MetrixData 360

Software Audit Defense Procedure

A Comprehensive Guide for the Defense and Preparation of a Software Audit

Your Company's Name:

_____

MetrixData 360 Inc.
Unit #10
265 Hanlon Creek Blvd.
Guelph, Ontario, N1C 0A1

First Edition

Software Audit Defense Policy

Document Control

Version No. for Final Release:	
Issue Date:	
Status (Draft or Final):	
Author:	
Reviewed by:	
Approval for Final Release:	

Document History

Date Issued	Version No.	Reason for Change	Initials

References

Ref. No.	Doc. ID & Version	Document Title / File name
1.		
2.		

Table of Content

Software Audit Defense Process Vision

The vision of the Software Audit Defense Process within [COMPANY NAME] is to account for the fact that software audits are steadily becoming unavoidable. The consequences of a poorly conducted software audit could mean significant and unbudgeted monetary loss, damage to the relationship with our software vendors, and potentially a tarnished reputation should the software audit result in legal action.

We, therefore, need to be prepared for the event of a software audit. We must ensure that whatever software products are adopted are managed by our IT department to offer clear visibility into our use of the software, and license compliancy. Being equipped to handle a software audit will ensure that if we are audited, we can minimize the time invested into the audit process (organizations who are not prepared can spend a year or longer defending an audit) and limit our financial exposure. These goals can be achieved through clear visibility of data, including effective software asset management and license optimization.

In many organisations, software audits are a reactive process, where disorganization and rushed responses leaves the data produced from such efforts to be lacking in both detail and accuracy. This allows the auditors to create artificially inflated compliance gaps, giving the appearance that the organization owes more than they actually do.

To avoid this fate, processes to prepare our company for a software audit should not be postponed until the software audit has arrived and instead should be a continuous effort throughout the year. An effective Software Audit Defense process will provide us with the tools that are needed to prove how much we are legally obligated to pay the software vendors and no more.
The primary objectives that are to be addressed through the implementation of this framework include the following:

> Data Visibility: Knowing exactly what has been deployed within our environment has many benefits. Data will act as evidence in any upcoming audit and therefore it is in our best interest to know how that data will contribute to our licensing position. Data visibility will also benefit our efforts to cut software spending as it will allow us to track the value of software that has been deployed when compared to actual usage data.

Back to Table of Contents

Reducing Time and Resource Wastage: An unknown expense throughout a software audit is the amount of time and resources that is required when our company is found unprepared. By preparing for a software audit, we can streamline any processes so as to minimize the wastage of company time and resources.

Minimizing Financial Exposure: By having insight into our software profile, we can reduce any risk of incurring heavy penalties that we would otherwise have to burden should we be found out of compliance by the software auditors. These penalties are often outside the planned budget.

Maintaining a Positive Relationship with Our Vendors: Software audits can leave an unpleasant strain between our company and our software vendors. By maintaining a proactive approach to software audits, we can work to preserve the relationship and help nurture it for more beneficial exchanges between both parties in the future.

Introduction

Software audits are only increasing in their regularity. Having the best technology will not prevent us from eventually incurring an audit. There are many reasons why software audits occur.

Revenue Generation: Software audits are an excellent form of revenue for the publishers and they will often use software audits to compensate for any shortcomings in sales. If we have decreased our spending with a vendor in any way, therefore, we are at a heightened risk of receiving an audit.

Sales Opportunity: Often a software audit will end with the software publisher pushing new products onto us without a consideration for whether the products will bring value to our company. Software audits can be viewed as a scare tactic in which we are placed at a heightened pressure to purchase.

Safe Investments: Software audits are treated as investments by the software publishers. This is why software audits tend to be geared towards companies with highly complex profiles. Companies that have multiple branches, companies who have gone through mergers or acquisitions, or companies who have simply failed to demonstrate to their publishers the procedures they have in place to monitor their complex infrastructure will be at a heightened risk of an audit. The software publishers will view auditing such companies as a guaranteed return on investment since there's a great likelihood that they are disorganized enough to be out of compliance.

Since software audits are viewed by the publishers mostly as a means for fiscal gain, even the most organized companies with mature Software Asset Management practices are still likely to receive an audit. Since even the best policies will not remove this risk completely, it is important to prepare for such an event, should one ever occur.

Back to Table of Contents

Glossary

Software Audit: A non-voluntary process that we are contractually obligated to adhere to. It allows the software vendor's auditing team, or a third-party auditor hired by the vendor to examine our network's data for evidence of non-compliance. Should we be found with a compliance gap, we may be obligated to purchase any missing licenses at full price. Some software companies may also charge an additional penalty (5 to 10%) while others might insead expect us to pay for the process of the audit, including the compensation of the auditors, and others still may require us to do both.

SAM Review/Engagement: An optional software compliance review that is run internally using our own resources or by a partner of the vendor. Usually under a SAM Review, if we are found to be out of compliance, we usually are able to purchase the new products at our contracted prices. Despite the fact that we are technically at liberty to refuse a SAM review, it is highly ill-advised since refusing to comply with a SAM review will likely result in incurring a full legal audit, which is non-voluntary and can result in steeper penalties.

License Statement: A list of all the licenses we own, which is then compared with our deployment data (what is actually deployed on our systems or in use by our employees), to come up with an Estimated License Position.

Estimated License Position: Towards the end of the software audit, the auditors will create an Estimated License Position (ELP), this document compares all of our complied deployment data to our License Statement. This number is not guaranteed to be correct, as it is only the auditor's findings based on how they chose to interpret the data we gave them. The auditors could potentially be paid to find the largest compliance gap possible, so when given the opportunity to make an assumption, they will assume the most expensive case is the reality. Poor data means that our ELP will most likely be artificially inflated to look like we owe far more than we actually do. Proving an already created ELP wrong can prove difficult.

True-up: A lump-sum payment that is paid to the publishers at the end of a specific period of time laid out in our contracts. At the end of a software audit, our true-up payment may be inflated to cover the costs of any missing licenses.

Back to Table of Contents

Compliance Gap: Any discrepancies found between licenses that we have purchased as opposed to software we are using. Compliance gaps are the number of licenses that are required to purchase to become compliant.

Receiving a Software Audit Notification

Software Audit Notification

The method of initial contact from the software publisher will depend on which type of audit we have received, whether it is a full audit or its lighter equivalent, a License Review (the exact name of these reviews varies from software vendor to software vendor). In the event of a full audit, we will most likely receive an official notice in the mail to an officer of the company (CIO or CFO). If it is a review, then we will be contacted through a more informal method such as an email or a phone call. Regardless of the method of contact, any request received should be reviewed carefully to ensure it is legitimate. Recently, phishing scams have popped up trying to gain sensitive information from companies. Should there be suspicious elements to the request such as an invalid virtual signature, spelling and grammatical errors, an upside-down logo, or a request to click a suspicious looking link, we should contact our Sales Rep or our Reseller to gage its legitimacy.

Our Response

Single Point of Contact: It is important to already have established who is responsible for corresponding with the auditors throughout the process. Having a single point of contact controlling the flow of information to the auditors will prevent any unknown statements or actions from employees within our company being used against us later in the audit process. Our auditing team should consist of experts in procurement, legal, finance, and the technology teams.

Determine if Compliance is Necessary: In most software contracts, we are legally obligated to adhere to a software audit request, and should we ignore an audit request, legal action can ensue which can result in serious fines. However, while reviews are optional, they may appear as optional, but not responding may push the vendor to more formal audit processes. The review options can sometimes have lesser penalties and we may be allowed to conduct the process internally using our own resources, as opposed to having a third-party auditor conduct the audit.

Back to Table of Contents

An NDA is Required: If there is a third-party software auditor involved such as Deloitte or KPMG, our first order of business, before any data is handed over to the auditors, is to set up a three-way non-disclosure agreement between the third-party auditor and our company. This will ensure that no information is passed off to the software vendor without our approval.

Ensure that the Scope Is Clearly Defined: We need to make sure that the scope of the audit is clear regarding the divisions that will be included and if the vendor has several products, which products will be examined. Failure to do this will result in the auditors requested information that is out scope of the audit and may cause unnecessary problems and time delays.

Begin Creating Our Own ELP: Having our own Estimated Licensing Position (ELP) ready will give us a strong case to oppose the auditor's findings, which will most likely have an overly inflated compliance gap. Our Estimated License Position should effectively compare our deployment data with our purchased licenses regarding the scope of the audit. We will want to review the vendor who is auditing us to see if we have the internal skills required to meet the demands of the audit or if we need to hire external experts (like MetrixData 360) to assist.

Ensure that the Timeline Is Reasonable: We will need to take ownership of the timeline and potentially delay for time if we need longer to understand our data or we are lacking visibility. The auditors will want the process done as quickly as possible and we must push against that to ensure it is done effectively.

The Kick-Off Meeting

The kick-off meeting will be conducted between us and the software vendor, their auditors, and any other stakeholders that they wish to be present. Here are a few likely topics that will be discussed during the kick-off meeting:

- The approach the auditors will take and how they will collaborate with us
- How the auditors will gather our data? Although, they may be vague about the data requirements.
- The tools that will be used to perform the actual inventory
- The creation of the Estimated License Position (ELP) and the various workbooks that go along with it
- How they will account for and review any license entitlements we own
- The timelines for completion
- The creation of a Statement of Work (SOW) or its equivalent

Our Response

Pay Close Attention to the Timeline: The Timeline will prove an important area for us to negotiate in order to make sure that we have enough time to complete the tasks the audit requires. Unless we negotiate for more time, we could easily be left with having only fifteen days to respond to the auditor's findings (which will mean sifting through hundreds of thousands of rows of data). Having an established timeline will also allow us to monitor any dilapidation of the software publisher and their auditors' enthusiasm in the process. During our audit, it is possible for them to become distracted by other projects or lose interest when it becomes apparent our audit will not reap the anticipated rewards. If the software publisher or their auditors haven't contacted us long past one of the dates for completion, our audit could become dormant.

Back to Table of Contents

Prepare a Defense for the Accuracy of our SAM tools: The auditors will most likely declare that our inventory tools fail to collect all the data that is relevant for them to complete the audit and for that reason they will demand to exclusively use their own.

Even if we have an inventory tool that the software publisher auditing us has approved, the auditor will often not accept the data that our tools have collected. It is in our best interest that our tools are used; it ensures that the tools we are using to count and monitor usage will stand up to the audits. If there are areas of inefficiencies, using our tool(s) will allow us to create processes to fix those in the future. It also prevents us from having to do security reviews of inventory tools from the auditors. We can offer the auditors the option of supplementing any missing data from our inventory tools with their own or we can offer the chance to extract data samples from our inventory tool to test its accuracy.

Clarify the Data Requirements: There are many things that the auditors will be intentionally vague about, such as the metrics that will be used to count our deployment data, our licenses, our user counts, or our authorized users. There will also be very little information provided on how virtualization will be monitored and determined. It is important that all these points are clearly defined. We must understand what exactly they will be asking for and why they need to see that data. Not everything they ask for will be relevant to the audit.

Data Collection

The auditors will most likely resort to collecting data remotely and will only travel onsite to do a data verification session, this is done for the sake of practicality. Remote data collection is a more ideal situation for us, as it will grant us strict control over what the auditors have access to.

The auditors might also schedule to gather data from the members of our team in person (usually through screen sharing sessions), more specifically they will want to gather information from the IT and procurement departments. This will either be obtained through an interview or through a simple observation. In the interview, they will likely be seeking information regarding the following:

- The processes behind purchasing and record keeping
- The life cycle of a desktop or server, including how we retire assets.

Interviews pose an ultimate strain on company resources as this process will take working hours out of our company's day.
In some scenarios the auditors might either ask us to self-declare our data or provide request records. Self-declare is most typical in the event of a SAM review since SAM's are usually governed internally. We will be allowed to gather our own data or the auditor's will simply send a form which will guide us through the steps of how to gather their requested data manually.

Our Response

Verify that Any Employees Who will be Interviewed are Prepared: Before staff is interviewed, it's important to make sure everyone is aligned on what will and won't be said. While we should never strive to hide things from the auditor, we should have a clear understanding of what our stance is with the vendor.

In order to achieve this, it's required that we know what questions the auditors are going to ask and help employees know how to answer those questions completely and effectively. Giving the auditors generalized and over-simplified information can cause incorrect assumptions to be made on the part of the auditor.

Back to Table of Contents

Review all Data Requests: Our Single Contact Person (SCP) needs to be reviewing all data requests to make sure the requests are reasonable and within the scope of the audit. It is important that we remain on high alert and ask questions, always make sure we understand why the auditor has asked for something and understand the impact each piece of data will have on our overall stance with the vendor. The SCP should also review each piece of data that is sent to the vendor to ensure we fully understand all information that is provided to the vendor and what it will be used for.

Our SCP Should Be Our Only Contact with the Vendor: Ensure all communication with the vendor is done exclusively through our SCP. Again, this is not done to keep things from the vendor, this will simply make it easier to keep effective tabs on our position with the vendor during the process.

Review Data Quality: Make sure that all the data our company releases to the auditors and the vendor are of good quality and do not conflict with each other. We must check to ensure the data released is not providing any unnecessary data that can be used to make assumptions that may harm our position.

Above all else, we must challenge the software auditors whenever we feel uncomfortable with the data we have been asked to release. If we do not know something, do not attempt to guess why they are requesting the data, ask questions to fully understand why they are asking for and what they are going to do with it.

If we don't know how to answer a question or obtain the requested data, explain what we do not know and propose solutions on how to retrieve that missing information.

Data Analysis and Estimated License Positions

After all the data has been compiled, the auditors will produce the Estimated Licensing Position (ELP) for our company, and they will ask whether we agree or disagree with the findings. It is important to remember that their findings are not set in stone, it is a mere interpretation of the data and can be read multiple ways.

The ELP will be presented as a large spreadsheet that will display the number of each product we have, the versions deployed, and compare those deployments with the number of licenses we have purchased. In any areas where we are out of compliance, the numbers will be lit up with red. Depending on the software vendor, the ELP might also include extra tabs or workbooks for every product found during the audit. These workbooks will provide the detailed data behind the inventory, including on which desktop or server a product is installed, details of what users are accessing servers, which management packs are installed, and the list goes on. After the auditors have produced this ELP, they will grant us only a small window of time, usually 15 days, to review hundreds of thousands of lines of data or more.

Once we have come to an agreement with the auditors over the ELP (with a NDA in place, they should not be able to send anything to the vendor prior to our agreement), the auditors will send their findings back to the vendor. They will give the vendor a brief summary of their research and our compliance gap.

Our Response

Compare the Auditor's ELP with our Own: Being able to cross compare the auditor's findings with our own will allow us to effectively challenge auditor's conclusions. One way to make sure we are prepared would be to have an accurate count on both our licences and our deployment data well before this point in the audit (or even before the audit begins). Investigate every area of the auditor's case that we know, suspect, or even feel to be inaccurate. Find which team provided the data that the auditor's used in their inaccurate assumptions and ask for validation. Seek clarification on items we do not fully understand, and have the auditors explain what they're planning on telling our vendor. Highlight any disagreements that we have on the auditor's findings, submit explanations for any grey areas or propose plans to fix any shortcomings.

Back to Table of Contents

Negotiate the Timeframe: After the data has been sent off and the fact-finding portion of the audit is closed, the vendor will begin setting up a timeframe for purchasing any license shortfalls. It is important to realize this is not a settlement but actually a negotiation at this point. We will need to push for a timeframe that works for our company's goals and interests, not the vendor's fiscal goals.

Negotiation and Settlement

After the software vendor has reviewed the ELP and our license position, they will send a starting quote for how much is owed to them. We should expect this number to be extremely high initially, depending on how much our compliance gap has been inflated due to worse-case assumptions made by the auditors. This is still a negotiation, not a settlement. This quote is not the final price and that is what needs to be kept in mind.
If we are found to be non-compliant, the remedy will differ depending on whether we have been given a SAM review or a software audit, which have previously been discussed. Remember though, this is a negotiation, and nothing is set in stone, including the penalties. For instance, if the vendor has a clause stating that we must pay list price, plus an additional 5% penalty and we are found to be noncompliant, we have the ability (that we should certainly use) to negotiate that we do not pay penalties.
One thing we are trying to accomplish during the negotiation is to have the vendor offer their initial findings, the concessions, and any discounts right away. We may be able to obtain this by ensuring that anything we disagree with in the ELP is documented with valid mitigation strategies to account for any faults in the ELP. There is no single formula that can applied to every negotiation, as negotiations are an art form.

How We Negotiate a Settlement

Consider the Multiple Stakeholders: There are many people involved in the audit from the vendor's side that are reporting to managers with different agendas from one another. Stakeholders involved in the audit include:

- The license compliance Team
- The technical resource Team
- The licensing or contract group, who may not be licensing experts, but are certainly responsible for selling licenses
- The Sales Team, which will include your account manager
- The vendor's legal team, including the lawyers

All of these different teams might be compensated in different ways; one team might be paid based on the revenue they manage to obtain, while another on whether this audit is conducted according to legal standards or on how satisfied we are with their work. When the vendor's representative says they need to obtain internal approval, these are the people they are consulting. We need to word our requests in a manner that appeals to all stakeholders involved.

Back to Table of Contents

Stay Calm: Know that we have done everything we possibly can to prepare for this software audit. Do not be pressured into timelines. Our goal is to have an ELP created that reflects our actual use and license requirements. Do not be forced into a settlement that is not accurate because we were not given enough time or because the vendor's year end is upon us.

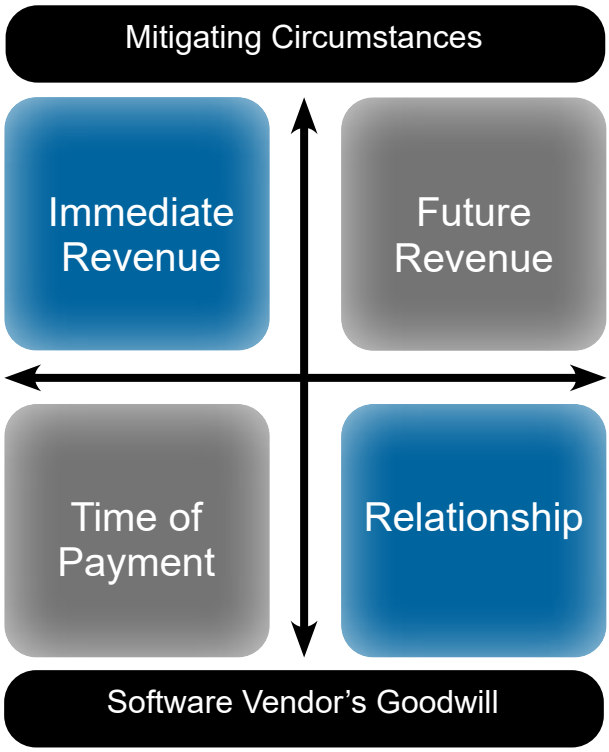
Be Prepared: Be ready to research the licensing terms and other claims the vendor makes.

Leverage: Be willing to leverage senior executives within our company and the vendor's. A well-timed call to the right person can be very effective to unblock a stalemate in the process.

Stay Focused: Our goal is to purchase only what we need. Often software audits are used as a sales tactic. Just when we feel cornered in the software negotiations, we can expect to be pushed towards purchasing new products. We must stay focused and strategic with our software purchases regardless of the pressure the software audit puts us under.

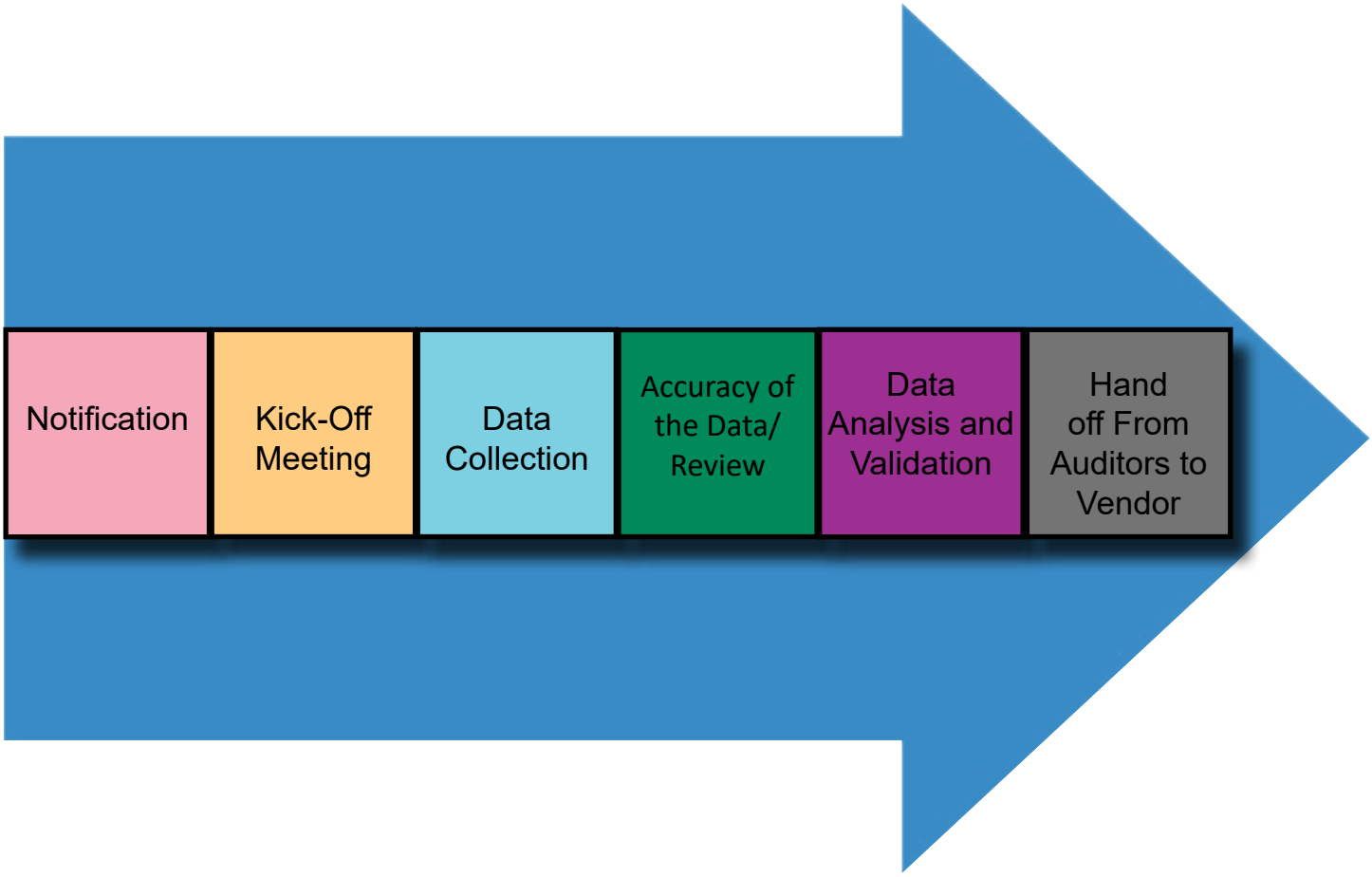
The Four Factors: During the negotiation process it is important to remember that it is a balancing act between four key factors. The first one is future revenue versus immediate revenue, the software vendor will try to lean more towards immediate revenue while we should try to put most of our argument towards future revenue such as deals we can strike with the vendor in the future given our company's projected growth.

The second two factors are time of payment versus the relationship between the vendor and us as a client. The vendor will try to push for getting their payment quickly and it would be helpful if we pushed from the angle of keeping the health of our relationship with that vendor intact.



The Closing Statement: Make sure we get a closing statement at the end of the negotiation, after final figures have been decided. Some vendors may indemnify us from future audits looking back past the date the audit closed and we should try and get this if possible. This will give us the freedom of not having to worry about another audit from that vendor for a minimum timeframe or they will be at liberty to audit us using findings that date back prior to the close of the audit.

The Software Audit Process Overview



Back to Table of Contents