8 Questions to Ask Before Choosing a Software Escrow Provider

A Practical Checklist for Technology Buyers, CIOs, and Legal Counsel

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

Executive Summary

Software escrow is not a commodity. Yet in practice, many technology buyers treat it like one — choosing a provider based on price alone, or defaulting to whichever name appears first in a procurement shortlist.

That approach carries significant risk. A poorly structured escrow arrangement — with a provider that lacks legal rigour, technical competence, or operational stability — is little better than no escrow at all. If your escrow provider cannot actually deliver the deposit materials when a trigger event occurs, you have paid for the illusion of protection.

This white paper gives IT procurement teams, in-house legal counsel, CFOs, and vendor management officers a structured framework for evaluating any software escrow provider. It distils twenty years of EscrowNXT's experience managing software escrow arrangements for Indian enterprises into eight essential questions — the questions that reveal whether a provider can truly protect your technology investment when it matters most.

Key Finding

Not every organisation that calls itself a software escrow provider has the legal standing, technical infrastructure, and operational systems to fulfil an escrow obligation under Indian law. Asking the right questions before you sign is the single most cost-effective risk mitigation step available to any technology buyer.

Why This Checklist Exists

When a software vendor goes out of business, gets acquired, or simply stops supporting a product, the consequences for the customer can be severe. ERP systems freeze. Manufacturing lines stop. Customer-facing platforms go dark. Legal obligations go unmet.

Software escrow exists to prevent exactly this scenario. Under a tripartite escrow arrangement, the vendor (licensor) deposits source code and related materials with an independent escrow agent. If a defined trigger event occurs — insolvency, acquisition, breach of support obligations — the escrow agent releases those materials to the licensee, enabling the business to continue operating or to migrate to an alternative solution.

The concept is straightforward. The execution, however, demands precision. The escrow agreement must be legally sound. The deposit materials must be complete, current, and verified. The escrow agent must be operationally capable of release under pressure. And the provider must still be in business — and in good standing — when the trigger event happens.

This checklist was developed to help buyers make an informed, rigorous selection decision. Use it when evaluating any escrow provider, at initial procurement or at contract renewal.

The 8 Questions

Q1 Are you an independent, specialist escrow provider — or is escrow a side offering?

Some organisations offer software escrow as an ancillary service attached to a law firm, a document storage business, or a data centre operation. Others are dedicated, pure-play escrow providers for whom this is the entire focus of the business.

The distinction matters. A specialist escrow provider has built its operations, legal frameworks, technical capabilities, and staff training specifically around the demands of escrow. A generalist offering escrow as one line item among many may lack the depth of expertise to manage complex release scenarios, multi-party disputes, or large-scale technology deposits.

- Ask the provider what percentage of its revenue comes from escrow services.
- Ask how long the escrow practice has been operating independently.
- Ask whether the team handling your account has dedicated escrow expertise or a divided focus.

WHY IT MATTERS *Escrow arrangements are typically dormant for years — and then suddenly critical. You need a provider whose entire institutional focus is on being ready for that moment.*

Q2 What certifications and regulatory standing does your organisation hold?

Certifications are not marketing badges — they are operational evidence. ISO 9001:2015 certification demonstrates that a provider has documented, auditable quality management systems for how it accepts deposits, manages escrow accounts, and processes releases. ISO 27001:2022 certification demonstrates that the provider has independently verified information security controls protecting your most sensitive IP.

In the Indian context, NASSCOM membership is a meaningful signal of industry standing and alignment with technology sector standards. Absence of certifications does not automatically disqualify a provider, but it should prompt harder questions about how quality and security are managed in the absence of third-party validation.

- Request copies of current ISO certificates — verify they are in scope for escrow operations.
- Ask when the certificates were last renewed and who the certifying body is.
- Ask about NASSCOM or equivalent industry memberships.

WHY IT MATTERS *If your escrow provider experiences a data breach or mishandles your deposit materials, you have no recourse against an uncertified provider. Certifications create an auditable chain of accountability.*

Q3 What does your standard escrow agreement include — and what are the release conditions?

The escrow agreement is the legal foundation of the entire arrangement. A well-drafted escrow agreement defines: the roles and obligations of all three parties (licensor, licensee, escrow agent); the deposit materials in precise scope (source code, build instructions, documentation, encryption keys, third-party components); the trigger events that permit release; the release procedure including verification and dispute resolution; and the governing law and jurisdiction.

Many providers use template agreements that are not tailored to the specific technology being escrowed or the commercial relationship between the parties. A blanket trigger event such as 'vendor insolvency' without defining what constitutes insolvency under Indian law, or without cross-referencing the specific legislation, creates ambiguity that could delay or prevent release precisely when you need it most.

- Request the provider's standard agreement and have it reviewed by in-house or external legal counsel.
- Ask specifically how trigger events are defined — and whether they are aligned with Indian insolvency and contract law.
- Ask what the release procedure is, step by step, including timelines.
- Ask whether the agreement includes a dispute resolution mechanism and what it costs to invoke.

WHY IT MATTERS *An escrow agreement that is legally vague or operationally ambiguous can be challenged by the licensor at the moment of release. The agreement is not a formality — it is the instrument on which your business continuity depends.*

Q4 How do you verify that the deposit materials are complete and functional?

Depositing source code into an escrow vault is only the first step. Without verification, you have no assurance that what has been deposited is actually the current, complete, buildable version of the software your business depends on. Verification is the technical audit that confirms the deposit materials are what they claim to be.

Verification services range from basic integrity checks (confirming the files exist and are not corrupted) to full functional testing (confirming the deposited source code can be compiled and executed to produce the licensed software). The appropriate level of verification depends on the criticality of the software and the complexity of the technology.

- Integrity Verification — confirms files are uncorrupted and complete in structure.
- Material Audit — confirms the deposit matches the agreed scope and includes all defined components.
- Complete Verification — confirms the source code can be built and executed to produce a working version of the software.

Ask the provider whether verification is included in the base fee or charged additionally. Ask who conducts the verification — internal staff, external technical experts, or automated tools. Ask for a sample verification report, and confirm that the report is written in plain language accessible to both technical and non-technical stakeholders.

WHY IT MATTERS *A deposit of incomplete or non-buildable source code is useless at the moment of release. Verification is the only mechanism that confirms your escrow arrangement has genuine protective value.*

Q5 How do you manage deposit updates as the software evolves?

Software is not static. Every major release, patch, and update to the licensed software should trigger a corresponding update to the escrow deposit. An escrow arrangement that holds a three-year-old version of a software product provides diminishing protection as the software evolves.

Providers differ significantly in how they manage deposit currency. Some require the licensor to proactively submit updates; others build deposit update schedules into the agreement and enforce them. Some provide online portals for deposit submission; others rely on physical media.

- Ask how deposit updates are scheduled — is there an automatic reminder or obligation mechanism?
- Ask how the provider confirms that a new deposit has been received and logged.
- Ask whether a new version triggers re-verification or whether the previous verification remains in effect.
- Ask what happens if the licensor fails to deposit updated materials — does the agreement create any obligation or remedy?

WHY IT MATTERS *The deposit that exists at the moment of a trigger event is the deposit you receive. If it is two major versions out of date, your recovery capability is significantly diminished.*

Q6 What are your physical and digital security standards for stored materials?

The materials held in escrow — source code, technical documentation, encryption keys, hardware schematics — represent some of the most sensitive intellectual property in your vendor's possession. The escrow provider holds these materials in trust. The security standards applied to their storage are therefore directly relevant to your own IP protection obligations, your data governance frameworks, and in some cases your regulatory compliance requirements.

Providers should be able to explain their physical security arrangements (access controls, CCTV, fire suppression, environmental monitoring at vault facilities), their digital security controls (encryption at rest and in transit, access logging, role-based access controls), and their

business continuity arrangements (what happens to your deposit materials if the escrow provider itself experiences a disaster).

- Ask for a description of the physical vault facilities — location, access controls, redundancy.
- Ask what encryption standards are applied to digital deposit materials.
- Ask about access logging — who can view your deposit materials, under what authority, and with what audit trail.
- Ask what the provider's own business continuity plan is, including how your materials are protected if the provider's systems fail.

WHY IT MATTERS *A breach of escrow materials could expose your vendor's IP — and potentially your own confidential system data — to third parties. Security standards are a non-negotiable element of escrow due diligence.*

Q7 What is your track record — and can you provide references or case experience?

An escrow provider's track record is the most direct evidence of operational capability. Any provider can describe their processes in a sales presentation. Fewer can point to a documented history of successful releases, multi-party dispute management, and long-term client relationships across different sectors and technology types.

In evaluating track record, distinguish between longevity of the organisation and depth of escrow-specific experience. A provider that has been in business for twenty years but has managed only a handful of escrow arrangements each year has a very different risk profile from a provider that has managed thousands of active escrow agreements across diverse technology environments.

- Ask how many active escrow agreements the provider currently manages.
- Ask how many release events the provider has managed — and whether any resulted in litigation or dispute.
- Ask for sector-specific references relevant to your industry.
- Ask whether the provider has experience with complex multi-party arrangements, international software vendors, or SaaS and cloud-based software escrow.

WHY IT MATTERS *An escrow release in a contested insolvency scenario is not the moment to discover that your provider has never managed a release before. Experience and track record are the most reliable predictors of capability under pressure.*

Q8 What is your pricing structure — and what is included in the base fee?

Escrow pricing is frequently less transparent than it appears. A low headline fee may exclude verification, deposit updates, multi-beneficiary arrangements, or release management.

Understanding the full cost of escrow — over a three-to-five-year contract horizon — requires mapping every scenario in which additional fees may apply.

The total cost of ownership for an escrow arrangement should be evaluated against the cost of the risk it mitigates. A major enterprise software system that takes eighteen months and significant capital to replace has a very different escrow calculus from a peripheral application. Price negotiation should happen in this context, not in isolation.

- Ask for a full schedule of fees — setup, annual management, verification (all levels), deposit updates, release management, and dispute resolution.
- Ask whether the fee covers a single beneficiary or multiple.
- Ask what fee adjustments apply if the software grows significantly in scope or complexity.
- Ask whether there is a fee for accessing the escrow agreement and deposit records for audit purposes.

WHY IT MATTERS	*An escrow arrangement priced to appear affordable but structured to generate significant fees on every operational event is not cost-effective over a multi-year contract. Total cost of ownership — not headline price — is the relevant metric.*

Quick-Reference Summary

Use this table as a rapid evaluation tool when comparing providers.

#	Question	What a Strong Answer Looks Like
Q1	**Specialist or generalist?**	Dedicated escrow provider; 100% focus on escrow services
Q2	**Certifications?**	ISO 9001:2015 + ISO 27001:2022 certified; NASSCOM member
Q3	**Agreement quality?**	Bespoke or well-drafted standard; clear trigger events; release procedure defined
Q4	**Verification services?**	Three levels offered; plain-language report; independent technical review
Q5	**Deposit update management?**	Scheduled updates; confirmation process; obligation mechanism for licensor
Q6	**Security standards?**	Certified physical vaults; encryption; access logging; BCP documented
Q7	**Track record?**	Hundreds of active agreements; documented release history; sector references
Q8	**Transparent pricing?**	Full fee schedule available; no hidden release or update fees

Conclusion

Selecting a software escrow provider is a risk management decision with long-term consequences. The questions in this checklist are designed to surface the difference between a provider that can genuinely protect your business continuity and one that simply fulfils a procurement checkbox.

Escrow is not a contingency plan for pessimists. It is standard infrastructure for enterprises that take technology dependency seriously. Ask these eight questions at the outset — and ask them again at every contract renewal. The answers will tell you everything you need to know.

Immediate Next Steps

- Distribute this checklist to your vendor management and legal teams before the next escrow procurement or renewal.
- Map your critical software systems against current escrow coverage — identify any gaps.
- Request verification reports from your existing escrow provider for all active deposits.
- Review your current escrow agreements against the trigger event and release procedure standards outlined in Question 3.
- If you have not reviewed your escrow arrangements in the past twelve months, schedule a provider review now.

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 & Testing, and secure Vaults. We are a NASSCOM member since 2011, trusted by market leaders across sectors who need assured access to business-critical technology.

Contact Us

Website
www.escrownxt.com
Email
info@escrownxt.com
Phone
+91 44 45535571 / 72 | +91 44 22505571

Address
C2-A, Industrial Estate
Guindy, Chennai – 600 032
Tamil Nadu, India
Request a Free Escrow Assessment
www.escrownxt.com/contact-us

Appendix: Glossary of Escrow Terms

The following terms are used throughout this white paper and in standard software escrow practice.

Deposit Materials	The source code, build instructions, documentation, encryption keys, and any other materials placed into escrow by the licensor under the terms of the escrow agreement.
Escrow Agent	The independent third party (the escrow provider) that holds the deposit materials and manages the escrow arrangement on behalf of the licensor and licensee.
Integrity Verification	A technical check confirming that the deposited files are complete, uncorrupted, and match the agreed deposit specification.
Licensor	The software vendor or developer who deposits materials into escrow and grants the licensee the right to use the software under a licence agreement.
Licensee	The technology buyer or end user who is the beneficiary of the escrow arrangement and entitled to receive deposit materials upon a trigger event.
Material Audit	A verification service confirming that the deposit matches the agreed scope and includes all defined components — source code, documentation, third-party components, and build instructions.
Complete Verification	The highest level of verification, confirming that the deposited source code can be compiled and executed to produce a working version of the licensed software.
Release Conditions	The defined circumstances under which the escrow agent is authorised to release deposit materials to the licensee.
Trigger Event	A specific event defined in the escrow agreement that entitles the licensee to request release of deposit materials (e.g., licensor insolvency, acquisition, or failure to maintain support obligations).
Technology Escrow	A broader form of escrow covering not only source code but also hardware schematics, manufacturing processes, formulas, blueprints, encryption keys, embedded software, and other proprietary technology.