diligence to manage and continuously monitor risks associated with Cloud Service Providers.

4.2.1 Requirements before moving to the Cloud

- Business drivers and goals stating the need for cloud adoption will be reviewed and approved by Berar Finance Limited's IT steering committee.
- The technology team shall evaluate on process for the adoption of a cloud solution to align with the existing business strategy, the goals adopted to the current IT application landscape, and associated costs.
- The adoption of cloud solutions varies from transferring only non-critical workloads to migrating essential business applications, such as adopting Software as a Service (SaaS). This decision should be based on a thorough business technology risk assessment.
- The Berar Finance may explore conducting multiple proof of concept (POCs) before moving application services to the cloud.
- Berar Finance shall review installed computing resources capacity and peak usages to determine systems that are feasible to move to the cloud.
- Data portability, interoperability of systems, and application portability as well as reverse migration requirements shall be reviewed.
- The interoperability of the systems involved will be reviewed.
- Overall technology architecture shall be assessed to incorporate a new cloud stack.
- Applications feasibility for re-architecting to provide micro-services that connect with cloud-native APIs will be reviewed.
- Cost savings analysis for various cloud deployment models will be reviewed.
- Cloud deployment and service models will be chosen by Berar Finance after carefully considering data privacy, data security, data, and service availability, costs and return on investments, operational and support requirements, and regulatory requirements.
- Risk assessments will be done before moving any application or service to the cloud.

4.2.2 Requirements Analysis – Roles and Responsibilities

IT Steering Committee	Evaluate key business drivers and state goals for cloud adoption.
Compliance Team	Review regulatory authority requirements
CISO Team	Provide security requirements as well as review security controls
Technology Team	Provide capacity utilization reports across storage, network, and application usage for at least 6 months
	Evaluate data portability, systems interoperability, and application portability requirements.
	Conduct Proof of Concepts and pilot implementations.
	Cost savings analysis
	Evaluate data security and access controls
	Select cloud deployment and service models

5. Selection of Cloud Service Provider

Berar Finance Limited shall ensure that cloud providers with proven expertise and reputation will be chosen through a thorough risk assessment. This includes cloud-based application selection. The critical factor for selection is to have a cloud setup of partners in India for all data localization requirements.

Subject to jurisdictions that uphold the enforceability of agreements and the rights available thereunder to Berar Finance Limited, including those relating to data storage, data protection, and confidentiality.

5.1 Cloud Provider Selection Criteria

Cloud provider selection criteria should cover, but not limited to:

- Redundant and High availability data centers located in India.
- Vetting process of personnel
- Quality and frequency of security and privacy awareness training provided to personnel.
- Security services provided
- Adoption of new technologies
- Change management procedures and processes.

Service level agreements (SLA) with cloud providers will be put in place. SLA terms should cover the following:

- Service levels and associated costs
- Service performance monitoring criteria
- Data security and privacy
- Data ownership with NBFC
- Data/Application isolation (from other tenants)
- Data storage location, computing resources location.
- Data preservation period
- Service availability
- Roles and responsibilities of Cloud provider and NBFC
- Sub-contracting by Cloud provider
- Regulatory requirements
- Right to audit
- Incident management
- Backup and recovery
- Security and vulnerability scanning
- Continued certification and accreditation
- Independent auditing of services
- Penalties
- Background vetting of employees

- Conditions for termination of services
- Exit rights.
- Data transfer / secure deletion after termination.

5.2 Selection of Cloud Service Provider – Roles & Responsibilities

Technology Team	Cloud provider screening and recommendation
	Monitor the performance of the Cloud provider
	Service Level Agreements / Contracts with Cloud provider
Business Team (in case of application deployment on the SAAS model)	Evaluation of features and journeys & flows

For SAAS application selection, the IT policy shall be referred for application acquisition, development & deployment.

5.3 Cloud Security Requirements

For defining security requirements for the cloud, the Technology shall refer to IS & Cyber policy for guidance. Below are controls, but not limited, to focus on for onboarding of cloud partner:

- Secure all administrative interfaces to prevent unauthorized access.
- Encrypt all customer, transactional, and authentication data.
- Establish systems for detecting and preventing data leaks.
- Deploy endpoint protection software on all virtual guest systems.
- Activate and monitor logging for database and storage API access.
- Use encryption for logs containing customer activities and application data.
- Separate duties among cloud administrators to reduce risks.
- Regularly update virtual machine images with the latest security patches.
- Establish baselines for virtual machine guests to ensure consistent security standards.
- Maintain detailed tracking of virtual machine hypervisor vulnerabilities and their mitigations.
- Design applications to avoid storing any sensitive or customer-related information in an unencrypted form on cloud servers.
- Retain exclusive ownership and control over data encryption keys.
- Regularly review the security of client/customer web browsers and their plug-ins/extensions for vulnerabilities.
- Divide security responsibilities between Berar Finance Limited and the Cloud Service Provider (CSP) per the shared responsibility model.
- Implement a federated identity management system to manage users across both the cloud provider and Berar Finance Limited.
- Enforce strict authentication and access controls for all applications and information assets.
- Conduct redundancy tests for cloud services biannually to ensure reliability.
- Perform comprehensive logging and threat analysis across various cloud components.
- Implement web application firewalls and Denial of Service protection systems to safeguard cloud systems and services.
- Rigorously apply network segmentation to separate web interfaces, applications, and database/storage APIs.
- Operate test and development networks independently from production networks and prohibit the use of production data in test environments.
- Control the migration of code from testing/UAT environments to production systems by adhering to Berar Finance Limited’s change management processes.

Implementation of Security Requirements

Technology team	Cloud systems baselining, patching, installation of endpoint protection software and monitoring software, incident response
	Security events logging and monitoring, scanning for sensitive data, data leakage detection, web application firewalls, incident response
	Network segmentation
	Identity and access roles provisioning
	Review implementation of separation of duties

6. Cloud Service Management and Security Considerations

6.1 Service & Technology Architecture

The architecture supporting cloud applications must comply with internationally recognized principles and standards.

Prefer architectures that offer secure container-based data management, with encryption keys and Hardware Security Modules

Architecture should provide standard tools and processes to manage containers, images, and releases. It should safeguard multi-tenant environments against risks to data integrity and confidentiality and prevent data co-mingling.

Architecture should be resilient, allowing for seamless recovery with minimal data security impact in case of any component failure.

6.2 Identity and Access Management

Berar Finance Limited and the Cloud Service Provider should agree on Identity and Access Management (IAM) that provides role-based access to cloud-hosted applications involving strict access controls, similar to those used for on-premises applications.

Segregation of duties and a role conflict matrix should be implemented for all user-access and privileged-access roles, regardless of the cloud service model.

Access provisioning should follow the principles of 'need to know' and 'least privileges. Multi-factor authentication should also be implemented for access to cloud applications.
resources, proper and secure configurations and monitoring of the cloud assets, and procedures for authorizing changes to cloud applications and related resources.

6.3 Robust Monitoring & Surveillance

Berar Finance Limited should define minimum cloud monitoring requirements. They must assess the Cloud Service Provider’s information/cyber security capability to ensure:

- The Cloud Service Provider has a security policy framework that aligns with its exposure to vulnerabilities and threats.
- The Cloud Service Provider can maintain its security capability considering changes in threats or vulnerabilities, including those from changes to information assets or its business environment.
- The Cloud Service Provider's control testing frequency and nature align with the materiality of outsourced services and threat environment.
- The Cloud Service Provider has mechanisms to assess subcontractors regarding data confidentiality, integrity, and availability, where applicable.

6.4 Integration of Logs & Events

Berar Finance Limited should integrate logs and events from the Cloud Service Provider into Berar Finance Limited’s SOC where applicable or retain relevant cloud logs for incident reporting and management related to cloud services.

6.5 Cyber Resilience Controls

The Cloud Service Provider's cyber resilience controls should supplement Berar Finance Limited's application security efforts. Both parties should ensure regular, continuous updates of security-related software, including upgrades, fixes, patches, and service packs, to protect against advanced threats/malware.

6.6 Vulnerability Management

Berar Finance Limited should confirm that Cloud Service Provider employs a well-governed, structured approach for managing threats and vulnerabilities, supported by suitable industry-specific threat intelligence capabilities.

7. Risk Management

Berar Finance Limited will ensure the risk management process covers risks arising out of taking cloud services.

- Review of third-party and subcontracting risk
- Review of Service availability and business continuity plans
- Legal and regulatory compliance risks
- Consider specific factors related to cloud service, such as multi-tenancy and multi-location data storage/processing while integrating cloud services,

Risk assessments will be conducted for cloud providers, applications, and services provided from the cloud at least annually or after any major change.
Identified risks and their mitigation status will be reported to the operational risk committee (ORCO) of the Bank

7.1 Risk Management – Roles & Responsibilities

Risk Team	Conduct a risk assessment for cloud provider, cloud service delivery, and customer services.
IT Steering Committee	Review of risk vs benefit and decide to move services to the cloud.

8. Training & Awareness

Cloud administrators including network administrators, database administrators, storage administrators, and security administrators shall be provided with requisite training and awareness of operations and associated risks.

9. Disaster Recovery & Cyber Resilience

The business continuity framework must support critical operations, even in case of a cloud services disaster or CSP failure, minimizing service disruption while maintaining data security and integrity.

CSP's cyber resilience readiness must involve robust incident response, recovery practices, and regular Disaster Recovery (DR) drills involving relevant stakeholders.

10. Exit Strategy

Berar Finance Limited shall evaluate the following while developing an exit strategy and draw reference from the Exit Strategy in the IT Outsourcing Policy:

- The exit strategy and SLA should consider agreed processes for returning Berar Finance Limited’s data and service collateral, data portability, secure data purging, smooth service transition, and clearly defined liabilities and penalties.
- Align exit plans with the ongoing design of applications and service delivery technology stack.
- Contractually agreed exit plans should detail how services and data will be removed from the cloud with minimal business impact while maintaining integrity and security.
- Prompt and systematic takeover of all transaction, customer, and operational data from the CSP should be ensured, followed by data purging at the CSP's end with independent assurance before final sign-off.

11. Audit & Assurance

Internal audit team shall plan for IS Audit of cloud setup or SAAS based application as per IS Audit policy.