WHITE PAPER

revenera

OSS Risk in M&A
A Playbook for Faster, Safer Deals

What's Inside

Open source software carries risks that can stall or even derail M&A deals. Learn the pitfalls to watch for, how to navigate the technical due diligence process, and ways to mitigate software risk effectively. The result is faster, safer deal execution and stronger long-term value.

The Reward and Risk of OSS

There's little question today about the value of open source software (OSS). The preexisting, proven, and free components spur innovation, speed up time to market, and come with a wealth of developer experience and expertise.

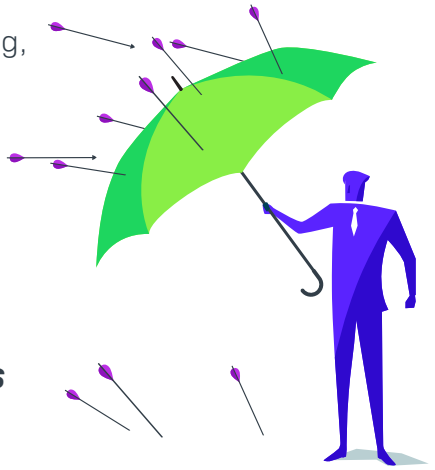
As usage continues to climb—OSS now comprises 80% of all proprietary applications—it's hard to overstate the value. Globally, companies would need to spend an estimated $8.8 trillion to recreate the open source software they now rely on, according to a working paper from Harvard Business School, "The Value of Open Source Software."

INSIGHT

86% of developers say they sometimes or always try to find open source options over other kinds of software.

While OSS usage is mission-critical for most organizations, it also comes with responsibilities and risks. While anyone can see and download OSS code for free, one common mistake is to equate OSS with "free software." Finding code on the internet that suits your purposes doesn't mean you have permission to use it. Most OSS is released under a license and requires a contractual relationship. Some licenses are extremely permissive, while others are much more restrictive.

In the context of a transaction, such as IPOs, loan applications, financing, divestitures, and specifically, mergers or acquisitions (M&A), the risks become much higher. Software is a key component of most M&A deals, and all parties should expect a complete picture before a successful transaction can be completed.



Unfortunately, in an M&A, OSS risk issues are sometimes overlooked, often not well understood, and almost always addressed much later than they should be.

5 Ways OSS Risk Applies to M&A

How might OSS usage impact an M&A? Here are five of the most common issues.

1. Licensing and compliance liabilities

Inappropriate code use or attribution failures are examples of how OSS may be misused, according to licensing terms. In these instances, you could be considered in breach of your contract with the software developer and accused of copyright infringement. Your entire program may be at risk of being viewed as a derivative of the OSS, which could force you to either release the entire program that uses the source code or pay a significant price for not doing so. The risk of having to turn over source code or paying to avoid a handover may impact valuation or, because the buyer could ultimately be buying a lawsuit, cause the entire transaction to fail.

2. Security vulnerabilities

Like commercial software, security vulnerabilities also impact OSS. Cyber criminals are known to inject malicious code into openly published libraries, and—if you're unclear on what's in your code— you may not notice an issue until it's too late, and the exploit has already done its damage. You can't launch defenses against risk you can't see, and, in an M&A, that risk could get passed on to the buyer.

3. Business and operational risk

If you use, modify, or distribute software covered by a copyleft license, you are required to make your modified version available under the same license. Often, such disclosures are the responsibility of one person, and—in an M&A— it's easy to lose this knowledge and expertise, which could result in compliance failure.

A failure to shut down abandoned projects, if they use OSS, could become both compliance and security issues because they aren't monitored or maintained.

4. Remediation costs

After a close review of your OSS and third-party components, you will probably also have a list of necessary remediation actions. This might include legal issues, securing licenses, code remediation needs that may involve removal and replacement, and a notice and attribution to-do list, which is required for compliance. These costs could impact valuation.

5. Recent enforcement and litigation

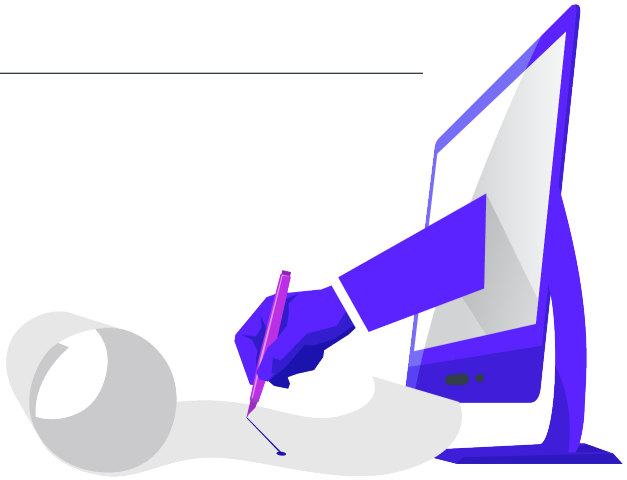
Vendors that release both OSS and commercial versions of code (known as dual licensing modes) are often selective about enforcement. They may not accuse a start-up of misuse, but unfortunately, once the calculus changes with the introduction of deeper pockets in an M&A, they may change their tune. Litigation is highly costly.

Other transaction-related risks to consider

There are other risks worth considering ahead of a transaction. Greater brand visibility can invite increased scrutiny and risk. So can changes in the distribution model after a sale. The brain drain that inevitably occurs when developers come and go is also standard.

Even if M&A isn't in your immediate plans, these software risks can and should be addressed now.

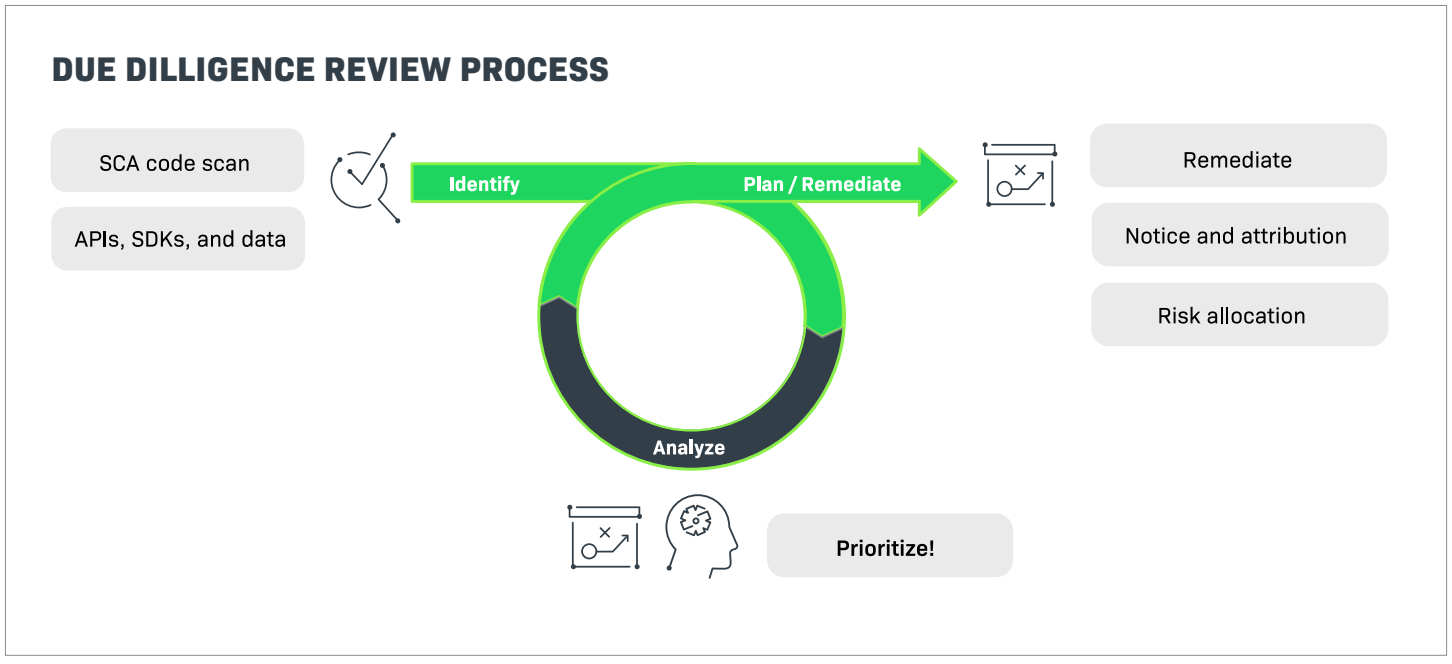
The more proactive a company is about software ahead of a potential transaction, the quicker an agreement can be drafted and closed with confidence, to the satisfaction of both buyer and seller.



Navigating the Technical Due Diligence Review Process

OSS and software misuse can change an M&A value proposition. For this reason, it's wise to begin with a technical due diligence review process. Diligence is how both buyers and sellers make informed decisions.

- **Buyers perform due diligence** to determine precisely what they are buying.
- **Sellers prepare for buyer due diligence** ahead of time to avoid surprises or delays.



The review process may seem daunting, but it doesn't have to be as complicated as it sounds. Follow these four steps.

Step One: Compile a list of all used OSS and third-party components.
Information will likely come from several sources, including developers self-reporting data and package managers that manifest files for dependencies, etc. A Software Composition Analysis (SCA) code scan will identify additional details, such as code snippets.

Step Two: Analyze the components, licenses, and particular use.
Examine the OSS in use, the associated licensing terms, and identify how the code is being used. In an M&A, the four primary code areas most often asked about are whether it's distributed, hosted, linked, or modified.

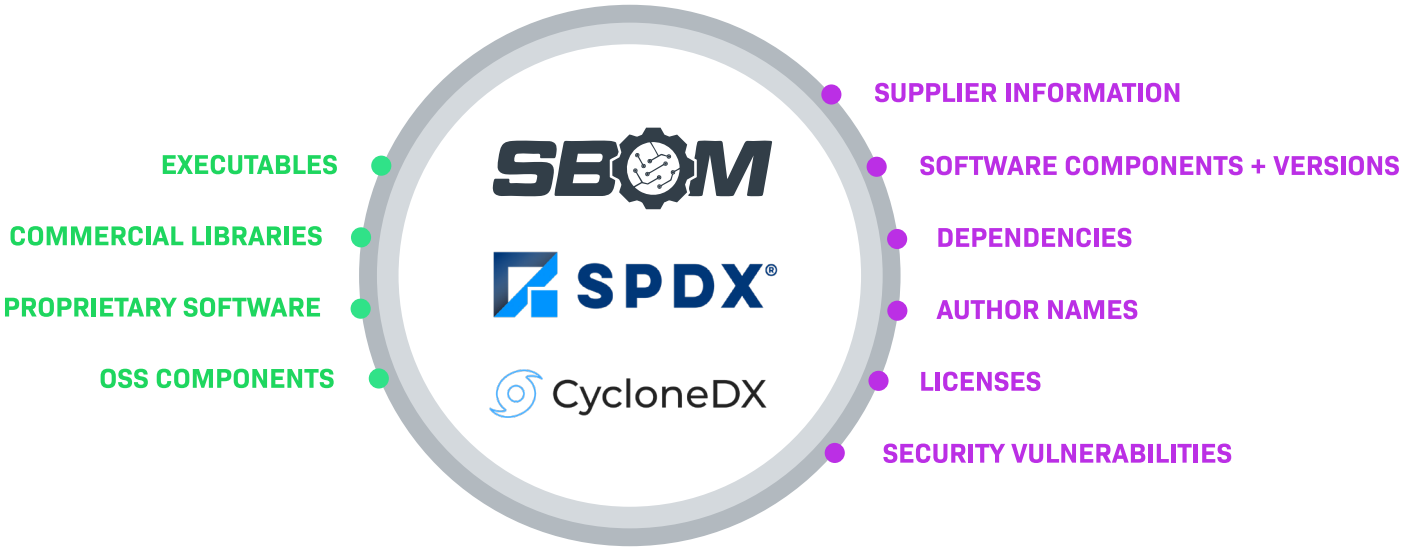
Step Three: Create a list of required remediation actions.
With a complete inventory, remediation steps will likely be necessary to achieve compliance. This could be code remediation or legal remediation. A failure to shut down abandoned projects, if they use OSS, could become both compliance and security issues because they aren't monitored or maintained.

Step Four: Formalize your notice and attribution file.
OSS and third-party software compliance includes notice and attribution requirements. This up-to-date list can be shared with the buyer during an M&A transaction. A diligence process review will transition you from unknown risk to known, analyzed risk. From here, buyers and sellers can effectively negotiate who owns the risk.

The good news is that by going through the diligence process, you're following OSS management best practices. This is important, regardless of whether a transaction is pending.

SBOMs

As you walk through a technical due diligence process, you will inevitably create a Software Bill of Materials (SBOM). A precise inventory of the components in your code, a SBOM offers critical, timely intelligence for software producers and users, as well as buyers and sellers.



An SBOM is complete, machine-readable code documentation. The queryable record includes details from multiple sources about a software application's connected components, versions, and dependencies. It accounts for all the commercial libraries, proprietary software, open-source dependencies, and information on the suppliers and code authors. Ideally, licensing information and security vulnerability reports are also included.

With this complete list of components, buyers and sellers can better understand the software supply chain and manage organizational risk accordingly.

Ready for diligence? Use this best practices checklist

CHECKLIST

Create OSS policies.
Create a succinct OSS policy (or policies) specific to your organization's goals, culture, and strategies that govern your use of OSS. When the time comes, you can provide this to the buyer/seller.

Define and implement processes.
Outline your organization's processes for OSS use. Include the rules for what may and may not be used, along with repercussions.

Create a third-party software inventory.
If you haven't already, compile a list of OSS and third-party commercial software. This will provide a complete picture of your risk posture. Consider closing abandoned OSS projects, ask your commercial suppliers and OEMs to disclose their use of OSS, and conduct deep scanning to help you discover your true inventory.

Maintain up-to-date notice and attribution files.
Maintain license text, copyright notices, and attribution statements so that they may be easily shared. Aim for full compliance, however onerous.

Track OSS contributions.
Most developers contribute to the OSS community—fixing bugs, adding features, or improving code quality. Implement a process that captures documentation on these contributions and provide that information to the other party in an M&A. It may impact IP and valuation.

By following these best practices, you will be well-prepared to effectively negotiate who bears the risk, ensuring both buyers and sellers receive the best value for their investment.

INSIGHT

An Open Source Program Office (OSPO) is a center of excellence for developing and managing OSS strategy.

Learn how to establish and enforce policies with your own OSPO in this white paper.

READ MORE >

OSS Management: How Revenera SCA Solutions Help

Managing growing application portfolios and an increasing reliance on OSS can't be purely manual. A strong toolset is required.

SCA tools from Revenera help you discover, assess, and manage license and security risk across all software applications. Learn more about how we support the construction of complete, accurate SBOMs, manage legal and security risk, and deliver compliance artifacts for comprehensive OSS management and in preparation for an M&A.

Manage complex SBOMs

Revenera SBOM Insights will collect and ingest SBOM parts from multiple sources to create an SBOM in a SaaS environment, aggregate that data into a single repository, and provide full visibility for security, legal, downstream supply chain partners, and transaction partners. Ensure your risk reports for license compliance and security risks are up-to-date and ready quick response when necessary, and a technical diligence review.

Comply with third-party notice requirements and identify security vulnerabilities

Code Insight is a single integrated solution for open source license compliance and security. Find vulnerabilities and remediate associated OSS risk during the build process and throughout their lifecycle. Implement a formal OSS strategy that balances business benefits and risk management, and manage open-source license compliance, including compiling third-party notices, to ensure your diligence review proceeds smoothly.

NEXT STEPS

Ready to mitigate OSS risk for a smooth M&A?

LEARN MORE >

Revenera provides the enabling technology to take products to market fast, unlock the value of your IP and accelerate revenue growth—from the edge to the cloud. **www.revenera.com**