



Verification Services: Fulfilling the Promise of Technology Escrow Agreements

Forward-thinking technology developers and their customers agree to put source code and other proprietary materials into escrow in order to secure access to mission critical technology if pre-determined events and conditions take place.

For the developer, safeguarding the intellectual property rights to their best selling products are high stakes indeed; for the licensee, continuity of business is not only a matter of survival, but increasingly required by good governance compliance regulations.

Great care goes into the wording of technology escrow agreements; the interests of all parties must be properly represented. But after the signatures have dried, and source code files and other proprietary materials are deposited, what ensures that this material will indeed fulfill the intended purpose of the escrow if a release condition occurs?

Demand for verification services has increased 20% over the past two years.¹ Savvy users of technology applications are taking extra precautions to maximize the pay-off from their investment in escrow deposits—and protect their total investment in software assets. They realize that for their escrow accounts to have maximum value when needed, it takes more than simply depositing a set of source code files. Verification services offer varied levels of assurance that the technology can actually be recreated and used if pre-determined events and conditions take place.

This paper examines the types of verification services used in the escrow industry today, and why verification has become a best practice for both the licensees and developers that benefit from escrow contracts and the lawyers who advise them.

This paper will discuss:

- **Reasons for Using Technology Escrow**
- **What Comprises a Useful Technology Escrow Deposit**
- **Levels of Deposit Verification Offered by Escrow Service Providers**
- **Benefits of Verification for Licensees and Developers**

¹ Source: Proprietary research of Iron Mountain. (2005/2006). Cited with permission.

REASONS FOR USING TECHNOLOGY ESCROW

Sixty percent of licensees surveyed set up escrow agreements to secure access to their technology if a vendor goes out of business—but more and more licensees include release conditions that protect them if a vendor stops or decreases support. Thirty seven percent of licensees seek escrow as part of an *overall risk management strategy*, increasingly on the advice of their attorneys, reflecting the growing influence of compliance with regulations for business continuity like those of the U.S. Sarbanes-Oxley Act.²

Most developers are motivated to establish escrow accounts to meet the prevailing expectation of prospects and customers that escrow will be part of the license agreement. Smaller developers or those in emerging markets may use escrow proactively, neutralizing objections when competing with larger or more established competitors. All developers, regardless of size, increasingly use escrow to create an audit trail and to help strengthen their intellectual property rights of their products.

Each of these reasons is key to the economic survival of the companies involved and demonstrates the growing sophistication of escrow users. The rising number of technology escrow accounts being opened demonstrates they are recognized as well worth their investment. But, as Gartner, Inc. notes:

“If you don’t plan to do regular audits, or verification that the version of the software you are using is in escrow, the agreement may be worthless...if the vendor falls behind on source code deposits, and has incomplete or unusable deposits, the escrow agreement will be useless.”³

WHAT COMPRISES A USEFUL TECHNOLOGY ESCROW DEPOSIT?

The type of software placed in escrow ranges from embedded code in chips to middleware to enterprise custom code developed for a specific use that runs on mainframes. The need for verification is largely dependent on how an organization would be affected by a sudden loss of support for the technology on which it relies. Verification is recommended for any technology which, when unavailable, results in a significant decrease in employee productivity or ability to deliver services to customers.

Many companies are more inclined to put into escrow software developed by smaller software developers in the event of bankruptcy—but it’s important to note that there are other “release conditions” that should be planned for that apply even to the largest software developers. An article published in *Contract Management* (July 2005) advocates carefully defining a variety of “release conditions” that define the circumstances under which an escrow deposit will be released—and advocates verification to ensure the technology in the deposit can be quickly and successfully recreated upon release. These conditions include:

- “Product bankruptcy,” which is failure to provide support, especially when a developer plans to phase out a product;
- Mergers or acquisitions or other change in business status where the new company may not be as dedicated to supporting the technology in escrow;
- Loss of key staff, whether development, maintenance or key management staff;
- Failure to do business in the ordinary course.⁴

Technical verification of the contents of an escrow deposit provides insight into how complete the deposit is in terms of what’s needed to recreate a working version of the technology. If the deposit is determined to be incomplete or non-functional which is often the case, these issues can be rectified with the help of the developer before it’s too late. Recent statistics show that 97.4% of all deposits sent in for analysis were determined to be incomplete and 74% of examined deposits required additional input from the developer in order to be

² Source: Proprietary research of Iron Mountain. (2005/2006). Cited with permission.

³ Source: Disbrow, J. and Park, A., “Be Aware of Contract Issues When Negotiating Software Escrows,” Gartner, Inc. Research Note, G00125669, February 7, 2005.

⁴ Source: Bruno, Frank, “Contract Language: The ‘Ts and Cs’ of Technology Escrow,” *Contract Management* (July, 2005), pp. 18-23.

compiled.⁵ The value of an escrow arrangement is heavily dependent on the quality of the deposit materials—a fact increasingly recognized by licensees and developers.

Discussion with an organization's technology professionals and legal staff helps identify the types of materials important to include in the escrow deposit. Typically, these fall into three categories.

1. General Information

- **Source code:** The essential core of the deposit;
- **Component dependencies:** Identifying cases where one software component requires another to have been built or compiled first;
- **Build environment:** Setup and configuration information, including configuration settings for all compilers and third party components;
- **Build control files:** Files and/or scripts that control the build process; these will vary depending on the operating system and tools used;
- **Applications:** Those needed to compile and build executable code, objects, dynamic libraries, etc.;⁶
- **Build instructions:** Detailed instructions and sequence of actions describing how to compile the escrow deposit and build executables; these should also specify required hardware and operating system requirements, including non-standard settings;
- **Design documentation:** Information regarding source code architecture, overall design of the source code and interactions among modules;
- **API's/program interface documentation:** Specifications for any API's that are exposed by the applications and documentation used by developers during the design, code test or maintenance phase of the software life-cycle (including maintenance tools);
- **Test diagnostics:** Regression tests involving automated scripts if available;
- **Roadmap of deposit materials:** High level overview where key items are located on deposit media, to save time in the event the deposit is released from escrow;
- **Deposit media information:** Media type, tape density, drive model(s), utilities or third part applications used to create tapes; non-default parameters used in creating tapes that would affect the extraction process;
- **Security information:** Encryption information, passwords required and/or keys required;
- **Extraction-related information:** Information required to produce a clear-text version of source code or other technical information required for timely extraction of the data;
- **Programmer contact information:** Names and home addresses of key technical employees of the developer.

⁵ Proprietary research of Iron Mountain. (2005/2006). Cited with permission.

⁶ These materials may include compilers, linkers, third party libraries, assemblers, pre-processors, and post-processors. If they cannot be deposited due to licensing restrictions, the depositor should provide names of all required applications, version number, vendor name and contact information.

2. Runtime/Production Information

- **“Live” environment requirements:** Key information required to establish the runtime/production environment, including third party libraries, dll's, applications, scripts and data;
- **Hosting configuration instructions:** Detailed steps needed to configure the environment hosting executable code;
- **Network design information**
- **Runtime environment configuration instructions:** Information regarding operating systems, diagnostics and instructions required to load the application onto a runtime/production environment (including third party components required);
- **User manuals/training guides**

3. Data/Database Information

- **Data:** Samples of data required to run the application;
- **Database schema/data model documents:** Details of design information for the database.

LEVELS OF DEPOSIT VERIFICATION OFFERED BY ESCROW SERVICE PROVIDERS

All leading technology escrow service providers offer some form of verification. At the simplest level, certain providers offer a sworn, statutory statement that merely describes the contents of a deposit, with no indication of its completeness or usefulness in the case of a release event. On the other end of the spectrum is usability testing that demonstrates the degree to which the technology will work properly if needed.

Each level of verification produces a higher degree of confidence that the escrow deposit will “pay off” in the event of a release and each level requires additional expertise on the part of the entity doing the verification, whether it's in-house technical staff of the licensee, the escrow service provider, or a third party.

The ability to select the appropriate level of verification, to safeguard an escrow deposit, is critically important to businesses, whether they are developers or licensees. One size does not fit all. The application put into escrow today may be characterized as important but not mission critical, representing a modest investment with a large, stable developer. Next year may see the introduction of new mission critical software resulting from a major investment made over several years with a brilliant but relatively new developer—with many components from third parties. The level of verification should be significantly higher for this technology because the return on investment is worth it—and an escrow deposit without adequate verification leaves the company dangerously exposed. Ideally, both levels of service should be available from the same escrow service provider with whom one has established a trusted relationship.

Although not all escrow service providers offer a full range of verification services, the following levels of verification services are typically offered in the escrow services industry:

- “Trust-based” verification
- File verification
- Compile test verification
- Usability test verification

TRUST-BASED VERIFICATION

The simplest (and cheapest) form of verification service essentially involves trust between two parties that the agreed upon materials are, indeed, in the deposit—and/or, accepting the assurance of one's own internal staff that the deposit contents are indeed complete.

A slight improvement from taking someone's word that deposits are complete is the practice of requiring a sworn statutory statement as to the contents of a deposit. In this process, the specific individual depositing the technology swears a statutory declaration before the company's attorney or a notary public, with the incentive for truthfulness being exposure to criminal charges.

While cheaper and easier than choosing a more advanced level of verification service, the sworn statutory statement only addresses the intentional honesty of the depositor—but does not protect the licensee against honest mistakes. If upon release the escrowed software is found to be useless because it is incomplete or erroneous, despite the best intent of the depositor, the licensee has invested in the escrow service in vain. Additionally, criminal charges will not make the software work—nor will it alleviate business hardships.

In fact, most depositors do make honest efforts to fulfill their obligations as their escrow agreement states—but given the number and variety of participants in a typical license agreement negotiation, both technical and non-technical, equally honest miscommunication is not uncommon. More importantly, the level of complexity of today's software is increasing constantly, comprising a wide variety of components from different sources—including open source software. To assume that release of a deposit will result in a functioning, mission-critical application with no verification process beyond trust is a highly risky strategy.

FILE VERIFICATION

The next level up in deposit verification entails file comparison and analysis. Results of this level of verification should include a file classification table displaying the number and types of files in the full inventory of the deposit compared to the contractual list.

Basic file verification should also ensure that the files are technically readable, not corrupted. This level of verification may also include a report on virus scan results for deposits submitted, any passwords or encryption keys, and confirmation that some form of “build instructions” is included. A basic file verification with more advanced options would include an inventory of the deposit components, with an analysis of potentially missing components, such as required source code languages and compilers, third-party software, libraries, operating systems, and hardware. This type of verification would also incorporate a confirmation that some form of “build instructions” is included in the deposit.

Recent data on escrow deposit testing using file verification reveals that 97.4% of deposits sent in for analysis were determined to be incomplete—had they not undergone independent file verification, these deposits would have been worthless due to the following reasons:

- Deposits did not contain any configuration or build instructions, which are critical to putting escrowed materials into deployment
- Deposited materials had either corrupt media or missing files⁷

File verification allows the licensee and depositor to resolve these discrepancies in a non-crisis environment—rather than discovering them during a release event when it's too late to correct and reach the developer's staff.

⁷ Proprietary research of Iron Mountain. (2005). Cited with permission.

COMPILE TEST VERIFICATION

An even more thorough type of escrow verification beyond file verification ensures that the executable code necessary to run the application can be created using the deposit materials. Doing this *before* a trigger event occurs gives the licensee and depositor time to clarify any issues and improve the usefulness of the deposit.

This compile test is usually conducted on the escrow service provider's equipment, ideally simulating the environment in which the software would typically run. The results of compile test verification not only summarize pass/fail results, showing whether the source code compiled properly, but should also provide the beneficiary with comprehensive build instructions which are necessary for rapidly recreating a functioning version of the software in escrow. Often, cooperation with developers after the compile test is completed helps improve the quality of the deposit materials and ensures the streamlined use of the deposit at some point in the future.

In addition to detailing the actual process of a successful compilation (a software build), instructions should provide guidance as to how problems can be circumvented or resolved if they occur during a test. Measures like these that troubleshoot and streamline the process are critical to getting the business back online if the technology needs to be rebuilt.

Results of escrow deposit testing using compile test verification have shown that 92% of all examined deposits required additional input from the developer in order to be compiled. The level of developer input needed ranged from clarification of build instructions to major omissions from or errors in build instructions to missing files discovered during the build process.

DEPOSIT USABILITY TEST VERIFICATION

The most powerful type of verification ensures not only that all required files are present in the deposit and will compile properly, but also that the resulting application will work properly in the event of a release.

One approach to conducting this test is to match a list of executable files generated by the compile test against the ones that are running in a current operation. A more comprehensive approach involves creating a specific set of functional requirements that must be met by the compiled software to indeed verify that the application works properly.

The test may be conducted at the escrow service provider's site, the licensee's site or the developer's site, depending on the requirements of the companies involved. Or, if contractually permitted, the escrow agent can release an executable version to the licensee for testing.

Usability results document whether or not the tester was able to successfully navigate and execute on the sample set of functionality specified for the test. Usability test verification is the most complete escrow verification service available, and guarantees, as much as possible, working escrowed technology.

BENEFITS OF VERIFICATION FOR LICENSEES

For software licensees, verification services maximize the return on their investment not only in technology escrow, but also in the technology itself, which can cost millions of dollars. Verification also helps safeguard business continuity, especially in large financial institutions, business services, health services and other industrial sectors for whom escrow of mission-critical technology has become a best practice.

Verification services strengthen the value of escrow in protecting investments and continuity because they ensure, to the degree chosen by licensees, the ability to recreate applications in circumstances beyond their operational control; for example, when support diminishes or ceases altogether due to bankruptcy, mergers and acquisitions or end-of-life events at the supplier level.

Verification services support users of technology escrow as part of their overall risk management strategy, helping them to avoid or minimize the following:

- Costs associated with replacing licensed software and hardware
- Lost profits and/or savings
- Lost time (downtime for customer response, order processing, accounts payable, etc.)
- Customer dissatisfaction
- Breach of contract(s)
- Costs associated with consultants' fees, court costs, arbitration fees and attorney's fees
- Costs associated with retraining personnel

New Jersey Transit Authority chose a high level of verification when its fare- and data-collecting system was upgraded. Almost every department in the NJTA relies on the licensed technology, which is critical to the proper and orderly functioning of this major metropolitan transit system. Business continuity was only one impetus for ensuring access to usable source code—the NJTA knew it would be expanding the software and wanted to ensure that they could continue to support future development even if the vendor ceased technical support down the road.⁸

Trans World Entertainment, one of the largest music and video retailers in the United States, felt that the cost of verification was “insignificant” compared to the effort and funding invested in a technology product vital to their competitive differentiation in the marketplace. It was critical in the event of an escrow deposit release that they be able to recreate this product in-house as quickly as possible—and to maintain it. They also chose the highest level of verification available to protect their investment. In an unforeseen turn of events, the software developer went out of business and Trans World ultimately needed to access and use the deposit materials in escrow—which were successfully recreated so that use of the technology could continue without interruption.⁹

BENEFITS OF VERIFICATION FOR DEVELOPERS

How do developers whose source code is the subject of verification benefit from these services? Clearly, in cases where developers establish an escrow account to create an audit trail for ownership of their intellectual property, verification provides the same protection of a deposit's usability as it does for licensees. This assurance is valuable whether the developer is required to provide proof of development if contested by a third party or business partner or build a case for market valuation in future sale, merger and acquisition activity. Developers also need to ensure business continuity in the supply of their major technology products, despite events that may occur to co-development partners.

Should developers be concerned about losing trade secret status for their technology by allowing their source code to undergo verification? It is not the fact that multiple people are aware of the trade secret information that impairs its value, but rather the failure to take reasonable measures to protect the secrecy and the availability of the information to those who will derive economic value from it.¹⁰ Developers should select an independent escrow service provider to act as an intermediary to provide limited information about the validity of the escrow deposit to a licensee without compromising the value of the trade secret.

⁸ Source: “Do You Know What's In Your Escrow?” (Iron Mountain Escrow Best Practices Paper).

⁹ Source: Trans World Entertainment Case Study

¹⁰ The Uniform Trade Secrets Act defines a trade secret as “information, including a formula, pattern, compilation, program device, method, technique, or process, that: (i) derives independent economic value, actual or potential, from not being generally known to, and not being readily ascertainable by proper means, by other persons who can obtain economic value from its disclosure or use, and (ii) is the subject of efforts that are reasonable under the circumstances to maintain its secrecy.”

The escrow service provider should also:

- Agree in writing to strict confidentiality (and require the same in writing of its employees);
- Conduct background checks on its employees and bond them;
- Carry substantial liability insurance;
- Have established procedures for secure and confidential testing and storage of proprietary information;
- Have a solid reputation with a history of successful releases.

Seventy-five percent of developers surveyed agreed that verification is a useful tool to close a sale or agreement if the licensee or technology partner insists on it—and, increasingly, they do.¹¹ Developers offering escrow as part of their standard contract to counteract prospective concern about their viability strengthen this competitive advantage if they promote verification as part of the escrow service—and they avoid tying up valuable resources scrambling to accommodate unexpected requests for verification on a case-by-case basis. Such a move also generates significant goodwill with prospects by illustrating their high level of interest in the licensee’s welfare.

FURTHER INVESTIGATION

If your organization has or is considering establishing a technology escrow account, consider the following factors in evaluating your need for verification services:

- What is the *criticality* of the technology under consideration for escrow? Mission-critical software warrants the highest level of verification.
- How *complex* is the software?
 - Is the software standard out-of-the box or has it been customized?
 - Does it contain software or customization developed by a third party who is neither the licensee nor the vendor of the technology? Gartner, Inc. advises “Although the licensee will not generally receive the source code for this third-party software, the escrow agent should still be given a media copy of the correct version that runs with the escrowed software.”¹²
 - Are there *elements in addition to source code* required to self-maintain the software? These may include build instructions, tools like special compilers or linkage editors, database or run-time configurations, external sub-routines, etc.
- What are the costs and risks associated with replacing the software (including lost revenue as a result of downtime) if you cannot recreate and maintain the original technology yourself?
- Are there any high-risk factors to consider (such as public safety or critical financial transactions?)

When considering verification services from providers, look for those who offer the full range of verification levels described in this paper—what meets the needs of today’s escrow deposit may not be adequate for a subsequent one in terms of enabling a quick, successful deployment of deposit materials. A full-service technology escrow provider will be able to offer tools and guidance, including a full risk assessment, which will assist in determining the appropriate level of verification services needed for each application. For more information on Iron Mountain Intellectual Property Management Services, and the range of verification services we offer, please visit our homepage www.ironmountain.com/ipm.

¹¹Proprietary research of Iron Mountain. (2005). Cited with permission. Gartner, Inc., op. cit.

¹²Gartner, Inc., op. cit

ABOUT IRON MOUNTAIN DIGITAL

Iron Mountain Digital is the world's leading provider of data backup/recovery and archiving software as a service (SaaS). The technology arm of Iron Mountain Incorporated offers a comprehensive suite of data protection and e-records management software and services to thousands of companies around the world, directly and through a world-wide network of channel partners. Iron Mountain Digital is based in Southborough, Mass. with European headquarters in Frankfurt, Germany. For more information on Iron Mountain Digital's Intellectual Property Management services, visit www.ironmountain.com/ipm.

ABOUT IRON MOUNTAIN

Iron Mountain Incorporated (NYSE:IRM) helps organizations around the world reduce the costs and risks associated with information protection and storage. The company offers comprehensive records management and data protection solutions, along with the expertise and experience to address complex information challenges such as rising storage costs, litigation, regulatory compliance and disaster recovery. Founded in 1951, Iron Mountain is a trusted partner to more than 90,000 corporate clients throughout North America, Europe, Latin American and Asia Pacific. For more information, visit the company's Web site at www.ironmountain.com.

Disclaimer: This white paper may be redistributed in its entirety provided that the copyright notice is not removed. It may not be sold for profit or used in commercial documents without the written permission of the copyright holder. These documents are provided "as is" without any express or implied warranty. While all information in this document is believed to be correct at the time of writing, this document is for educational purposes only and does not purport to provide legal advice. If you require legal advice, you should consult with an attorney. The information provided here is for reference use only and does not constitute the rendering of legal, financial, or other professional advice or recommendations by Iron Mountain. The listing of an organization does not imply any sort of endorsement and Iron Mountain does not take any responsibility for the products or tools listed.

© 2007 Iron Mountain Incorporated. All rights reserved. Iron Mountain and the design of the mountain are registered trademarks and Iron Mountain Digital is a trademark of Iron Mountain Incorporated. All other trademarks are the property of their respective owners.



745 Atlantic Avenue
Boston, Massachusetts 02111
(800) 899-IRON

Iron Mountain Digital, the world's leading provider of data backup/recovery and archiving software as a service (SaaS), offers a comprehensive suite of data protection and e-records management software and services to thousands of companies around the world. For more information, visit our Web site at www.ironmountain.com/digital.