PRAXIS
TECHNOLOGY ESCROW

Whitepaper:

Mitigating Risks of Disruption to Business-Critical Software and SaaS Applications Through Vendor Failure

Third-Party Risk Management (TPRM) professionals are tasked with safeguarding organizational resilience by anticipating and mitigating risks tied to critical vendors. Today, **software escrow** and **SaaS escrow** agreements have become essential because business-critical applications now sit entirely in the hands of external providers. If those providers fail, the results can be catastrophic: downtime, financial losses, regulatory penalties, and reputational damage.

This paper explains why vendor failure is among the most urgent risks to address—and how PRAXIS Technology Escrow delivers unmatched protection with:

- **Automated Escrow™**: The only escrow solution built to keep pace with agile development.
- **Infinite Retention™**: Exclusive archival of *all* deposit versions, forever.
- **Technical Verification**: Independent assurance that deposits are complete, current, and usable.

By integrating these services, enterprises can protect business-critical software and SaaS applications from disruption, ensuring continuity even in the face of vendor bankruptcy.

Introduction

Over the past 30 years, organizations have steadily increased their reliance on third-party software and technology vendors. In the early days of commercial software, enterprises typically purchased perpetual licenses, installed applications on their own servers, and maintained them internally. Vendor risk existed, but it was easier to manage because clients had physical possession of the software.

That changed with the rise of **outsourced development, SaaS models, and cloud-native applications**. Today, most organizations run mission-critical systems that are fully controlled by external vendors—whether through proprietary source code, hosted platforms, or subscription services. This shift delivered agility, cost savings, and scalability, but it also introduced a serious dependency: if the vendor fails, the client may suddenly lose access to essential tools and data.

The **software escrow industry** emerged to address this risk. At its core, escrow is simple: a neutral third party holds a vendor's source code, documentation, or SaaS data-access materials in trust. If the vendor fails, those materials are released to the client under predefined conditions.

In the 1980s and 1990s, escrow deposits were usually **manual**—physical media (like tapes or CDs) shipped once or twice per year. These deposits were quickly outdated and often incomplete, leaving beneficiaries exposed when they needed them most.

As development practices evolved—especially with the widespread adoption of **agile methodologies**—manual escrow became obsolete. Agile teams update code continuously. A static deposit updated once a year cannot keep up.

That is why PRAXIS Technology Escrow was founded: to modernize the industry with solutions built for today's software environment. PRAXIS pioneered:

- **Automated Escrow™**: Direct integration with GitHub, GitLab, Bitbucket, and Azure DevOps. Deposits update in real time.
- **Infinite Retention™**: A unique "never delete" policy that archives every version of every deposit, forever.
- **Technical Verification**: Testing to ensure deposits are complete, accurate, and buildable.

Together, these services transform escrow from a **paper safeguard** into a **true continuity solution** that matches the speed and complexity of modern software and SaaS ecosystems.

What Is Software Escrow?

A **software escrow agreement** is a three-party arrangement between:

- **Vendor (Depositor):** The software or SaaS provider.
- **Beneficiary (Client):** The organization relying on the software.
- **Escrow Agent (Neutral Third Party):** A professional like PRAXIS Technology Escrow.

The vendor deposits source code, documentation, or SaaS data-access tools into escrow. If specific "trigger events" occur—such as bankruptcy or service failure—those materials are released to the client.

The Risks of Vendor Failure

What Vendor Failure Looks Like

Vendor failure may take the form of bankruptcy, insolvency, acquisition, or operational collapse. In each case, the outcome is the same: loss of access to software, updates, and hosted data.

The Consequences

- **Operational Downtime:** Core systems grind to a halt.
- **Data Inaccessibility:** SaaS customers lose access to critical information.
- **Financial Costs:** Emergency migrations and replacements are expensive.
- **Reputational Harm:** Customers and partners lose trust.
- **Regulatory Exposure:** In industries like healthcare or finance, downtime may trigger penalties.

Why Bankruptcy Is Especially Dangerous

Bankruptcy is particularly disruptive. Intellectual property may be frozen or sold in proceedings, and hosted environments may become inaccessible overnight. Without escrow, clients have little recourse.

Real-World Example: Escrow in Action During Vendor Bankruptcy

A global energy technology company (the **Depositor**) developed dozens of proprietary applications powering renewable energy systems worldwide. A fast-growing clean energy project developer (the **Beneficiary**) relied on these applications to manage large-scale storage operations and fulfill contracts.

Before signing major deals, the Beneficiary required a **software escrow agreement** with PRAXIS. The Depositor submitted **48 applications** into escrow, and PRAXIS performed **full technical verification** on a subset of them, ensuring they could be built, tested, and deployed if released.

Soon after, the Depositor filed for **Chapter 11 bankruptcy protection**. As staff layoffs mounted—including key engineers—support deteriorated. The escrow agreement was triggered, and PRAXIS released the verified deposits.

Because verification had been performed, the Beneficiary knew the escrow materials were **complete, current, and functional**. They continued operating seamlessly while the Depositor reorganized. Without verification, they would have faced an emergency scramble to replace business-critical applications—a costly and potentially catastrophic disruption.

Lesson learned:

- For Beneficiaries, verification transforms escrow from a “check-the-box” safeguard into a **true continuity solution**.
- For Vendors, cooperation in escrow protects reputation—even during insolvency.

Why Manual Escrow Is Obsolete

- **Then:** Vendors shipped physical media (tapes, CDs, hard drives) to escrow agents once or twice a year.
- **Problem:** Deposits were outdated and incomplete.
- **Now:** Agile development updates code daily or weekly. A static deposit is useless.
- **Solution:** PRAXIS **Automated Escrow™**, which keeps deposits current by integrating directly with repositories like GitHub and Bitbucket.

Why PRAXIS Escrow Agreements Are Different

The Role of Escrow

A **software or SaaS escrow agreement** ensures critical materials—source code, documentation, SaaS data export tools, APIs—are deposited with a neutral escrow agent and released under specific conditions like bankruptcy or service failure.

PRAXIS' Differentiators

- **Automated Escrow™:** Continuous updates aligned with agile development.
- **Infinite Retention™:** No other escrow agent maintains a permanent archive of every version.
- **Agile Escrow™:** A bundled solution for modern SaaS environments.
- **Technical Verification:** Assurance that deposits are usable—not just stored.

Benefits

- **Continuity:** Systems remain operational during vendor failure.
- **Agility:** Escrow keeps pace with rapid development cycles.
- **Compliance:** Supports regulatory readiness.
- **Speed:** Recovery in days, not months.
- **Trust:** Demonstrates proactive risk management to stakeholders.

Key Terms You Should Know

- **Software Escrow:** Protects on-premises software source code and documentation.
- **SaaS Escrow:** Includes SaaS data export tools, APIs, and sometimes hosted environments.
- **Code Escrow:** Another term for software escrow.
- **Technology Escrow:** Broader category, covering software plus other IP like formulas, designs, or manufacturing processes.

The Importance of Verification

Why It Matters

Escrow deposits only help if they're usable. Without verification, beneficiaries risk receiving incomplete or corrupted materials.

Verification Process

- Completeness checks.
- Build testing in a controlled environment.
- Dependency mapping.
- SaaS data export/API validation.
- Documentation adequacy review.

Frequency

At minimum, verification should occur annually or semi-annually. PRAXIS's Automated Escrow™ makes this process seamless because deposits are always current.

Case Study Connection

In the **energy technology bankruptcy case**, verified deposits enabled seamless continuity. Without verification, the Beneficiary would have faced devastating downtime.

What Is Technical Verification?

Verification ensures escrow isn't just files in storage but a true continuity safeguard. At PRAXIS, verification includes:

- Checking deposit completeness.
- Building code in a controlled environment.
- Confirming dependencies are documented.
- Testing SaaS data exports and APIs.
- Reviewing documentation quality.

Best Practices for TPRM Professionals

- **Risk Assessments:** Evaluate vendor financial health and identify critical systems.
- **Escrow Agreements:** Implement PRAXIS Automated Escrow™ and Infinite Retention™.
- **Verification:** Schedule regular testing.
- **Ongoing Monitoring:** Track vendor stability and adjust agreements as needed.

Case Study Recap: Business Continuity Preserved

When the Depositor entered bankruptcy, PRAXIS's escrow and verification enabled the Beneficiary to continue operations without disruption. Regulatory compliance was maintained, downtime was avoided, and reputational damage was averted. This real-world example underscores why escrow—done right—is essential.

Vendor failure is not a hypothetical—it's inevitable. Traditional escrow cannot keep up with agile development and SaaS environments. PRAXIS sets the new standard with:

- **Automated Escrow™**: Always current.
- **Infinite Retention™**: Always complete.
- **Verification**: Always usable.

For TPRM professionals, PRAXIS transforms escrow from a legacy checkbox into a strategic **business continuity solution**.

TPRM professionals should:

1. Review contracts for business-critical vendors.
2. Implement PRAXIS Automated Escrow™ with Infinite Retention™.
3. Schedule periodic verification.
4. Educate stakeholders on escrow's role in vendor failure risk mitigation.

With PRAXIS, you don't just protect your software—you protect your business.

Disclaimer

This whitepaper is for informational purposes only and does not constitute legal or financial advice. Organizations should consult legal and technical experts when implementing escrow agreements.

About PRAXIS

At PRAXIS Technology Escrow, we combine innovation with security to protect your most critical software and technology assets. As innovators in the field, PRAXIS offers the most advanced solutions in the industry, ensuring your deposits are always up to date and never lost, thanks to our Automated Escrow™ solution and Infinite Retention Policy™. Providing services worldwide from our U.S. headquarters, we pride ourselves on delivering flexible, tailored escrow agreements that meet each client's unique needs, backed by PRAXIS' unmatched personal service. Our team of experts provides trustworthy and responsive support, ensuring your business continuity is always protected.

PRAXIS Technology Escrow, LLC

(800) 213 9802 / (770) 459 1202
www.praxisescrow.com or info@praxisescrow.com