

How to Minimize Risk with a Software Vendor 'Prenup'

Safeguard technology investments against contract breaches, discontinued support and vendor bankruptcy — before signing your next software agreement.

Research conducted by

IDG Research Services



Sponsored by



Executive Summary



Nothing is irrevocably written in stone. Not even personal promises. In our high-tech world, then, most vendor contracts are provisional at best.

Still, CIOs routinely strike up negotiations with vendors in pursuit of solid relationships. At the start, their bonds are strong, with all eyes on success. But what happens if something goes horribly wrong—if the vendor files for bankruptcy, for instance, or more commonly, discontinues its software support?

Smart CIOs protect themselves from the possibility of unfortunate circumstances with Technology Escrow agreements.

“Technology Escrows are like ‘prenups’ for software vendor relationships,” explains John Boruvka, vice president of intellectual property management at Boston-based Iron Mountain Digital. “No one goes into a marriage thinking it’s going to fail, but prenuptial agreements make for great safeguards—just in case.”

With escrows in place, CIOs ensure themselves access to critical application source code should disaster strike. And technical verification services provide added assurance that escrowed software is what CIOs need, when they need it.

In a recent online survey, Framingham, Mass.-based IDG Research Services set out to gauge information technology leaders’ perspectives on escrow agreements, as well as the importance of including verification services within them. The results proved intriguing:

- Technology Escrows are entered into based on the criticality, complexity and cost of applications.
- Nearly half of respondents say technical verification is an important component of escrowing.
- Confidence in escrow deposits is markedly higher among those that take advantage of technical verification services.

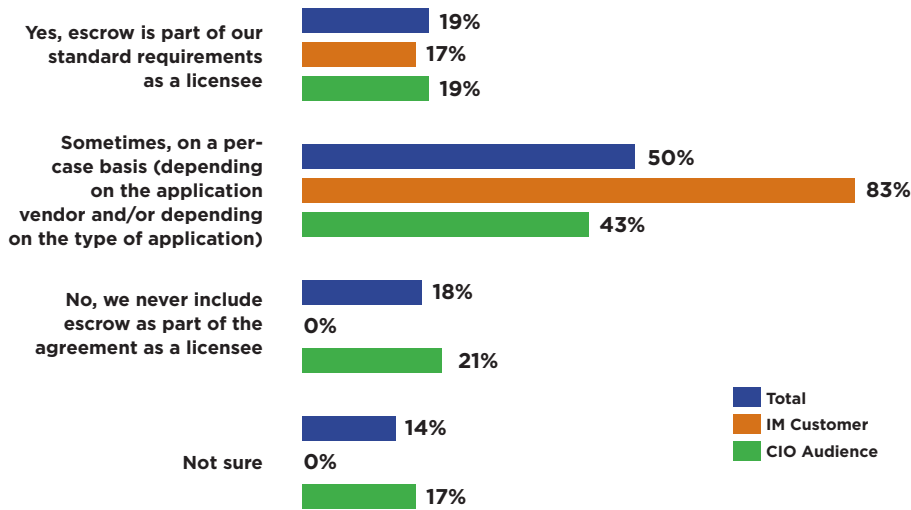
Escrow Prenups for Critical Apps

Kris Brady, IT director for Scottsdale, Ariz.-based Taylor Morrison, has no doubt that the company’s ERP application requires a technology prenup. Its application houses accounting, purchasing and sales records, and even pushes data to the company’s CRM application and external portals. It’s the very definition of mission-critical for Taylor, one of the nation’s largest homebuilders.

If its software vendor ceased operating—and there was no escrow in place—Taylor would be in trouble, according to Brady. “We would have to use whatever grace period we could get to flush out programmers to either hack into, or emulate the functionality of, the ERP source code,” he says, pointing out that software bugs could easily complicate that process. Long-term, he adds, the company would have to implement an entirely new ERP package, which would quickly raise the company’s angst level to high.

Luckily, Taylor has a Technology—or software—Escrow, which is a contractual arrangement under which the licensee requires its vendor to deposit source code into an account held by a third-party agent to ensure ongoing accessibility of the software. The deposit safeguards valuable technology assets—for both traditional on-premises software and SaaS licensing models—in secure, access-protected escrow accounts, much like a financial escrow.

Escrow Agreement as Part of Contract



As part of its survey, IDG Research Services polled the CIO audience and Iron Mountain customers separately on whether Tech Escrow is part of their software license strategy. This chart shows the results broken out by audience and the total response.

Source: IDG Research, August 2008

If the vendor files for bankruptcy or otherwise fails to maintain or support the software as contracted, the source code is released to the licensee. This ensures timely access rights to source code and maintenance materials, satisfies legal compliance and minimizes the risk of business disruption. What's more, licensees with an escrow deposit can verify that their media is there, check that it's readable, perform a complete build of the software, and conduct usability tests.

Given the fluctuating nature of the high-tech industry—the comings and goings, the mergers and layoffs and the march toward next-generation product releases—escrow arrangements are becoming commonplace. In fact, according to an IDG Research Services poll of information technology and business

leaders across a broad range of industries, 62 percent of responding companies always or sometimes include escrow as part of their software agreements. This was a two-phase survey. Phase 1 surveyed 174 *CIO* magazine readers employed at companies with 250 or more employees. Phase 2 polled 35 Iron Mountain customers and prospects, for a total of 209 qualified respondents.

Why do CIOs resort to escrow arrangements? Most respondents point to the obvious: They're a precaution should the licensing vendor go out of business. Slightly fewer respondents, meanwhile, say it protects them in case the vendor stops or decreases support, while still others say it's part of a larger risk-management policy.

"At the end of the day, people are doing it out of fear that their vendor will go out of business," Boruvka says. "But historically, more software is released for loss of support."

A Plan is in Order

Not surprisingly, escrow decisions involve prioritization. Some 59 percent of IDG respondents escrow the most critical applications. "We escrow those applications that we deem to be mission-critical, Brady says, "meaning back-office applications used by accounting, production, construction and sales." At the same time, 51 percent safeguard complex applications that would be hard to replace and 48 percent escrow applications with a high cost of replacement.

"People naturally gravitate toward costly and big," Boruvka says, "but a process is necessary by which IT and legal stakeholders work with the business owners to determine how software impacts the business." For example, how does one handle an inexpensive application with big business impact? Or a seemingly less critical application that has been highly customized?

Still, only 31 percent of IDG's survey respondents have a process in place. Most agree, however, that risk management is a shared responsibility between IT managers and legal counsel. In other words, legal looks out for the broader organization while IT worries about keeping the individual application running. Business owners, meanwhile, give direction on criticality. It's a perfect marriage of the right oversight.

Technology Escrows: Disaster Recovery for Enterprise Applications

Technology escrowing is like disaster recovery for enterprise applications. “It’s ridiculous for a company to identify 10 mission-critical applications to sustain business and not have an escrow account for them,” says Iron Mountain Digital’s John Boruvka.

Think of it this way: Enterprises routinely spend millions on disaster recovery plans with which to protect those same applications against natural disasters, terrorist sabotage and other emergencies. The greatest source of business interruption, however, is software error and the inability to use software as needed. Every fire, tornado and flood combined wouldn’t add up to the number of software failures that companies experience. Still, the practice of escrowing doesn’t garner the same attention.

“Trust, but Verify”

While an escrow deposit ensures that source code is tucked away for safekeeping, simply escrowing that deposit may not be enough to avert all risk.

Former U.S. President Ronald Reagan may have said it best: “Trust, but verify.”

Putting software in an escrow account makes certain that code will be released if and when disaster hits, as stipulated by the contract. Yet, there is no guarantee that the software will be complete and usable, or even readable. That’s why many CIOs are using verification services in order to validate the completeness and accuracy of their escrow deposits while increasing their confidence in them. In fact, in the IDG survey, 46 percent of respondents reported that they consider it critical or very important that their escrow agreement includes the rights to perform verification services by a third party.

Verification services provide a quality control mechanism for validating that an escrow deposit contains what’s needed—and what’s contracted—and that the code will be usable when it’s needed. There are varying levels of service, chosen based on the unique requirements and risk thresholds associated with specific applications. Among the most popular functions:

- Cataloging the files contained in escrow and confirming the ability to read the media
- Identifying the tools needed to maintain the Technology Escrow deposit
- Compiling the product and building the executable code
- Testing the functionality of the compiled deposit
- Confirming the usability of files built when installed

To Verify or Not to Verify

“One of the leading misconceptions in escrowing is the assumption that the escrow agent is doing something to technically verify the completeness and accuracy of the deposit,” Boruvka warns. **Even though there’s a good faith intention on the part of developers to comply with escrow agreements, the reality**, according to Iron Mountain Digital statistics, is that 66 percent of Technology Escrow deposits are incomplete; while an astounding 92 percent require additional input from programmers.

The whole idea behind any Technology Escrow is to be able to put released software to work immediately, according to Boruvka. “Yet, as these statistics suggest, we routinely find that there is not enough information to hit the ground running,” he says. “Once the software is released from escrow, if you have to spend 60 days sleuthing it out, you’d be better off having spent the money upfront on verification services.”

Forty-five percent of IDG respondents report that it is critical or very important that their Technology Escrow agreements include the right to perform verification. That’s especially interesting in light of the finding that 66 percent of Technology Escrow deposits are called “incomplete.” The reason, they say, is that they’re a precaution against vendors who may go out of business or cease offering product support. This sense of security, however, points more to the value of making a Technology Escrow deposit in the first place.

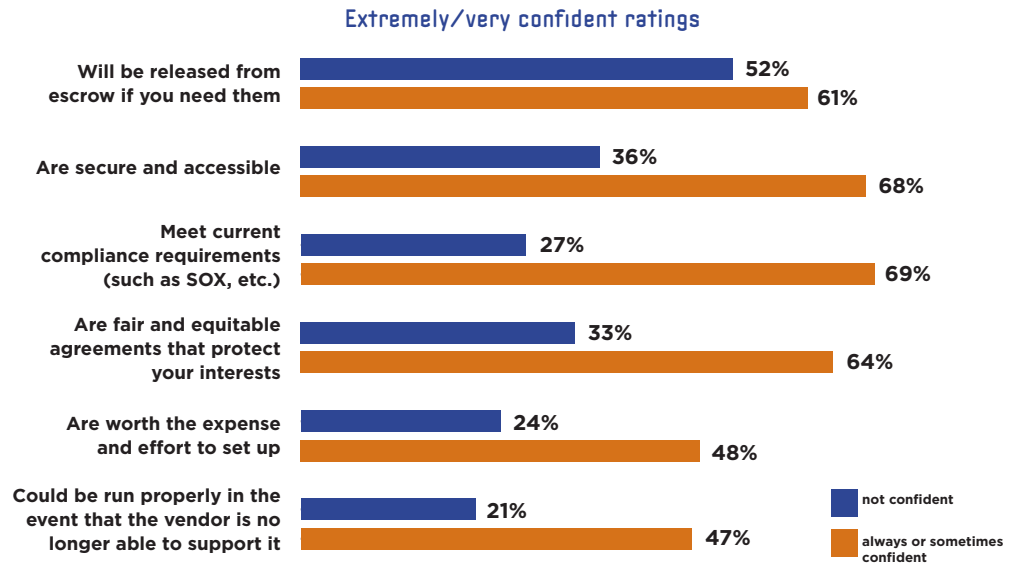
All of this has CIOs taking action. When it comes to specific services, for instance, IDG respondents say they are most often verifying that necessary files have been deposited. They’re also going deeper, however, by verifying that the software complies, confirming build instructions and performing usability tests. Other service functions—such as checking encryption and performing virus scans—are somewhat less popular.

Prioritizing Applications for Verification Services

There is much to consider when prioritizing verification services for escrow deposits. So where's a CIO to start? Here are five things to consider:

- **Operational dependencies:** Consider the number of users, customer impact, lost productivity and lost revenue.
- **Time:** Ask yourself, "How long would an application take to recode? Are substitute products available? How much time is required to renegotiate?"
- **Costs:** Calculate the budget items that go beyond the initial investment, such as license fee, installation, retraining, customization, reprogramming, and hardware.
- **Vendor assessment:** Evaluate company stability, subcontractor partnerships, breadth of product lines, and staff commitment.
- **Business disruption:** Consider the impact of service disruption on the top and bottom lines of the business, as well as whether your company can survive that disruption.

Confidence in Escrowed Applications Among Those With and Without Verification/Validation Included in Standard Escrow Agreement



IDG Research Services asked, "How confident are you that your current escrowed applications.." followed by the categories shown above. For example, "How confident are you that your current escrowed applications will be released when you need them?" The blue bar represents the level of confidence among those respondents whose escrow agreements do not include verification services. The orange bar shows the level of confidence among those respondents whose escrow agreements do include verification services, pointing out the value of the "trust, but verify" approach to escrow.

Source: IDG Research, August 2008

For Taylor Morrison's Brady, escrow verification is all about peace of mind. "So far, we have never had to enforce a default event, but if we have to, the escrow is our only backstop to ensure continued operations," he says, adding that the company verifies deposits only. "As long as we can get to the source code, we can find programmers to ensure usability and decrypt code as necessary."

Closing Thoughts

In the end, one fact comes shining through: IDG respondents who verify their deposits show much greater confidence in their escrowed applications. Verification services serve the dual purpose of identifying and rectifying escrow deposit deficiencies, as well as educating developers on what constitutes a full and complete set of source-code materials for escrow purposes.

"If you agree that escrowing mission-critical, complex and costly applications is important, then verification is a logical component of that process—whether it's performed by the developer, licensee or an outside consultant," Boruvka says. "Without it, you're still at risk—escrow or not."

CALL TO ACTION:

To learn more about Technology Escrow and Verification services, please go to www.ironmountain.com/ipm

© 2008 Iron Mountain Incorporated. All rights reserved. Iron Mountain and the design of the mountain are registered trademarks, and IronMountain Digital is a trademark of Iron Mountain Incorporated in the U.S. and other countries.