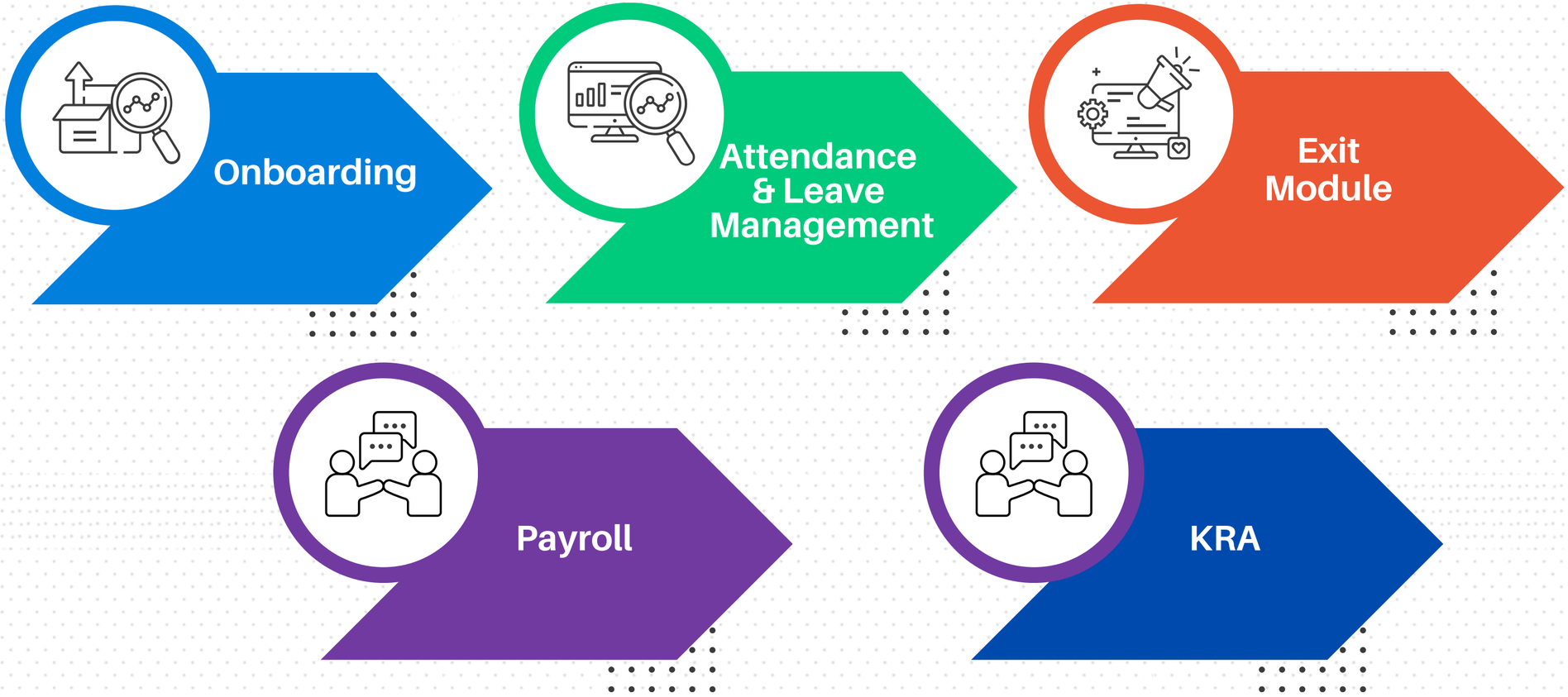
Application ERA of LIFC

Business Application			Customer Service	Internal Use
Sales App	Syno Collection	LOS	Dialler	HRMS
Syno LMS	Business 360 MS Dynamic	Credit App	Whatsapp Chatbot	Email
CRM	Laxmi Mitra	Vendor Suite (Legal & Technical)	Messaging	AIMS
				VISITOR APP

HRMS


Onboarding
Attendance & Leave Management
Exit Module
Payroll
KRA

EMAIL

01

Cloud base mail service used by us

02

Internal department mail communication is used privately.

03

Outside mail sending and its monitoring.

04

Group message communication can be sent.

Loan Origination System (LOS)

01

Integration Capabilities With API, Various Mobile App

02

Automatic Document Identification

03

Powerful Automation Of Loan And Customer Details

04

360-degree Customer And Loan Reports

05

User-Friendly Interface

06

Lead To Disbursal Loan Journey

SynoCollection App

01

EMI Collection from Customer

02

Visit Capturing of Field Executive

03

Case Allocation / DE Allocation

AIMS

01

Asset Requestion and Request

02

Asset Allocation and Approval

03

Inventory Management and Reports

Dialler

Answering Machine Detection

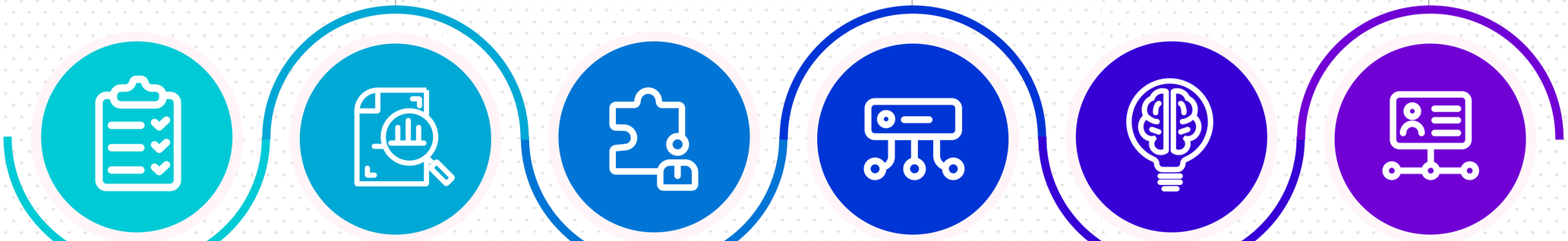
Call back Scheduling and reminders

Report & Analytics

Call Recording

Do Not Call Management

Campaign Management



Business 360 MS Dynamic

01

Get everything you need to run your business with Dynamics 365 Business Central

02

Audit Trail for all transaction

03

A platform for a complete accounting solution

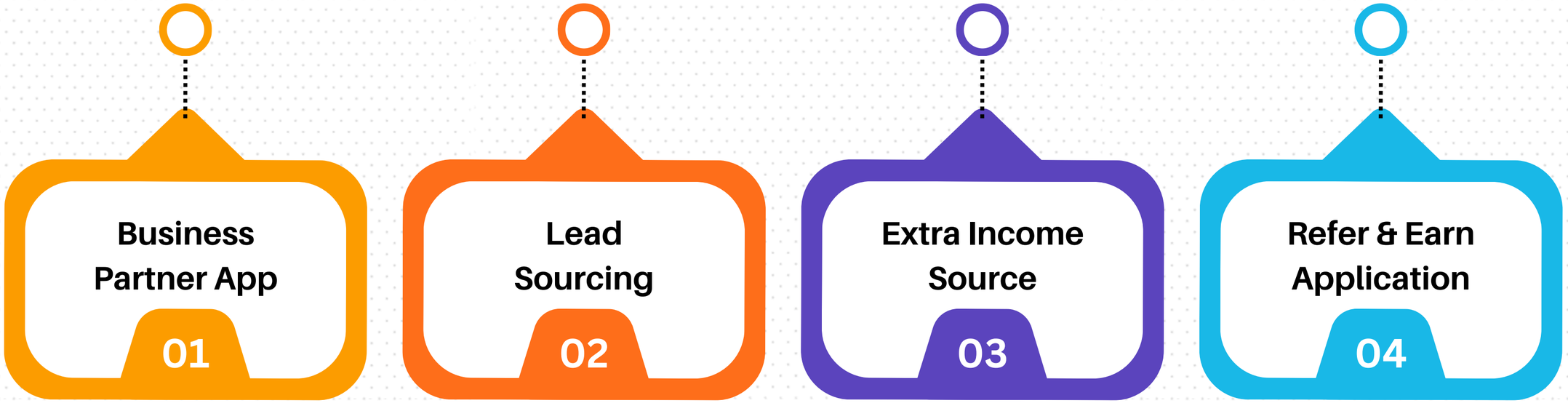
04

Easy-to-use cloud base application

05

Smart reports and easy to Customization

Laxmi Mitra


Business Partner App
01
Lead Sourcing
02
Extra Income Source
03
Refer & Earn Application
04

Syno LMS

01

Exact Information Related To Loan Customer

02

Finance/ Disbursal

03

Manage Customer Loan Deposit

04

Manage Customer Loan Accounts

05

Maintain Customer and loan Compliance Query

Credit App

01

Personal Discussion (PD) Management

02

Profile-Based/Income-based/Property-based Questions

03

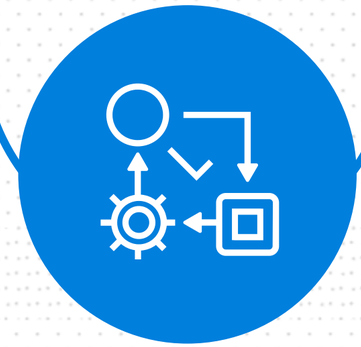
Digital KYC/Property Papers/ Credit Bureau Verification

04

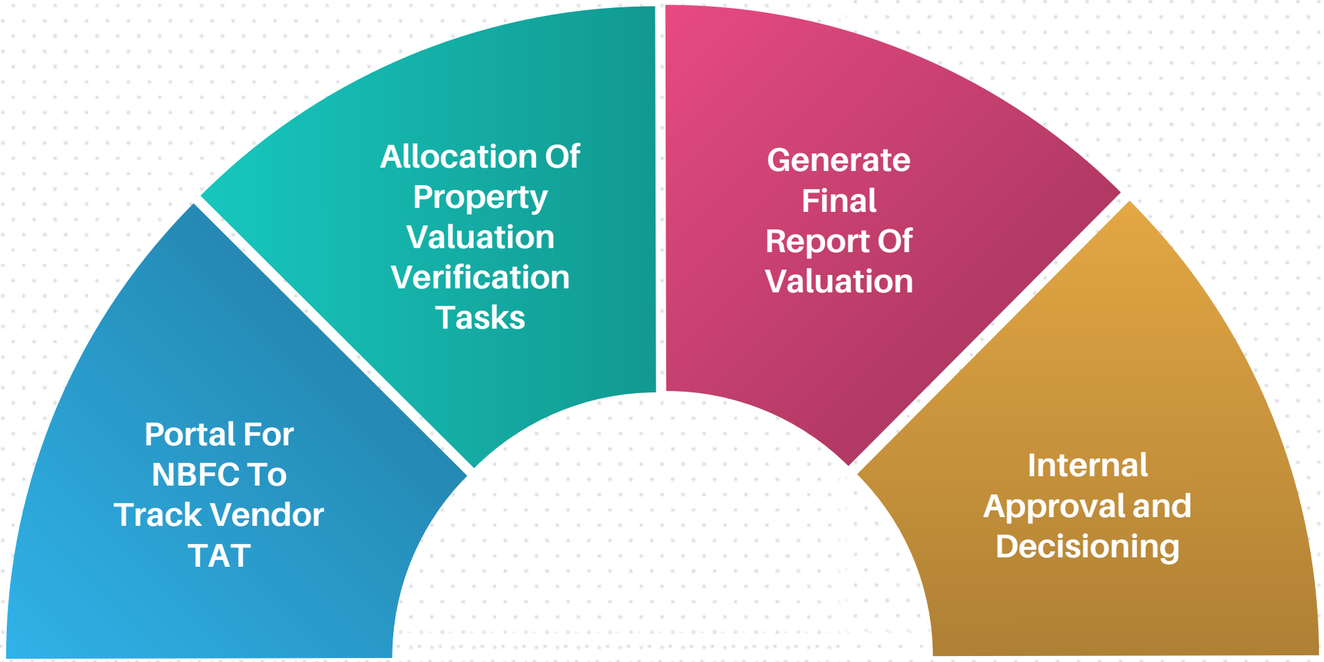
Digitization Sanction Process

05

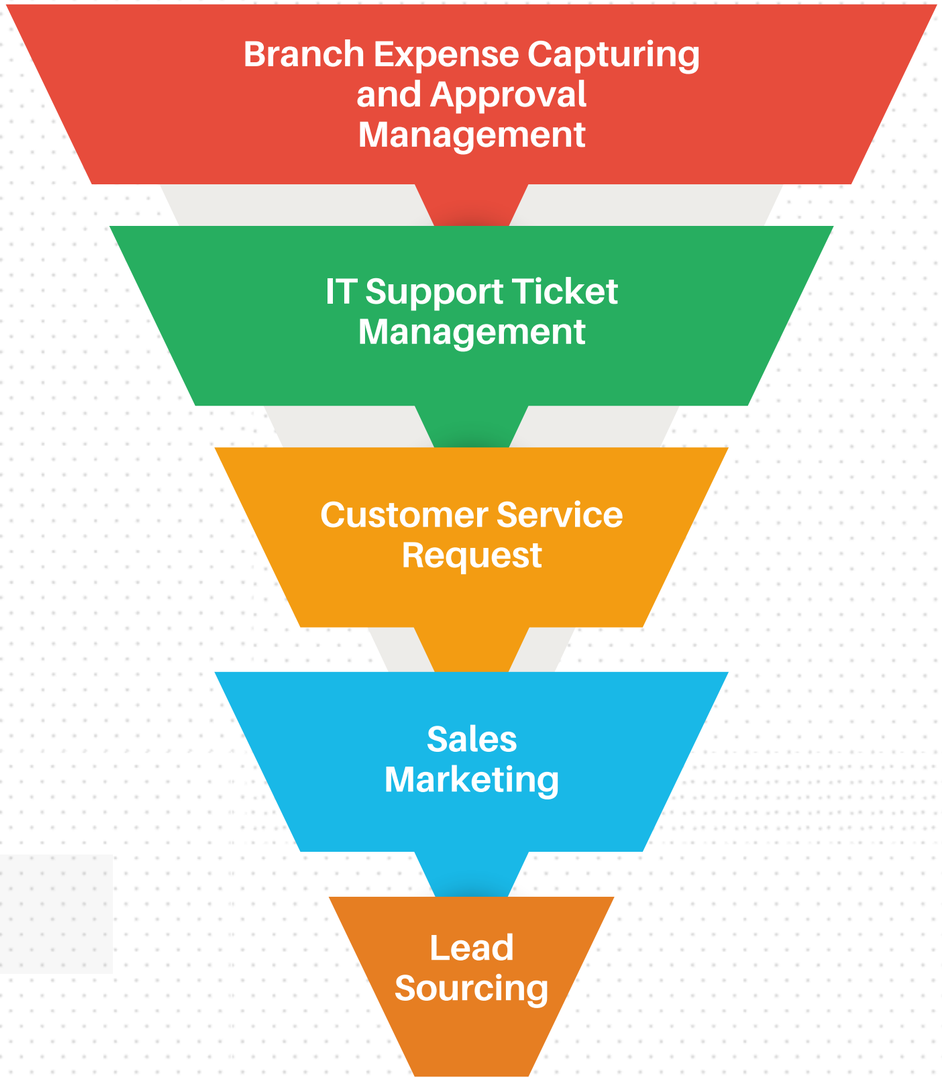
Integration capability, Google location, Credit bureau's and KYC verification



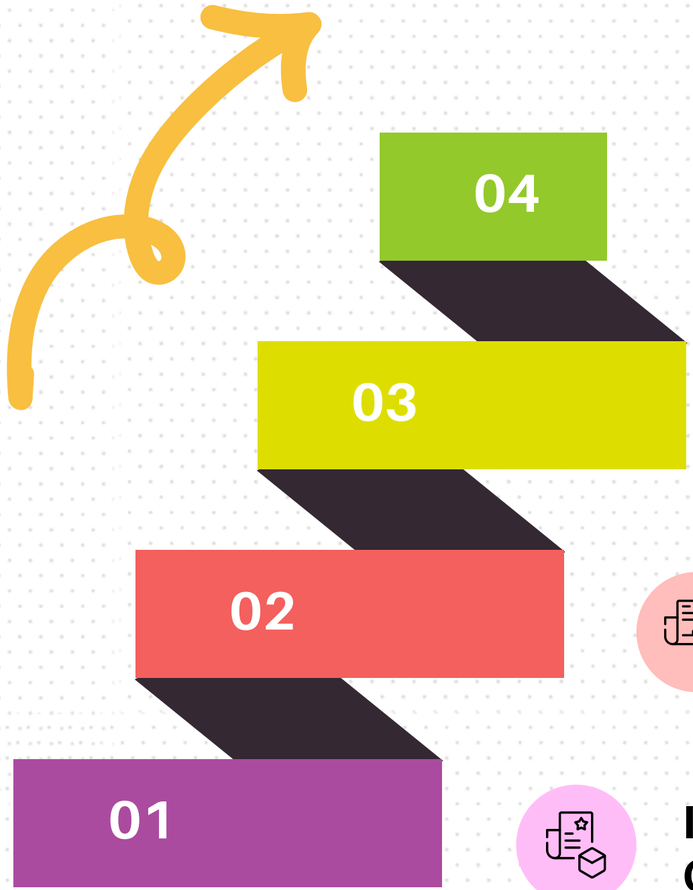
VENDOR SUITE (LEGAL & TECHNICAL)



CRM



SALES APP



Paper Less Digital Loan Journey

Lead Management System

Tracking Customer Loans

Intergration Cabilities

MESSAGING & WHATSAPP CHATBOT

- EMI Reminder
- EMI Bounce Alert
- Promotional offer
- New Updates

VISITOR APP

VISITOR MANAGEMENT

Simplify check-in/out and capture visitor details like name and contact number.

APPOINTMENT BOOKING

Schedule visits with required information.

CUSTOMER DETAILS CAPTURE

Securely collect visitor information for record-keeping.

ALERT NOTIFICATIONS

Keep staff informed of arrivals and changes.

FEEDBACK COLLECTION

Gather visitor feedback for improvement

New Automations

01 Collection App

- Automated visit scheduling with real-time tracking for field agents.
- Seamless payment integration supporting autopay across multiple gateways.
- Customizable reports with one-click generation for performance insights.

02 LOS Revamping

- Improved user interface for ease of use.
- Automation of workflows, reducing manual intervention.
- Enhanced risk assessment and loan eligibility determination.
- Advanced analytics for monitoring loan performance and optimizing loan approval rates.

03 Esign & Estamping Integration

- Legally binding electronic signatures, ensuring compliance with regulatory standards.
- Automated e-stamping for official documentation, eliminating the need for physical stamps.
- Real-time document processing with secure data encryption.

New Automations

04 Document Scan

- Collect Customer Document
- Scan Document In Docket Format
- Start Verification of Customer documents
- Query Resolution within various department users
- Complete Digital Disbursement Process

05 BRE Integration

- Flexible rule management that allows easy modifications without coding.
- Automated decision-making in areas such as loan approval, risk assessment, and compliance.
- Seamless integration with core systems for real-time rule enforcement.

06 Customer App

- Service request facility related to his loan
- Allow Customers EMI deposition online
- Platform given to customer for raise loan related query
- Refer Loan to company
- Updation of company Schemes and notification

IT ERA OF LIFPL

01

Firewall

Filters network traffic to prevent unauthorized access.

02

Antivirus (AV)

Detects and removes malware from endpoints.

03

Data Loss Prevention (DLP)

Controls sensitive data movement to prevent leaks.

04

Intrusion Detection/Prevention Systems (IDS/IPS):

Monitors for and blocks suspicious network activity.

05

Email Security

Protects against email-based threats like phishing and malware.

10

Vulnerability Management

Identifies and patches security vulnerabilities promptly

09

Security Training

Educates employees on cybersecurity best practices.

08

Compliance with RBI Regulations

Ensures adherence to industry security standards.

07

Encrypted Backup

Secures backup data to prevent unauthorized access.

06

Zero Trust Network Access (ZTNA)

Grants network access based on strict identity verification.

IT-INFRA

Risk Category	Risk	Mitigation
Cyberattacks		
Malware	Unauthorized system modifications by users with administrative privileges.	Install antivirus software on all devices and update it regularly. Train staff to recognize suspicious emails and links. Regularly check antivirus sync status with users.
Phishing	Unauthorized external email communication.	Teach employees how to spot phishing attempts. Use email filters to catch phishing emails
Human Error		
User awareness	Lack of knowledge about common threats and how to mitigate them.	We run the "Secure Laxmi" campaign where we conduct security awareness programs to educate staff about common threats and how to avoid them. Encourage a culture of security awareness.
Data Loss		
Hardware failure	Data loss due to file server failure or corruption.	Have backup systems ready and keep important files securely backed up offline. Encourage employees to store important files on the file server for regular backups.
Human error	Accidental or malicious data leakage via email.	Implement DLP solutions on each user's system to prevent unauthorized sharing of sensitive information via any medium.
Software Vulnerabilities		
Patch management	Failure to update software with the latest security patches.	Keep software up to date with the latest security patches. Periodically check antivirus sync status with users.
Vulnerability scanning	Undetected security weaknesses in software and systems.	Regularly scan for and fix security weaknesses in software and systems.
Lack of Scalability		
Scalable architecture	Inability to adapt IT systems to accommodate business growth.	Design IT systems to grow with the business. Use cloud services for flexible resources. Ensure cloud backups are encrypted with passwords.
Cloud services	Dependence on insufficiently scalable cloud resources.	Utilize cloud services for easy scalability and dynamic resource allocation.
Compliance Violations		
Regulatory compliance	Non-compliance with regulatory requirements and industry standards.	Stay informed about relevant regulations and industry standards. Regularly audit systems for compliance. Implement controls to address any compliance gaps. Ensure IT policy compliance with RBI regulations.

Risk Category	Risk	Mitigation
Additional Measures		
Asset theft	Theft or unauthorized use of company assets.	Have employees sign asset allocation agreements to deter theft.
Network vulnerability	Vulnerabilities in network infrastructure leading to potential breaches.	Maintain two firewalls for redundancy to mitigate the risk of network breaches if one fails.
Active Directory Security		
User access rights	Unauthorized system modifications by users with administrative privileges.	Enforce user rights without administrative privileges to prevent unauthorized system modifications. Ensure passwords are changed every 15 days with a minimum of 8 characters.
Application restrictions	Installation of unauthorized or potentially harmful applications.	Restrict access to unauthorized applications, to prevent potential security risks.
File server backup	Data loss due to file server failure or corruption.	Regularly backup files stored on the file server to protect against data loss and ensure business continuity.
Application server and database server backup	Data loss or unavailability of critical application and database data.	Backup application server and database server data three times a day, both in the cloud and physically, to ensure data integrity and availability.
Mail Server Security		
Restricted outgoing mail	Unauthorized external email communication.	Configure the mail server to only allow sending emails within the company domain. Implement two-factor authentication and encryption for email communication. Implement attachment restrictions in emails.
Data Loss Prevention (DLP)	Accidental or malicious data leakage via email.	Install DLP solutions on each user's system to prevent unauthorized sharing of sensitive information.
Branch Security		
Zero Trust Network Access (ZTNA)	Unauthorized access to company systems from branch locations.	Implement ZTNA solutions on branch systems to restrict access to company applications only.
Branch audits	Security breaches or non-compliance issues at branch locations.	Conduct regular audits of branch systems and networks to ensure compliance with security policies and detect any vulnerabilities or anomalies.
Network Security		
MAC Binding	Unauthorized access to the network by unknown devices.	Implement MAC binding for both Wi-Fi and LAN access to ensure that only authorized devices can connect to the network.
Guest Wi-Fi	Risk of unauthorized access to the network by visitors.	Provide a separate guest Wi-Fi network that does not allow access to internal resources or systems.
Strong Firewall Policy	Unauthorized access to the network by malicious entities.	Implement and regularly update a strong firewall policy to block unauthorized access and prevent security breaches.
Vulnerability Assessment and Penetration Testing (VAPT)	Presence of vulnerabilities in IT infrastructure.	Conduct regular VAPT assessments by external experts to identify and address any vulnerabilities in the IT infrastructure. Ensure IT infrastructure is free of vulnerabilities identified in VAPT assessments.