Software Escrow: A Practitioner's End-to-End Handbook

A Comprehensive Guide for Legal Counsel, CIOs, Compliance Officers, and Technology Vendors

Published by
EscrowNXT Services Private Limited
India's First ISO 9001:2015 & ISO 27001:2022 Certified Pure-Play Software Escrow Provider

Foreword: About This Handbook

Software escrow is one of the most important and most misunderstood risk management tools available to enterprises that depend on licensed software. Thousands of organisations across India have software escrow agreements in place. A fraction of those agreements would survive contact with an actual release event.

This handbook was written to close that gap.

The problem is not a lack of awareness — most CIOs and legal counsels know what software escrow is. The problem is a lack of rigour at every phase: agreements drafted without enforceable release conditions, deposits made once and never updated, verification skipped because it costs extra, and post-release plans that have never been tested. When a vendor finally goes dark, what remains is a document that was supposed to provide protection but, in practice, provides none.

This handbook takes a lifecycle view of software escrow — from the initial decision to pursue escrow through to the post-release restoration of business continuity. Each chapter corresponds to a phase of the escrow lifecycle, with practical guidance, checklists, and worked examples drawn from two decades of escrow practice in India.

How to Use This Handbook

This handbook is not designed to be read once and filed. It is a lifecycle reference:

- Legal counsel negotiating an escrow provision should focus on Chapters 3, 8, and the Quick-Reference Tools in Chapter 9.
- CIOs and IT procurement teams should start with Chapters 1, 2, and 5 before reviewing Chapter 6 on ongoing management.
- Compliance managers in regulated sectors (BFSI, healthcare, government) should pay particular attention to Chapter 8 and the RBI IT Directions guidance at Section 8.1.
- Software vendors acting as depositors will find Chapters 3, 4, and 5 directly relevant to their obligations and risk exposure.

A Note on Indian Law and Cross-Border Considerations

This handbook is written primarily for practitioners operating under Indian law and within the Indian regulatory environment. Where relevant, it addresses cross-border considerations — particularly where the software vendor is a foreign entity or the governing law is non-Indian. Section 8.3 addresses FEMA implications and international arbitration for cross-border escrow arrangements specifically.

"Don't Risk It. Escrow It."

EscrowNXT Services Private Limited has spent over two decades making software escrow reliable, certified, and trusted in India. This handbook reflects that accumulated expertise.

Chapter 1: Understanding the Software Escrow Arrangement

1.1 What Is a Software Escrow Arrangement?

Software escrow is a tripartite arrangement in which a neutral third party — the escrow agent — holds source code, documentation, and related technical materials deposited by a software vendor, for the benefit of a licensee, to be released only upon the occurrence of defined trigger events.

The purpose is straightforward: to protect the beneficiary's ability to maintain, support, and continue operating mission-critical software if the vendor can no longer do so. Without escrow, a licensee has access to the executable application but not the underlying source code. If the vendor ceases operations, is acquired, or stops providing support, the licensee is left unable to fix bugs, apply security patches, or adapt the software to changing business needs.

The three parties to every software escrow arrangement have distinct roles:

Party	Also Called	Role
Software Vendor	Depositor / Licensor	Places deposit materials in escrow; obliged to keep the deposit current
Licensee	Beneficiary	The organisation whose business continuity is protected; entitled to release upon a trigger event
Escrow Agent	Custodian / EscrowNXT	Neutral custodian; holds the deposit, verifies it, and executes release per agreed conditions

1.2 When Is a Software Escrow Arrangement Necessary?

Not every software relationship warrants an escrow arrangement. The test is vendor dependency risk — the degree to which your organisation would be exposed if the vendor ceased to provide the software or support it.

High-risk indicators that typically warrant escrow include:

- Sole-source software — there is no commercially available equivalent that could be deployed without significant disruption or cost
- Heavily customised platforms — the software has been adapted specifically for your processes, making migration to an alternative extremely complex
- Unsupported legacy systems — the vendor's product roadmap has diverged from your version, meaning security patches and bug fixes depend entirely on vendor goodwill
- Mission-critical operations — the software underpins financial processing, patient management, logistics, or other functions where downtime has direct and severe consequences
- Small or financially exposed vendors — startups, private-equity-backed companies undergoing restructuring, or overseas vendors with limited Indian presence

Sector-Specific Regulatory Triggers

In regulated sectors, escrow is not merely prudent — it is frequently mandated:

- **BFSI:** The Reserve Bank of India's Master Direction on Information Technology Governance, Risk, Controls and Assurance Practices, 2023 (RBI IT Directions, 2023) requires regulated entities to maintain software escrow arrangements for critical technology systems. This is addressed in detail at Section 8.1.
- **Government and Defence:** Procurement frameworks for government IT systems routinely include escrow obligations as a condition of contract award.
- **Healthcare and Pharma:** Systems managing patient data or clinical operations attract heightened continuity obligations.

The Cost of Not Having Escrow — A Scenario

A mid-sized NBFC deploys a core lending platform from a boutique fintech vendor. The vendor is acquired by a larger group, which decides to sunset the product. With no escrow in place, the NBFC has access to the running executable but cannot patch a critical security vulnerability discovered three months post-acquisition. Regulatory scrutiny follows. The cost of emergency migration exceeds the cost of a decade of escrow fees.

1.3 Types of Software Escrow Arrangements

Understanding the different structures available allows practitioners to select the arrangement that fits their risk profile:

Arrangement Type	Description	Best For
Single-beneficiary	One agreement covering one licensor–licensee relationship	Custom enterprise software; bespoke deployments
Multi-beneficiary (preferred)	One vendor deposit accessible to multiple licensees under separate release conditions	SaaS and commercial software with many licensees; more cost-efficient
Traditional / On-premise Escrow	Secures source code for software installed on the beneficiary's own infrastructure	ERP, HIS, SCADA, and legacy on-premise platforms
SaaS / Cloud Escrow	Secures code, configuration, and data export capabilities for cloud-delivered software	CRM, HRMS, and cloud-native platforms where data portability is also at risk
Technology Escrow	Extends beyond software to hardware schematics, manufacturing processes, embedded firmware, and encryption keys	IoT deployments, defence, and industrial automation

Continuous / Automated Deposit	Deposit materials are updated automatically on each code commit or version release via API integration	Agile development environments with frequent release cycles

Chapter 2: Phase 1 — Needs Assessment and Provider Selection

2.1 Assessing Whether Escrow Is Warranted

Before approaching an escrow agent, organisations should conduct an internal needs assessment. This assessment should be documented — both to build the internal business case and to serve as a reference point when the escrow agreement is eventually reviewed or renewed.

A practical software criticality scoring exercise should rate each system under consideration across four dimensions:

Dimension	What to Assess	Risk Signal
Operational Dependency	Could the business continue if this system was unavailable for 30, 60, or 90 days?	High: revenue-critical or patient-safety critical systems
Replaceability	How long and costly would it be to migrate to an alternative?	High: estimated migration cost > 12 months or INR 1 crore
Vendor Financial Health	Is the vendor financially stable? Is it startup, PE-backed, foreign?	High: startups < 5 years old; vendors with known financial stress
Contractual Support Term	How long does the vendor's support obligation last? Is it evergreen or fixed-term?	High: support term < 3 years or terminable at will

Stakeholder mapping should identify who within the organisation must be involved in the escrow decision: the CIO or CTO for technical requirements; legal counsel for contractual drafting; the compliance or risk function for regulatory obligations; and finance or procurement for budget approval and vendor assessment.

2.2 Selecting the Right Escrow Agent

The escrow agent is not a passive file storage provider. The agent's operational capabilities directly determine whether the escrow arrangement functions as intended when a release event occurs. Selection should be rigorous.

Key Evaluation Criteria

- **Security certifications:** The agent should hold at minimum ISO 27001:2022 (information security management) and ISO 9001:2015 (quality management) certifications. EscrowNXT is India's first pure-play escrow provider to hold both.
- **Verification capability:** Agents who cannot offer Level 2 or Level 3 verification (see Chapter 5) should not be selected for mission-critical applications.

- **Jurisdictional reach:** For cross-border arrangements, confirm whether the agent can execute release and hold deposits across jurisdictions.
- **SLA responsiveness:** Review the agent's committed response times for deposit receipts, verification reports, and release execution.
- **Dispute resolution capacity:** Does the agent provide independent dispute resolution, or does it simply halt on contrary instructions and leave the parties to litigate?
- **Deposit update processes:** How does the agent receive, record, and confirm deposit updates? Is the process automated, manual, or a combination?

Red Flags — Disqualifying Characteristics

- Agents who market themselves primarily as document storage providers without technology-specific escrow expertise
- No independent dispute resolution mechanism — only a notification role
- No verification services or only Level 1 (existence-only) verification
- No clear deposit update protocol or version register
- Foreign agents with no Indian entity, no RBI-compliant processes, and no local counsel on retainer

Chapter 3: Phase 2 — Negotiating the Agreement

3.1 Negotiating Escrow into the Software Licence Agreement

The most important practical principle in escrow negotiation is timing: escrow is significantly easier to negotiate at the point of initial software licensing than after the relationship is established. Once a vendor's software is embedded in an organisation's operations, the vendor's leverage increases and the licensee's negotiating position weakens.

Legal counsel should treat escrow as a standard commercial term — not an extraordinary demand — and should include a model escrow clause in the initial draft of every software licence agreement where the software meets the criticality threshold identified in Chapter 2.

When Vendors Resist — Practical Negotiation Tactics

- Reframe escrow as IP protection for the vendor — escrow protects the vendor's source code from being copied or misused; the agent is a neutral custodian, not a conduit for the licensee to obtain the code without a trigger event
- Offer a cost-sharing arrangement — escrow costs are modest relative to the total contract value; offer to bear the agent's fees as part of the commercial package
- Reference regulatory obligations — for BFSI clients, RBI IT Directions, 2023 creates a compliance imperative that the vendor cannot reasonably ask the licensee to waive
- Use multi-beneficiary arrangements to reduce vendor friction — a single deposit serving multiple licensees is less onerous for the vendor than separate agreements for each

Model Escrow Clause for Insertion into a Software Licence Agreement

"The Licensor shall, within [30] days of the execution of this Agreement, enter into a Software Escrow Agreement with [EscrowNXT Services Private Limited / a mutually agreed escrow agent] ('Escrow Agent'), under which the Licensor shall deposit the Deposit Materials (as defined in the Escrow Agreement) with the Escrow Agent. The Licensor shall maintain the currency of the Deposit Materials and submit updated deposits within [30] days of each Major Version release. The Licensee shall be named as a beneficiary under the Escrow Agreement and shall be entitled to release of the Deposit Materials upon the occurrence of a Release Condition as defined therein. The costs of the Escrow Agent shall be borne by [specify party]. This clause shall survive the termination or expiry of this Agreement."

3.2 Key Terms Every Practitioner Must Master

Term	Definition	Practitioner Note
Deposit Materials	All items placed in escrow — source code, build scripts, documentation, and related technical materials	Define exhaustively in the Deposit Schedule. Never use 'source code' alone — it is chronically under-inclusive

Release Conditions	The trigger events that entitle the beneficiary to access the deposit materials	Insist on objective, documentary triggers. Avoid vague formulations such as 'material failure to provide support'
Verification	Technical testing of the deposit materials to confirm they are complete, buildable, and functional	Mandate Level 2 minimum; Level 3 for mission-critical systems. Unverified escrow is decorative, not protective
Contrary Instructions	The vendor's right to dispute a release request by notifying the agent within a defined period	Cap the contrary instructions window at 10–15 days. Longer windows expose the beneficiary to extended uncertainty during a crisis
Post-Release Licence	The rights granted to the beneficiary upon release of the deposit materials	Define scope (internal use, third-party maintenance, right to modify), duration, and restrictions explicitly. Do not leave this to implication
Update Obligations	The vendor's obligation to refresh the deposit when the software is updated	Link to each Major and Minor version release, plus defined security patches. 'Annual' updates are insufficient for actively developed software

3.3 Drafting Release Conditions: The Most Contested Clause

Release conditions are the heart of the escrow agreement. Poorly drafted release conditions are the single most common reason escrow arrangements fail to provide the protection they were designed to deliver.

Standard Release Triggers

- Vendor insolvency — filing for protection under the Insolvency and Bankruptcy Code, 2016; appointment of a Resolution Professional; voluntary liquidation
- Winding up — order for compulsory winding up under the Companies Act, 2013
- Cessation of business — the vendor ceases to carry on business operations in the relevant jurisdiction
- Material breach of support obligations — the vendor fails to provide contracted support services and does not remedy the breach within a defined cure period
- Change of control — the vendor is acquired by a competitor or entity whose ownership creates a conflict of interest for the beneficiary
- Long-stop trigger — the vendor has not responded to support requests for a defined period (typically 30 consecutive days), regardless of the underlying cause

Objective vs. Subjective Triggers

The critical drafting distinction is between objective and subjective release triggers. An objective trigger is one that can be established by documentary evidence without requiring an assessment of intention or adequacy: an insolvency filing is an objective event. A subjective trigger — such as 'the vendor has materially failed to meet its obligations' — requires someone to adjudicate whether the threshold has been met, inviting dispute and delay.

Practitioners should insist on documentary evidence standards for each trigger: for insolvency, a copy of the insolvency filing or order; for cessation of support, a log of unanswered support tickets and formal written notification; for change of control, public announcement or Companies House / MCA filing.

3.4 Rights Granted Upon Release

The post-release licence defines what the beneficiary may do with the deposit materials once released. This clause is frequently overlooked during negotiation and is often critically deficient in practice.

- **Scope:** At minimum, the beneficiary needs the right to use the software for internal business purposes, to fix bugs and apply security patches, and to engage a third-party developer or maintenance firm to do so on its behalf. A licence restricted to 'internal use' without an explicit right to engage third parties leaves the beneficiary unable to obtain maintenance services.
- **Duration:** The post-release licence should last for a defined period — typically two to three years — sufficient to allow an orderly migration to an alternative system.
- **Restrictions:** Standard restrictions include no commercialisation (the beneficiary may not market or distribute the software), no sublicensing, and confidentiality obligations applying to the released source code.

3.5 Governing Law, Jurisdiction, and Dispute Resolution

For India-domiciled parties, Indian governing law and jurisdiction in the relevant High Court is the standard approach. Where the vendor is a foreign entity, the choice of governing law requires more careful consideration.

- **International arbitration:** For cross-border arrangements, arbitration under SIAC, ICC, or DIAC rules provides a neutral forum with internationally enforceable awards under the New York Convention.
- **Expert determination:** For technical disputes — particularly whether a release condition has been met — expert determination by a named technology specialist can be faster and more appropriate than arbitration.
- **Interim relief:** Beneficiaries in urgent situations can seek interim injunctions from Indian courts under Section 9 of the Arbitration and Conciliation Act, 1996 or under Order XXXIX of the CPC. The escrow agreement should expressly preserve this right.

Chapter 4: Phase 3 — Making the Deposit

4.1 What Must Be Deposited: The Complete Deposit Schedule

The single most common cause of escrow failure is an inadequate deposit. 'Source code' alone is nearly always insufficient. A beneficiary who receives source code without build scripts, dependencies, configuration files, and documentation will be unable to rebuild a working system — the code becomes an artefact rather than a tool.

The deposit schedule should be defined with reference to nine categories of materials:

1. **Source Code:** All modules, microservices, libraries, and version-tagged releases. Specify the version control system (Git, SVN) and branching convention used.
2. **Build Scripts and Compilation Instructions:** Makefiles, Gradle scripts, Maven configuration, CI/CD pipeline definitions — anything required to compile the source code into a working executable.
3. **Third-Party Libraries, Frameworks, and Dependencies:** All external packages and libraries, including version-pinned specifications (requirements.txt, package.json, pom.xml). Note any commercially licensed components.
4. **Configuration Files and Environment Variables:** Application configuration files, environment variable definitions, and any secrets or credentials required for operation (appropriately managed and documented).
5. **Database Schemas and Migration Scripts:** All DDL scripts defining the database structure, along with migration scripts for version upgrades. Include seed data required for system initialisation.
6. **Infrastructure and Deployment Instructions:** Infrastructure-as-Code templates (Terraform, CloudFormation), Docker Compose or Kubernetes configurations, and deployment runbooks.
7. **Test Suites and Test Data:** Automated test scripts (unit, integration, end-to-end) and representative test data sets — essential for Level 3 functional verification.
8. **Technical and Operational Documentation:** System architecture documents, data flow diagrams, API documentation, operator manuals, and known issue logs.
9. **Licences, Keys, and Certificates:** Third-party software licences, code-signing certificates, SSL/TLS certificates, and encryption key management documentation.

4.2 Delivery Methods and Formats

- **Secure portal upload:** Most escrow agents provide an encrypted portal for electronic deposit. This is the standard method for initial and periodic manual deposits.
- **Automated API integration:** For continuous deposit arrangements, the escrow agent's platform integrates directly with GitHub, GitLab, or Bitbucket — triggering an automatic deposit on each version tag or release event.
- **Physical media:** Encrypted USB drives or optical media are occasionally used for very large deposits, air-gapped environments, or where the parties have concerns about transmission security. The physical chain of custody should be documented.

All deposits should be labelled with the software name, version number, deposit date, and the responsible individual at the vendor. Handover should generate a formal deposit receipt.

4.3 The Deposit Receipt

The deposit receipt is a critical document — frequently undervalued in practice. A valid receipt should confirm:

- The date and time of deposit receipt by the agent
- The software name and version covered by the deposit
- A list or hash-based inventory of the materials received
- The identity of the depositing individual and the recipient agent representative

The receipt protects all three parties: the vendor has documentary evidence of compliance; the beneficiary can confirm the deposit is current; the agent has a liability shield confirming it received exactly what is documented. Best practice is to issue a receipt per deposit version — not merely a single receipt at the inception of the arrangement.

Chapter 5: Phase 4 — Verification

5.1 Why Verification Is Non-Negotiable

Verification is the test of whether the escrow arrangement works. An unverified deposit is an assumption — a belief that the deposited materials are complete, buildable, and functional. When the release event occurs, assumptions are useless.

Industry experience consistently shows that a significant proportion of first-time verifications reveal material deficiencies: missing dependencies, obsolete build environments, incomplete configuration files, or documentation so sparse as to be unusable. These deficiencies are remediable before a crisis. They are not remediable after one.

The Escrow That Almost Wasn't

A financial services company with a software escrow in place requested verification for the first time in year four of a five-year agreement. The verification revealed that the deposit contained source code but no build scripts and no database schema — omissions that had been present since day one. The vendor remediated within 60 days. Had the release event occurred before verification, the escrow would have been worthless.

5.2 The Three Levels of Verification

Level	What Is Tested	Recommended For
Level 1 — Existence Verification	Confirms the deposit was received, is accessible, and matches the materials listed in the deposit schedule	Minimum baseline only — not sufficient for operational reliance
Level 2 — Build (Integrity) Verification	The source code is compiled in an isolated environment and produces a functional executable. Dependencies are confirmed present and version-consistent	Standard for all commercial software. Should be mandatory in every escrow agreement
Level 3 — Functional Verification	The built software is executed against agreed test scripts to confirm it operates as documented — processing transactions, generating outputs, or performing core functions	Mission-critical systems; regulated sector deployments; any system where business continuity is paramount

5.3 The Verification Process: Step by Step

10. The escrow agent receives the deposit and issues a receipt confirming materials received.
11. The beneficiary requests verification, or verification is triggered automatically per the agreement schedule.

12. The agent establishes an isolated build environment, configured to mirror the vendor's specified operating environment (OS, runtime versions, compiler settings).
13. The build attempt is executed against the deposited source code and build scripts.
14. For Level 3 verification, the built software is executed against the agreed functional test scripts, and outputs are recorded.
15. The agent issues a formal Verification Report — with a result of Pass, Conditional Pass (pass with noted deficiencies), or Fail — within the agreed SLA.
16. On a Fail result: the vendor is formally notified and is obliged to remedy the identified deficiencies and submit a corrected deposit within a defined period (typically 30–60 days).

5.4 Handling Verification Failures

Verification failures fall into several common categories:

- Missing dependencies — the source code references libraries or packages that were not included in the deposit
- Outdated build environment specifications — the deposited build scripts reference tools or runtimes at versions that are no longer available or that conflict
- Incomplete configuration — environment variables or connection strings required for compilation or operation are absent
- Documentation gaps — build instructions exist but are insufficiently detailed for an independent party to execute

On a verified failure, the vendor has a contractual obligation to remedy and re-deposit within the specified cure period. The beneficiary's rights if the vendor fails to remedy — including treating the failure as a material breach of the software licence — should be specified in the escrow agreement.

5.5 Periodic Re-Verification

Initial verification establishes that the escrow arrangement works at a point in time. Software is not static. Re-verification should be tied to:

- Each Major Version release — new functionality and architectural changes may introduce new dependencies or build requirements
- Annual cycles — at minimum, the arrangement should be verified annually, regardless of release activity
- Significant infrastructure changes — cloud migration, containerisation, or changes in third-party platforms

Cost allocation for periodic verification is a negotiable term. Best practice is for the beneficiary to bear the cost of annual verification as part of the ongoing escrow maintenance budget, with the vendor bearing the cost of re-verification following a verified failure.

Chapter 6: Phase 5 — Ongoing Management

6.1 Managing Deposit Updates

A software escrow arrangement is only as valuable as the currency of its deposit. An agreement with a deposit that is three major versions behind the production system protects against a release event — but releases a system that cannot run the beneficiary's data or support its current processes.

Update obligations should be linked to specific, documentable events:

- Every Major Version release (e.g., 4.x to 5.x) — mandatory within 30 days of release to production
- Every Minor Version release (e.g., 5.1 to 5.2) — mandatory within 45 days of release to production
- Critical security patches — mandatory within 15 days of patch release
- Significant architectural changes — even within a version, changes to the infrastructure, cloud platform, or database architecture should trigger an updated deposit

For organisations using automated continuous deposit via API integration with their version control system, these obligations are substantially self-executing. For manual deposit arrangements, a version register — maintained by the escrow agent — is essential for monitoring compliance.

6.2 Annual Escrow Review

Beyond deposit currency, the escrow arrangement itself requires periodic review. An annual review should address the following questions:

#	Review Question	Responsible Party
1	Is the deposit current with the production version of the software?	Escrow agent / Vendor
2	Have release conditions changed due to new regulatory requirements or updated risk assessment?	Legal Counsel / Compliance
3	Are all party details (vendor entity, beneficiary entity, authorised signatories) still accurate?	Legal Counsel / Procurement
4	Has the escrow agent maintained its ISO and other certifications, and is service quality satisfactory?	Beneficiary IT / Risk
5	Is the post-release licence scope still appropriate given current software usage?	Legal Counsel / CIO
6	Has verification been conducted since the last major version deposit?	Beneficiary / Escrow Agent
7	Has the vendor's financial health changed in ways that increase the risk of a release event?	Finance / Risk / Legal

6.3 Change of Escrow Agent

Circumstances occasionally require a change of escrow agent — agent insolvency, service quality deterioration, or cost rationalisation. This transition must be managed with care to avoid any gap in protection.

- Provide formal notice to the incumbent agent per the agreement's notice provisions
- Appoint the new agent and execute a new tripartite agreement before initiating the transfer
- Request a formal transfer of all deposit materials from the incumbent agent — document each item transferred
- Require the new agent to conduct an existence verification of all transferred materials immediately upon receipt
- Do not terminate the incumbent agreement until the new agent has confirmed receipt and the transfer is complete

Chapter 7: Phase 6 — Triggering and Executing the Release

7.1 Recognising a Release Event

Release events do not always announce themselves clearly. The most common failure is an organisation recognising a release event late — after the vendor's systems are already offline, support communications have ceased, and the crisis is acute. Monitoring for release events should be a defined responsibility, not an ad hoc activity.

Evidence Standards by Release Trigger

- **Insolvency filing:** Obtain a certified copy of the IBC filing or order from the NCLT; confirm the appointment of the Resolution Professional in the public register.
- **Cessation of business:** Compile formal support communications that have gone unanswered, any public announcements by the vendor, and MCA filings (if the company has been struck off).
- **Material breach of support:** Document the support requests made, the SLA commitments in the licence agreement, and the failure to respond or remedy within the contractual cure period.
- **Change of control:** Obtain evidence of the acquisition or change — public announcement, stock exchange filing, MCA Form MGT-6, or regulatory approval notification.

7.2 The Release Process: Step by Step

17. The beneficiary's authorised representative formally notifies the escrow agent in writing of the release condition, attaching the supporting evidence compiled above.
18. The escrow agent formally notifies the vendor of the release request and initiates the contrary instructions window — typically 10 to 15 days per the agreement.
19. If no contrary instructions are received within the window: the agent releases the deposit materials to the beneficiary per the agreed delivery method.
20. If contrary instructions are received: the dispute resolution mechanism specified in the agreement is activated. The agent holds the deposit pending resolution.
21. Post-resolution: the agent executes the release or confirms rejection per the dispute outcome, and issues a formal release receipt.

7.3 When the Vendor Disputes the Release

A vendor's contrary instructions are legitimate if they contest the occurrence of the release condition on factual or legal grounds. Common vendor objections include disputing whether an insolvency event has occurred (e.g., arguing that an IBC filing was subsequently dismissed) or asserting that the support breach has been remedied.

During a disputed release, the beneficiary faces a period of uncertainty. Practical interim measures include:

- Activating any disaster recovery arrangements or backup systems to maintain business operations
- Seeking urgent injunctive relief from the relevant court or invoking the emergency arbitrator provisions of the chosen arbitral rules

- Engaging an alternative support provider who can work with the executable software while the source code dispute is resolved

Dispute resolution costs — legal, arbitral, and expert fees — should be addressed in the escrow agreement. A provision requiring the unsuccessful party to bear costs provides a disincentive against bad-faith contrary instructions.

7.4 Post-Release: Restoring Business Continuity

The release of deposit materials is the beginning of the continuity recovery process, not the end. Organisations should have a post-release action plan prepared in advance — ideally as part of the annual escrow review.

- **Immediate (Day 1–7):** Confirm secure receipt of deposit materials; verify against the deposit schedule; engage legal counsel to confirm post-release licence scope.
- **Short-term (Week 1–4):** Engage a qualified third-party developer or maintenance firm; establish the build environment using the deposited infrastructure instructions; conduct an internal assessment of pending patches or support issues.
- **Medium-term (Month 1–6):** Address security vulnerabilities identified during the transition; assess data continuity and credentials management; manage compliance obligations arising from the vendor relationship change.
- **Longer-term (Month 6–24):** Evaluate the strategic path — continued self-maintenance, migration to an alternative, or re-procurement of a new system. The post-release licence duration should govern this timeline.

Chapter 8: Special Topics for Indian Practitioners

8.1 RBI IT Directions, 2023 and Software Escrow Obligations

The Reserve Bank of India's Master Direction on Information Technology Governance, Risk, Controls and Assurance Practices, 2023 (RBI IT Directions, 2023) represents the most significant regulatory driver of software escrow adoption in the Indian financial sector.

Section 12(f) of the RBI IT Directions, 2023 requires Regulated Entities (REs) — banks, non-banking financial companies, urban co-operative banks, and other entities within the RBI's supervisory perimeter — to maintain software escrow arrangements for critical technology systems. The Direction specifies that:

- Software escrow agreements must be in place for all critical and important IT systems
- The escrow must cover source code and all materials necessary to maintain and operate the system
- The arrangement must be subject to periodic testing to verify that the escrowed materials are complete and operational

Compliance obligations extend beyond simply executing an agreement. The IT Steering Committee (ITSC) governance framework required by the Directions demands documented evidence of:

- The escrow agreement itself, including the deposit schedule and release conditions
- Verification reports demonstrating that the deposit has been tested and confirmed functional
- Version registers confirming that the deposit is current with the production system
- Board or Senior Management approval of the IT risk governance framework within which escrow sits

Compliance Gap Assessment

Regulated entities that have escrow agreements in place but have never commissioned verification, or whose deposits are multiple versions behind the production system, are likely non-compliant with the spirit and intent of the RBI IT Directions, 2023. EscrowNXT's verification and deposit management services provide the documented evidence trail required for regulatory reporting.

8.2 Software Escrow Under Indian Contract Law

The software escrow arrangement is a tripartite contract governed by the Indian Contract Act, 1872. Several specific legal dimensions are relevant for Indian practitioners:

- **Release conditions as conditions precedent:** Under Indian contract law, release conditions are properly characterised as conditions precedent — the agent's obligation to release is contingent on the occurrence of a defined event. Until the condition is fulfilled, the obligation does not arise. Objective, documentary release conditions are essential for enforcement.
- **IBC, 2016 — timing of release:** Where the vendor is undergoing insolvency resolution under the Insolvency and Bankruptcy Code, 2016, the moratorium imposed under Section 14 of the IBC may affect the ability to enforce release obligations. Practitioners should ensure that the escrow

agreement addresses IBC scenarios explicitly and take advice on whether the deposit materials constitute 'assets' for moratorium purposes.

- **DPDPA, 2023 — deposit materials containing personal data:** Where the deposit materials include database schemas, migration scripts, or test data containing personal data, the Digital Personal Data Protection Act, 2023 (DPDPA) may impose obligations on the vendor as a Data Fiduciary and on the escrow agent as a Data Processor. The escrow agreement should include appropriate data processing provisions.

8.3 Cross-Border Escrow Arrangements Involving Indian Parties

Many Indian enterprises license critical software from overseas vendors — particularly in the enterprise software, cloud services, and specialised industrial technology sectors. Cross-border escrow arrangements introduce additional complexity:

- **Jurisdiction and enforcement:** A release order from an Indian court may not be directly enforceable against a foreign vendor or its assets. International arbitration — with awards enforceable under the New York Convention — provides a more reliable enforcement pathway. The escrow agreement should specify the arbitral seat, rules, and the language of proceedings.
- **Using an India-domiciled escrow agent:** For entities regulated by RBI, SEBI, or IRDAI, the use of a foreign escrow agent introduces regulatory risk — both in terms of supervisory access and the enforceability of the escrow arrangement under Indian law. An India-domiciled, RBI-aware escrow agent substantially reduces this risk.
- **FEMA considerations:** Payment of escrow fees to a foreign agent constitutes a cross-border remittance. FEMA compliance — including AD Bank reporting and purpose code compliance — must be addressed. The vendor may be better positioned to bear escrow agent fees where the agent is foreign, to simplify the beneficiary's FEMA obligations.

Chapter 9: Quick-Reference Tools for Practitioners

9.1 Master Checklist: Software Escrow Arrangement Lifecycle

✓	Action Item	Responsible Party
☐	Conduct software criticality assessment for all major licensed systems	CIO / IT Risk
☐	Document internal business case for escrow	CIO / Legal Counsel
☐	Identify regulatory obligations (RBI IT Directions, IRDAI, etc.)	Compliance Manager
☐	Evaluate prospective escrow agents against evaluation criteria	Procurement / IT / Legal
☐	Confirm agent holds ISO 27001:2022 and ISO 9001:2015	Procurement
☐	Confirm agent offers Level 2 / Level 3 verification	IT / CIO
☐	Insert escrow clause in initial software licence agreement draft	Legal Counsel
☐	Define deposit materials exhaustively in the Deposit Schedule	Legal Counsel / IT
☐	Draft objective, documentary release conditions	Legal Counsel
☐	Define post-release licence scope, duration, and restrictions	Legal Counsel
☐	Specify verification obligations and frequency	Legal Counsel
☐	Agree governing law, jurisdiction, and dispute resolution mechanism	Legal Counsel
☐	Vendor makes initial deposit within agreed timeframe	Vendor / Escrow Agent
☐	Deposit receipt issued and filed	Escrow Agent
☐	All nine deposit material categories confirmed in receipt	Beneficiary / Legal Counsel
☐	Commission Level 2 / Level 3 verification within 60 days of initial deposit	Beneficiary
☐	Review verification report — confirm Pass or action remediation	Beneficiary IT / Legal
☐	Schedule periodic re-verification linked to version releases	Beneficiary / Escrow Agent
☐	Monitor vendor for deposit update compliance against version register	Beneficiary IT / Legal

☐	Conduct annual escrow review using the seven-question framework	CIO / Legal / Compliance
☐	Monitor for release event indicators	Legal / IT Risk
☐	Compile evidence per release condition documentary standards	Legal Counsel
☐	Formally notify escrow agent with supporting documentation	Legal Counsel
☐	Execute post-release action plan	CIO / IT / Legal

9.2 Deposit Materials Schedule Template

This template is ready for insertion as a schedule to any Software Escrow Agreement. Version tracking fields should be completed at each deposit event.

Category	Description of Materials	Version / Date	Deposited ✓
1. Source Code	All modules, microservices, libraries (specify VCS and branch)		
2. Build Scripts	Makefiles, Gradle, Maven, CI/CD pipeline definitions		
3. Dependencies	All third-party packages with version-pinned manifests		
4. Configuration	Config files, environment variable definitions, secrets documentation		
5. Database	DDL scripts, migration scripts, seed data		
6. Infrastructure	IaC templates, Docker/Kubernetes configs, deployment runbooks		
7. Test Materials	Automated test suites, test data sets		
8. Documentation	Architecture docs, API docs, operator manuals, known issue logs		
9. Licences & Keys	Third-party licences, code-signing certificates, SSL/TLS certs		

9.3 Escrow Agent Evaluation Scorecard

Use this weighted scoring matrix to compare prospective escrow agents. Score each criterion from 1 (poor) to 5 (excellent) and multiply by the weight.

Criterion	Weight	Agent A Score	Agent B Score	Notes

ISO 27001:2022 certification (current)	25%			*Disqualify if absent*
ISO 9001:2015 certification (current)	10%			
Verification capability (Level 2 & 3)	25%			*Disqualify if Level 2 unavailable*
Deposit update processes and automation	15%			
Independent dispute resolution mechanism	10%			
SLA response times (deposit, release, report)	10%			
India-domiciled / RBI-aware operations	5%			*Mandatory for regulated entities*

9.4 Release Event Evidence Checklist

Compile the following documentation before formally notifying the escrow agent of a release condition:

- Written notification to the vendor of the alleged release condition and the vendor's response (or absence of response)
- For insolvency: certified copy of IBC filing, NCLT order, or voluntary liquidation resolution
- For cessation of business: MCA strike-off notice; evidence of website / communication channels going dark; unanswered support tickets with timestamps
- For material support breach: the relevant SLA provisions from the licence agreement; log of support requests with dates and ticket references; evidence of breach and expiry of cure period
- For change of control: public announcement, stock exchange filing, or regulatory approval notification
- Legal counsel confirmation of the legal basis for release
- Board or Senior Management authorisation of the release request (as required by internal governance)

9.5 Glossary of Key Escrow Terms

Term	Plain-Language Definition
Beneficiary	The enterprise or organisation that is protected by the escrow arrangement and is entitled to receive the deposit materials if a trigger event occurs. Also called the licensee.
Build Test	Level 2 verification — a technical test in which the escrow agent attempts to compile the deposited source code into a working executable in an isolated environment.
Contrary Instructions	A formal dispute lodged by the vendor (depositor) within the specified window following a release request, challenging whether a trigger event has occurred.

Deposit Materials	All items placed in escrow — source code, build scripts, dependencies, configuration files, database schemas, infrastructure instructions, documentation, licences, and keys.
Deposit Receipt	A formal document issued by the escrow agent confirming receipt of the deposit materials, the version covered, and the date of deposit.
Depositor	The software vendor or developer who places deposit materials in escrow. Also called the licensor.
Escrow Agent	The neutral third party (such as EscrowNXT) that holds the deposit materials, verifies them, and executes release per the agreed conditions.
Functional Test	Level 3 verification — testing in which the built software is operated against agreed test scripts to confirm it performs its core functions as documented.
Post-Release Licence	The rights granted to the beneficiary upon release — typically internal use, bug-fixing, and engagement of third-party maintainers, subject to defined restrictions.
Release Condition	A defined trigger event (such as vendor insolvency or cessation of support) that entitles the beneficiary to request release of the deposit materials. Also called a trigger event.
Tripartite Agreement	A software escrow agreement with three parties: the depositor (vendor), the beneficiary (licensee), and the escrow agent.
Update Obligation	The vendor's contractual duty to submit refreshed deposit materials whenever the production software is updated to a new version.
Verification	Technical testing of the deposit materials to confirm they are complete, buildable, and functional — available at Level 1 (existence), Level 2 (build), and Level 3 (functional).
Version Register	A log maintained by the escrow agent recording each deposit event — the software version, deposit date, and materials received — used to monitor deposit currency.

Conclusion and Next Steps

Software escrow, properly implemented, is not a contingency plan for pessimists. It is standard infrastructure for enterprises that take business continuity seriously — a documented, tested, and enforceable mechanism that converts vendor dependency risk from an open-ended threat into a managed, bounded liability.

The six phases of the escrow lifecycle — needs assessment, provider selection, agreement negotiation, deposit, verification, and ongoing management — each require deliberate attention. An arrangement that addresses five of the six phases adequately but fails on verification or deposit currency is only marginally more protective than no arrangement at all.

The practical guidance in this handbook — the checklists, templates, and frameworks in Chapter 9 in particular — is designed to be used, not filed. Practitioners are encouraged to incorporate these tools into their standard technology procurement workflows, annual risk review cycles, and vendor management processes.

Minimum Viable Next Steps

22. Identify your top five licensed technology systems and score them for vendor dependency risk using the criticality framework in Section 2.1.
23. For any system scoring high risk, check whether an escrow agreement is in place — and if so, when it was last verified and whether the deposit is current.
24. If operating in a regulated sector, review your obligations under the RBI IT Directions, 2023 or equivalent sector regulator guidance and assess compliance gaps.
25. For any new software licence negotiation above the criticality threshold, instruct legal counsel to include the model escrow clause at Section 3.1.
26. Contact EscrowNXT to commission a verification of any existing escrow arrangement that has not been tested within the past 12 months.

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.

— EscrowNXT Services Private Limited

Contact EscrowNXT

CIO / CTO: Book a free risk assessment — www.escrownxt.com/contact-us

Legal / Compliance: Request a sample escrow agreement — info@escrownxt.com

CFO / Procurement: Discuss cost-benefit and coverage options — +91 44 45535571/72

Software Developers / ISVs: Learn how escrow strengthens your enterprise sales — www.escrownxt.com

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.

EscrowNXT is a NASSCOM member since 2011 and is trusted by leading brands, market leaders, and corporate houses across India's financial services, healthcare, manufacturing, government, and technology sectors.

Our Services

Service	Description
Software Escrow	Tripartite agreement securing source code and documentation; released on trigger events including vendor bankruptcy, litigation, and material breach of support obligations
Technology Escrow	Broader protection: source code, hardware schematics, manufacturing processes, formulas, blueprints, encryption keys, embedded software, and other intellectual property assets
IP Archive	Secure, long-term archival of intellectual property assets with documented chain of custody
Verification & Testing	Technical validation — Integrity Verification, Material Audit, and Complete Verification — with plain-language reports accessible to technical and non-technical stakeholders
Vaults	Secure, compliant, dedicated storage facilities for sensitive technology and legal materials

Contact Details

Website: www.escrownxt.com

Email: info@escrownxt.com

Phone: +91 44 45535571 / +91 44 45535572 / +91 44 22505571

Address: C2-A, Industrial Estate, Guindy, Chennai – 600 032, Tamil Nadu, India