The Jurisdiction Question

How Your Escrow Vendor's Domicile Determines Your Compliance Position

A Compliance and Risk Governance Guide for RBI, SEBI, and IRDAI Regulated Entities

Published by

EscrowNXT Services Private Limited

India's First ISO 9001:2015 & ISO 27001:2022 Certified Pure-Play Software Escrow Provider

Executive Summary

India's regulated financial sector — banks, non-banking financial companies (NBFCs), insurance companies, stockbrokers, and market infrastructure institutions — operates under a dense, overlapping web of IT governance obligations issued by the Reserve Bank of India (RBI), the Securities and Exchange Board of India (SEBI), and the Insurance Regulatory and Development Authority of India (IRDAI). These obligations carry board-level accountability, audit trail requirements, and enforceable incident-reporting timelines measured in hours.

Within this framework, software escrow sits at a critical intersection: it is simultaneously an IT outsourcing arrangement, a data custody mechanism, a legal instrument for business continuity, and a vendor risk mitigation tool. Yet a question that procurement heads, CIOs, and legal teams rarely examine is: does it matter where the escrow vendor is incorporated and physically based?

This white paper argues that the answer is an unambiguous yes — and that for Indian Regulated Entities (REs), appointing an India-incorporated, India-domiciled software escrow vendor is not a matter of commercial preference but a regulatory risk management imperative.

> *Key Finding: The RBI Master Direction on Outsourcing of IT Services (2023), SEBI's Cybersecurity and Cyber Resilience Framework (2024), and IRDAI's Information and Cyber Security Guidelines (2023) collectively impose audit access rights, data localisation requirements, jurisdictional enforceability obligations, and incident-reporting timelines that a foreign-based escrow vendor cannot practically fulfil in the same manner as an India-domiciled, ISO-certified provider.*

EscrowNXT Services Private Limited — India's first ISO 9001:2015 and ISO 27001:2022 certified pure-play software and technology escrow provider, founded in 2005 and headquartered in Chennai — was built precisely for this regulatory environment. This paper walks compliance officers, CIOs, legal counsel, and procurement heads through the five-dimensional risk framework that makes vendor domicile a board-level governance question.

1. The Regulatory Landscape: Why Software Escrow Is Now a Governance Matter

India's financial sector regulators have, over the last three years, substantially elevated their expectations of how Regulated Entities manage their technology vendor relationships. Software escrow — long treated as a contractual add-on — has been repositioned within this framework as a material IT outsourcing service with direct compliance implications.

1.1 RBI Master Direction on Outsourcing of IT Services, 2023

Issued on 10 April 2023 and effective from 1 October 2023, the RBI's Master Direction on Outsourcing of IT Services ('Master Direction') is the most comprehensive regulatory framework governing third-party technology vendors of RBI-regulated entities. It applies to Scheduled Commercial Banks (including foreign banks licensed in India), Small Finance Banks and Payments Banks, Primary (Urban) Co-operative Banks (excluding Tier 1 and Tier 2), Non-Banking Financial Companies in the Middle, Upper, and Top Layers, Credit Information Companies, and All India Financial Institutions including EXIM Bank, NABARD, NaBFID, NHB, and SIDBI.

The Master Direction defines 'material outsourcing of IT services' as any service that, if disrupted or compromised, would significantly impact the RE's business operations or materially affect customer data. A software escrow arrangement — which holds source code, technical documentation, build instructions, and encryption keys — clearly meets this threshold when the escrowed software underpins critical banking, lending, insurance, or market infrastructure operations.

The Master Direction's implications for vendor selection are direct and consequential. Audit rights require that both REs and the RBI retain the right to audit third-party service providers, including those based outside India. Data localisation provisions require that outsourcing agreements address applicable localisation requirements; escrow deposit materials relating to Indian customer data are subject to these norms. Cyber incident reporting must occur without undue delay so that the RE can report to the RBI within six hours of detection. Agreements must specify governing law and ensure that foreign jurisdictions do not override Indian regulatory authority. Finally, REs must maintain a tested exit strategy and vendors must cooperate in data transition.

1.2 SEBI Cybersecurity and Cyber Resilience Framework (CSCRF), 2024

SEBI's Cybersecurity and Cyber Resilience Framework, issued in 2024, establishes structured compliance timelines and audit expectations across Market Infrastructure Institutions, stockbrokers, mutual funds, portfolio managers, and other SEBI-regulated entities. The CSCRF mandates continuous monitoring, deep control testing, and high audit frequency — all of which extend to the technology vendor ecosystem, including escrow providers that hold software assets critical to trading and settlement continuity.

1.3 IRDAI Information and Cyber Security Guidelines, 2023

IRDAI's 2023 consolidated cyber security guidelines apply to insurers and insurance intermediaries. They explicitly reference global standards, including the NIST Cybersecurity Framework, and impose governance and control coverage requirements that cascade down to third-party technology vendors. Insurers operating

mission-critical software under escrow arrangements are expected to demonstrate that their escrow vendors meet the requisite security and audit access standards.

> *The convergence point across RBI, SEBI, and IRDAI: all three frameworks establish that the Regulated Entity's liability for IT governance does not reduce because of outsourcing. What the vendor cannot provide — auditability, data localisation, rapid incident reporting, jurisdictional enforceability — the RE itself must compensate for. Choosing a vendor that structurally cannot meet these requirements is not a commercial risk; it is a regulatory risk carried by the RE.*

2. The Five Dimensions of Vendor Domicile Risk

When an Indian Regulated Entity selects a software escrow vendor, five distinct risk dimensions are directly influenced by where that vendor is incorporated and physically operates. Each dimension has a regulatory signature — an explicit or implicit expectation that a foreign-domiciled vendor structurally struggles to satisfy.

Dimension 1: Regulatory Audit Access

Under the RBI Master Direction, both the RE and the RBI must have the right to audit the technology service provider. For an escrow vendor, this means regulators must be able to inspect the physical vault where deposit materials are stored, the access control systems, the version management records, and the incident logs.

A foreign-based vendor — even one with sound internal governance — presents a structural audit access problem. Indian regulators have no direct territorial jurisdiction over facilities located in Singapore, the United Kingdom, or the United States. The RE must negotiate specific contractual provisions allowing RBI inspection access across foreign borders, arrange for travel and coordination costs, and manage time-zone and jurisdictional friction in the event of an audit. This surfaces as a compliance risk during RBI supervisory inspections.

An India-incorporated, India-domiciled vendor eliminates this risk entirely. The RBI's audit authority is unambiguous, the storage facility is accessible, and the RE's internal audit team can conduct routine reviews without cross-border complexity.

Dimension 2: Data Localisation and Sovereignty

The deposit materials held in a software escrow arrangement frequently include source code that interfaces with customer data systems, payment processing infrastructure, and core banking applications. In several categories — particularly payment system data and financial customer records — RBI guidelines impose explicit data localisation requirements: certain data must be stored only in India.

A foreign-based escrow vendor that stores deposit materials on servers located outside India creates a potential data sovereignty issue for the RE. Even where the escrow materials do not themselves constitute customer personal data, the systemic risk of commingling governed data with ungoverned foreign storage creates audit exposure and regulatory uncertainty.

An India-domiciled escrow vendor with physically secured vaults in India — and an ISO 27001:2022 certified information security management system — provides the RE with a clean, auditable data localisation position.

Dimension 3: Incident Reporting and Response

The RBI's six-hour cyber incident reporting timeline is among the most demanding vendor obligations in any jurisdiction. The cascade runs: detection by the escrow vendor → notification to the RE → RE's report to the RBI, all within six hours.

For a foreign-based escrow vendor operating across time zones, this timeline is operationally strained. A vendor in a different time zone may not detect an incident — or may detect it when the Indian RE's IT team is not monitoring. Escalation paths between countries add minutes and hours to incident timelines that the regulator measures in a six-hour window.

An India-based vendor operating in Indian Standard Time, with an Indian operations team and an ISO 9001:2015 certified incident management process, aligns structurally with the RBI's reporting expectations. The notification lag is minimised; the escalation path is direct; the regulatory timeline is achievable.

Dimension 4: Jurisdictional Enforceability

A software escrow arrangement is, at its core, a tripartite legal agreement that depends on enforceability. The release mechanism — the trigger event and the custodian's obligation to deliver deposit materials to the licensee — must be enforceable in a court of competent jurisdiction.

For Indian Regulated Entities, whose continuity obligations are enforceable by Indian regulators, an escrow agreement governed by foreign law and enforceable only in foreign courts introduces a jurisdictional gap at the most critical moment: when the escrow needs to be released. The RBI Master Direction explicitly notes that foreign jurisdiction should not extend to the RE's operations in India merely on the basis of data processing in a foreign jurisdiction.

An India-incorporated escrow vendor operates under Indian contract law. Indian courts have jurisdiction, and the release mechanism is enforceable without cross-border legal complexity — precisely when the RE needs it most.

Dimension 5: Concentration and Country Risk

The RBI Master Direction specifically calls out concentration risk in IT outsourcing — the risk that a critical third-party vendor failure creates systemic exposure. For software escrow, concentration risk has an additional layer: country risk. An escrow vendor incorporated in a jurisdiction subject to geopolitical disruption, trade restrictions, data protection regulation conflicts, or sudden government access orders may find its ability to fulfil escrow obligations compromised by factors entirely outside the RE's control.

India-domiciled escrow vendors are not subject to these extraterritorial foreign legal risks. The RE's risk assessment is confined to Indian legal and regulatory conditions — conditions that the RE's compliance team already monitors and manages.

3. Compliance Risk Comparison: Foreign Vendor vs. India-Domiciled Vendor

The table below maps the core regulatory requirements of RBI, SEBI, and IRDAI against the structural compliance position of a foreign-based escrow vendor versus an India-domiciled, ISO-certified provider.

Regulatory Requirement	Foreign-Based Escrow Vendor	India-Domiciled Vendor (EscrowNXT)
RBI physical audit access	Complex: cross-border access negotiations required; RBI has no direct territorial jurisdiction	Straightforward: RBI has direct jurisdiction; facility accessible to all auditors without cross-border friction
Data localisation compliance	Risk of non-compliance if deposit materials stored on foreign servers	Full compliance: vaults physically in India; ISO 27001:2022 certified
6-hour cyber incident reporting	Structurally difficult across time zones; escalation paths add delay	IST-aligned operations; ISO 9001:2015 certified incident management; direct escalation
Jurisdictional enforceability of escrow release	Foreign law and courts; potential legal delay at the critical trigger moment	Indian contract law; Indian courts; swift, enforceable release mechanism
Country and concentration risk	Exposed to foreign legal orders, geopolitical risk, conflicting data regulations	Confined to Indian regulatory environment; no extraterritorial foreign legal risk
SEBI CSCRF audit compliance	Third-party audit arrangements required; not natively India-audit-ready	India-incorporated; directly auditable under SEBI framework
IRDAI cyber security governance	Requires specific contractual bridging; governance may not align natively	Aligns natively; ISO certifications provide structural alignment with IRDAI guidelines

This is not an argument that foreign vendors are incapable of providing contractual protections. Many do. The argument is that an India-domiciled vendor provides these protections structurally — without requiring expensive contractual bridging, audit access negotiations, or incident-response workarounds. For an RE operating under board-level governance accountability, structural compliance is materially preferable to contractual workarounds.

4. Illustrative Scenarios: When Vendor Domicile Becomes Critical

The five risk dimensions described above manifest in specific, practical scenarios that Indian Regulated Entities encounter when managing their technology ecosystems.

Scenario A: The RBI Supervisory Inspection

A mid-sized NBFC in the Upper Layer is subject to an RBI supervisory inspection. The inspection team requests evidence of IT vendor risk management practices, including documentation of all material outsourcing arrangements. The NBFC's core lending management software is covered by a software escrow agreement with a Singapore-based vendor.

The inspection team requests audit access to the escrow vault. The NBFC's compliance team must now navigate: which Indian legal instrument grants the RBI audit access to a Singapore facility? What is the inspection timeline given cross-border coordination? Does the escrow agreement explicitly grant RBI audit rights? If it does not, the NBFC faces a compliance gap — documented and on record during a supervisory inspection.

Had the NBFC appointed an India-based escrow vendor, the RBI's audit access would be unambiguous, the vault accessible, and the inspection concluded without incident.

Scenario B: The Cyber Incident at 2 a.m.

A payment bank's critical transaction processing software is held under escrow with a UK-based provider. At 2:17 a.m. IST, a ransomware event is detected at the escrow vendor's data centre. The UK vendor's IT team is not at work — it is 9:47 p.m. GMT. Notification to the Indian RE does not occur until 6:00 a.m. IST, when the UK team comes online.

The RE's six-hour RBI reporting window — which runs from the point of detection — has already expired. The RE faces a regulatory reporting failure for an incident that originated at its third-party service provider. An India-based escrow vendor, with an IST-aligned operations centre, would have detected, notified, and escalated within the regulatory window.

Scenario C: The Software Vendor Insolvency

A private sector bank's core banking system vendor files for insolvency. The bank triggers the release condition under its software escrow agreement. The escrow custodian — a US-incorporated entity — is obligated to release the deposit materials. However, the US vendor's counsel advises that under US bankruptcy law, the escrow release may be subject to a temporary stay pending insolvency proceedings.

The bank's business continuity plan assumed that the escrow release would be immediate and enforceable. Instead, it is entangled in a foreign legal process. Core banking operations are at risk, and the RBI's operational resilience requirements are not being met.

An India-incorporated escrow vendor, operating under Indian contract law, releases deposit materials under the Indian Insolvency and Bankruptcy Code framework — a process the bank's legal team can manage directly and swiftly.

> *The common thread: the escrow arrangement worked on paper but failed in practice because the vendor's domicile created a gap between the regulatory assumption and the operational reality. In each case, an India-domiciled vendor would have eliminated the gap entirely.*

5. What 'India-Domiciled' Actually Means: The EscrowNXT Standard

Not every vendor registered in India meets the standard required by regulated financial sector entities. 'India-domiciled' is a necessary but not sufficient condition. Regulated Entities should evaluate escrow vendors against a multi-dimensional framework that distinguishes genuine compliance infrastructure from a registered office in an Indian city.

Pillar 1: Sturdy Legal Framework

The vendor must be incorporated in India under the Companies Act, 2013. Escrow agreements must be tripartite instruments governed by Indian law with Indian courts as the exclusive seat of jurisdiction. Release conditions must function within the Indian legal framework, including consistency with the Insolvency and Bankruptcy Code where vendor insolvency is a trigger event.

Pillar 2: Certified Operations and Security Management

ISO 9001:2015 certification ensures the vendor's operational processes, incident response procedures, and deposit management workflows meet internationally recognised standards. ISO 27001:2022 certification ensures that the data held in escrow — source code, build documentation, encryption keys, database schemas, and configuration data — is protected by a certified framework that Indian regulators recognise and that aligns with RBI, SEBI, and IRDAI cybersecurity governance expectations.

Pillar 3: Transparent Verification and Testing

An escrow deposit that has never been tested is a legal instrument with an unknown operational value. A compliant India-based escrow vendor must offer structured verification and testing services — from integrity verification confirming deposit materials are complete and uncorrupted, through to complete verification confirming the source code can be built, installed, and operated by the licensee. These services must be documented in plain language accessible to both technical and non-technical stakeholders.

Pillar 4: Physical and Digital Safety

Escrow vaults must be physically located in India, with documented access controls, encryption standards, and version control systems. The vendor must be able to demonstrate these controls to the RE's internal auditors, external auditors, and regulators on demand.

EscrowNXT: Built for the Indian Regulatory Environment

EscrowNXT Services Private Limited has spent over twenty years building the infrastructure that Indian Regulated Entities now need as a regulatory requirement. As India's first ISO 9001:2015 and ISO 27001:2022 certified pure-play software and technology escrow provider:

- EscrowNXT is incorporated in India, headquartered in Chennai, with operations fully within Indian jurisdiction.
- Every escrow agreement is governed by Indian law, with Indian courts as the seat of jurisdiction.
- Physical vaults are located in India, accessible to RBI, SEBI, IRDAI inspectors, and RE auditors without cross-border complexity.

- Operations are IST-aligned, with a certified incident management process supporting the six-hour RBI reporting timeline.
- Verification and testing services — Integrity Verification, Material Audit, and Complete Verification — are available for every deposit, with plain-language reports suitable for board reporting and regulatory audit files.
- As a NASSCOM member since 2011, EscrowNXT operates within the recognised Indian technology services ecosystem.

> *EscrowNXT's founding principle — 'Don't Risk It. Escrow It.' — was built for Indian enterprises. Today, it is precisely aligned with what Indian regulators require of the enterprises it serves.*

6. A Practical Procurement Checklist for Regulated Entity Teams

For compliance officers, CIOs, and legal counsel advising their organisations on software escrow vendor selection, the following checklist translates the regulatory framework into practical due diligence questions. Each criterion should be documented in the vendor assessment file, available for regulatory inspection.

Evaluation Criterion	What to Ask Your Escrow Vendor	EscrowNXT Position
Incorporation and domicile	Where is the legal entity incorporated? Where are operations based?	Incorporated in India; headquartered in Chennai, Tamil Nadu
Governing law and jurisdiction	Which law governs the agreement? Which courts have jurisdiction?	Indian law; Indian courts exclusively
Physical vault location	Where are deposit materials physically stored?	Physical vaults in India; accessible to all regulators on demand
ISO certifications	Are you ISO 9001:2015 and ISO 27001:2022 certified?	India's first certified pure-play software and technology escrow provider under both standards
Incident reporting capability	How do you ensure 6-hour cyber incident notification to Indian REs?	IST-aligned operations; certified incident management process
RBI/SEBI/IRDAI audit access	Can Indian regulators directly audit your facilities?	Yes — no cross-border complexity; direct regulatory access
Verification and testing	What verification services do you offer and how are they documented?	Integrity Verification, Material Audit, Complete Verification; plain-language reports
Industry standing	Are you a member of recognised Indian industry bodies?	NASSCOM member since 2011
Track record	How long have you been providing escrow services in India?	20+ years; founded 2005

This checklist should be supplemented by the organisation's standard Third-Party Service Provider due diligence framework as required under the RBI Master Direction. For SEBI and IRDAI regulated entities, the same framework applies with the addition of sector-specific audit documentation requirements.

7. Conclusion and Next Steps

India's regulated financial sector has reached an inflection point in its relationship with technology vendors. The regulatory frameworks issued by RBI, SEBI, and IRDAI in 2023 and 2024 make clear that technology risk governance is a board-level accountability — and that the RE bears full responsibility for the compliance gaps of its third-party service providers.

For software escrow specifically, the question of vendor domicile is not a secondary consideration to be resolved by legal counsel after commercial terms are agreed. It is a primary governance question that shapes whether the escrow arrangement can actually fulfil its purpose: ensuring business continuity when the software vendor fails.

The five-dimensional risk framework — audit access, data localisation, incident reporting, jurisdictional enforceability, and country risk — collectively makes the case that an India-incorporated, India-domiciled, ISO-certified escrow vendor is not a premium preference. It is the baseline requirement for an Indian Regulated Entity operating under RBI, SEBI, or IRDAI oversight.

> *Escrow is not a contingency plan for pessimists. It is standard infrastructure for enterprises that take continuity seriously. EscrowNXT has spent twenty years making that infrastructure reliable, certified, and trusted — in India, for India.*

Recommended Next Steps

- Audit all existing escrow arrangements and confirm vendor domicile, governing law, vault location, and ISO certification status.
- Update your Board-approved IT outsourcing policy to include an explicit requirement for India-domiciled vendors for material IT outsourcing arrangements.
- Include vendor domicile as a standalone criterion in your Third-Party Service Provider risk assessment framework with a defined scoring methodology.
- Review existing escrow agreements for RBI audit access rights and assess whether those provisions are practically enforceable across borders.
- Ensure deposit materials are verified at least annually. An escrow arrangement without verified deposits is a legal instrument with unknown operational value.
- Consult your legal and compliance team on whether current escrow arrangements require amendment in light of the RBI Master Direction 2023 obligations.

Speak with EscrowNXT

EscrowNXT's team is available to assist Regulated Entities with free compliance gap assessments of existing escrow arrangements, customised software and technology escrow agreements for RBI, SEBI, and IRDAI regulated contexts, verification and testing of existing escrow deposits, and transition services for organisations moving from foreign-based to India-domiciled escrow arrangements.

Audience	Recommended Action
CIO / CTO	Book a free escrow risk assessment — www.escrownxt.com/contact-us
Legal / Compliance	Request a sample India-law escrow agreement — info@escrownxt.com

CFO / Procurement	Discuss coverage options and vendor migration — +91 44 45535571/72
Board / Executive	Request an executive briefing — info@escrownxt.com

Appendix: Glossary of Key Terms

Regulated Entity (RE)

As defined by the RBI Master Direction on Outsourcing of IT Services (2023): Scheduled Commercial Banks, Small Finance Banks, Payments Banks, Primary (Urban) Co-operative Banks (excluding Tier 1 and Tier 2), Non-Banking Financial Companies in the Middle, Upper, and Top Layers, Credit Information Companies, and All India Financial Institutions.

Material Outsourcing of IT Services

Any IT outsourcing service that, if disrupted or compromised, would significantly impact the RE's business operations or materially affect customer data. Software escrow arrangements covering mission-critical software qualify under this definition.

Software Escrow

A tripartite legal arrangement under which the licensor deposits source code, technical documentation, and related materials with an independent custodian, to be released to the licensee upon defined trigger events.

Trigger Event

A contractually defined event — such as vendor insolvency, acquisition, material breach, or cessation of support — that entitles the licensee to receive deposit materials from the escrow agent.

Deposit Materials

The materials held in escrow: typically source code, build instructions, technical documentation, encryption keys, database schemas, and any other materials necessary to operate the software independently.

Technology Escrow

An expanded form of software escrow covering a broader range of intellectual property assets, including hardware schematics, manufacturing processes, formulas, blueprints, and embedded software.

Integrity Verification

A verification service confirming that deposit materials are complete, uncorrupted, and correctly labelled — without testing whether the materials can be successfully built or operated.

Complete Verification

A comprehensive verification service confirming that deposit materials can be built, installed, and operated as intended — providing the licensee with assurance that the escrow is operationally reliable.

Data Localisation

The regulatory requirement that certain categories of data — particularly financial customer data and payment transaction data — be stored on servers physically located within India.

ISO 9001:2015

The international standard for quality management systems, covering process control, operational consistency, incident management, and continuous improvement.

ISO 27001:2022

The international standard for information security management systems, covering the protection of confidential data, access controls, encryption, and security governance.

About EscrowNXT

EscrowNXT Services Private Limited (formerly EscrowTech India Pvt. Ltd.) is India's first ISO 9001:2015 and ISO 27001:2022 certified pure-play software and technology escrow services provider. Founded in 2005 and headquartered in Chennai, EscrowNXT has spent over two decades protecting the technology investments of leading enterprises, software developers, and corporate houses across India.

Our services include Software Escrow, Technology Escrow, IP Archive, Verification and Testing, and secure Vaults. Every arrangement is governed by Indian law, stored in Indian vaults, and managed by an India-based team — making EscrowNXT the structurally compliant choice for Regulated Entities operating under RBI, SEBI, and IRDAI oversight.

Website	www.escrownxt.com
Email	info@escrownxt.com
Phone	+91 44 45535571 / 45535572 | +91 44 22505571
Address	C2-A, Industrial Estate, Guindy, Chennai – 600 032, Tamil Nadu, India