Anglepoint

Managing a Software License Compliance Audit

Anglepoint's win-win approach

Managing a Software License Compliance Audit

1

What a license audit is really about.

As the entity that owns the source code of proprietary software, a software publisher has an obligation to its shareholders to protect its intellectual property (IP). One way it does so is by performing audits of end-user organizations to verify whether they're using the licenses they've purchased according to their contractual terms and conditions. During an audit, publishers seek to recover revenue from software that's been deployed without being paid for. Unless stipulated otherwise in the governing contract, these audits can be initiated without warning at any time and in different guises. If an organization's software assets haven't been managed properly, the results can be painful, including exorbitant non-compliance fees, unbudgeted true-up costs, significant resource demands/distractions, and regrettable reputational damage.

Publishers seek to recover revenues from software that's been deployed without being paid for.

When it comes to establishing license compliance, the burden of proof rests with the licensee. Ultimately, it's their responsibility to understand and adhere to the licensing terms and conditions they agree to and manage their software assets accordingly.

But applying an ever-changing (and often ambiguous) complex set of rules to dynamic hybrid IT environments is anything but simple. Just taking a complete snapshot of the quantities of licenses you are entitled to and comparing it to the quantity of licenses you are consuming within a publisher's product portfolio is notoriously difficult—something most organizations fail to do with audit-level accuracy. Even with investment in a best-of-breed SAM tool, custom procedures are almost always necessary to account for finer licensing nuances or specially negotiated terms. Publishers know this, which is why uncovering and exploiting these realities in an audit is so profitable for them. Specific expertise is therefore required to gather and analyze data to determine license entitlement and consumption correctly, and to manage the response in such a way that minimizes exposure.

In a lot of ways, a software license audit is a highly sophisticated form of technical negotiation, and gaining and maintaining control of it requires mastery of many skills and situations. Some publishers carry out audits directly, while some authorize a third party on their behalf. The scope of licensable products may be specific or all-inclusive. Most large enterprises have overlapping agreements, each with different terms, clauses, license grants, and restrictions that are tricky to navigate. Auditors are motivated to widen the scope of entities, products, and environments as much as possible. What's more, the auditor is an expert at their craft—they do this every day, multiple times a day. They know exactly where to look, how to probe, what to gloss over, and how to make this a profitable endeavor. There's not much they haven't seen that you could surprise them with.

Most SAM practitioners, on the other hand, have only experienced an audit by being audited and rarely by the same publisher more than a couple of times, which puts them at a severe disadvantage. The mismatch is akin to a weekend pickup game player going up against a professional athlete—not a particularly wise thing to do, especially with significant money on the line. To close this gap, an exceptionally skilled resource is needed to proactively manage the audit vis-à-vis the auditor—ideally, someone who has been a license auditor themselves (or coached by one) and can stay several steps ahead. Otherwise, the audit scope and process aren't likely to be expertly managed, resulting in an exercise that is unnecessarily disruptive, costly, contentious, and of little value.

2

Don’t treat all publishers the same.

Some publishers are more likely to audit than others. Some have formal license compliance programs that operate at scale, and some of those are known to be particularly aggressive in their tactics. Others audit periodically, but not necessarily programmatically or at scale. Others only have membership in an industry trade association like the BSA (Business Software Alliance) or FAST (Federation Against Software Theft) that have enforcement arms authorized to audit on behalf of their members. And some publishers have never been known to audit their customers but maintain default contractual rights to do so.

Some publishers are more likely to audit than others.

To manage your audit risk effectively, it’s important to know which publishers fall into which category, track how much you spend with them, and manage their estates corresponding with such factors.

However, just because you don’t spend a relatively large amount with a publisher, doesn’t mean you can automatically de-prioritize it from your SAM efforts. Some of those small-spend publishers have software products that are very easy to get out of compliance with. Knowing this, these publishers operate expert audit programs very profitably at scale. Your compliance liability may indeed be disproportionate to the amount you spend with them. As such, it’s best to prioritize publisher-specific SAM efforts based not only on average annual spend but also considering audit likelihood and ease of over-consumption/under-licensing.

During this post-pandemic, high-inflationary period, many publishers have ramped up their audit efforts, with more operating formal compliance programs at scale than ever before. Publishers that audit are more likely to do so at certain times and under certain conditions. Yes, they have an obligation to protect their IP. But in practice, however, many license audits are more concerned with generating or “recovering” revenue than they are about compliance with the four corners of a contract. To be fair, 100% compliance doesn’t exist—in the world of dynamic, hybrid IT environments, autoscaling of ephemeral virtualization, and serverless architectures, any auditor’s snapshot of consumption is already out of date the second it is taken. And so, most audits come thinly veiled under the guise of seeking reasonable assurance that IP is being protected but are truly about extracting a forecasted amount of revenue within a certain timeframe.

Understanding the publisher’s overall financial performance, year-end and quarterly sales cycles, and current regional SPIF (Sales Performance Incentive Fund), and can provide useful context behind the timing and intent of the audit, and therefore how to respond more strategically.

citrix
IBM
BROADCOM
ca
ptc
opentext
AUTODESK
MICRO FOCUS
bmc
tableau
VELOCITY
GENESYS
CISCO
okta
Red Hat
PEGA
DATASTAX
Microsoft
ORACLE
Symantec
Akamai
APPTIO
MathWorks
HCL SOFTWARE
TIBCO
Adobe
software AG
VERITAS
workday
DELL EMC
DASSAULT SYSTEMES
Quest
HITACHI
vmware
SAP
splunk

Read tips from our experts on some of the tier 2 publishers.

3

So, what triggers an audit?

While publishers may maintain that they audit all their customers and insist that your audit is routine, this is only partially true. Just like your tax authority may do some routine audits, in most cases, they're prioritizing their targets based on a set of metrics or flags—data anomalies and trends that point to probable **misreporting.** It's no surprise that software publishers operate similarly. Understandably, they seek to maximize their audit ROI and look for targets that are most likely to be highly profitable. Typical macro-level audit flags include whether spend has decreased (e.g., less net new demand, cancellation of support, etc.) while organizational growth has increased. But there are other activities that increase the figurative target on your back.

In most cases, publishers prioritize their targets based on a set of metrics or flags.

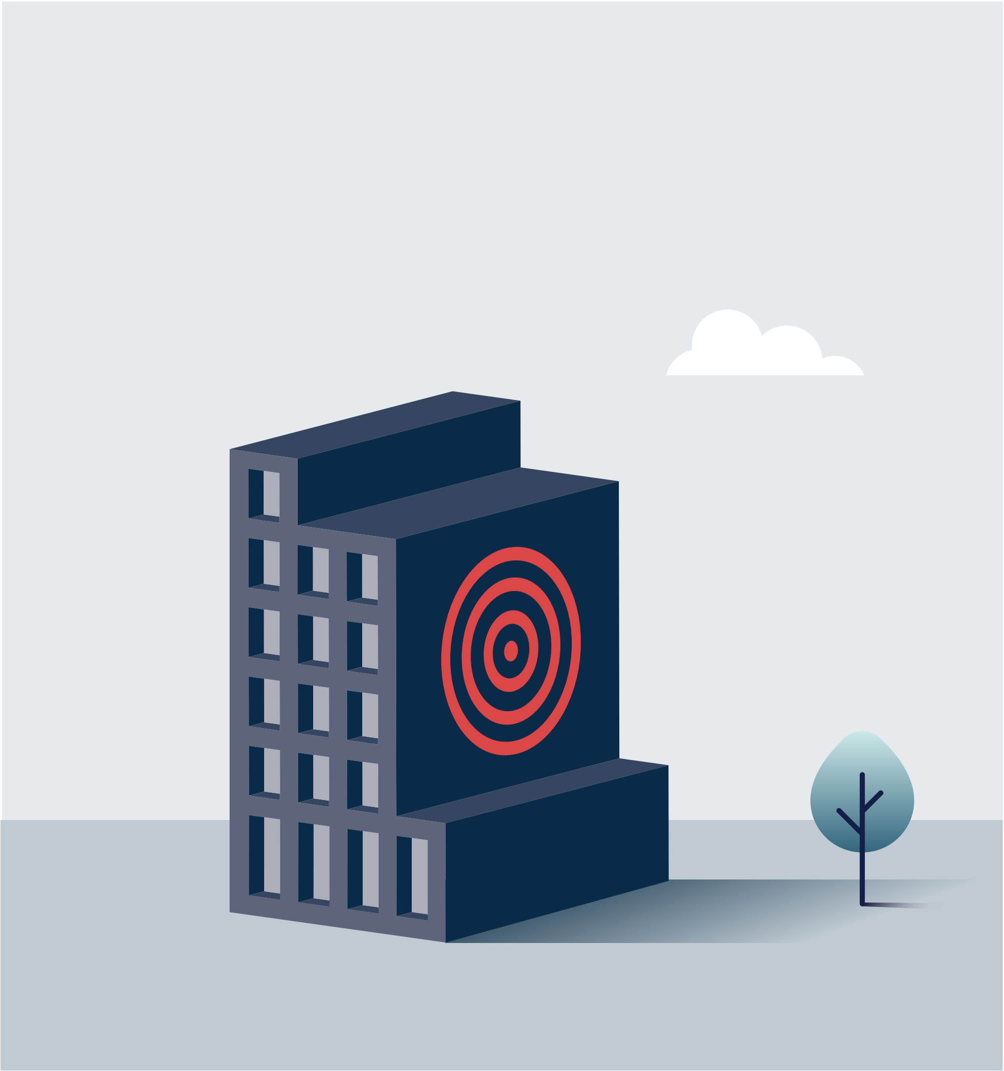
Whether your company has recently experienced a significant **merger/acquisition or divestiture** will eventually trigger an audit. Such changes almost always create compliance issues—not only around the number of licenses entitled but also the usage and consumption of those licenses. Ownership of the license and where the product is deployed are likely to come under scrutiny. While there is usually an allotted amount of time for license transfer and contract novation to take place, companies are often so focused on the operational aspects of post-merger integration that licensing issues (and the complexity to resolve them) are easily overlooked or underestimated. It is important to remember that it may also be an event in the software publisher's world that triggers an audit.

If a software **publisher is acquired,** for example, then the acquisitor will want to take stock of what they have purchased and establish clear visibility of the lines of revenue in their customer base.

It can be worth keeping an eye on your software **publisher's year-end results,** as a poor result may see a software publisher looking to recoup losses by employing aggressive auditing tactics. Vendors who are struggling to achieve earnings targets can also implement commercial models, such as an audit policy of customers who demonstrate spend shrinkage or zero true-ups.

Ultimately, if there is money or misuse of software to be found, like any other business, auditors will look for it – compliance audits are first and foremost a revenue-generating exercise.

Transformation projects and infrastructure migrations can also cause substantial changes in the software products you use and where they are deployed. For example, lifting and shifting on-premises workloads to third-party cloud environments often have a significant impact on license consumption, and in some cases, cause a breach of contractual terms. Should a publisher have insight into such initiatives (e.g., via support ticket information, implementation consultants, casual sales conversations, etc.), it will most certainly



raise their interest to understand what products you will be using, and how and where you will be using them. Even if such changes involve migrating off some of the publisher's technology, an audit is an effective tool the sales rep can employ to squeeze revenue out of a sunsetting account by finding cases of historical noncompliance, especially if they perceive they have little to lose by doing so.

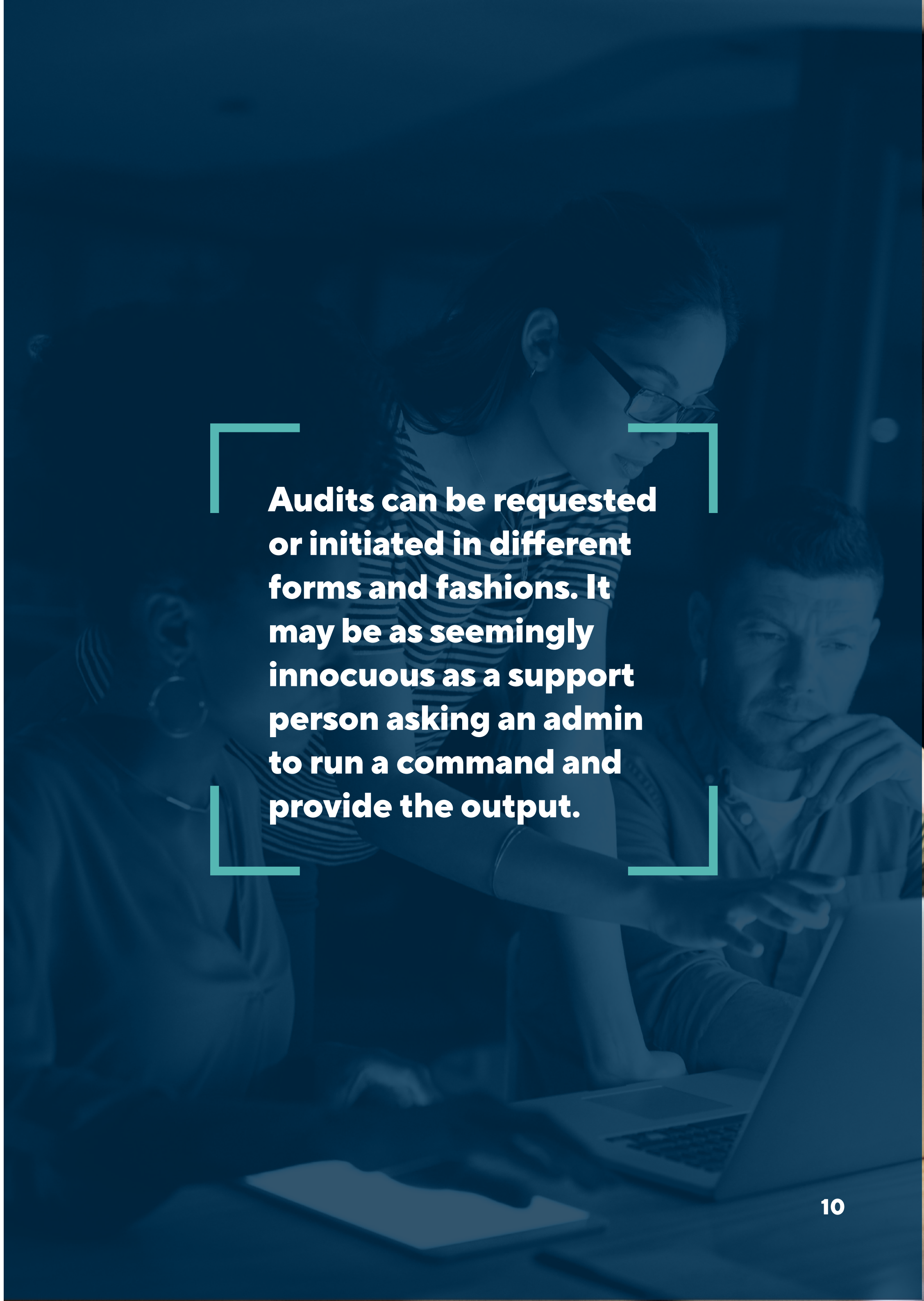
Some publishers have more granular triggers, such as whether **support tickets** are being opened for products the organization doesn't own, or those support tickets suggest volumes incongruent with their purchase history. Other publishers can collect some degree of usage or configuration data remotely, be it through automated systems that "dial home", registration/syncing of node-locked license keys, or simply the data natively available to a SaaS publisher on their customers' instances. In some cases, a new sales rep has recently been put on your account and an audit is deemed an effective way to deconstruct the account during the transition and find easy money while the relationship cost is at its lowest.

Whether your organization has expanded suddenly, either organically or through investment, or has gone through significant technological change, more than likely **software has been rapidly deployed** to ensure business continuity with no downtime. As such, software publishers will want to verify whether you have purchased adequate licenses and are using their software per the relevant terms and conditions.

4

Whatever they call it, it's still an audit.

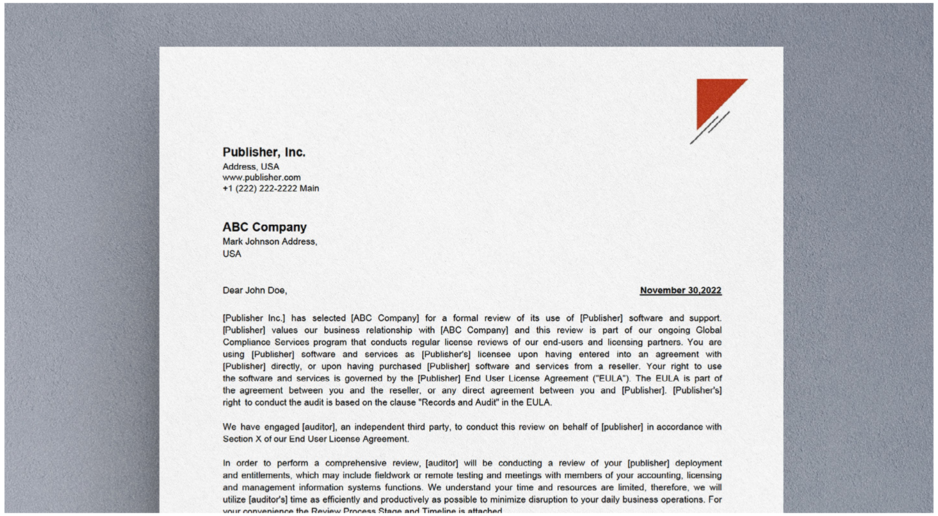
Audits can be requested or initiated in different forms and fashions. It may be as seemingly innocuous as a support person asking an admin to run a command and provide the output. Or it may come as a casual conversation with a sales rep about establishing a deployment baseline in prep for renewing an agreement. It may be an email from some overseas operation asking you to fill out a spreadsheet template with information. In some jurisdictions, it may even be an in-person visit by a local magistrate. Or, as is most often the case, the publisher sends you a formal notification letter via email and/or registered mail. Regardless of what the initiator may call it, you should treat any exercise asking you to disclose deployment or purchase data to an organization incentivized to sell you software, as the audit it is. However, unless the publisher is invoking a specific contractual right (or the local magistrate has due authority under the applicable penal code), whether you respond to such requests is completely optional.



Audits can be requested or initiated in different forms and fashions. It may be as seemingly innocuous as a support person asking an admin to run a command and provide the output.

Any audit rights that a publisher may have, are granted under an active audit clause applied to a relevant scope of licensable products. It circumscribes how, when, and by whom the audit can be conducted. Be aware that an auditor can get in the door using any active audit clause, such as one from an expired contract in which the audit clause survives the term, or from a default clickwrap agreement from a license purchased outside of a separately negotiated contract. Most audit clauses lack specific details, especially on what an audit can cover and how it is to be conducted. But fortunately, many have some element of "as mutually agreed" or at least contain some reference to reasonableness, such as "shall not unreasonably interfere with End User's business activities", which gives the licensee a potential lever point. It's true that ambiguity in a contract typically favors the licensor. But in the case of an audit clause, a licensee can use ambiguity to their advantage if they make the right expert moves.

It's surprising how often vendor managers or procurement officials will defend their sales rep with something along the lines of "they would never audit us, we have such a good relationship" or rely on their commercial status with "because of who we are and how much we spend, they'd never audit us." In reality, it's usually the sales rep that nominates an account to be audited in the first place, or at the very least they give their consent/support. Knowing this, wise SAM practitioners don't allow the sales rep to exit stage right once the audit curtain opens, only to have them enter the final act to play the "good cop" once supposed findings are on the table. It's best to involve them throughout the entire process. By so doing, you gain some degree of leverage, such as when it comes to making appeals to "reasonableness", as they have a longer-term relationship at stake, as opposed to the short-term focus of the compliance auditor.



Publisher, Inc.
Address, USA
www.publisher.com
+1 (222) 222-2222 Main

ABC Company
Mark Johnson Address,
USA

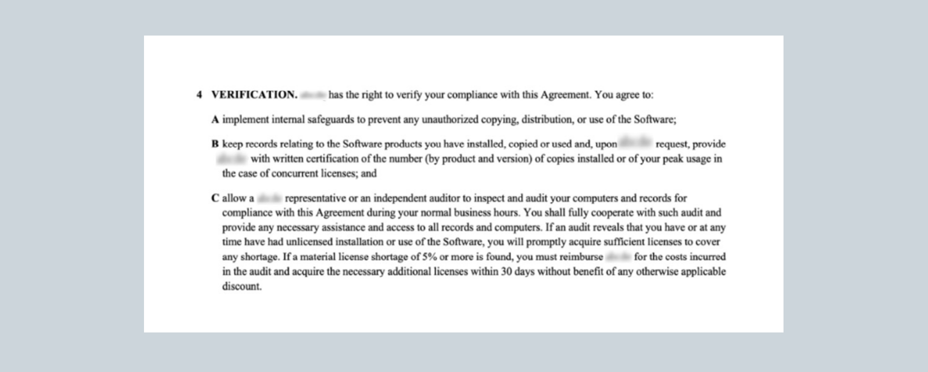
Dear John Doe, **November 30,2022**

[Publisher Inc.] has selected [ABC Company] for a formal review of its use of [Publisher] software and support. [Publisher] values our business relationship with [ABC Company] and this review is part of our ongoing Global Compliance Services program that conducts regular license reviews of our end-users and licensing partners. You are using [Publisher] software and services as [Publisher's] licensee upon having entered into an agreement with [Publisher] directly, or upon having purchased [Publisher] software and services from a reseller. Your right to use the software and services is governed by the [Publisher] End User License Agreement ("EULA"). The EULA is part of the agreement between you and the reseller, or any direct agreement between you and [Publisher]. [Publisher's] right to conduct the audit is based on the clause "Records and Audit" in the EULA.

We have engaged [auditor], an independent third party, to conduct this review on behalf of [publisher] in accordance with Section X of our End User License Agreement.

In order to perform a comprehensive review, [auditor] will be conducting a review of your [publisher] deployment and entitlements, which may include fieldwork or remote testing and meetings with members of your accounting, licensing and management information systems functions. We understand your time and resources are limited, therefore, we will utilize [auditor's] time as efficiently and productively as possible to minimize disruption to your daily business operations. For your convenience the Review Process Stage and Timeline is attached.

Sample Audit Notification Letter



4 **VERIFICATION.** [redacted] has the right to verify your compliance with this Agreement. You agree to:

A implement internal safeguards to prevent any unauthorized copying, distribution, or use of the Software;

B keep records relating to the Software products you have installed, copied or used and, upon [redacted] request, provide [redacted] with written certification of the number (by product and version) of copies installed or of your peak usage in the case of concurrent licenses; and

C allow a [redacted] representative or an independent auditor to inspect and audit your computers and records for compliance with this Agreement during your normal business hours. You shall fully cooperate with such audit and provide any necessary assistance and access to all records and computers. If an audit reveals that you have or at any time have had unlicensed installation or use of the Software, you will promptly acquire sufficient licenses to cover any shortage. If a material license shortage of 5% or more is found, you must reimburse [redacted] for the costs incurred in the audit and acquire the necessary additional licenses within 30 days without benefit of any otherwise applicable discount.

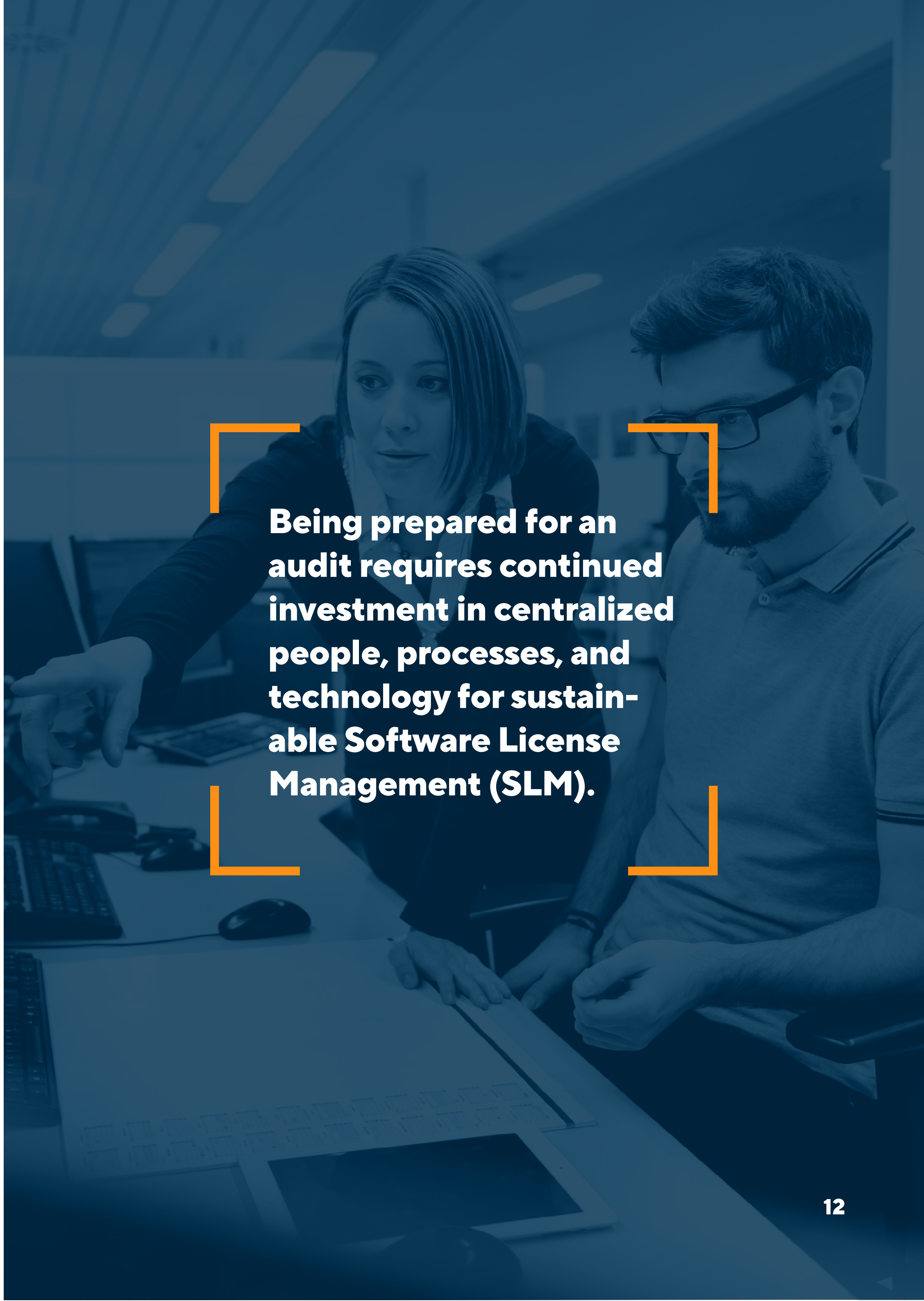
Redacted Audit Clause

5

Planning your audit process.

Understanding why software publishers audit and what can trigger them into action is useful to give you a hint of a potential audit notification, but being prepared for the audit is a whole other story. The best preparation for an audit is to start from the beginning by negotiating the most favorable terms possible in your original contract when signing with the vendor. For example, you could dictate a self-audit with no 3rd parties and a significant lead time or notification, while capping the number of audits in a designated timeframe (e.g., once per 3-year term). Excluding regions or subsidiaries will be to your benefit, including stringent stipulations on data management (which may render an audit very hard to deliver).

Being prepared for an audit requires continued investment in centralized people, processes, and technology for sustainable Software License Management (SLM). Having a well-developed strategy accompanied by tactical handling of the audit will require the careful execution of a well-developed Audit Response Plan.



Being prepared for an audit requires continued investment in centralized people, processes, and technology for sustainable Software License Management (SLM).

Your audit response framework

Your Audit Response Framework will provide a repeatable and robust protocol for delivering a proactive and well-managed response. Having a framework in place will help minimize liability and maximize value from any software license audit.

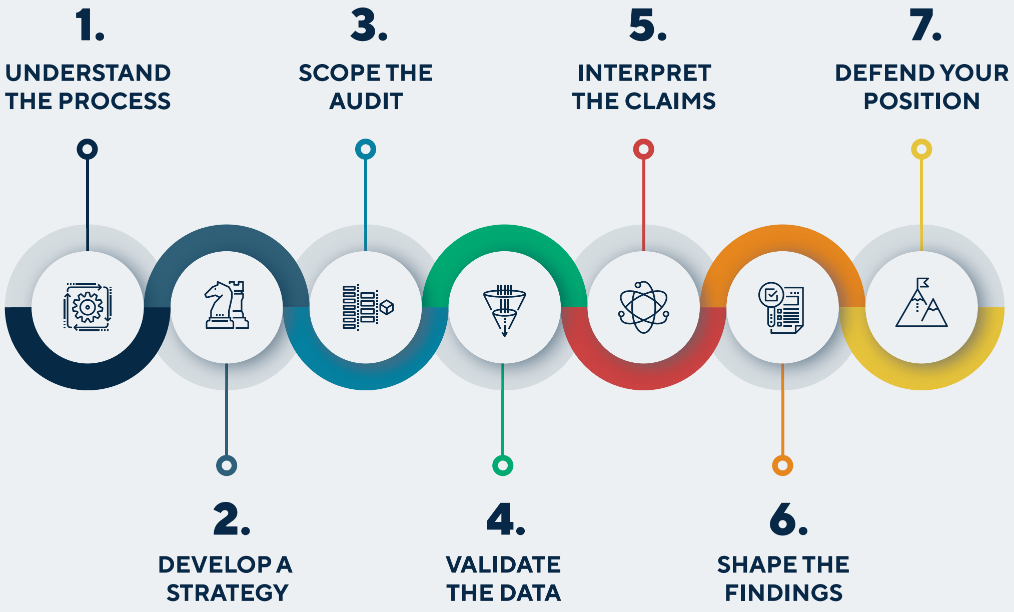
The following aspects should be considered in your design:

- ✓ **Repeatable** — contains role definitions, process flow, checklists.
- ✓ **Robust** — contains guiding principles and policies.
- ✓ **Proactive** — is explicit that the customer take leadership role versus the requester.
- ✓ **Controlled** — lays out strict communication protocol and procedural requirements.
- ✓ **Minimizes liability** — controls scope and procedures, raises the standard of accuracy such that requester may prefer to withdraw.
- ✓ **Maximizes value** — audit exercise concludes with agreed upon entitlement position, methods for calculating license consumption, and definitive results such that the same scope and time period of license usage should never need to be audited again.

Your audit response plan

Defining your Audit Response Plan within this Framework must include all stakeholders in the process, as well as those responsible for the outcome – C-Level, Sourcing Procurement & Vendor Managers, Finance, and Legal.

Consider using a responsibility assignment matrix (RACI) as this should clearly define each role's participation in the process - what is required and when. The process must be clearly documented for every step of the audit, and everyone must understand their involvement. The processes outlined should be repeatable and include an update after every audit to ensure the process is future-proof as well as continuously improving.


1. UNDERSTAND THE PROCESS

2. DEVELOP A STRATEGY

3. SCOPE THE AUDIT

4. VALIDATE THE DATA

5. INTERPRET THE CLAIMS

6. SHAPE THE FINDINGS

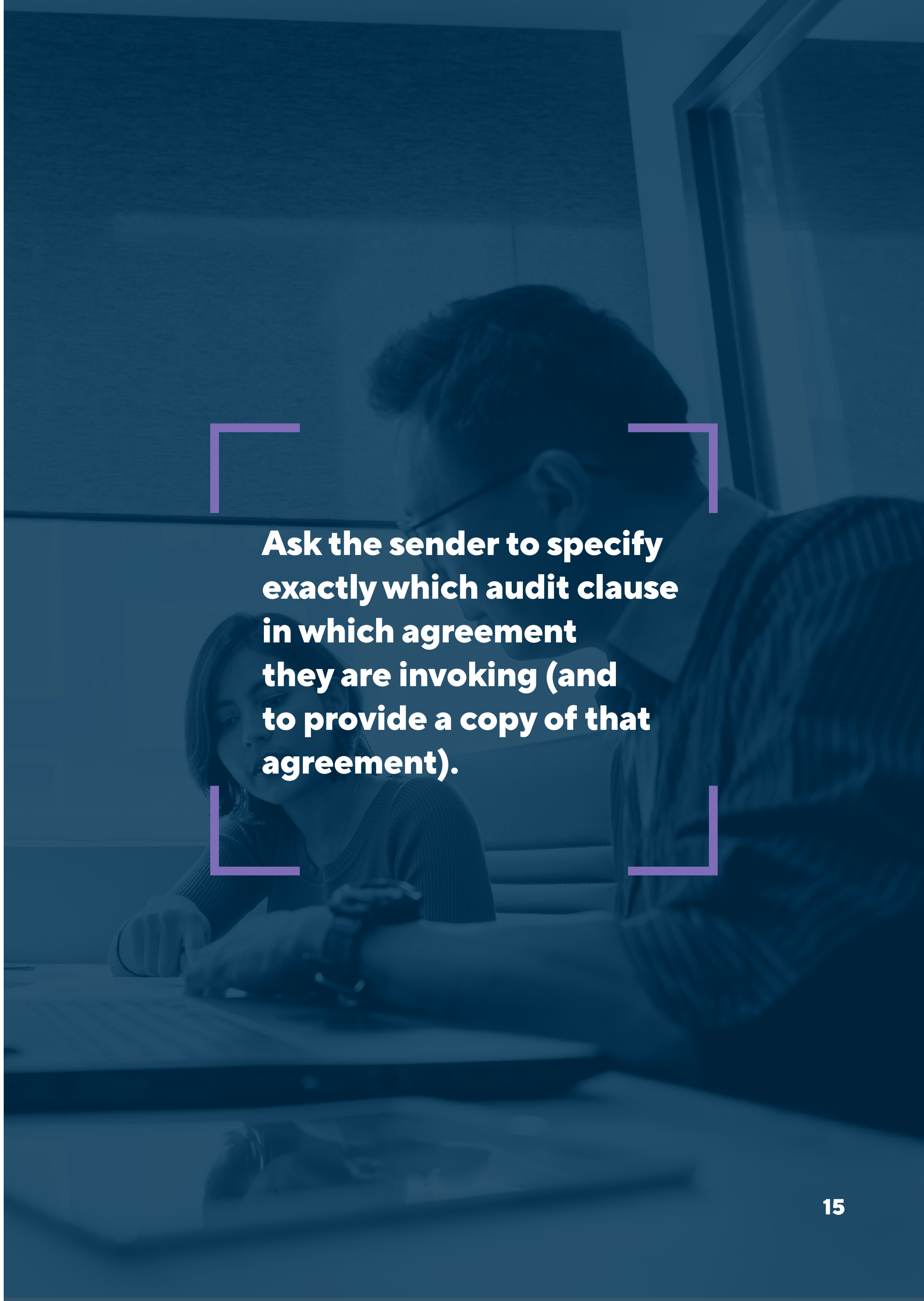
7. DEFEND YOUR POSITION

6

How to respond to an audit.

When a contractual obligation is referenced, such as within a formal audit notification letter, the first step is to ask the sender to specify exactly which audit clause in which agreement they are invoking (and to provide a copy of that agreement). With the help of a publisher-specific licensing expert and/or your legal department, you can then determine the validity of their claim to effective audit rights. If after this assessment you do decide to honor the request, you now have the specific audit clause to evaluate and determine how prescriptive are those rights, especially as it relates to specifying the products and entities in scope, as well as how and by whom the audit is to be conducted. Follow these steps whilst doing so:

1. **Take your time responding**
2. **Ask for an extension**
3. **Put your plan in motion**
4. **Control the written record**



Ask the sender to specify exactly which audit clause in which agreement they are invoking (and to provide a copy of that agreement).

4 step approach to audit response.

1. Take your time responding

If the communication you receive is referencing a 'proposed' or 'potential' audit, do not respond as this may provide the auditor with information to support the audit's intent.

Be cautious of taking action yourself to uninstall software or buy the licenses in question. This may be traceable and it will raise an immediate red flag during the audit. In addition, most publisher contracts contain terms and conditions that prohibit making ANY changes to your environment once you have received an audit notification. Deinstalling or purchasing software once you are aware of an audit might violate these terms and at the very least can weaken your negotiating position. It's important to engage SAM experts immediately to obtain advice and understand exactly what actions, if any, are required.

2. Ask for an extension

There are appropriate justifications for postponing an audit. If undertaking the audit process would impact a business-critical activity - particularly one with time constraints for which audit could detract valuable resources - then an appropriate time can be agreed upon to reengage, suiting your business needs and not those of the software publisher.

3. Put your plan in motion

Once you decide to commence with the audit proceedings, you will need to proactively manage the process you have defined from the start and stick firmly to your internally designed Audit Process. This includes setting up all meetings, tracking action items and deadlines, following up with action owners, and demonstrating to the auditor how you are supporting the progression of the process.

4. Control the written record

Always be the one to set and communicate agendas. If the software publisher sends an agenda first, be sure you send one as well and utilize it as the official guide for any meetings. Be the first to send out all call and meeting minutes that document what was discussed and agreed upon, including conclusions, actions, owners, deadlines, etc. Set a deadline by which this documented record can be challenged.
Document the entire process in detail, as this will provide a record should any issues arise and can provide valuable information for the audit review once it is complete, enabling updates to your existing processes and policies.

Bring your principles or code of conduct into play. Be firm and always follow through.

Guidelines for communicating with an auditor:

1. Set the tone clearly and early so that the outcome of this process will directly impact future commercial decisions and partnerships, particularly if there is an upcoming tender or upsell opportunity for the vendor.
2. Be clear with expectations. If they are unmet, voice concerns clearly with supporting reasons.
3. Never let a question go half-answered or an action goes half-completed. Address these straight away, setting expectations to address the full requirement.
4. Always hold the auditor accountable to the utmost for everything that is and has been agreed upon – this is another advantage to timely and complete documentation of all meetings and decisions.
5. Manage each call and meeting to your prepared agenda and don't allow deviations from that agenda.
6. Don't be afraid to cancel or reschedule a call or meeting when and if the auditor is unprepared. For example, if the technical team from the software publisher is unavailable, do not let the conversation stray to contractual points – instead, cancel and reschedule when the agreed-upon agenda topics can be discussed.

When engaging with the software publisher or auditor be courteous, personable, and genuinely nice - there is no reason not to be - but don't be afraid to repeat yourself or to sit through an awkward silence when necessary. Keeping the process business-like and civil will go a long way when the time comes to negotiate and work with the publisher moving forward.

Maintain control of the audit process.

Remove the 3rd party auditor

Pay particular attention to the contractual language around who can conduct the audit – will it be conducted by the vendor themselves, a 3rd party (such as a "Big 4" firm) or can it be conducted as a "self-audit" with the information provided by the end-user organization.

In many cases, removing 3rd party auditors from the process is appropriate so understanding who is explicitly stated as being able to carry out the audit and conducting due diligence is vital. For example, there may be a conflict of interest or compliance issues where the 3rd party may be deemed impartial, and their involvement could lead to further legal issues. Your contract, after all, is with the software publisher, not the auditor. Contractual challenges should be supported by your IT Legal department.

Agree on processes, principles, & terms

Be clear about your principles or code of conduct - both internally and with your software publisher. This establishes a level of trust and confidence. It also highlights the importance of the commercial relationship you have with them, offering assurances around confidentiality and transparency, and your requirements for them to follow suit.

Employing a defined process that you outline to the auditor will establish your position of control, help foster transparency, and will let them know how you plan to proceed. Request clear terms for the audit in return – how they plan to collect data and the metrics on which the audit will be based. Agree on who the spokespeople will be for both parties and the process for communication. Once both parties agree on all aspects of the audit, an NDA can be signed, and the audit may proceed.

Determine scope & data requirements.

When gathering data to provide to the auditing party be sure that the data being provided is only that which you are legally obligated to provide, nothing more. Requesting the vendor demonstrate compliance in how they handle data may be beneficial. Within areas such as GDPR, regional adherence, and who has access to data can be key.

Carefully review the data being gathered by tools and scripts internally and avoid processes where the data can be collected and sent to the software publisher without a checkpoint. The provision of data points not in the scope of the audit may identify other areas of non-compliance. The data provided should be anonymized before transmission but do not change or remove the required information. Once data has been approved by the responsible persons outlined in your response plan, it can be provided for review by the vendor.

Plan your response and negotiation.

Once the data has been collected, it is important to understand your Effective License Position (ELP). Understanding this position of compliance and what to expect when the publisher responds will allow you to plan your negotiations. Be prepared.

This stage in the process will be where you can benefit most from a high level of license expertise both in planning your side of the negotiation and in ensuring that all the points the software publisher addresses are accurate regarding your contracts and agreements. You will need to know what actions can be taken to remediate potential non-compliance and optimize your estate. Where you can't take action to remediate, the expert will need to recommend actions to re-establish compliance and to ensure that you remain in compliance moving forward. These can all be included in the negotiations with the software publisher.

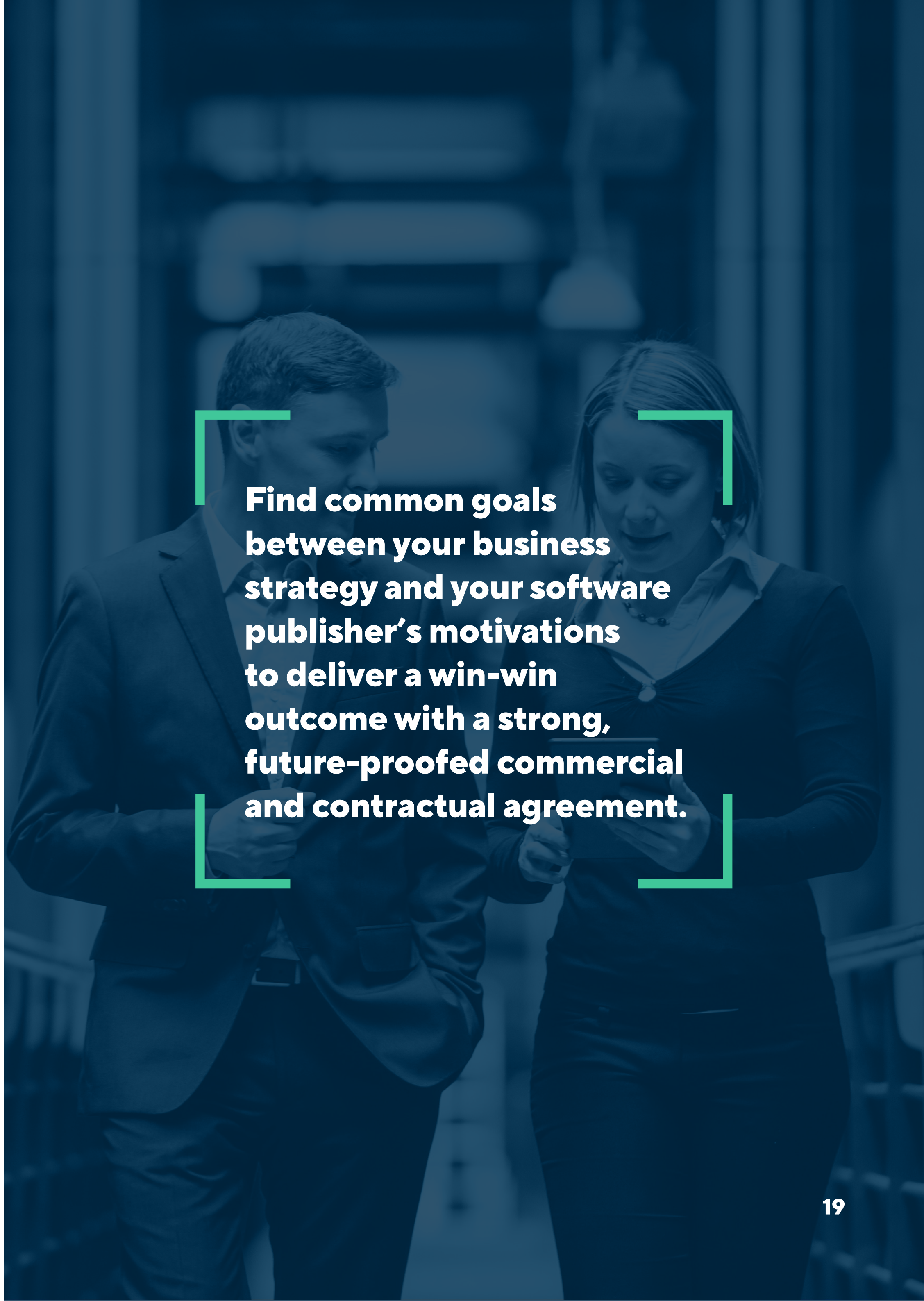
7

Leverage the audit to drive negotiations.

An audit may end with a request for payment to settle the cost of licenses but armed with good knowledge of what motivates the publisher from revenue to product targets, the final fees can be reduced substantially and deliver a far less painful outcome. Understanding this will provide an informed foundation for negotiations. Find common goals between your business strategy and your software publisher's motivations to deliver a win-win outcome with a strong, future-proofed commercial and contractual agreement.

It is also a good idea to align negotiations to your technical requirements and roadmap, often they will just require revenue recognition so will be happy with an alternative product you were planning to purchase over an unrequired product that is installed but not used.

Requesting clear, consistent, and concise contracts will help to remove ambiguity and lay a solid foundation for ongoing compliance.



Find common goals between your business strategy and your software publisher's motivations to deliver a win-win outcome with a strong, future-proofed commercial and contractual agreement.

8. Seek expert advice.

Planning an audit process can be time-consuming and ensuring that you have considered all aspects often means a bit of trial and error.

Engaging with an external service provider to develop a best-in-class process can dramatically shorten the time to value, allowing lessons from other organizations to be included in the process and policies.

Engaging with an expert also brings a wealth of knowledge to the table to support and help manage the process, as well as ensure a continued positive relationship with your software vendor that often provides the platform for an integral part of the business' day-to-day.

Anglepoint's audit team has managed hundreds of audits covering tier-one, long-tail, and industry-specific publishers. Often the highest risk sits within a client's estate with the latter group and the risk can amount to multiple millions of dollars.

SUCCESS STORY

Anglepoint Supports US Health Insurance Provider with Conga Audit and Delivers $500k in Cost Avoidance.

The experience and knowledge provided by Anglepoint's licensing experts secured a complete retraction of the audit fees and an additional discount on a planned five-year contract. Through these carefully navigated negotiations, the client strengthened the relationship with Conga. Further intelligence from the analysis of the contracts by Anglepoint also resulted in reduced user commitments, and thus reduced cost. Anglepoint also advised on amendments to the contract language in the client's favor to help protect them in the future – for example, what constitutes a qualifying user.

Today the client has a highly favorable five-year deal with Conga and a new governance program in place to monitor this product and mitigate the future risk of audits.

If you would like to find out more about how Anglepoint's experts can support you at any stage of this process, please contact us.

To get help with your audit, click here.

Help, we're getting audited!