

Originala 

A Practical Guide to IBM Third-Party Software Maintenance

January 2024

Table of Contents

Introduction	3
What is third-party software maintenance?	4
Five scenarios for TPSM	5
Debunking the myths about TPSM	7
What's best for your business?	10
Answers to third-party software maintenance questions	11
About Origina	15

Introduction



Independent third-party software maintenance (TPSM) is a proven, tried, and tested option for organizations that are looking for a more innovative approach than traditional megavendor support. TPSM combines responsive service and flexibility with considerable cost savings — up to 50% annually versus megavendor support and maintenance pricing.

While these substantial savings are what might initially appeal to organizations that move care of their IT estates to TPSM providers, more and more companies that transition away from megavendors are discovering the value of the enhanced and expanded service offerings that are bolstering the growth in the TPSM market.

With added benefits including services like license and audit consultation, enhanced cybersecurity protection, and one-on-one workshops with global IBM experts, third-party software maintenance is moving away from the traditional break-fix model into more of a strategic partner role, someone who can help extend the life and value of IBM software as well as support it.

What is third-party software maintenance?

Generally, independent TPSP providers offer a lower-cost alternative to the escalating maintenance, support, and consulting fees charged by megavendors like IBM. Though technically different functions, software maintenance and software support are two sides of the same coin.

Software maintenance consists of ongoing actions that keep your software efficient and secure. It extends the application's longevity and lifecycle while also enhancing performance and functionality. Software support, on the other hand, deals with putting out fires when things go wrong and mitigating urgent issues that can cause costly downtime.

Where software support ensures that applications continue to operate without error, software maintenance enables businesses to

realize a true return on investment.

According to Forrester® research, enterprises that are embracing third-party support and maintenance will save over \$5B through 2027.¹

In its most recent report, Gartner found the third-party market offered substantial operations savings and value-added services², including:

- Reducing software budgets
- Customizing support contracts for increased flexibility to meet customer needs
- Providing specialized services to support custom code, modifications, and unique product-specific requirements
- Offering improved SLAs



“[Original] was the first time I realized there is an alternative to going directly to IBM or through its partners for support.”

– Steven Wynants, Toyota Motor Europe

¹ “Enterprises Embracing Third-Party Software Support & Maintenance to Save Billions,” US Cloud.com.

² Gartner “Market Guide for Independent Third-Party Software Support for Megavendors,” Rob Shafer et al, November 27, 2023.

Five scenarios for TPSM

IT leaders who take a close look at the impact of being dependent on megavendor maintenance and explore existing alternatives can turn the tide on years of software overspending. These companies are able to maintain all versions of their software solutions

in a flexible way that supports their path toward digital transformation.

Here are five common scenarios that Gartner believes will contribute to continued growth in the third-party software support and maintenance market.³

1

Cloud migrations. TPSM can be beneficial for customers who are migrating to the cloud but who will still need support for their installed products until they switch over. Third-party software maintenance can offer technical support for the customer-entitled version at up to 50% less than megavendor costs.

2

Migration to alternative vendors or solutions. Why pay a megavendor for full support when you're moving off to another product? Add third-party support to the mix when looking for alternative solutions to replace on-premises software products.

3

Low-value maintenance needs. TPSM can be a perfect alternative for software versions that are stable and don't have many incidents or create a lot of tech support tickets.

4

End-of-Support (EOS) announcements or notifications.

Older versions of software can still be used for certain applications, but oftentimes megavendors won't support them past EOS without additional fees and customized support agreements. This is a good time to talk to a TPSM provider. Third-party software maintenance companies often support older versions and allow you the choice to upgrade when you want to, not when the megavendor mandates.

5

Absent or expiring maintenance increase caps for price protection in contracts.

Some contracts do not have any price protections in place, particularly three-to-five-year enterprise license agreements (ELAs). In these circumstances, there can be a risk of escalating maintenance and support costs or EOS announcements during the term.

³ Ibid.

The frequency of these scenarios has led to an uptick in the demand for third-party software maintenance. According to a Forrester Opportunity Snapshot, 79% of IT and procurement leaders have already moved some of their software estates to a third-party provider, and 80% of those would recommend it to their peers.⁴

TPSM is a feasible alternative compared to other savings opportunities typically with a multiyear ROI. “It can help keep budgets flat by eliminating the ongoing year-over-year software vendor maintenance and support increases when organizations are challenged to meet cost-savings goals and initiatives,” says Gartner.

79%

of IT and procurement leaders use some form of third-party maintenance, and

80%

would recommend it to their peers.

— Forrester Opportunity Snapshot, 2020



“Working with a third party, we have discovered there are ways and means to fix that vulnerability and remove that vulnerability without needing to move to the next version. There’s really no point investing good time, money, and resources into the next version.”

— Gillian Leicester, Global Category Lead, PwC

⁴ Forrester Opportunity Snapshot, 2020.

Debunking the myths about TPSM

IBM drives many businesses around the globe. A move to third-party software maintenance will not diminish the power or capabilities of your IBM systems. On the contrary, it will add a more innovative, flexible, tailored approach to support and maintenance that megavendors seldom offer.

So why are some organizations still hesitant to move?

Here are three myths about TPSM and the reasons why these inaccuracies are inhibiting your company's future growth.

Security fixes and protection

Imagine this scenario. You've purchased your software licenses, so you assume you'll receive security fixes and patches for the lifetime of the software. It's a natural assumption to make, but, unfortunately, it is not always true. You must sign up for a support contract with a megavendor after the first year of purchase to have access to OEM-provided security fixes and patches.

Regardless of the number of software licenses you have or the terms of your support contract, megavendors typically will not supply security fixes for unsupported versions of software, so you might be encouraged to upgrade to the latest version. If your version has reached end of support (EOS) or end of life (EOL), you could be left unprepared to deal with any security vulnerabilities that could arise.

Even if the software is not EOS or EOL, it could be months before a patch or fix is released — months that your organization could run the risk of being exposed to security vulnerabilities.

A viable alternative to the OEM patch/fix/upgrade cycle, third-party software maintenance providers are rewriting the narrative on cybersecurity issues.

Origina supports all versions of OEM software, no matter what the version number, custom code, or configuration, allowing your business to stay technologically proactive and liberating you from the reactivity inherent to continuously upgrading to the latest product version.

We have a team of security professionals with global cybersecurity and engineering experience who analyze available threat and vulnerability information. Many have worked within the fields of government, military, finance, and national infrastructure. These specialized personnel focus on understanding what vulnerabilities might be present and how to reduce the likelihood of exploitation.

Minimizing cybersecurity threats requires a layered, forward-thinking approach that limits exposure to vulnerabilities. The question is, do you have a trusted partner in this battle?

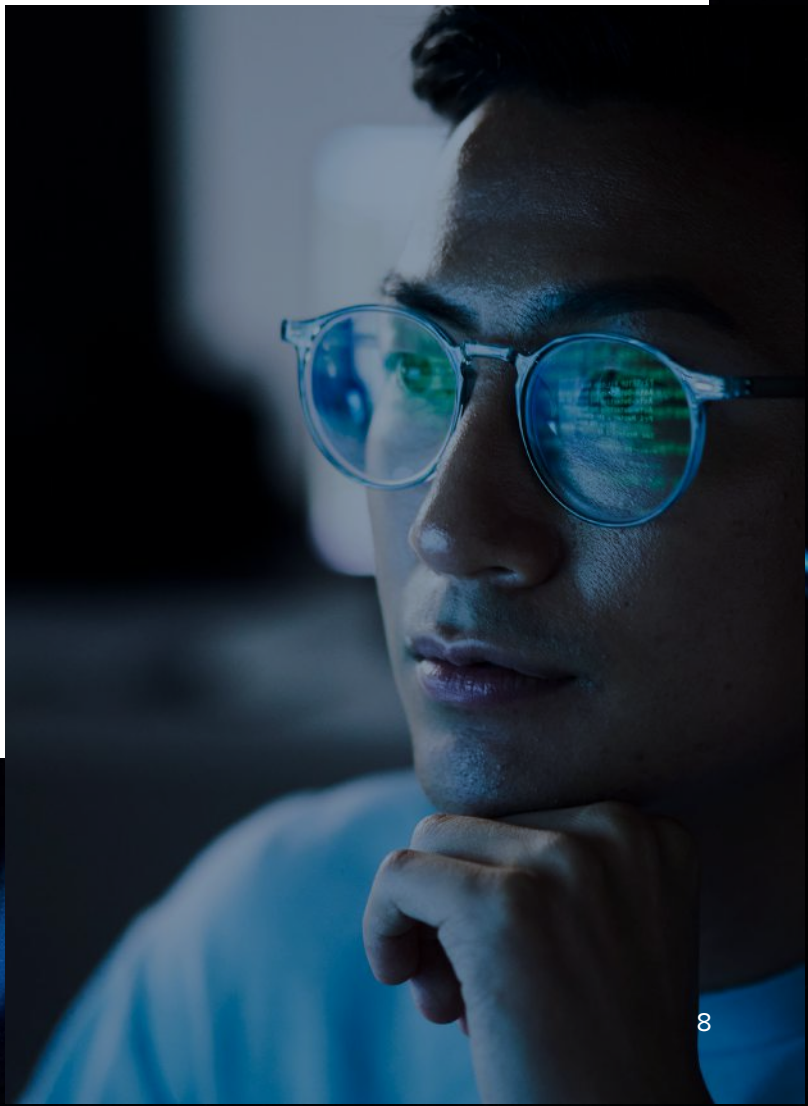
Greater risk of software licensing audit

Honestly, it's highly likely you're going to be audited whether or not you move to third-party software maintenance. OEMs like IBM make substantial revenue from audits. Moving to a TPSM provider has no effect on whether you are paying the right license fees or not.

IBM licensing is complex. Companies can face steep additional fees for noncompliance with IBM licensing rules. TPSM providers know how to ensure every customer has a 100% Effective License Position.

Origina's licensing services almost outweigh our technical services in terms of customer demand. Delivered by ex-IBM license auditors, our Audit Defense Service guides you through the IBM license audit to ensure a successful outcome.

The IBM License Metric Tool (ILMT) services help make sure our customers are accurately reporting on usage consumption. For those products ILMT cannot measure, our IBM experts can help pull the statistics for accurate reporting.



Can TPSM product knowledge measure up to OEM support?

One of the main reasons IT and procurement leaders are hesitant to switch to third-party software maintenance is fear of losing access to OEM expertise.

That's understandable, but what if you could actually gain the knowledge of 15+ years of IBM experience and in many cases much more?

Origina's 600+ independent Global IBM Experts (GIEs) are subject matter experts and software engineers for the products we support. Each has a minimum of 15 years of experience working with their specific products.

Megavendor customers often struggle to get support from technicians who are familiar with

the software, especially for older versions that have reached end of support or end of life. Not an issue with Origina.

In fact, many of our GIEs were the original architects and developers behind the solutions you use every day.

We assign a primary and secondary GIE for each product. The same GIEs work with the same customers, which makes the issue resolution process quicker. Since GIEs are already familiar with their customers' environment, they can jump right in and fix the issue in a timely manner.

All Origina customers are also entitled to four Meet the Expert sessions each year, which are quarterly consultative workshops with their GIEs to proactively address potential issues.

Going beyond solving incidents, Origina's GIEs work closely to help achieve mission-critical priorities of your IT roadmap.



“Moving to a third-party software maintenance provider opens up all kinds of opportunities. It truly gives everyone complete control of their roadmap.”

– Mike Rozsa, Former CIO, NiSource

What's best for your business?

IT leaders who explore alternatives to OEM support and maintenance can turn the tide on years of overspending and reallocate those budget funds toward strategic initiatives. These companies are able to maintain all versions of their software solutions and support their paths toward digital transformation.



ASK YOURSELF

Do you feel you aren't getting enough value from your support?

Would you like to have more contractual freedom?

Do you have strategic initiatives you are unable to fund?

Would you prefer to sweat out the value and improve ROI from existing software without forced upgrades?

Do you lack internal resources with IBM expertise, especially for the older products?



“The third-party relationship is more of a personal service that's tailored to you.”

– Gillian Leicester,
Global Category Lead,
PwC

Most IT leaders — 79% — are already using some form of third-party software maintenance to combat increasing megavendor support costs. While TPSSM often supplies better service at a more affordable cost, it also offers improved agility, increased security vulnerability, and a strategic partnership that can help optimize your IT estate to usher you into the next phase of growth for your business.

Answers to third-party software maintenance questions

Origina helps you extend the longevity of your enterprise software products against a backdrop of ever-changing IT roadmaps. By providing the expertise needed, including feature enhancements, we help you avoid the cost and disruption of unnecessary upgrades or migrations while also reducing your risk exposure.

Q What is the benefit to moving our IBM® and HCL® software maintenance and support to an independent third party?

A You might think the most important answer is up to 50% savings on your annual support fee. And yes, it is important but there are several other crucial reasons to move to third-party software maintenance including:

- Ultra-responsive concierge support
- Continuing to run legacy systems after End of Support without being forced to upgrade
- Multilayered security approach that is superior to dependence only on patches
- IT roadmap guidance and services
- **Freeing up budget to reallocate to strategic initiatives**

Examples and Proof Points

Disneyland Paris achieved:

- \$3 million savings in IT maintenance costs that is being reinvested into innovation initiatives
- Concierge-level support, maintenance, and security for their IBM software
- Guidance and active service on tricky migration tasks that originate in the legacy estate

Q How can you provide fixes for our IBM® and HCL® software when you can't modify the source code?

A Proven break/fix solutions exist outside of traditional IBM support. Patches require regression testing and downtime, and we all know of instances in which a patch had to be backed out because it broke the system.

Alternate methodologies like configuration changes, shell scripts, or even external changes to the product at the operating system level are employed. The majority of bugs, vulnerabilities, and security risks are not in proprietary source code but in open-source code packaged with the products or at the configuration or operating system level. All of our 600+ independent Global IBM Experts (GIEs) have 15+ years of experience working with their products. Some GIEs originally wrote these software products and can quickly identify how best to create solutions to minimize disruption for our customers.

Examples and Proof Points

In one case, a highlighted hidden radio button would not work when the administrator selected it, which resulted in sensitive information being displayed to end users. Origina developed code independent of the product's source code. By leveraging APIs in IBM Case Manager, our independent code is called and overrides the default functioning to ensure that the radio button works as originally intended.

[Capital One](#) received new functionality for IBM® OpenPages from Origina without an upgrade.

Q Are we exposed to a greater audit risk if we use TPSM?

A The risk of an audit is no different whether you leave IBM or stay. IBM can't target you just because you have chosen to leave IBM. That would constitute anti-competitive practices, and they would face legal action (IBM's market share of the aftersales S&M market for IBM software is very high). That said, you want to be in compliance. Our [License Validation Service](#) ensures every customer has a 100% accurate Effective License Position (ELP).

If you are audited, our [Audit Defense Service](#) guides you through the IBM license audit process to ensure a successful outcome. This is delivered by ex-IBM license auditors who are well-versed in IBM's approach to audits.

Our [IBM License Metric Tool \(ILMT\) Service](#) help customers make sure they are accurately reporting on usage consumption.

Examples and Proof Points

A leading U.S. transportation company, who was facing uncertainties in the post-pandemic landscape, sought to address potential audit expenses from IBM software. After internal analysis and spending \$150,000 to reactivate unsupported licenses, the company turned to Origina for proactive defense. Origina's expertise helped navigate an audit notice in 2021, saving over \$3 million. The ongoing partnership with Origina resulted in bottom-line savings, estimated at around \$24 million and provided ongoing security for the company's compliance posture.

Q How can you secure my system when you can't write security patches?

A With Origina's multilayered, in-depth proactive approach to vulnerabilities, you will get a high degree of security that may provide greater protection than an OEM single-layered patch approach to vulnerabilities.


1. Many cyberattacks can't be prevented with patches. In fact, the majority of cyberattacks in 2023 were due to misconfiguration or human error. And roughly 75% of vulnerabilities (e.g. Log4J) are in open-source components for which anyone, including Origina, can write patches or workarounds.
2. IBM typically does not provide security patches for [End of Support software or ongoing Extended Support](#) (after the first year).¹
3. OEM patches can often be slow in arriving to fix a vulnerability. Origina typically **responds within three days after the vulnerability is discovered**. Origina provides mitigations to identified vulnerabilities in a timely manner. Patches require regression testing and can end up causing problems plus they require downtime.
4. Origina offers proactive solutions, such as our [Vulnerability Shielding Solution](#) and [hardening guides](#). 85% of known vulnerabilities can be mitigated today just by employing proper hardening procedures. Plus, there's no downtime or regression testing.
5. And Origina doesn't restrict which product versions we support, so **ALL versions (regardless of IBM EOS status) get full support**.
6. You will have access to all security patches and upgrades released prior to the expiration date of IBM S&S (provided you have downloaded them prior to that date).


Examples and Proof Points

In [December 2021](#), Origina provided mitigation to the Log4J vulnerability within three working days with each mitigation action developed to meet the intent and rigor of original control requirements. This, while IBM's website said they were still working on a solution. Log4J was an open-source Apache vulnerability for which upgrades and patches are available to all and not merely through IBM S&S.

[One major telecom](#) faced with varying OEM responses on Log4J turned to Origina. In three days, Origina's cybersecurity team devised a Log4j mitigation offering specific fixes for open-source components of IBM software. This proactive approach allowed the telecom to swiftly address the vulnerability, avoiding delays associated with OEM patches and achieving rapid protection. The tailored guidance and expertise provided was crucial in securing the enterprise.

[One customer](#) had the latest IBM fix pack applied (8.5.5.17) for WebSphere® Application Server, yet a vulnerability scan by their internal security team identified eight high-risk vulnerabilities. We used our Vulnerability Shielding solution to neutralize all these issues.

 How can you provide the same level of support as IBM?


 You deserve a long-term personal relationship with Origina-designated staff. We believe that contrasts very differently to OEM models in which resources are allocated on a task-by-task basis without long-term relationships and trust. We call this **Concierge Support**. We assign a **Primary and Secondary IBM expert per product** who remain in place during their support, promoting knowledge continuity, speed of resolution, and call efficiency. Each Global IBM Expert (GIE) has a minimum of 15 years working with IBM products. They know how to keep your estate humming with 99% uptime, and they get fully onboard with your business as proactive problem-solving partners.

Additionally, Origina SLAs start with Priority 1 and 2 incidents having a **30-minute response time and carry target resolution times**. Origina commits to using "all reasonable endeavors" to fix all problems from Priority 1 to Priority 4 and, in the case of Priority 1, as quickly as possible. For a P1, this means Origina staff and experts will work nonstop to resolve the problem until it is fixed.² IBM does not give the same level of commitment.³

Examples and Proof Points

[The U.K. grocery chain, Sainsbury's](#), doubted Origina's support claims and conducted a trial for support against IBM for six months and logged support tickets with both. At the end of six months, the Chief Technical Architect who was initially the biggest skeptic said, "Let's just say we didn't have to battle with you guys to get your technical experts at the end of a phone." Five years later, Origina was awarded top honors in the ["Save to Invest" category at Sainsbury's Tech Supplier Day 2022](#).

 How can you allow us to operate older versions for as long as we like?

 One reason organizations think they must upgrade their IBM software is because of changes in software that interface with the IBM product. Check the Interoperability Matrices or Software Product Compatibility Reports. While your old version might not be listed, it doesn't mean it won't work. And of course, IBM is never going to validate versions that have ended support. Origina's **Interoperability Validation Service** is designed to prove older IBM software product versions work with newer third-party versions. Once we validate and the customer accepts, Origina supports that configuration for as long as the customer requires it.

Examples and Proof Points

[Citizen's Bank](#) faced a challenge as its newer platforms encountered compatibility issues with its older IBM systems. Citizens had Origina address a critical slowdown issue in its IBM systems. Origina's solution involved reconfiguring the system architecture, which reduced a 24-hour load time to 15 minutes. This approach not only improved performance but also enabled Citizens to redirect resources towards digital initiatives.

Q How will we get new software releases for new functionality?

A OEM release cycles have slowed, and user forums and industry discussions often highlight a perceived lack of game-changing features or business value in recent updates. The cloud has given rise to innovative companies filling the void left by the slow-paced industry leaders. These agile companies are dedicated to delivering functionality that large vendors struggle to provide in a timely manner. You should only ever upgrade to get a new technical feature. And chances are we could probably create that new feature for you using our [Feature Enhancement Service](#) allowing you to avoid the upgrade.

Examples and Proof Points

To migrate [financial data](#) from IBM® OpenPages® to a new system, a financial institution faced challenges extracting attachments. Although standard data objects were extractable via Excel, attachments lacked a native extraction method. Our independent Global IBM Experts devised a solution, using custom SQL to link obscured file names to originals. A batch process was developed using Java to extract and rename attachments. A custom Cognos report was created, offering an indexed list of with record context and hyperlinks for direct access.

Q What are some of the use cases when I should consider third-party software maintenance?

A Gartner⁴ recommends considering TPSM for the following:

- **Cloud migrations** – TPSM can be a “safe haven” for customers migrating to the cloud but will still need support for their installed products until cut-over. TPSM provides great value and lower risk with our expertise than staying with IBM during the transition.
- **Migration to a new technology or solution** — why pay IBM full support when you are moving off to a new product?
- **Low value for maintenance dollars** — few or no tickets.
- **End of Support deadlines** — say no to forced upgrades!
- **Endless annual price increases** — dictated by the vendors with no caps on increases.

Examples and Proof Points

“Market Guide for Independent Third-Party Software Support for Megavendors,” Gartner, November 2023

[Get the report now](#)

¹ [New IBM Extended Support Offering](#).

² Or in the rare case where it cannot be fixed, until it is determined exhaustively that it cannot be fixed.

³ IBM merely warrants only to use “commercially reasonable efforts to respond to cases raised by your authorized contacts within the criteria specified for your offering.”

This is a substantially lower threshold than “all reasonable endeavors” which is akin to “best endeavors” (<https://www.ibm.com/support/pages/ibm-support-guide> [accessed 13th Dec 2023])

⁴ Market Guide for Independent Third-Party Software Support for Megavendors, Gartner, Nov 2023

About Origina

Origina is a global provider of independent third-party IBM software support and maintenance that is committed to delivering outstanding software maintenance services. Our dedicated team of **600+ independent global IBM product experts** is passionate about championing end-user rights and unlocking value for our customers. We work proactively to protect, extend, and enhance all versions of IBM® and HCL® Passport Advantage software on open systems and mainframes, providing a cost-intelligent alternative to traditional software megavendors.

Visit origina.com to learn more.

Check out more from Origina

Locations



IRELAND, Dublin
+353 1 524 0012



UNITED STATES, Dallas
+1 888-206-4862



UNITED KINGDOM, London
+44 2033 183790

Follow us