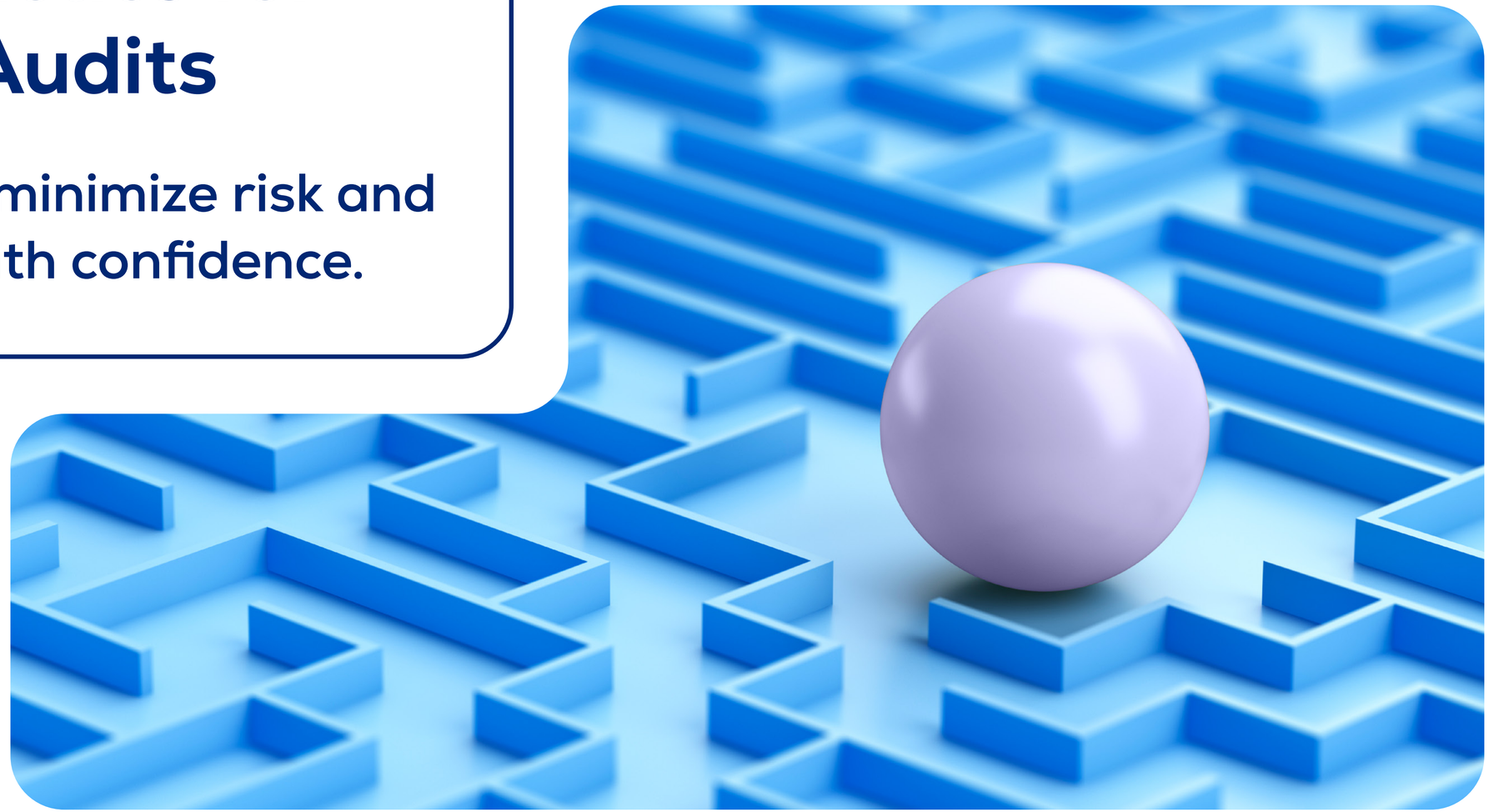
White Paper

Survival Tactics for Software Audits

Proven ways to minimize risk and handle audits with confidence.



Content

Introduction 3

Why You're Still Being Audited 4
The 6 Main Indicators 5

The Vendor Audit Process in 6 Steps 6
Step 1: Audit Target Selection 7
Step 2: Customer Notification 8
Step 3: Audit Scoping & Initiation 9
Step 4: Audit Target Selection 12
Step 5: Accuracy Check 14
Step 6: Settlement Discussion 15

Microsoft, SAP + Co: How to Manage Audits of Big Vendors 16
Microsoft 17
SAP 19
IBM 21
Oracle 23

Conclusion: Beat the Audit Today, Prevent the Audit Tomorrow 25

Introduction

Software license audits cost businesses millions each year—not just in penalties, but in time and effort too. Without the right strategy, you're left navigating a complex, stressful process. This guide helps you take control. You'll get step-by-step advice for every stage of an audit, plus insights into the most common compliance challenges that can lead to audit penalties and how to avoid them.

What's inside:

- Why vendors audit—and what they're looking for
- Common triggers for license audits
- The full audit process, explained
- How to manage big vendor audits

We also show how the right mix of tools, processes and expertise helps you stay audit-ready—and protect your bottom line.

Why Preparation Pays Off

- → 86% of companies face extra financial claims during audits
- → Many audits result in exposure worth 2–3 times annual spend
- → A typical audit lasts more than six months
- → Strong IT Asset Management (ITAM) practices can cut license costs by up to 30%

Why You're Still Being Audited

License compliance has been a key revenue driver for major software vendors for years—especially for large legacy vendors who've slowed innovation and now depend on audits to boost profits. Here are the top three reasons they audit.

1

Audits Deliver Pure Profit
Most vendors still run audits because they're profitable. Unlike sales, there's no cost of sale. Vendors are simply collecting payments customers technically already owed. That money goes straight to their bottom line, making audits hard to resist.

2

Don't Be Intimidated by Inflated Claims
Most audit gaps aren't deliberate—they come from unclear terms or accidental use. Some vendors inflate claims, sometimes over $100 million, knowing they won't collect that amount. These verbal "shock numbers" are used to pressure you in negotiations.

3

Audit Claims Don't Always Equal Real Needs
Big audit claims often come from technical missteps, not overspending. A simple misconfiguration can trigger a major breach. Even if you don't need more licenses, you may be pushed to settle by buying new—often cloud-based—software that doesn't match your needs.

The 6 Main Indicators

The most common triggers for a software license audit are:

- Customer’s purchase level with the vendor
- Complexity of licensing model agreed
- Level of organizational change such as M&A activities
- Organizational structure complexity
- Purchase pattern that does not reflect growth
- SAM maturity intelligence gathered from account team

The Vendor Audit Process in 6 Steps



1. Audit Target Selection

License audits are not as random as they appear. How do the vendors select their audit targets? What can trigger an audit?

2. Customer Notification

How should you respond when you receive an audit notification letter or email? What are the key first steps in successful audit defense?

3. Audit Scoping & Initiation

Understand exactly what the vendor is contractually entitled to do during the audit and ensure you are prepared for what comes next.



4. Audit Data Collection

What are the most common information gathering techniques used by vendors and how should you manage this activity?

5. Factual Accuracy Verification & Confirmation

How should you review the data behind the draft compliance report issued by the vendor? Where can you identify any discrepancies or inaccuracies at this stage?

6. Settlement Discussions

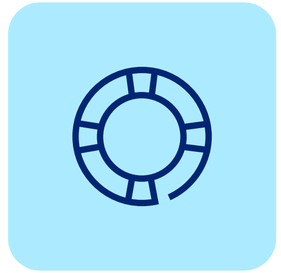
Understand how you can negotiate claims for non-compliance, minimizing your settlement fee.

Step 1: Audit Target Selection

What Happens?

Vendors don’t want to spend time and money on audits that reveal no compliance gaps and no revenue. That’s why they usually don’t choose targets at random.

Instead, they use specific indicators to estimate the potential return and focus on the most likely candidates.

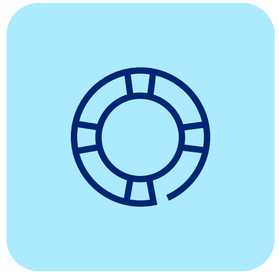


How to Survive

Many audit risk factors are out of your hands—but you can still take smart steps to reduce your chances:

- → Build a strong, transparent relationship with your account managers. Share why you’re not renewing or buying and show how you manage license use.
- → Avoid hard-to-measure license models—especially if the software doesn’t include usage reporting.

Step 2: Customer Notification



What Happens?

Your vendor or their auditors will send an official letter or email, usually to the contract signatory requesting a kick-off meeting to outline the audit process and timeline.

They'll likely state that any licenses bought after the notice date won't count toward your license balance for the audit.

Ask Yourself

- Are you aware of all license restrictions and obligations stated in the EULA?
- Can you measure software usage that is not licensed on a user or install basis?
- Does your Discovery tool cover non-Windows or test/dev servers?
- Is your compliance calculation based on words or validated facts?

How to Survive

→ **Start with your license agreements**
Check your contracts for audit clauses. Let key stakeholders know and pull together a team with the right knowledge and resources.

→ **Assess your compliance early**
If you're unsure about your current status, run a quick internal audit. If you're short on time or expertise, bring in external support.

→ **Get ahead of the vendor**
Know your compliance position before the auditor does. You don't need to hide anything. Auditors usually find it anyway. Instead, be proactive. Many vendors offer steep discounts for early settlements to avoid a full audit.

Step 3: Audit Scoping & Initiation

What Happens?

This first meeting with the vendor and their auditors defines the audit's scope, approach and timeline.

Scope can be based on region, organization or product families. Auditors will also explain what data they need and how they plan to collect it.



How to Survive

Take these steps to stay in control:

- → **Limit the scope** to licenses you directly own and manage. Exclude subsidiaries or overseas entities unless covered under your agreement.
- → **Request an NDA** to prevent your audit data from being used elsewhere.
- → **Ask for a realistic timeline—**especially if you're short on resources or in the middle of a migration. You're not contractually bound to a fixed deadline.

Use the Right Data to Define Your Audit Scope

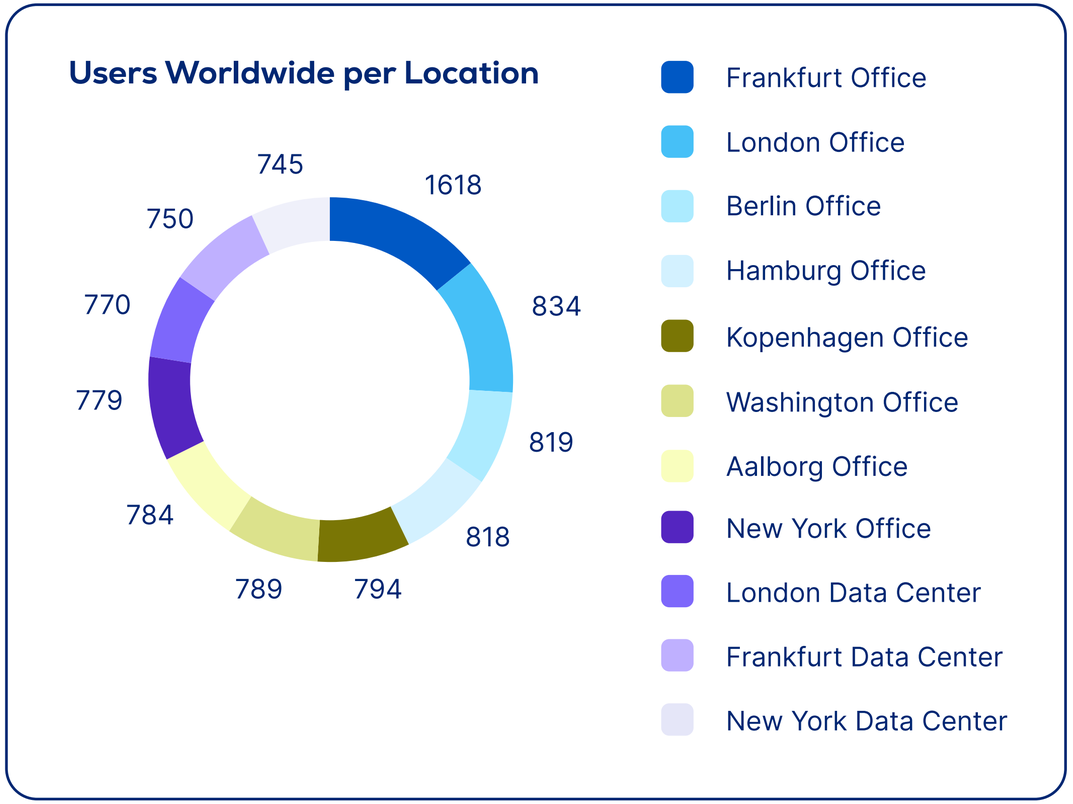
Accurate, up-to-date data is essential before the audit begins. It's usually collected through automated tools or third-party integrations.

Make sure you have a clear view of where users and devices are and which organizational units they belong to.

This helps you quickly confirm whether users or devices fall within the audit scope and identify local stakeholders if needed.

It also strengthens your position when negotiating scope based on regional or organizational structure. Pro tip: Focus the audit on areas you can control.

Typically, the audit scope can be geographic, organizational or limited by product families.



Step 4: Audit Target Selection

What Happens?

The auditors will start the audit by gathering information after the kick-off meeting. The most common types of information gathering include:

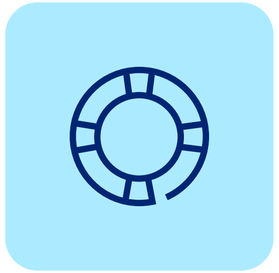
Interviews
Auditors talk to your staff and collect information verbally or through on-screen observations.

Self-declaration
You will be provided with a guided template to populate software usage information.

Request existing records
These can be any records that you already own from CMDB reports to HR records.

In-App reports
The auditors may ask you to generate built-in reports in some applications, such as user or connection reports.

Execute scripts/tools
The auditors may ask you to run software they provide to scan your machines.



How to Survive

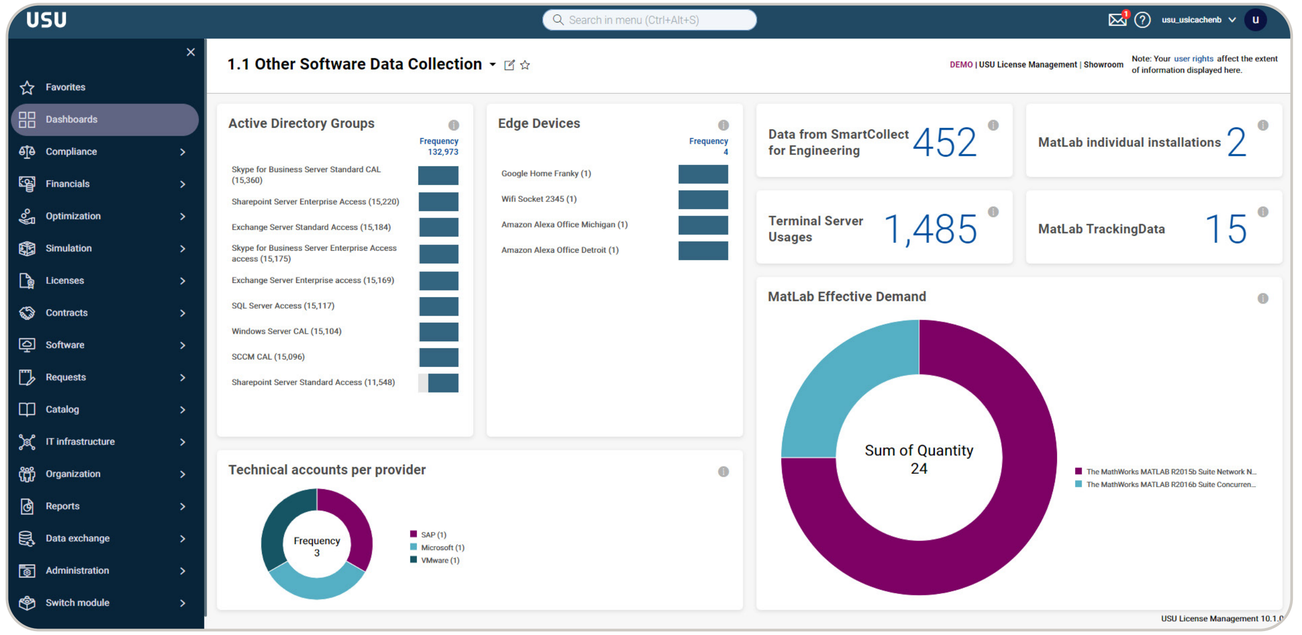
Stay in control of data collection: Only share what's relevant and requested. Here's how to manage the process effectively:

- → **Assign a project manager** who understands the audit scope. Don't leave it to IT alone.
- → **Always ask why data is needed** or why a script is being run. Know the purpose behind each request.
- → **Double-check before you declare anything.** If you're unsure, take the time to verify rather than risk triggering more scrutiny later.

Good Data Leads to Better Audit Outcomes

Audit results depend on both the quality and completeness of your data. Start by identifying all relevant data sources, and make sure your team knows exactly what to share—and what not to. **Sharing extra or off-scope data can backfire and benefit the auditor.**

Track expected data, like the number of devices from your main inventory tool, to spot gaps or anomalies. If something looks off, check it with the responsible colleague right away. **Missing key data sources means missing key proof.**

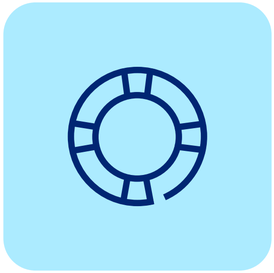


Step 5: Accuracy Check

What Happens?

Review the draft compliance report carefully: Once data collection is done, auditors will create a Draft License Compliance Report with Effective License Positions (ELPs) for each software title you use.

Some may send it to the vendor right away, but most will first ask you to review it and confirm the facts before sharing it further.



How to Survive

Double-check before you accept the report!
This is your last chance to correct mistakes—like outdated user info or old servers. Once you accept the report, it's hard to walk anything back.

- → Review the full report, not just the ELP summary. Focus on any under-licensed (red) titles.
- → Ask for clarification if anything's unclear—it's the auditor's job to explain.
- → Involve the person who provided the raw data to ensure nothing was misread.
- → Replace any assumptions made due to missing data. If you can, fill the gaps with accurate info.
- → Ask for a realistic timeline—especially if you're short on resources or in the middle of a migration. You're not contractually bound to a fixed deadline.

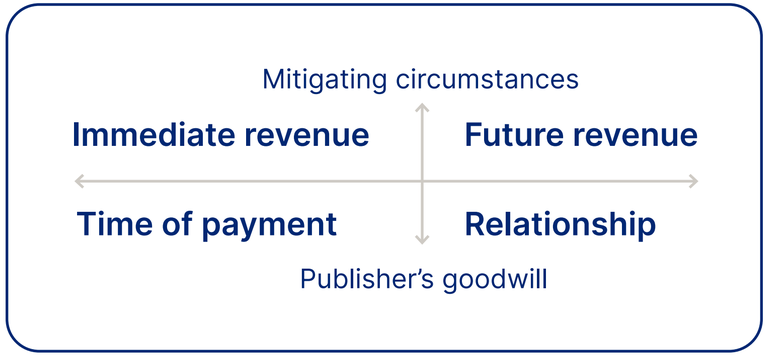
Stage 6: Settlement Discussion

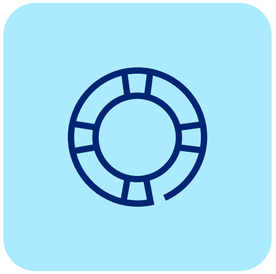
What Happens?

Non-compliance comes with a cost: Any red or negative lines in the compliance report mean you owe the vendor money.

Depending on the vendor and severity, you may need to **buy licenses at full list price,** pay back-maintenance and even cover audit costs—often within four weeks.

These **unplanned expenses can strain your OPEX** budget, and asking your CFO for extra cash isn't a conversation anyone enjoys.





How to Survive

Going solo? Know the basics first: If you're handling the audit on your own, keep these points in mind:

- → **Mitigating circumstances** – Clear, verifiable reasons for accidental misuse may reduce your liability.
- → **Vendor goodwill** – Stay cooperative. Working with the vendor often leads to more flexibility than pushing back hard.
- → **Negotiation levers** – Vendors want quick wins: fast payments, future revenue, minimal conflict. Know what you can offer and plan your approach wisely.

Microsoft, SAP + Co: How to Manage Audits of Big Vendors

Most of the big software vendors run compliance programs that include audits. For you, this always carries some risk—whether from **accidental installations or unclear license terms.** The risk depends on your level of investment in a vendor. For instance, if you rely heavily on SAP ERP, your compliance exposure is high, while minimal IBM use means little risk.

Big software vendors such as **Microsoft, IBM, SAP and Oracle** are often your largest exposure. Their audits vary, but if you're a large or fast-growing business, chances are you rely on at least one of them. With investments that can reach tens or even hundreds of millions, combined with complex license rules, these vendors demand close attention. As a SAM or License Manager, make them a top priority.

What Connects Big Vendors

- High complexity in contract and license models
- High difficulty in discovering, measuring and interpreting license usage
- Mature audit practice often performed by Big 4 auditor firms
- Most vendors prefer remote or automated data collection

Software audits can be highly intrusive, often requiring deep data collection and technical checks. The financial impact can be severe—many audits result in exposure worth 2–3 times annual spend. Larger cases with partitioning, indirect access or misconfigured metrics can indeed reach 5–10 times spend.

Let's investigate the big vendor specifics and how you can prepare yourself for the next audit.

Audit Approach

- Official compliance audits are conducted by Big Four firms (KPMG, Deloitte, PWC, EY) and initiated by a Microsoft entity. For example, in EMEA, they can only be launched through Microsoft Operations Limited in Ireland.
- ITAM reviews are “unofficial audits” carried out by Microsoft ITAM partners and started by local Microsoft teams. They’re officially voluntary, less intrusive and more cooperative—but usually lower in quality.
- The approach can range from a simple remote review (Verified Self-Audit) to a detailed onsite engagement.

License Measurement Tools

- Microsoft audits typically use in-house SAM tools, often supported with extra scripts.
- Movere, once a common in-house tool, was retired on March 1, 2024. You should now use Azure Migrate to discover and assess on-premises workloads.



Key Microsoft Licensing Traps to Avoid

- SQL Server often carries the **biggest compliance risks.** Make sure you have enough core licenses and active Software Assurance in virtual environments to enable License Mobility.
- Enterprise Agreements (EA) for desktop and server software could cause issues if you miscounted or overlooked subsidiaries that should have been included. While EA is still relevant, Microsoft increasingly promotes **Microsoft Customer Agreement** (MCA) and **Microsoft Product & Services Agreement** (MPSA), which bring similar risks if not carefully managed.

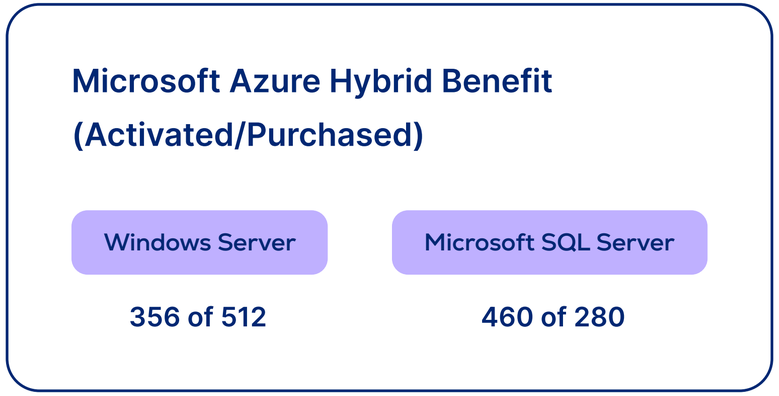
Tough on Gaps—but Open to Deals

- If compliance gaps are found, Microsoft typically seeks to recover license costs at recommended retail price and audit expenses (if noncompliance exceeds five percent). Additional penalties are rare.
- Microsoft values long-term relationships and is usually open to negotiation. In many cases, you can redirect compliance costs toward new solutions instead of paying penalties.

How to Prepare Microsoft Audits

Before your next “friendly” Microsoft audit, review areas where you can optimize. Start by checking Microsoft 365 subscriptions to make sure they’re assigned effectively. Explore licensing conditions that provide added benefits, such as unlimited virtualization rights with Windows Server Data-center and SQL Server Enterprise (when licensed according to the current Microsoft Product Terms).

Other areas worth checking include Visual Studio subscriptions with MSDN licensing and remote access via Remote Desktop Services (RDS).



Cost Optimization in the Cloud

- **Azure Hybrid Benefit.** Microsoft promotes a “bring your own license” option for Windows Server and SQL Server in the Azure cloud. This lets you **apply your on-premises licenses to reduce cloud costs.** It also applies to Red Hat Enterprise Linux (RHEL) and SUSE Linux Enterprise Server (SLES) subscriptions. Be careful, though—if you over-allocate licenses under this benefit, you risk noncompliance.
- **Microsoft 365.** Many organizations run hybrid M365 environments, where not all services are online but everything is covered by a subscription. An ITAM solution like USU IT Asset Management helps you track online subscriptions and combine them with on-premises usage. This gives you accurate reporting and **multiple ways to save money** before and during an audit.

Understand SAP's Audit Types

Most audits are run by SAP's Global License Audit and Compliance team—either locally or offshore. Enhanced audits may also involve third-party firms, like the Big Four.

- **Basic audits** are annual, based on SAP's standard process. They rely on automated reports and self-declarations, usually focused on a few products to support steady sales. These audits typically cover on-premises software.
- **Enhanced audits** go deeper and may include onsite checks. These cover more products and can include topics like indirect access.
- **SAP Private Cloud Metering** is a newer approach and relevant for all Private Cloud (RISE) clients. Clients are facing **automated monthly license measurement based on authorizations.**

SAP's Evolving Model: Higher Risk, Higher Costs

- You must always **stay compliant with FUEs**—temporary usage spikes can still trigger license costs.
- Indirect access through third-party apps requires full licenses and has led to multi-million-dollar lawsuits.
- **License costs are rising.** Early reviews show the new Private Cloud Metering model often results in higher license requirements.

License Measurement Tools

- **SAM4U:** Delivers a clear, consolidated view of SAP systems, users and engine usage. It supports SAP license measurement **(USMM/LAW)** and prepares audit-ready reports. As part of SAP's official toolchain, it feeds directly into SAP's compliance checks—without any customer-side simulation or optimization.
- **SAP Passport/SAP Digital Access** tracks indirect access through document counts (digital access). This is required for accurate **Full Use Equivalent (FUE)** calculations.

Rethink SAP Licensing: Track, Optimize, Repeat

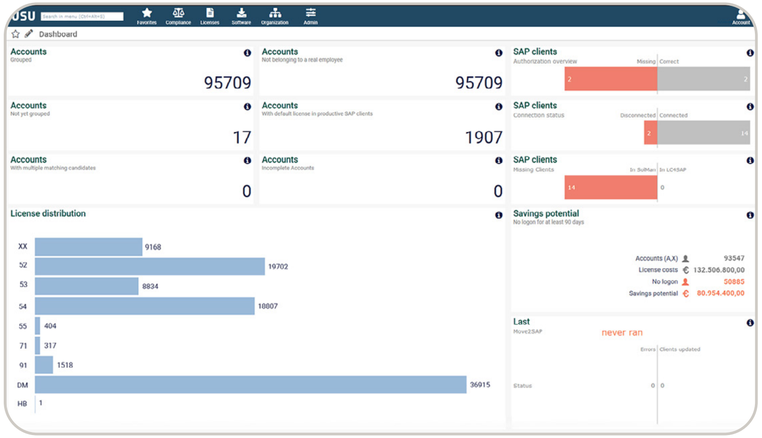
- **Usage-based licensing is outdated—** optimization now depends on user authorizations.
- You'll need to monitor Full Use Equivalent (FUE) consumption trends, not rely on yearly snapshots.
- With Private Cloud Metering, continuous license tracking through dedicated tools is essential—one-off consulting won't be enough.

How to Get SAP Audit-Ready

Staying ahead of your annual SAP audit (LAW) is more important than ever. With rising license costs and stricter audit practices, being unprepared can lead to unexpected expenses.The good news? With the right tools and strategy, you can turn this challenge into an opportunity to save.

- **Use a dedicated SAP license management tool** – A modern solution like USU SAM for SAP® Software gives you full transparency across your SAP environment. It tracks real usage, identifies inactive users and automatically assigns the most cost-effective license types.
- **Rely on smart automation** – Make sure your ITAM tool supports STAR rules and Full Use Equivalent (FUE) metrics. These rules help automatically determine the correct license class based on actual usage and authorizations—ensuring compliance without over-licensing.
- **Review and clean your data regularly** – Keep your user data accurate and up to date. Regular cleanup helps avoid false positives in audits and ensures inactive or duplicate users don't inflate your license needs.
- **Monitor indirect access** – Tools like SAP Passport and SAP Digital Access are essential to track document-based usage, which affects FUE calculations and can easily go unnoticed without proper monitoring.
- **Don't wait for the audit** – Run internal checks regularly and simulate license positions before the official audit begins. Being proactive gives you time to adjust—and negotiate—before SAP steps in.

With the right mix of technology and expertise, you can stay compliant, avoid surprises and reduce unnecessary spend.



What to Expect from an IBM Audit

Auditors – Global audits are usually handled by Deloitte or KPMG. Audit approach: expect a hands-on process with scripts, as most IBM license models are complex and lack automated reporting (except PVU).

Regional differences – Audit quality is highest in Europe and the US. If data is incomplete, auditors often apply “worst case” assumptions.

Enterprise agreements – Audits often happen before renewals to push larger, multi-year deals. Exposure is sometimes converted into prepaid credits (CBA or substitution clause).

License Measurement Tools

IBM License Metric Tool (ILMT) – ILMT is mandatory for sub-capacity licensing. Poor setup or maintenance can result in full-capacity penalties.

Tool integration – Most SAM tools connect with ILMT, but quality varies. Flexera may replace ILMT, but only with IBM’s prior approval.

Watch for High-Risk IBM Compliance Traps

- Sub-capacity licensing is the most common and costly non-compliance issue—accounting for over 80% of exposure in our experience.
- Non-PVU metrics (like user, connection or terabyte-based licensing) are often overused, since most SAM tools don’t track them automatically.

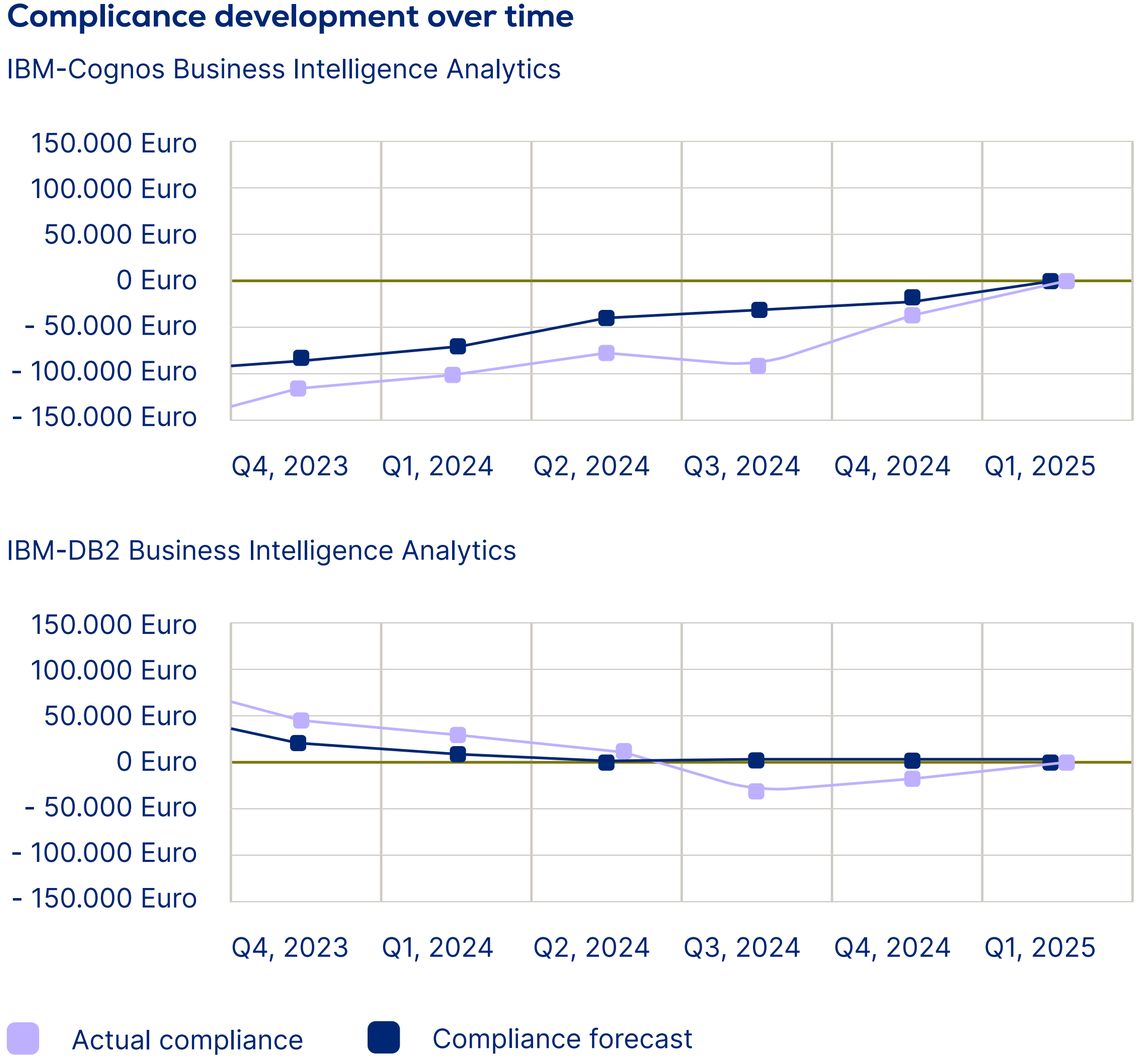
IBM Focuses on Revenue, Not Penalties

- IBM’s goal is to sell new licenses, not penalize accidental deployments. This approach is known as a “value settlement” (though they will accept cash if pushed).
- Expect deeper discounts near quarter- or year-end, especially for multi-year deals, Cloud Paks or dual entitlements.
- So far, there’s no known legal precedent from IBM audit disputes.

Preparing for IBM License Audits

IBM audits are becoming more frequent—and they often check your compliance status for the past 90 days, not just your current setup. That's why your SAM system should track compliance over time, not just provide one-off snapshots.

- **Track compliance over time:** IBM looks back up to 90 days, so one-off snapshots aren't enough.
- **Get entitlements in order:** Keep contracts, enterprise agreements and license records organized and accessible.
- **Use ILMT correctly:** For sub-capacity licensing, ILMT is mandatory. Misconfigurations can trigger full-capacity penalties.
- **Monitor all license metrics:** PVU, user, connection and terabyte-based models all matter. Most SAM tools don't track them automatically.
- **Watch Cloud Paks and assumptions:** Cloud Pak entitlements add complexity. Auditors often apply "worst case" assumptions if your data is incomplete.



How Oracle Approaches License Audits

- Oracle audits are usually led by its **Global License Advisory Services (GLAS)** team, which now includes both the traditional License Management Services (LMS) auditors and the newer Software Investment Advisory (SIA) team.
- Smaller audits may be handled by **Oracle LMS Partners**—third-party firms that often work on referral fees or margins, so they aren't truly independent.
- **Triggers for audits** typically include ending support contracts, suspected non-compliance or expiring enterprise agreements such as Unlimited License Agreements (ULAs).

License Measurement Tools

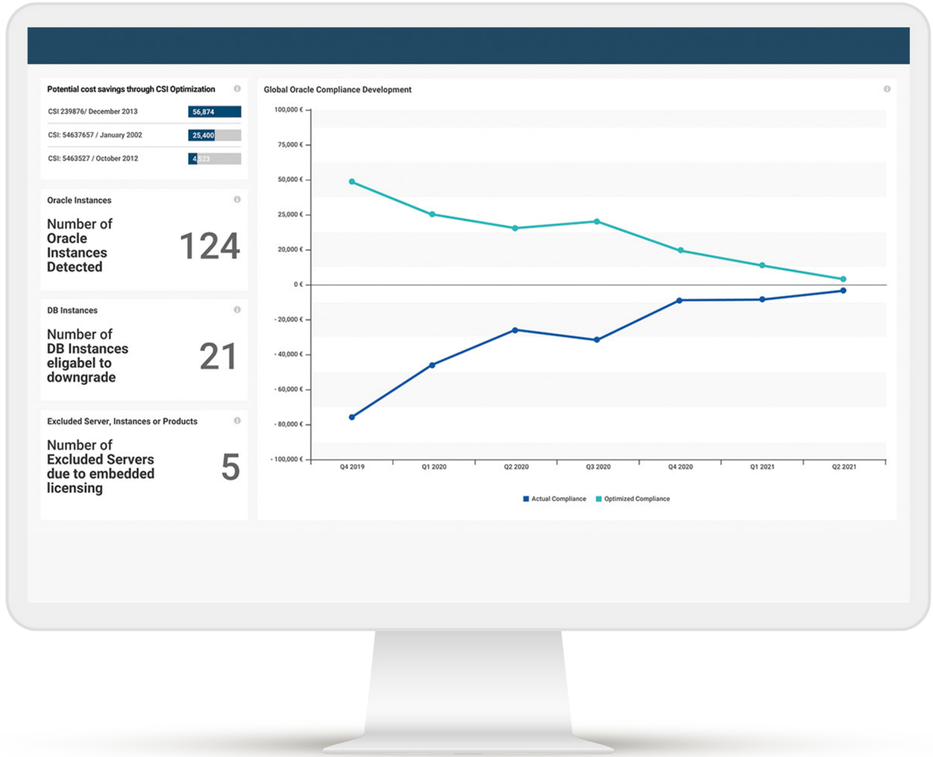
- Data on Oracle Databases and Middleware is usually gathered with the **Oracle Server Worksheet (OSW)** and Oracle's **LMS Collection Tool.**
- While less common in the past, Oracle is now pushing **scanning tools** more often to capture the full IT environment—including **Java deployments.**

Avoid Oracle's Top Audit Traps

- **Soft vs. hard partitioning:** With VMware and similar setups, Oracle often requires processor licenses for the full host or cluster—not just the VM.
- **Options and packs:** Installed packs can trigger license costs even if they're never used. Always check what's deployed.
- **Java licensing:** Oracle now audits Java. Free use is limited—production or commercial features may need a license.
- **Test and dev environments:** Non-production systems may still require licenses unless your contracts clearly cover them.
- **Policy vs. Contract:** Oracle auditors rely on policies that go beyond contract terms. Stick to your signed agreements.

How to Master Oracle Settlement

- **Expect list prices and back maintenance:** Oracle typically calculates at RRP and may add backdated support, with partitioning issues multiplying costs.
- **Negotiate for a balanced outcome:** Oracle values long-term relationships and often agrees to middle-ground deals, new licenses or tailored terms.
- **Convert exposure into new deals:** Findings are frequently turned into commitments for future revenue, like cloud contracts or bundles, instead of penalties.



Be Audit-Ready: 4 Essentials for Oracle Compliance

- **Know your entitlements** – Keep contracts, ULAs and support agreements organized and easy to access.
- **Use an Oracle-verified SAM tool** – Ensure it exports in **LAW format** and documents **exclusions** to avoid inflated compliance counts.
- **Monitor deployments continuously** – Track virtualization, cloud usage and options/packs that may activate without notice.
- **Simulate audits in advance** – Run internal checks to catch gaps before Oracle does.

Conclusion: Beat the Audit Today, Prevent the Audit Tomorrow

Showing that you're in control of software license compliance sends a clear signal to vendors. It means you can respond quickly and professionally, back your case with reliable data and negotiate from a position of strength—because you know your estate better than they do.

A professional ITAM tool makes this possible. With **USU IT Asset Management,** you gain accurate visibility across deployments, configurations, licenses and usage—powered by our comprehensive SKU catalog. That means fewer compliance risks, faster responses and the ability to uncover real cost savings.

Even if you're already under audit, a 100% web-based SAM tool can start delivering insights right away. It's your ace up the sleeve—helping you handle audits with confidence while lowering the risk of being targeted again.

With the right strategy and the right SAM tool, you don't just survive audits—you turn them into opportunities.

Get in Touch

Do you need further information, a live demo or do you have any questions? The best way to get answers to your questions is by giving us a call. Schedule a meeting now.

About USU

With a 20-years track record of excellence, USU emerges as the go-to partner for leading organizations such as Bayer, General Electric, T-Mobile, JP Morgan Chase and BMW.

Whether analyzing software usage and simulating licensing needs on-prem or in the cloud, our comprehensive suite of tools and services empowers businesses to navigate the intricacies of software asset management, while ensuring compliance, cost transparency and saving potential.


USU
Empowered by
understanding
Discover more
on our website:
usu.com
info@usu.com