

IT OUTSOURCING POLICY



Infina Finance Private Limited [Infina]
7th Floor, Dani Corporate Park,
158, C.S.T Road, Kalina,
Santacruz (East), Mumbai-400098
India

INTERNAL

Table of Contents

Background.....	3
Purpose.....	3
Scope	3
Out of Scope	3
Owner	4
Review Frequency and Approving Authority.....	4
Definition	4
Policy Statement.....	4
High Level Actions	5
Annexure	5
References	6
Document Control	6

Background

For delivering innovative and rapid services to the Customer, Infina Finance Private Ltd. (also referred as "Infina" or "the Company") has to rely on third party services related to Information Technology (IT) activities and IT enabled Services (ITeS) to support Infina's business model and products offered to the customers. This document directs the policy of Infina for outsourcing of IT activities/ services based on the circular number RBI/2023-24/102 DoS.CO.CSITeG/SEC.1/31.01.015/2023-24 dated April 10, 2023 issued by RBI with a subject Master Direction on Outsourcing of Information Technology Services.

Purpose

Outsourcing of IT activities/ services lead to variety of risks like cyber security, privacy, regulatory and/ or legal etc. Infina shall have to establish a framework or process to decide the materiality of the IT activity/ service to be outsourced, identify and mitigate the probable risks throughout the outsourcing life cycle of IT activities or services and to achieve the necessary compliance to the information/ cyber security related policies of the Company devised in-line with applicable regulatory / legal requirements.

Scope

The third party service providers/ vendors delivering below listed IT activities / services are falling in the scope of this policy:

- a IT infrastructure management, maintenance and support (hardware, software or firmware);
- b Network and security solutions, maintenance (hardware, software or firmware);
- c Application Development, Maintenance and Testing; Application Service Providers (ASPs);
- d Services and operations related to Data Centres;
- e Cloud Computing Services;
- f Managed Security Services; and
- g Management of IT infrastructure and technology services associated with payment system ecosystem.

This policy shall be immediately applicable for the third party getting onboarded post Board approval of the policy.

For existing vendors of Infina, the vendor continuity shall be assessed and the relevant compliance activities shall be carried out post Board approval of the policy for those vendors whose services will be continued for more than 2 months. For such vendors, the compliance to this policy shall be achieved within maximum of 5 months post approval of the policy.

Out of Scope

- A. Services / Activities not considered under the scope of this policy : Corporate Internet Banking services obtained by regulated entities as corporate customers/ sub members of another regulated entity, External audit such as Vulnerability Assessment/ Penetration Testing (VA/PT), Information Systems Audit, security review, SMS gateways (Bulk SMS service providers), Procurement of IT hardware/ appliances, Acquisition of IT software/ product/ application (like CBS, database, security solutions, etc.,) on a licence or subscription basis and any enhancements made to such licensed third-party application by its vendor (as upgrades) or on specific change request made by the Infina, any maintenance service (including security patches, bug fixes) for IT Infra or licensed products, provided by the Original Equipment Manufacturer (OEM) themselves, in order to ensure continued usage of the same by the Infina, applications provided by financial sector regulators or institutions like CCIL, NSE, BSE, etc., platforms provided by entities like Reuters, Bloomberg, SWIFT, etc., any other off the shelf products (like anti-virus software, email solution, etc.,) subscribed to by the regulated entity wherein only a license is procured with no/ minimal customisation, services obtained by a Infina as a sub-member of a Centralised Payment Systems (CPS) from another Regulated Entity, Business Correspondent (BC) services, payroll processing, statement printing.
- B. Vendors / Entities who are not considered as Third-Party Service Provider (TPSP) for the purpose of this Master Direction: Vendors providing business services using IT. Example – BCs, Payment System Operators authorised by the Reserve Bank of India under the Payment and Settlement Systems Act, 2007 for setting up and operating Payment Systems in India, Partnership based Fintech firms such as those providing co-branded applications, service, products

(would be considered under outsourcing of financial services), Services of Fintech firms for data retrieval, data validation and verification services such as (list is not exhaustive): a. Bank statement analysis, b. GST returns analysis, c. Fetching of vehicle information, d. Digital document execution, e. Data entry and Call centre services; Telecom Service Providers from whom leased lines or other similar kind of infrastructure are availed and used for transmission of the data, Security/ Audit Consultants appointed for certification/ audit/ VA-PT related to IT infra/ IT services/ Information Security services in their role as independent third-party auditor/ consultant/ lead implementer.

Owner

Head-IT is the owner of this policy.

Review Frequency and Approving Authority

The policy shall be reviewed at least annually by IT Strategy Committee (ITSC) and the Board of Infina and approved by the Board of Infina.

Definition

- I. "Material Outsourcing of IT Services" are those which:
 - a) if disrupted or compromised shall have the potential to significantly impact the RE's business operations; or
 - b) may have material impact on the RE's customers in the event of any unauthorised access, loss or theft of customer information.
- II. "Service Provider" means the provider of IT or IT enabled services including entities related to the RE(Infina) or those which belong to the same group or conglomerate to which the RE belongs.

Policy Statement

- Though the IT activity / service is outsourced, the accountability, including customer grievance, shall lie with the Board and Senior Management of Infina without any compromise on service level agreement and Customer focus and rights;
- IT Outsourcing framework shall have 5 phases - Need of Outsourcing, Servicer Provider Selection, Service Provider Commissioning, Service Provider Monitoring and Service Provider De-Commissioning;
- Mechanism shall be established through which ITSC shall assess the need, cost-benefit and model of outsourcing.
- Establish a due diligence process at the time of the onboarding of service provider which shall assess the critical aspects, including but not limited to, technical, legal, statutory, regulatory, financial, reputational, conflict of interest with Infina etc. in relevance to the activity/ service to be outsourced;
- Infina shall have in place a Governance structure depicted below with primary responsibilities:
 - Board – govern the mechanism to assess risks related to material outsourcing IT activities;
 - Senior Management – establishing the mechanisms proposed in the IT Outsourcing Policy and implementation of procedure, contingency planning, capacity monitoring etc. with regard to the activity getting outsourced;
 - IT Function – assist Senior Management in identifying, measuring, monitoring, mitigating, and managing the organization's IT outsourcing risk, maintain central database in excel/ in application of outsourced IT activities and execution of processes established to comply to this policy;
- Controls shall be established to assess and mitigate risks (specifically for Customer personal data breach, cyber security and concentration risks) across each phase of the IT Outsourcing Framework and assessed during quarterly review of ITSC for continuous improvement;
- Access to Customer data shall be strictly on 'need to know' and 'as on need basis' principles;
- Contractual agreement shall cover clauses explicitly addressing the key points like right to audit of Infina/ regulator, confidentiality, privacy, service level, incident / breach management and reporting, relevant regulatory / statutory / legal requirements etc;

- Cross border outsourcing shall be preferred. In exceptional cases, due diligence and risk assessment shall be carried out and PESTEL (Political, Economic, Social, Technological, Environmental and Legal) analysis shall be carried if the risk persist.
- Infina shall give prime importance to the data security right from the time of entry of data into the cloud till the data is permanently erased;
- Availability of Business Continuity and Disaster Recovery Plans, related to the service(s) provided to the Infina, at the service provider's end shall be required along with the assurance of regular testing of the said plans. Third party audit reports of the Service Provider related to internationally recognized standards (e.g. ISO27001, SOC 2 etc.) / framework (e.g. NIST CSP 2.0 etc.). Infina shall assess the feasible alternative arrangements to deal with the 'worst case scenario' and triggering of alternative arrangement shall be the decision of the Board;
- Infina shall conduct the annual audits of material service providers either by their internal auditors or appointing external subject matter experts. Compliance of sub-contractor(s) to the IT Outsourcing Policy and contractual requirements of Infina shall be the responsibility of the material service provider. ITSC reserves the right to conduct sub-contractor's audit if considerable risks associated with them is/ are observed during the service provider's audit. The audits should be against the IT, Information and Cyber Security policies of the Infina and parameters assessed in due diligence and any other risk(s) observed;
- If activity is outsourced to any of the entity of Infina group, that entity shall be considered as the 'Service Provider' and has to comply to this policy;
- For de-commissioning of the Service Provider an Exit Strategy shall be followed as agreed in the agreement or devised by Head-IT (along with the help of respective Service Provider) addressing business continuity during and after exit. alternative arrangements, co-operation of the Service Provider to migrate to different service provider smooth transitioning, data handover and purging of data;
- In the case of cloud computing, Infina shall address the risks of multi-location storing and processing of data to ensure adherence to the applicable laws, strong authentication mechanism, adequate security controls, CSP's monitoring mechanisms / integration with Infina's SOC etc;
SOC service shall be outsourced by Infina with transparency in the asset ownership, access to the rules configured, structured SOC incident reporting and escalation process agreed with the vendor, regular monitoring of SOC performance.;
- Supporting documents shall be prepared to outline the details indicating implementation of this policy.

High Level Actions

- Parameters to assess need of outsourcing
- Checklists to assess materiality of outsource activity
- Due Diligence checklist;
- Vendor performance monitoring
- Following the proposed policy for the service providers in the process of onboarding
- Documentation readiness for existing service providers

Annexure

- Annexure 1: Material_IT-Services_ACTIVITY_v1.0.xlsx
- Annexure 2: Non_Material_IT-Services_ACTIVITY_v1.0. xlsx
- Annexure 3: Material_IT Services_Activity_Monitoring_v1.0. xlsx
- Annexure 4: Non_Material_IT-Services_Activity_Monitoring_v1.0. xlsx
- Annexure 5: IT Outsourcing Procedure.docx
- Annexure 6: BCP and DR Plan
- This policy addresses the following ISO27001:2022 Controls:
 - A.5.19 - Information security in supplier relationships
 - A.5.20 - Addressing information security within supplier agreements

○ A.5.21 - Managing information security in the information and communication technology (ICT) supply chain

References

1. RBI Guidelines on Management of Intra-Group Transactions and Exposures' issued vide circular DBOD.No.BP.BC.96/21.06.102/2013-14 dated February 11, 2014;
2. RBI 'Guidelines on Managing Risks and Code of Conduct in Outsourcing of Financial Services by banks' issued vide circular DBOD.NO.BP.40/ 21.04.158/ 2006-07 dated November 3, 2006
3. Cloud Adoption Policy of Infina
4. IT Act,2000

Document Control

Date	Author	Approved By	Version	Comments
25/04/2025	CTO	Board	V 1.0.	