BLACKDUCK®

WHITE PAPER

Top Considerations for Evaluating the Tech in Tech M&A

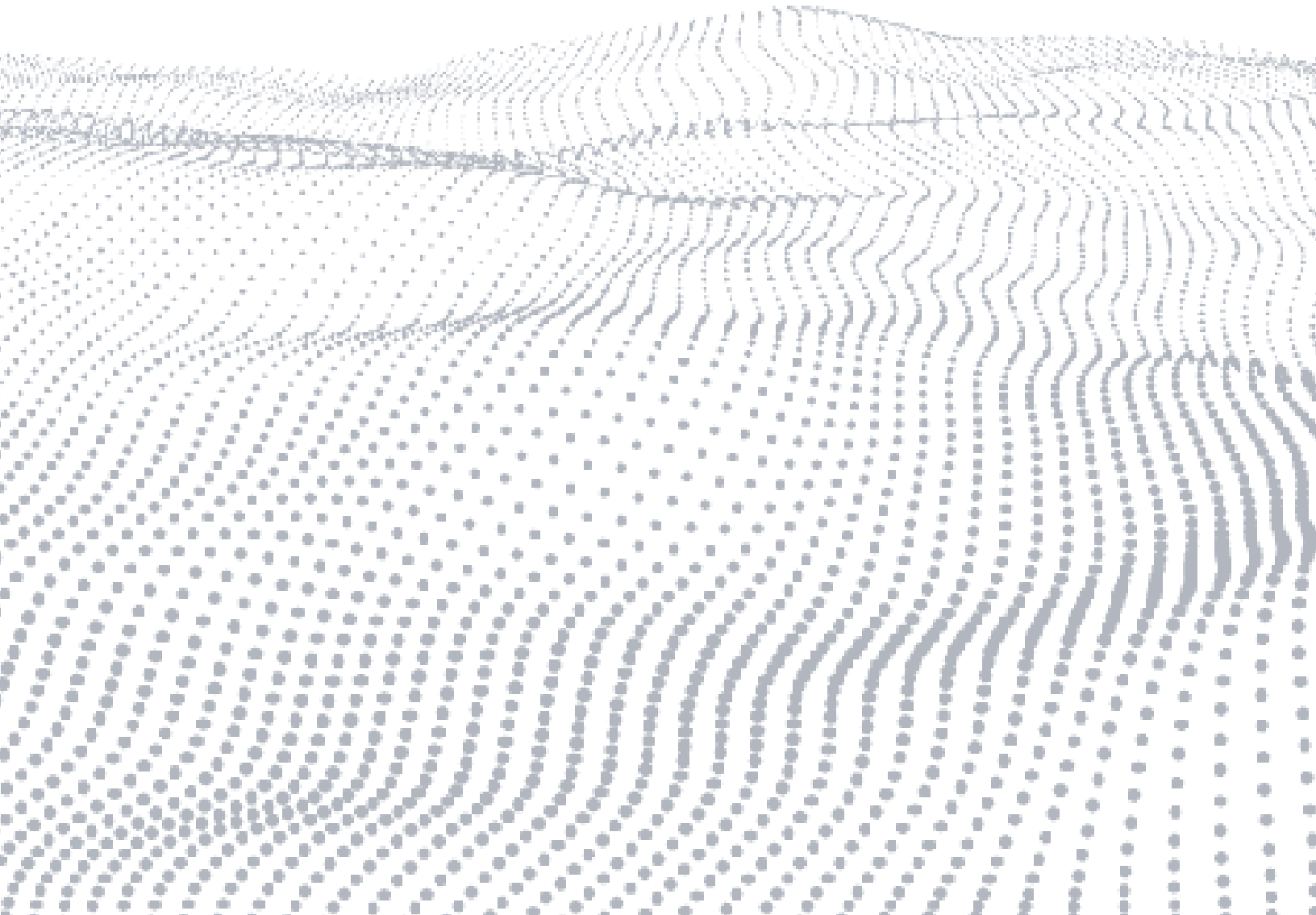

Table of contents

Purpose of M&A due diligence

With thousands of transactions and billions of dollars spent on technology mergers and acquisitions (M&A) every year, acquirers must ensure solid investments by conducting due diligence. Due diligence is "the detailed examination of a company and its financial records, done before becoming involved in a business arrangement with it," as the Cambridge Dictionary defines it. M&A due diligence allows acquirers to do three important things:

Confirm the premise of the deal. When considering an acquisition, the buyer amasses information about the target company and formulates an investment thesis. The first aim of M&A due diligence is to confirm this thesis.

Gather information to plan the integration. Another aim of M&A due diligence is to collect information related to integrating the target into the buyer's operation. An acquirer must figure out how the target's people and products fit into the organization and plan integration costs. This is critical to a successful outcome.

Identify unknown risks. Even in the best-laid plans, there are unknowns. Some unknowns put the business plan and efficacy of the investment at risk. To the greatest extent possible, acquirers need to unearth and address risks before closing.

This white paper examines some of the risks that an acquirer might encounter in an M&A transaction involving software, and how a software audit can help you discover these risks so you can mitigate them.

Things to worry about in M&A

M&A transactions are high stakes. At public companies, shareholders depend on wise capital investment to maximize their stock value. So the reputation of the company's management among investors is at stake in every transaction. Similarly, private equity investors are beholden to their limited partners. For sellers, a successful outcome might ensure a comfortable retirement or a private university education for their children. Thus, the pressure on all sides of a deal is understandable.

Much can negatively affect the value of a deal. To avoid surprises and ensure a solid transaction, buyers must examine the target from multiple dimensions:

- Financial (accounting, quality of earnings, taxes)
- Legal (intellectual property, corporate governance, antitrust)
- Customers (contracts, warranties, customer satisfaction)
- Employees (payroll, employment contracts, cultural fit)
- Technology (product, people, process)

The technology dimension in technology transactions

Software and systems companies derive their worth from their technology. Their product is software or is driven by software, and the intellectual property (IP) embodied in the software is the real value of the company. The acquisition of a software or systems company is often called a technology transaction. The assessment of the software in technology transactions spans from the strategic to a granular analysis of the code.

Product/strategy

Understanding the target's products and strategy is of paramount importance. Corporate or strategic acquirers must fully comprehend the target market, competitive landscape, and product roadmap, and evaluate how the product fits into their product portfolio and corporate strategy. Private equity buyers need to understand how the product fits into their portfolio and with their market focus, and recognize any risk it poses to achieving their financial goals.

People

Transactions based on technology cannot succeed without involving people. If personnel are part of the transaction, you must evaluate their skills for future scaling, developing, and maintaining the software. Even in an assets-only tech purchase, you'll still rely on subject matter experts from the seller to consult on the knowledge transfer and integration for the first 6 to 24 months, depending on software complexity. This consultation will overlap with employee due diligence and HR matters, but from a technical perspective, it's critical to identify who you will need and for how long, to ensure they are on board. In addition, it's important to identify leadership holes that may need to be filled and to include those hires in the business case.

Process/tools

In a technology transaction, a strategic acquirer will have one of two viewpoints on due diligence of the processes and tools.

- If you plan to buy the entire operation and keep it intact, you should assess how the target conducts software development and with which tools.
- If you plan to integrate the target company into your organization, you must become familiar with the target's processes that directly affect the integration and potential risks. And even though the new team will eventually employ your way of working, the acquired company will continue business as usual for some period.

Private equity acquirers, which usually keep targets intact, should make sure that the target's development process, tools, and supporting infrastructure are up to industry standards. Some firms enlist consultants if they lack internal technical expertise.

Where processes are lacking, you need to dig deeper when assessing the code and planning the processes to put in place. For example, if the target has no process for managing open source components, it's particularly important that you analyze code for open source licensing or security issues, as outlined in a 451 Research report.[1] Similarly, if the target lacks processes for "designing in" application security or at least performing security testing on the software as part of development or QA, it's particularly important to evaluate the code for vulnerabilities.

Software technology

Due diligence on the software must consider both the architecture and the code itself. The architecture provides the foundation, defining how the code is assembled and structured. You must ensure the foundation is sound from an integration and maintainability perspective. In a software transaction, the codebase is where the value lives. Understanding how the codebase was written and any inherent problems it contains is essential to valuing the deal and assessing the future of the product.

These considerations complement insights gained from talking through processes and higher-level looks at how the product is built. A process deficiency can suggest the need for particular code analyses. But even where the process looks solid, the rubber meets the road in the code. Software is built over time, and much of the code may predate the current process. Code issues can also indicate the efficacy of a process; for example, the design may look good on paper but without a process to ensure the design is maintained, who knows how the code is really structured? Also, code analysis can confirm that there are good quality processes in place and the code is not overly buggy. Good news for everyone.

Software risks in tech M&A

Modern software contains a mix of open source, third-party, and proprietary code. They all contribute to the dimensions of risk.

Legal risk

For open source and third-party software, legal risk is real. Over 85% of transactions audited in the Black Duck® "Open Source Security and Risk Analysis" (OSSRA) report contained license conflicts. Being out of license compliance can have real-world consequences, including:

- Concerns for buyers when divesting
- Impact on corporate reputation (if sued for licensing, etc.)
- Lawsuits
- Loss of IP (if license compliance requires distribution of source code)

Security risk

To create a full risk profile of the technology you're acquiring, you must examine its security risk across multiple dimensions. Issues with the architecture, proprietary code, or open source components could lead to points of weakness or entry, making the software vulnerable to attack. The Harvard Business Review notes that in the last several years, concerns about data security and hacking have risen, specifically in M&A.[2] The Black Duck® Audit Services team reported that almost 80% of transactions involved code with high-risk vulnerabilities. The consequences associated with such vulnerabilities include:

- Unplanned work to remediate security issues
- Regulatory issues (e.g., GDPR, HIPAA, PCI DSS)
- Attacks by bad actors
- Data breaches (e.g., losses of customer data, intellectual property)

Software quality risk

Software quality risk may not have as immediate an impact as a lawsuit or security breach, but it's more insidious. Low-quality code written in a nonmodular way is hard to maintain and significantly reduces productivity in adding features, fixing bugs, and patching vulnerabilities.

Low-quality code represents technical debt—non-value-added activities (e.g., bug fixes, brittle code maintenance, code refactoring)—a burden now that steals resources from the future by reducing developer availability. The impact: Developers working on poorly structured codebases are 60% less productive than those working on well-structured codebases.[3]

Evaluating the software technology

There are several best practices for acquirers evaluating software from a legal, security, and software quality perspective.

Legal evaluation

To surface and mitigate legal problems latent in the codebase under consideration for M&A, you need to identify all components in the codebase, as well as their respective licenses and the obligations and terms of those licenses. This examination should highlight obligations in open source and third-party licenses and any conflicts entailed by the distribution model and licensing for the entire work. It also should determine which components in the codebase require commercial licenses so you can verify that the target has them in place. For completeness, the process must also identify third-party code that may have vague grants of right in code comments, or as is often the case, no applicable license at all. Software licensing can be complex. It's important to involve an open source–savvy lawyer to provide guidance.

Security evaluation

A security evaluation should include a look for high-level design flaws, which account for 50% of security vulnerabilities,[4] and ensure security controls are designed into the architecture. Next, it's important to analyze the proprietary code for security bugs—both from the outside-in via penetration testing and from the inside-out with static analysis tools. With open source comprising the majority of many codebases these days, it's also critical to examine open source and third-party components for known vulnerabilities (e.g., CVE-2017-5638, the Apache Struts vulnerability that was exploited in the famous Equifax breach).

Software quality evaluation

The first step in evaluating software quality is to conduct a high-level architectural assessment that provides insight into the overall quality and health of the software's design. From this assessment, you can determine whether the software is modular and hierarchical and therefore easy to modify and scale. Bear in mind that it's not unusual for the actual architecture to differ from what the target's CTO has on paper. Walking through such a diagram will provide some insight but understanding the reality of the architecture requires analyzing what's going on in the code.

A great architecture can be undermined by poor implementation and vice versa, so it's also important to dig into the quality or bugginess of the code. Ideally, the proprietary code is well-written and the open source components are up-to-date and well-supported by the community. According to the OSSRA report, 95% of transactions contained open source components that either were more than four years out-of-date or had no development activity in the past two years.

"Technology due diligence is not one consideration but a spectrum of considerations."

Due diligence considerations and disclosures

Some information is easy to access (e.g., news sites, analyst reports), but some is proprietary and only available from the target under restrictions. Before asking for proprietary information, you can scan a target's website for business data, view videos of their CEO's technical product strategy, assess their technical people by looking at their experience and education on LinkedIn, and review their developers' work on public open source projects.

While conducting due diligence, you'll request all kinds of disclosures from the target. In a technology transaction, you should start with high-level information about policies, process documentation, software Bills of Materials (SBOMs) of open source components, security breaches, and other documentation related to software. You can follow up on these disclosures by entering discussions with the target about its processes, debugging procedures, different use cases, and more. If you intend to proceed with the deal, you also need to perform a detailed analysis of code quality, security, and open source content.

When you start exploring the target's processes, architecture, and real code, information gets more confidential. Even after being formally approached with a letter of intent and putting NDAs in place, most targets shy away from sharing architecture and code details. Acquirers are also mindful of becoming "contaminated" by access to the code. The concern is that a rejected seller might later claim their intellectual property was stolen by an acquirer with competitive offerings. It's customary for acquirer's technical staff to get a "peek over a developer's shoulder" at small samples of the source code, but for any analysis that requires deep inspection of the code, the norm is to work with a third party trusted by both buyer and seller.

Division of labor in due diligence

Clearly, software due diligence is not one consideration but a spectrum of considerations. Most acquirers use a combination of resources to perform the range of due diligence tasks.

Due diligence happens quickly and is split between different teams with different areas of expertise. To perform due diligence on the higher-level topics such as the compatibility and fit of the target's product/strategy, people, and process/tools requires domain-specific knowledge of the acquiring company and the target's market. Corporate (strategic) acquirers generally assemble an internal team of subject matter experts. The strategic technical elements of the analysis are often led by the CTO or VP of engineering. Private equity acquirers often outsource this part of due diligence to a trusted strategy consultant.

Performing due diligence on the architecture and code is best handled by a third party. In technology transactions, much of the value of the target company is in the code, and the seller will generally not hand over their "family jewels" lest the deal fails and they find themselves with new competition. For the buyer, a third party provides an arm's-length evaluation of the technology. This distance protects you against downstream claims of IP theft by the seller if the deal doesn't close and you come out with a competing product later.

How to deal with issues that arise in software due diligence

Due diligence can uncover issues that you and the target must address. Some of those issues may warrant technical remediation, with the seller agreeing to fix the issue before or after the close. You can also use language in the definitive agreement to appropriately allocate risk. If you identify a risk that the seller deems a nonissue, the seller may provide a warranty, for example.

Sometimes, you'll want more protection against a risk that surfaces in due diligence—for example, a license issue that could lead to IP litigation, or a major security concern. You and the target can agree to hold back money for you to draw from to cover future costs as needed. Typically, you'll set aside a percentage of the deal value as insurance for a finite time in case issues arise. This percentage can increase if major unexpected issues appear. Extreme surprises that arise could even lead to a lower deal valuation, and though rare, the deal getting derailed altogether.

What to look for in an audit vendor

When you're looking for a vendor to provide an M&A software audit solution, two qualities are table stakes: competent people to work with and good tools. But that's not all. M&A projects fundamentally differ from general IT technical consulting. M&A due diligence imposes special demands that many consultancies cannot meet. So it's critical to find a firm that has M&A experience. And with short due diligence timeframes (e.g., two- to four-week turnarounds), you also need a firm that is:

- **Hyperresponsive.** A deal's pace could be measured in days or hours.
- **Trusted.** Both acquirers, and more critically, sellers should know of and trust the firm.
- **Secure.** The vendor should handle the code for safekeeping.
- **Comprehensive in its services.** With all the loose ends in a deal, it's better to use fewer vendors.

Black Duck Audit Services

Black Duck Audit Services comprehensively assesses the software in M&A due diligence. We offer these types of software audits:

- Open source and third-party software audits
- Application security audits
- Software quality audits

To learn more about Black Duck Audits and how we can help you understand software risks, please visit blackduck.com/open-source-audit.

References

1. 451 Research, Business Impact Brief: Don't Leave Open Source Analysis Out of M&A Due Diligence, 2018.
2. Chirantan Chatterjee and D. Daniel Sokol, Don't Acquire a Company Until You Evaluate Its Data Security, Harvard Business Review, April 16, 2019.
3. Dan Sturtevant, Modular Architectures Make You Agile in the Long Run, IEEE Software 35:1, Jan./Feb. 2018.
4. Gary McGraw, Software Security: Building Security In, Addison-Wesley, 2006.

About Black Duck

Black Duck® offers the most comprehensive, powerful, and trusted portfolio of application security solutions in the industry. We have an unmatched track record of helping organizations around the world secure their software quickly, integrate security efficiently in their development environments, and safely innovate with new technologies. As the recognized leaders, experts, and innovators in software security, Black Duck has everything you need to build trust in your software. Learn more at www.blackduck.com.