24 Die Auditrisiken managen

In diesem Kapitel erfahren Sie u. a.,

- welche Faktoren eine unlizenzierte Nutzung von Software beschreiben,
- aus welchen Motiven Hersteller Software-Audits durchführen und in welchem Zusammenhang damit eine Audithäufigkeit steht,
- aus welchen Bestandteilen ein gültiger Lizenznachweis im Allgemeinen besteht,
- welche rechtlichen Aspekte im Umfeld eines Software-Audits auftreten und zu beachten sind,
- wie Auditklauseln der Hersteller zu verstehen bzw. zu interpretieren sind,
- welche Auditauslöser es geben kann und warum Sie sich eine Auditstrategie erarbeiten sollten,
- wie ein grober Software-Audit-Prozessablauf aufgestellt sein sollte,
- welche Verhaltensregeln bei der Durchführung eines Software-Audits beachtet werden sollten,
- über welche Phasen ein Software-Audit abläuft und welche Daten und Informationen dafür vom Auditor benötigt werden,
- wie viel Auditverteidigung möglich ist, weshalb Sie ein Augenmerk auf die Validierung der Auditor-Prüfergebnisse haben sollten und welche „Lessons Learned" nach einem Software-Audit zu beachten sind.

Dieses Kapitel möchte Ihnen einen Überblick über das umfangreiche und komplexe Thema „Software-Audit" geben. Beginnend mit einem kurzen Überblick über die möglichen Formen unlizenzierter Softwarenutzung und was das eigentlich für ein mögliches Software-Audit zu bedeuten hat, geht das Kapitel auch darauf ein, welche rechtlichen Fakten und Aspekte in Deutschland zu beachten sind, welche Auslöser es für ein Software-Audit geben kann, wie die Auditklauseln der Hersteller zu bewerten sind und warum Sie sich eine Auditstrategie erarbeiten sollten. Lesen Sie weitere Informationen über die Phasen eines Software-Audits und welche Informationen die Auditoren für die Durchführung des Software-Audits bereitgestellt haben wollen. Erfahren Sie in einer beispielhaften Beschreibung, wie ein Software-Audit für IBM-Softwareprodukte ablaufen könnte und was für Aufgabenstellungen und Aktivitäten nach dem Abschluss des Software-Audits zu empfehlen sind.

Eine enorme Verschiebung der bisherigen Vorgehensweisen zum Thema Software-Audit prognostiziert Gartner in seiner Studie,[1] und zwar dass bis 2024 40 % der Unternehmen Software Asset Management als primäre Disziplin zur **Reduzierung der Kosten** für SaaS-Verträge mit marktbeherrschenden Anbietern einsetzen werden. Das bedeutet, dass sich die bisherigen „klassischen" Software-Audit-Verfahrensweisen verändern werden, teils weniger werden, weil die Bereitstellung von Softwareprodukten über Abonnement- und Subskription-Lizenzmodelle einen immer größeren Anteil einnehmen wird und damit einhergehend die Steuerung und das Managen von „IaaS"-, „PaaS"- und „SaaS"-Services und deren Verbräuche und Nutzungsbedarfe im Vordergrund stehen werden. Das Szenario zu beherrschen, wird nur noch wenigen SAM-Tool-Herstellern mit ihren Lösungen gelingen und die Konsolidierung im SAM-Tool-Umfeld noch schneller voranschreiten lassen.

Haftungsausschluss

Die in diesem Kapitel beschriebenen Sachverhalte, Anmerkungen und Empfehlungen erheben keinen Anspruch auf Vollständigkeit und bilden keine von mir formulierte Rechtsmeinung ab. Auszüge von Rechtsmeinungen oder Zitate sind immer mit der jeweiligen Quelle gekennzeichnet. Es werden keine Garantien und Haftungen bzgl. der Allgemeingültigkeit und/oder rechtlichen Korrektheit der hier beschriebenen Inhalte übernommen. Dieses Kapitel stellt keine Rechtsberatung dar. Wenn Sie rechtliche Beratung benötigen, wenden Sie sich bitte an eine darauf spezialisierte Rechtsanwaltskanzlei. Die im Kapitel genannten Weblinks aus dem Internet wurden im März 2021 aufgerufen und waren zu diesem Zeitpunkt noch als Quelle verfügbar.

Software-Audit-Fakten

Übertragen in unsere Softwarewelt, versteht man unter einem Audit die Überprüfung der eingesetzten und aktiven lizenzkostenpflichtigen Softwareprodukte auf die Einhaltung der vertraglich erlaubten Nutzungsform und -intensität im Unternehmen.

„Software-Audit" – wird dieser Suchbegriff beispielsweise bei Google eingegeben, werden ca. 363.000.000 Ergebnisse (Stand März 2021) angeboten, obwohl diesen Begriff noch nicht einmal der Duden kennt. Der Duden kennt nur „Audit" mit der Bedeutung „[unverhofft durchgeführte] Überprüfung",[2] was in unserem Fall nicht ganz 1:1 anwendbar ist, denn die „Überprüfung" kommt nicht unverhofft, sondern wird bereits mehrere Wochen vorher angekündigt. Die Anzahl der Suchtreffer täuscht aber nicht darüber hinweg, dass die vielen angebotenen Informationen meist nur oberflächlich und fachlich nicht ausreichend fundiert ausformuliert sind. So ist das auch zu diesem Thema, neben Angeboten von Dienstleistern wird teilweise viel Halbwissen verbreitet bzw. der informationssuchende Leser mit Paragrafen und Rechtsmeinungen malträtiert. In den Suchergebnissen taucht u. a. auch die

[1] Gartner Reprint – *https://www.gartner.com/doc/reprints?id=1-25EJ437D&ct=210308&st=sb*
[2] *https://www.duden.de/rechtschreibung/Audit*

Begriffserläuterung zu „Audit“[3] in Wikipedia auf. Beschrieben wird hier erst einmal nur der allgemeine Charakter eines Audits und in welchen Varianten und Formen Audits im Allgemeinen durchgeführt werden. Erst im Abschnitt „*Informationstechnik*“ findet sich ein kurzer Hinweis auf „*Überprüfung, ob ein Unternehmen für die verwendete Software eine ausreichende Anzahl an Lizenzen besitzt (Lizenzaudit)*“[4] – das sich immer noch im Nebulösen befindliche Themengebiet Lizenz- bzw. Software-Audit.

Eigentlich könnte man annehmen – denn das Thema Softwareasset- und Lizenzmanagement gibt es ja nicht erst seit ein paar Jahren –, der SAM-Prozess für den lizenzkonformen Einsatz von Software sowohl gegenüber den Herstellern als auch gegenüber dem Gesetzgeber (Urheberrecht) müsste doch so ziemlich ausgereift sein. Das Gegenteil ist aber der Fall. Das Thema wird durch die stetig wechselnden bzw. neuen Nutzungsbedingungen der Hersteller, natürlich auch bedingt durch die rasante digitale Transformation, immer komplexer und für die SAM-Verantwortlichen Rollen entsprechend immer schwerer nachzuhalten. Dass Software (auch Open Source) prinzipiell einer Lizenzpflicht unterliegt, findet sicherlich auch Ihre Zustimmung, denn in einem SAM-Betrieb muss jegliche Software betrachtet und verwaltet werden. Die gute Nachricht: Nicht jedes eingesetzte Softwareprodukt ist auf eine Einhaltung der lizenzkonformen Nutzung zu überwachen respektive zu prüfen. Denn in einem Software-Audit interessiert nur der korrekte, den vereinbarten Nutzungsbedingungen entsprechende Einsatz Ihrer **lizenzkostenpflichtigen** Softwareprodukte. Die Unternehmen müssen immer mehr des verfügbaren IT-Budgets in den Kauf von Software und in Wartungsverträge investieren. Es muss ein enormer Aufwand betrieben werden, um die mittlerweile fast vollständig von der IT abhängigen Geschäftsprozesse zu managen. Doch kaum ein Unternehmen hat einen transparenten Überblick über seine eingesetzten Softwareprodukte (Open Source und lizenzkostenpflichtige Software) und die damit verbundenen einzuhaltenden Nutzungsbedingungen. Hinzu kommen die Transformation und Migrationen von „On-Premises“-Lizenzen (auch in Form von BYOL) und deren lizenzkonformer Einsatz. Auch wenn einige Hersteller durch den Wechsel ihrer Lizenzmodelle in Richtung Abonnement und Subskription vorantreiben und sich damit auch die Auditaktivitäten verringern (z. B. bei Adobe und Microsoft), verbleibt noch ein erheblicher Anteil an „On-Premises“-Lizenzen, die zu wiederholten Software-Audits und auch verdachtsunabhängigen Lizenzprüfungen führen.

24.1 Quo vadis Software-Audit

Den Herausforderungen, die für einen anstehenden Audit erforderlichen Nutzungsdaten über die eingesetzten Softwareprodukte und Technologien bereitzustellen, kann ohne ein SAM-Tool im heutigen IT-Betrieb kaum noch ausreichend transparent begegnet werden. Angesichts der sich häufenden Berichte in letzter Zeit, dass die (augenscheinlich) durchgeführten Software-Audits – aufgrund der zunehmenden Cloud-Transformation – abnehmen

[3] Audit – Wikipedia – *https://de.wikipedia.org/wiki/Audit* –
und hier im englischsprachigen *https://en.wikipedia.org/wiki/Software_audit_review*

[4] Lizenzaudit – Wikipedia – *https://de.wikipedia.org/wiki/Lizenzaudit*

(siehe auch Tabelle 24.1 „Aufstellung (Rangliste) Hersteller über ihre Software-Audit-Aktivitäten"), könnte behauptet werden, dass deshalb Software-Audits nicht mehr wichtig sind. Quo vadis[5] Software-Audit?

Leider ist das Gegenteil der Fall und Audits bleiben deshalb auch weiterhin noch im Fokus aller und auch sehr zeitaufwändig weil:

a) *Die Audithäufigkeit hat sich eigentlich nicht verringert, sondern das Motiv hat sich „verlagert".* Auch wenn die „On-Premises"-Lizenzmodelle von den Herstellern immer mehr in Richtung Abonnement und Subskription transformiert werden und von Kunden darauf gehofft wird, dass das „Messen", „Wiegen", „Zählen" weniger werden würde, wollen Hersteller die für sie so einfachen Einnahmequellen nicht so ohne weiteres aufgeben.

- *Die IT-Infrastrukturen sind beständig im Wandel und in der Optimierung.* Hybrid-Cloud, Azure Hybrid Benefit, Multi-Cloud – die IT-Infrastrukturen entwickeln sich rasant weiter, die Hersteller kommen hier oftmals selbst nicht schnell genug hinterher (siehe Gartner Blog-Eintrag[6]), wenn neue Nutzungsbedingungen überhastet publiziert werden. So können u. U. bereits nach kurzer Zeit bestehende Compliance-Regeln wieder obsolet sein und erhöhen damit die Komplexitäten für beide Seiten.

Könnten Sie diese Fragen ohne größeres Nachdenken mit „Ja" beantworten?

- Ist unser Unternehmen im Fall einer Auditankündigung gut vorbereitet oder müssten noch in einem „Fire Fighter"-Einsatz weitere Softwarelizenzen beschafft werden, um lizenzkonform zu werden?
- Können wir unseren laufenden IT-Betrieb aufrechterhalten, obwohl parallel ein Software-Audit erfolgt und dadurch unsere Ressourcen über mehrere Wochen gebunden werden?

Eine von Snow Software und IDG[7] durchgeführte Studie im Jahr 2019 ergab, dass 73 % der befragten Organisationen im vergangenen Jahr von mindestens einem Anbieter geprüft wurden. Von den befragten Organisationen gaben 42 % der IT-Verantwortlichen an, dass die Verlagerung der IT-Ausgaben in die Geschäftsbereiche dazu geführt habe, dass die Prüfungsvorbereitungen zeitaufwändiger und komplexer waren. Die Software-Audits werden tatsächlich immer mehr, obwohl manch einer wohl dachte, dass es mit den Cloud-Themen (Software-as-a-Service, SaaS) und den damit einhergehenden Abonnement-Abrechnungsmodellen für die Hersteller einfacher wäre, ihre Kunden lizenzkonform zu „zählen". Deshalb werden uns die Software-Audits der Hersteller noch eine ganze Weile erhalten bleiben, aber mit anderen Schwerpunkten, wie bereits schon angesprochen. Umso wichtiger ist es deshalb, mit geeigneten SAM-Tools Transparenz und Sichtbarkeit über seine IT-Assets zu erlangen und sich darauf zu fokussieren, diese zu optimieren und lizenzkonform zu betreiben. Aus Studien (u. a. von Gartner) der letzten Jahre geht hervor, dass viele Hersteller, die bisher konsistent auch die meisten Audits durchgeführt hatten, diese auch weiterhin durchführen werden, allerdings mit schnell wechselnden Ranglistenplätzen aufgrund der Transformationsphase von „On-Premises" in die Cloud (Hybrid) und den Umsatzverschiebungen zu den Cloud-Lizenzen (siehe dazu auch die Tabelle 24.1).

---

5 *https://de.wikipedia.org/wiki/Quo_vadis%3F*

6 *https://blogs.gartner.com/stephen-white/2020/06/11/has-microsoft-taken-steps-which-limit-supply-to-the-european-2nd-user-licensing-market*

7 *https://go.snowsoftware.com/IDGcampaign-Whitepaper-English*

Seit dem 9. Juni 1993 müssen die Paragrafen des Urheberrechtsgesetzes (UrhG) auch auf Software und deren Nutzungsrechte angewendet werden. Die Aufnahme von Software in das UrhG soll vor allem den Urheber und sein Werk vor unerlaubter Vervielfältigung schützen und ist beispielsweise im Paragraf 69c UrhG beschrieben. Um eine unerlaubte Vervielfältigung oder rechtswidrige Nutzung nachzuweisen, muss erst einmal beschrieben werden, was eine rechtswidrige Nutzung ausmacht. Im Zuge dessen passiert es sehr oft, dass unbeabsichtigt eine „unlizenzierte Softwarenutzung“ erfolgt.

24.1.1 Was bedeutet unlizenzierte Nutzung?

Eine Vielzahl von Softwareprodukten, die für einen IT-Betrieb erforderlich sind, bringen entsprechend diverse Lizenzmodelle und -metriken mit sich. Je komplexer der Hersteller seine Nutzungsbedingungen „definiert“, umso häufiger werden von den Herstellern Software-Audits initiiert, um die Einhaltung der Lizenzkonformität zu überprüfen, und umso häufiger taucht dabei immer irgendeine der hier beschriebenen Formen von „unlizenzierter Softwarenutzung“ auf.

Formen von unlizenzierter Nutzung sind:

- **Un**-*lizenzierte Software.* Es wird Software verwendet und eingesetzt, für die überhaupt keine rechtmäßige Lizenz erworben wurde.
- **Unter**-*lizenzierte Software.* Eine wiederholte Installation von Software, die den vereinbarten Nutzungsumfang überschreitet (z. B. automatisierte Softwareverteilung ohne Prüfung auf ausreichend vorhandene kaufmännische Nutzungsrechte), erzeugt eine Unterlizenzierung und stellt somit eine rechtswidrige Nutzung des Softwareprodukts dar.
- **Falsch** *lizenzierte Software.* Die Software wird für Zwecke eingesetzt, die nicht von den im Vertrag festgelegten Nutzungsvereinbarungen abgedeckt sind (z. B. der Einsatz von Software mit temporären Lizenzkeys oder Testlizenzen in einer produktiven Umgebung). Um eine rechtswidrige Nutzung handelt es sich auch, wenn eine Software in einem IT-Architektur-Szenario falsch eingesetzt wird oder Funktionen genutzt werden, die nicht lizenziert wurden. Das ist sehr oft beim Einsatz von Oracle-Datenbanken der Fall (falsche Edition oder es werden Funktionen bei der Installation zusätzlich mit ausgewählt, die dann eine Lizenzpflicht auslösen) oder z. B. wenn Server-Betriebssysteme in Verbindung mit einer Virtualisierungsumgebung falsch eingesetzt werden
- *Mehrfachkopien.* Es werden mehr Kopien von Originalmedien erstellt als erlaubt und mehrfach auf unterschiedlichen PCs installiert oder ein einzelner Lizenzkey wird für mehrere Installationen verwendet (siehe auch Unterlizenzierung).
- *Raubkopien und Fälschungen.* Komplette Softwarepakete werden gefälscht und als Originalsoftware verkauft. Wer ein solches Produkt installiert, nutzt die Software rechtswidrig.

In vielen Fällen ist es für den Laien nur sehr schwer erkennbar, ob er es mit einer Fälschung zu tun hat. Microsoft bietet hierfür auf mehreren Webseiten Informationen an:

http://www.microsoft.com/de-de/howtotell/default.aspx

Bericht bzw. Meldung von nicht lizenzierter Software:

https://www.microsoft.com/de-de/howtotell/cfr/report.aspx

Dazu auch die Webseite mit FAQs:

https://www.microsoft.com/DE-DE/howtotell/cfr/FAQ.aspx

Und eine Webseite mit weiteren Hinweisen zum Kauf von Original-Software:

https://www.microsoft.com/mea/genuine/how-to-tell.aspx

Außerdem stellt Microsoft auch eine Webseite „Microsoft Produktidentifikationsservice" (kurz: „PID-Service") zur Überprüfung von Produktmerkmalen zur Verfügung:

https://www.microsoft.com/de-de/rechtliche-hinweise/pidservice.aspx

Für Adobe-Produkte können Sie diesen Weblink verwenden:

http://www.adobe.com/de/aboutadobe/antipiracy/auctioncaution.html

- *Internetpiraterie.* Im Internet werden immer häufiger Downloads von illegaler Software angeboten, manchmal auch ganze Webportale von Herstellern gefälscht. Auch stehen oft illegale Kopien über Auktionshäuser oder Hackerforen zum Verkauf. Eine weitere Methode besteht darin, günstige Software über Spam-E-Mails zu offerieren.
- *Hard-Disk loading.* Viele Fachhändler, die Hardware verkaufen, installieren teilweise Software auf den PCs vor und liefern u. U. dem Käufer dazu die erforderlichen rechtmäßigen Lizenzmedien nicht mit aus.
- *Produktmanipulationen.* Werden einzelne Bestandteile von Originalsoftware verkauft, spricht man von Produktmanipulationen, da die Käufer kein vollständiges Produkt erhalten. Um Manipulation handelt es sich auch, wenn Bestandteile der Originalsoftware mit gefälschten Komponenten ergänzt und als komplettes Originalprodukt angeboten werden.

  Eine weitere, nicht gleich erkennbare Version der Produktmanipulation ist der Vertrieb von Upgrade-Boxen als Vollversionen. Hier sagen die Nutzungsbedingungen ganz klar, dass für die korrekte Nutzung eines Upgrades eine vorhergehende Vollversion als Basislizenz vorhanden sein muss. Zudem muss diese auch in derselben Sprache verfasst sein (eine Basislizenz in Englisch und ein Upgrade in deutscher Sprache wären z. B. nicht zulässig, da es sich dabei um keine „Multilanguage-Version" handelt, sondern um zwei eigenständige, lokalisierte Sprachversionen).

  Adobe weist zurzeit beispielsweise verstärkt auf sogenannte „Vollversions-Bundle" hin:

  Ein solches Bundle besteht dann nicht aus zwei generischen, zusammengehörigen Lizenzen, sondern lediglich aus einem neueren, meist originalen Upgrade und – als vermeintliche Basislizenz – entweder aus

  - einer Raubkopie der Programme „Adobe Photoshop 6.0 OEM" oder „Adobe Photoshop 7.0",

- einer bloßen Registrierkarte mit aufgeklebter (gefälschter) Seriennummer ohne weitere Bestandteile wie Datenträger, Handbuch und/oder Umverpackung,
- einem bloßen Endbenutzer-Lizenzvertrag mit aufgeklebter (gefälschter) Seriennummer ohne weitere Bestandteile wie Datenträger, Handbuch und/oder Umverpackung oder
- einer bloßen, auf dem Upgrade-Produkt zusätzlich aufgeklebten (gefälschten) Seriennummer.

Letztgenannte Fälschungsart kommt derzeit insbesondere bei dem Produkt „Adobe Photoshop“ oder dem Produktpaket „Adobe Creative Suite“ vor. Ein solches Bundle verschafft dem Käufer indessen nicht die zur Installation und Nutzung des Upgrades erforderlichen Lizenzrechte.[8]

- *Vertriebskanalmissbrauch.* Nicht selten werden Vollversionen von originalen Softwareprodukten, die nur für eine besondere Lizenzform Gültigkeit besitzen, als „normale Vollversionen“ weiterverkauft, z. B. Softwareprodukte, die die Kennzeichnung „Not-for-Resale (NFR)“ haben, oder Produkte und Lizenzen, die ausdrücklich nur für Forschung und Lehre eingesetzt werden dürfen (Campus-Lizenzen).
- *Verkauf gebrauchter Software.* Wenn Sie gebrauchte Software erworben haben und einsetzen, kann das ebenfalls zu rechtswidriger Nutzung führen, z. B. wenn zwar ein Vertrag mit einem Lizenzgeber über eine ausreichende Anzahl von Lizenzen abgeschlossen wurde, aber der Lizenzgeber zur Lizenzerteilung gar nicht berechtigt war. Das passiert oft im Gebrauchtmarkt von Software, wenn beim Kauf/Verkauf nicht auf die Nutzungsbedingungen des Herstellers geachtet wird (z. B. bei Veräußerungen von Volumenlizenzen).

  Was sagt Microsoft offiziell dazu? *https://apogiz.com/wp-content/uploads/Microsoft_Vorgaben_Handel_mit_gebrauchter_Software_2018.pdf*

Fehllizenzierungen sind häufige Lizenzierungsfehler[9]

- **Fehllizenzierung***: Verwechseln eines Upgrades mit einer Volllizenz.* Volumenlizenzverträge decken ausschließlich Windows-Software-Upgrades ab. Ein PC muss über eine vorinstallierte vollständige Basislizenz verfügen, um sich dafür zu qualifizieren.
- **Fehlversion:** *Verwenden eines Volumenlizenz-Upgrades auf Consumer-PCs.* Consumer-PCs sind für Volume-Lizenzierungs-Upgrades für Windows Professional nicht qualifiziert.
- **Verwenden von gefälschter Software:** Stellen Sie sicher, dass Sie ein Gerät mit echter installierter Software kaufen. Dies kann durch 1) vorinstalliert durch den OEM (Original Equipment Manufacturer) im Werk oder 2) durch den System Builder bzw. Reseller erfüllt werden.
  Alle Windows-PCs müssen über eine Lizenz verfügen, sodass Sie Ihre Version über die Volumenlizenzierung aktualisieren können.
  Weitere Informationen zur Windows-10-Volumenlizenzierung finden Sie unter *https://www.microsoft.com/en-us/licensing/product-licensing/windows10*

[8] Quelle: *http://www.adobe.com/de/aboutadobe/antipiracy/auctioncaution.html*
[9] Microsoft | Buy Genuine – How To Tell – *https://www.microsoft.com/mea/genuine/how-to-tell.aspx*

Abgesehen davon, dass alle „größeren“ Hersteller ein berechtigtes Interesse daran haben, dass ihre Softwareprodukte lizenzkonform betrieben werden, gibt es doch immer wieder eine kleine „Rangfolge“ derer, die oft und umfassend auditieren über verifizierte Auditoren, wie beispielsweise die großen Wirtschaftsprüfungsgesellschaften. Manche Hersteller haben aber auch eigene Abteilungsbereiche, die sich wie beispielsweise die von Oracle gegründete „Software Investment Advisory (SIA)“[10] eher als „Supporter“ verstehen wollen, aber hier ist es im Endeffekt auch nur alter Wein in neuen Schläuchen, weil es defacto eine Ausgliederung aus der Audit Division „License Management Services (LMS) ist“.[11]

Was aber könnte die Hersteller noch dazu bewegen, ihre Software-Audits beizubehalten?

24.1.2 Auditmotive

Es besteht durchaus die Möglichkeit, dass Unternehmen in naher Zukunft, trotz aller Cloud-Abonnement-Thematik eine Ankündigung zu einem Software-Audit erhalten werden. Durch die massive Nutzung von mobilen Geräten im gesamten Unternehmen wurde die Art und Weise, wie im Unternehmen Informationstechnologie konsumiert wird, grundlegend verändert. Hinzukommen häufig wechselnde Nutzungsbedingungen in Bezug auf Virtualisierung und Cloud mit entsprechend erhöhten Komplexitäten. Das kann ohne optimale SAM-Prozesse und SAM-Tools kaum noch permanent lizenzkonform nachgeführt werden. Dadurch werden (unbewusst und ohne Vorsatz) viele Unternehmen bei der Einhaltung der Lizenzvereinbarungen unbeabsichtigt Schwierigkeiten haben. Wachstumsbedingt und beschleunigt durch die Pandemie mit dem Ruf nach schneller Transformation und Digitalisierung in allen Bereichen ist es schwieriger geworden, die Nutzung der Softwarelizenzen ausreichend zu verfolgen und zu überwachen. Hinzukommen, als ein weiterer Faktor für die Audittätigkeiten, die Migrationen von „On-Premises“-Lizenzen in die Cloud. In der Übergangs- und Umstellungsphase – weg von „On-Premises“ hin zu jährlichen Abonnementgebühren – wird es in der Regel zu Einnahmeverlusten bei den Herstellern kommen. Audits sind daher eine willkommene Einnahmequelle, damit diese Lücke möglichst klein bleibt. Denn nach wie vor stehen die Geschäftsinteressen der Hersteller im Vordergrund und eher nicht die Sorge um eine lizenzkonforme Einhaltung ihrer Verträge. Es sollte also immer ein Schwerpunkt Ihrer IT- und Software-Asset-Management-Strategie sein und auch bleiben, sich durch ausreichend Transparenz den Software-Audits gegenüber **rechtzeitig** gut aufzustellen und somit möglichst wenig Risiken steuern zu müssen.

Der häufigste Grund für die Ankündigung und Durchführung eines Software-Audits durch Hersteller oder von ihnen beauftragte Dritte sind Veränderungen im kaufmännischen bzw. vertraglichen Umfeld (Verringerung von aktiven Wartungsbeständen, Mindermeldung von Softwarelizenzen wie beispielsweise bei einer True-Up-Meldung, Bekanntgabe von Bilanzen mit Meldungen zu Steigerungen und Ausbau von IT-Strukturen etc.).

[10] *https://www.oracle.com/corporate/software-investment-advisory/*
[11] *https://www.oracle.com/corporate/license-management-services/*

24.2 Audithäufigkeit

Dass die großen und wichtigen Softwarehersteller ihre Marktstellung ausnutzen und es dem SAM-Betriebs- und Lizenzmanagement-Teams nicht gerade einfach machen, die komplexen „rein kaufmännischen" Lizenzmodelle zu verstehen und lizenzkonform umzusetzen, ist leider tägliches Brot. Auch sind die Hersteller nur mäßig daran interessiert, die Komplexität herauszunehmen (das gilt auch für die Cloud-Abrechnungsmodelle) und selbst ein Stück weit für Transparenz zu sorgen. Hier hilft es leider nur, sich ständig mit der Materie auseinanderzusetzen, bei komplizierten Fragestellungen entsprechende fachliche Expertise einzuholen und alles Mögliche im Vorfeld zu tun, um eine größtmögliche Transparenz über die eigenen IT-Assets zu erhalten, sowohl auf der technischen als auch auf der kaufmännischen und lizenzrechtlichen Seite.

Welche Hersteller auditieren häufig?

Die nachfolgend aufgeführten Hersteller orientieren sich in der Reihenfolge auch an Tabelle 24.1 im Abschnitt 24.2.1.

- **Oracle** (momentan die Rangliste anführend) ist immer sehr aktiv, was die Software-Audits betrifft, und hat leider wegen seiner bekannten meist unfreundlichen Vorgehensweisen im Umgang mit seinen Kunden bzgl. der Einhaltung seiner Lizenzbedingungen keinen allzu guten Ruf. Zudem setzt der lizenzrechtlich korrekte Einsatz der Produkte von Oracle auch sehr viel Sach- und Fachverständnis voraus, damit nicht aus Versehen bei der Installation eine Option zu viel ausgewählt wird, die dann vielleicht nicht mit der vereinbarten Nutzung abgedeckt ist (Stichwort Fehler bei der Paketierung bzw. Installation). Darauf setzt auch Oracle, ist meistens gnadenlos, wenn einem Administrator dieser Fehler bei der Installation unterlaufen ist, und verlangt nachträgliche Lizenzgebühren. Hinzu kommt der Eindruck, dass Oracle seine Software-Audits auch als „Vertriebskanal" für die Cloud-Abo-Modelle nutzt und bei Streitigkeiten im „On-Premises"-Umfeld dem Kunden eine kostengünstige „Heilung" zusagt, wenn im Gegenzug das auditierte Unternehmen in Oracle-Cloud-Produkte „investiert".
- **IBM**, aktuell auf Rang zwei, behauptet schon seit längerem diesen vorderen Bereich der Rangliste, vor allem in Bezug auf die Dauer und Häufigkeit seiner Software-Audits. Oftmals komplett aus dem Kundenfokus geraten und dann ein Riesenthema während des laufenden Audits sind die teils problematischen Regeln zur Einhaltung der Sub-Capacity-Virtualisierungsbestimmungen, die u. U. die Verwendung des IBM License Metric Tools (ILMT) erfordern, um weiterhin die reduzierten PVU-Verbräuche anwenden zu können.
- **Microsoft** hat den Ruf, die Sache mit weniger Aggressivität anzugehen, und liegt aktuell auch „nur" auf Rang drei, obwohl in Sachen Marktumsatz auf Rang eins stehend. Bereits vor einigen Jahren hat Microsoft noch die Software-Asset-Management-Initiative („SAM") ins Leben gerufen, um Microsoft-Kunden im SAM-Betrieb bei der Einhaltung der Lizenzkonformitätsprozesse zu unterstützen. Dabei hat Microsoft erklärt, hier Volumenlizenzkunden mit einem SAM-Engagements zu „helfen". Zwischen den Zeilen gelesen bedeutet dies, dass Microsoft-Volumenlizenzkunden u. U. kurz vor der Erneuerung eines EA-Vertrags entweder mit einem Software-Audit durch einen von Microsoft beauftragten Auditor „beglückt" werden oder über einen der Partner bzw. Wiederverkäufer mit einem SAM-Engagement zu

rechnen haben. Denken Sie daran, dass der Wortlaut des Volumenvertrags festlegt, dass Microsoft jederzeit ein Audit einleiten kann. Viele Kunden bemerken aber nicht, dass diese möglichen angetragenen SAM-Verpflichtungen jedoch nur eine andere Vorgehensweise sind und Kunden glauben lassen, dass sie auditiert werden, aber in Wirklichkeit ist diese „SAM-Verpflichtung" rechtlich gesehen eine **freiwillige** Kooperation (siehe nachfolgende Zitierung aus den FAQs). Es gibt hierfür auch eine Microsoft-FAQ-Seite,[12] wo diese beiden Aspekte noch einmal näher erläutert werden.

So wird hier (übersetzt mit Google) beispielsweise gefragt:

Frage: *Was ist Microsoft Software Asset Management („SAM")*

Antwort: *Das Microsoft-SAM-Programm ist ein vertrauenswürdiger IT-Beratungsservice, der auf Branchen-SAM-Standards basiert und Kunden dabei hilft, Dateneinblicke zu gewinnen, die Lizenzierung zu optimieren, Risiken zu minimieren und mit ihren IT-Investitionen produktiver zu sein. SAM-Engagements bieten einen 360-Grad-Überblick über die IT-Infrastruktur des Kunden und eine Reihe von Empfehlungen, wie die Richtlinien und -verfahren für das gesamte Asset Management, das Lizenzmanagement und die SAM-Richtlinien und -Verfahren verbessert werden können. Mit dieser umfassenden Sicht erhalten Kunden wertvolle Empfehlungen zu Bereichen, die für ihr Unternehmen am schwierigsten sind. SAM-Engagements werden von Microsoft SAM Certified Partners durchgeführt und sind freiwillig. Wir glauben, dass SAM ein strategischer Vorteil für alle unsere Kunden sein kann.*

Frage: *Einige Quellen behaupten, dass Microsoft Software Asset Management (SAM) und die Überprüfung der Lizenzkonformität (allgemein als „Audit" bezeichnet) identisch sind. Stimmt das?*

Antwort:

1. Microsoft Software Asset Management (SAM)

– Art des Engagements – **Freiwillig**

– Durchgeführt von – Microsoft SAM Certified Partners mit mehr Flexibilität im Prozess

– Ziel – Kunden helfen, den Wert zu maximieren, Risiken zu minimieren und mit ihren IT-Investitionen mehr zu erreichen.

2. Überprüfung der Microsoft-Lizenzkonformität (Audit)

– Art des Engagements – Obligatorische vertragliche Anforderung

– Durchgeführt von – Unabhängigen, international anerkannte zertifizierten Wirtschaftsprüfungsgesellschaften. In einigen Rechtsordnungen werden die Überprüfungen jedoch auch von autorisierten Beratern im Auftrag von Microsoft durchgeführt.

– Ziel – Helfen Sie Kunden bei der Erreichung und Aufrechterhaltung der Lizenzkonformität und beim Schutz der geistigen Eigentumsrechte von Microsoft.

– License Compliance Verification FAQ | Microsoft Volume Licensing

[12] Häufig gestellte Fragen zur Überprüfung der Microsoft-Lizenzkonformität – License Compliance Verification FAQ | Microsoft Volume Licensing – *https://www.microsoft.com/en-us/licensing/learn-more/compliance-verification-faq*

- **SAP** hat seine Kunden eigentlich schon immer durch seine eigene Systemvermessung (das SAP-eigene Tool Licence Administration Workbench) an die Lizenzreports und periodischen Systemvermessungen gewöhnt und liegt deswegen üblicherweise in der Rangliste nicht ganz so weit vorne – aktuell auf Rang vier. Meistens sind Nachlizenzierungen notwendig, weil die SAP-Anwender sich nicht ausreichend mit der Lizenzthematik von SAP auseinandersetzten. Allerdings könnten die SAP-Anwender bei richtiger Vorgehensweise noch erhebliche Lizenzkosten einsparen. Wobei es SAP den Anwendern nicht gerade einfach macht, beispielsweise SAP-User zu identifizieren, die das System wenig bis gar nicht nutzen. Hier hilft nur eine konsequente Steuerung und Überwachung der Userberechtigungen und Namenskonventionen. Denn auch wenn ein SAP-User physisch nur einmal existiert, der Name aber z. B. in Form verschiedener Schreibweisen mehrfach auftaucht (Stichwort: Doubletten), wird es gleich teurer. Ein anderer beliebter Fehler ist die fehlende Klassifizierung des SAP-Users (darum muss sich der SAP-Anwender selbst kümmern), denn ohne eine solche wird dieser automatisch in die teuerste Lizenzkategorie eingeordnet.
- **VMware** hat sehr umfangreiche Lizenzplausibilisierungen in seine Softwareprodukte integriert, somit ist die Gefahr einer unlizenzierten Nutzung nicht sehr groß. Deshalb ist VMware auch eher auf den hinteren Rängen zu finden. Dem Umstand geschuldet, sieht die Standard-Endbenutzer-Lizenzvereinbarung (EULA) auch höchstens einmal pro Jahr eine Überprüfung vor. Sofern nach dem Audit eine Diskrepanz von mehr als fünf Prozent entsteht, werden Nachzahlungen gefordert, oder wenn ein Kunde seine Aufzeichnungspflichten grob verletzt. Im Allgemeinen prüft VMware seine Kunden nicht sehr häufig, eine Auditankündigung wird aber gerne verwendet, um den Abschluss oder die Erneuerung einer ELA[13] zu „beschleunigen“, was häufig zu übermäßigen Kosten führen kann.
- **Adobe** ist seit längerem fast nur noch auf den hinteren Rängen zu finden und bestätigt damit auch das bereits seit längerem „Gefühlte“ mit weniger Auditaktivitäten. Aufgrund der sehr frühen Umstellung und Transformation der „On-Premises“-Lizenzen auf Cloud-Abonnements hat Adobe es geschafft, seine Produktpalette fast komplett in Subscription-Modelle zu transformieren. Aufgrund der damit verbundenen Transparenz (für Adobe) über die Lizenzkäufe der Anwender, sind einhergehend auch die Auditaktivitäten heruntergefahren worden. Auch das Thema BYOL, tangiert Adobe so gut wie überhaupt nicht mehr. Trotz der fast vollständigen Transformation bleiben Adobe-Produkte immer noch etwas komplex in der „SAM-Verarbeitung“ und das macht es dann oftmals nicht gerade einfach, den Überblick zu behalten.

24.2.1 Audithäufigkeit, aktuelle Rangliste (Hersteller)

Aufgrund der enormen Transformation in die Cloud-Umgebungen und des Wechsels der zu generierenden Umsätze weg vom „On-Premises“ hin zu den Abonnement-Abrechnungsmodellen, verschieben sich auch die vertretenen Positionen der Hersteller zu den Themen Auditaktivität und Audithäufigkeit. In der Tabelle 24.1 sehen Sie den derzeitigen Stand, erhoben von Gartner in der Gartner Studie „Software Industry Transformation Requires Software Asset Management Programs to Follow Suit“.[14]

[13] *https://www.vmware.com/content/dam/digitalmarketing/vmware/en/pdf/solutions/epp-program-guide.pdf*, *https://www.vmware.com/content/dam/digitalmarketing/vmware/de/pdf/solutions/SPP-QRG.pdf*

[14] Gartner, Published 24 February 2021 – ID G00735254 – *https://www.gartner.com/doc/reprints?id=1-25EJ437D&ct=210308&st=sb*

Tabelle 24.1 Aufstellung (Rangliste) Hersteller über ihre Software-Audit-Aktivitäten

Softwarehersteller	Position in Bezug auf das Software-Audit-Volumen	Position Marktumsatz
Oracle	Nr. 1	Nr. 2
IBM	Nr. 2	Nr. 3
Microsoft	Nr. 3	Nr. 1
SAP	Nr. 4	Nr. 4
VMware	Nr. 5	Nr. 8
Micro Focus	Nr. 6	Nr. 12
BMC	Nr. 7	Nr. 25
OpenText	Nr. 8	Nr. 17
Quest-Software	Nr. 9	Nr. 39
Adobe	Nr. 10	Nr. 7

Interessant ist in dieser Studie auch, dass Gartner die SAM-Funktionen und SAM-Tools als einen wichtigen geschäftskritischen Bestandteil betrachtet, um über „Cloud Center of Excellence (CCOE)“ die zukünftigen erforderlichen Managementaktivitäten und deren Risikosteuerung sicherstellen zu können.

Gartner bezeichnet das SAM als „**Nexus of all Technology Environments**“ und weist auch hiermit u. a. darauf hin, was uns schon in der Norm ISO/IEC 19770-1:2017 aufgezeigt wird: dass „nur“ noch das „IT-Asset“ und dessen Management und Risikosteuerung im zukünftigen IT-Betrieb, egal ob noch lokal oder in der Cloud, im Fokus stehen wird. Aber bevor es so weit ist, benötigen wir noch einmal einen kurzen Abstecher zum Thema, was ein gültiger Lizenznachweis ist.

24.2.2 Was ist ein gültiger Lizenznachweis?

Für den Nachweis gültiger Lizenzen benötigen Sie diverse Informationen und Unterlagen. Eine Auswahl finden Sie in der folgenden Aufstellung. Aufgrund der Fülle an Softwareprodukten und Herstellern kann diese Aufstellung aber nur eine grobe Übersicht vermitteln.

Ausführliche Informationen zum Thema Lizenznachweise finden Sie auch im Kapitel 13 „Erfassung von Lizenznachweisen – Best Practise“.

Leider gibt es keinen allgemeingültigen Standard, wie eine gültige Lizenz nachgewiesen werden kann. Je nachdem, welches Softwareprodukt im Einsatz ist und über welchen Distributionskanal die Lizenzen erworben wurden, gibt es unterschiedliche Anforderungen an einen gültigen Lizenznachweis. Dieser kann dann aus den unterschiedlichsten Bestandteilen zusammengesetzt sein.

Mögliche Bestandteile und Arten von Lizenznachweisen

- Originalverpackung mit dem gesamten originären Inhalt bei Kauf,
- Original-Software-Medien (CDs, DVDs, USB-Sticks, Memory-Cards, evtl. Disketten),
- Lizenzvereinbarung, Garantieschein, Echtheitszertifikat, Handbuch,
- Rechnung, Zahlungsnachweis, Quittung, Kaufbeleg, Bestellformular (in Richtung Lieferant, Hersteller).

Nicht als Lizenznachweis anerkannt werden z. B.

- Lizenzurkunden, die nicht vom Hersteller ausgestellt wurden (ein großes Problem bei Lizenzverkäufen auf dem Gebrauchtsoftware-Markt, da hier teilweise mit von Notaren ausgestellten Lizenzzertifikaten ein rechtmäßiger Erwerb der Nutzung vorgetäuscht wird),
- notarielle Bestätigungen (siehe Lizenzurkunden),
- Lieferscheine,
- gefälschte (nicht originale) Softwareprodukte (Raubkopien),
- Softwareprodukte (auch wenn diese original sein sollten) in einzelnen Bestandteilen, also z. B. einzelne Originaldatenträger, einzelne Echtheitszertifikate (Certificates of Authenticity, COAs),
- unrechtmäßige Bundles von Softwareprodukten (siehe Abschnitt 24.1.1 „Was bedeutet unlizenzierte Nutzung?“).

Formen gültiger Lizenznachweise unterschiedlicher Hersteller

Microsoft

- Einzelhandelspaket (FPP)-Software (z. B. aus einem Elektronikmarkt, muss aber vollständig sein, so wie bei Kauf erworben)

  Zahlungsnachweis, Rechnung vom Lieferanten, Echtheitszertifikat, Originalverpackung, Originaldatenträger, Handbuch, Endbenutzerlizenzvertrag (EULA) oder Microsoft Software License Terms (MSLT)

- OEM und System Builder (SB), z. B. von einem Fachhändler

  Zahlungsnachweis, Rechnung vom Lieferanten, Echtheitszertifikat (COA-Label), Datenträger (wenn mitgeliefert), Handbuch (wenn mitgeliefert), Endbenutzerlizenzvertrag (EULA) oder Microsoft Software License Terms (MSLT)

- Enterprise Agreement (EA) oder Select Plus

  Vertragsdokumente, Beitrittsnachweis, Bestätigung der Bestellung des Beitrittsunternehmens, Nachweise der Lizenzübertragung, Zahlungsnachweis, Dokument „Transfer of License“ (Lizenzen, die über diesen Weg in eine andere Firma übertragen wurden, werden nicht im VLSC-Portal abgebildet, daher muss dieses Dokument von Microsoft als einzig gültiger Lizenznachweis aufbewahrt werden)

- Select Plus

  Vertragsdokumente, Bestellung, Bestätigung der Bestellung des registrierten verbundenen Unternehmens, Nachweise der Übertragung, Zahlungsnachweis, Daten aus dem VLSC-Portal

- Open Value

  Vertragsdokumente, Bestätigung der Bestellung, Dokumentation, die die Lizenzübertragung nachweist, Zahlungsnachweis, Rechnung vom Lieferanten

- Open License

  Online-Unterlagen (eOpen), Vertragsdokumente

Adobe

- Rechnungen, Daten des Kunden vom Lieferanten, vorhandene Lizenzzertifikate, Vertragsdokumente, Bestelldaten aus der Adobe-Lizenzdatenbank (Lizenzkeys werden nicht als Nachweis anerkannt). Adobe stellt einen eigenen „License Manager" für E-Licensing zur Verfügung.

Oracle

- Auszug aus der Lizenzdatenbank, originales Bestellformular, Zahlungsnachweis

IBM

- Vertragsdokumente: Passport Advantage Express (PAE) (für kleinere und mittlere Unternehmensgrößen) oder Passport Advantage für größere Unternehmen mit verschiedenen Rabattstaffeln
- Die Lizenzdokumente für beide Varianten: Der Softwarelizenznachweis und das Dokument „Software Subscription & Support" mit der Übersicht der erworbenen Softwareprodukte und Lizenzen sowie Wartungslizenzen (andere SKU-Nummer) werden nach Abschluss von IBM an den Kunden ausgeliefert und sind die gültigen Lizenznachweise.
- Außerdem können die Lizenzdokumente bzw. die erworbenen Softwareprodukte auf dem Passport-Advantage-Online-Portal verwaltet werden.[15]

Hinweis

Sie sollten sich unbedingt angewöhnen, alles schriftlich zu dokumentieren, was in irgendeiner Form mit der Kommunikation zwischen Ihnen und Ihren Lieferanten oder Vertriebsleuten des Herstellers zu tun hat. Legen Sie bei mündlichen Vereinbarungen (z. B. in Meetings oder Telefonaten) Aktennotizen oder Gesprächsprotokolle an (oder wenigstens ein Gedächtnisprotokoll, wenn kein offizielles erstellt wird) und versichern Sie sich damit noch einmal schriftlich bei Ihrem Gesprächspartner, ob der besprochene Sachverhalt so Bestand hat. Wenn Sie es auf Seiten des Herstellers oder Lieferanten mit wechselnden Ansprechpartnern zu tun haben, kann es Ihnen sonst passieren, dass eine getroffene vertragliche Vereinbarung vom Nachfolger, weil nirgends dokumentiert, nicht mitgetragen wird.

Im nächsten Abschnitt erfahren Sie ein paar rechtliche Fakten zu den bisher ausgeführten Aspekten und können sich damit auf eine mögliche Software-Audit-Situation besser vorbereiten.

[15] Overview – IBM Passport Advantage – *https://www.ibm.com/software/passportadvantage/*

24.3 Audit, rechtliche Fakten

Die Softwarehersteller haben zugegebenermaßen ein berechtigtes Interesse daran, die Einhaltung der lizenzkonformen Nutzung ihrer Softwareprodukte zu überwachen. Um dieses Interesse zu wahren, sind in den Softwareverträgen häufig Klauseln zu finden, die dem Lizenzgeber mehr oder weniger umfangreiche Auditrechte zugestehen sollen. Diese Auditklauseln sind ein beliebtes Thema in der Softwarebranche und müssen sich an den gesetzlichen Regelungen in Deutschland messen lassen (UrhG, BGB). Das macht es den Herstellern nicht gerade leicht.

24.3.1 Vertragliche Grundlagen

Die Softwarehersteller vereinbaren daher in ihren Lizenzverträgen vertragliche Lizenzauditklauseln, nicht nur um aus Sicht der Softwarehersteller bei konkreten Anlässen, d. h., wenn Anhaltspunkte für einen Lizenzverstoß vorliegen, sondern auch um anlassunabhängig Auskünfte einzuholen und Lizenzüberprüfungen bei Unternehmen vornehmen zu können.

Dazu ein Beispiel einer vertraglichen Standardauditklausel in einem Standardlizenzvertrag eines größeren Softwareherstellers:[16]

> *„Der Softwarehersteller darf Ihre Nutzung der Programme prüfen („Audit"), vorausgesetzt, der Softwarehersteller kündigt die Prüfung 45 Tage im Voraus schriftlich an. Sie verpflichten sich, bei dem Audit des Softwareherstellers behilflich zu sein, den Softwarehersteller in angemessenem Rahmen zu unterstützen und dem Softwarehersteller hinreichenden Zugang zu Informationen zu gewähren. Zudem verpflichten Sie sich, gegebenenfalls zu wenig bezahlte Gebühren innerhalb von 30 Tagen nach schriftlicher Aufforderung nachzuentrichten. Wenn die Zahlung nicht erfolgt, ist der Softwarehersteller berechtigt, Ihre technische Unterstützung, Ihre Lizenzen sowie diesen Vertrag außerordentlich zu kündigen. Sie erklären sich damit einverstanden, dass der Softwarehersteller nicht für Kosten einzustehen hat, die Ihnen durch die Mithilfe bei einem Audit entstehen."*

24.3.2 Rechtliche Wirksamkeit

Eine vertragliche Standardauditklausel könnte nach den Regelungen zur Gestaltung rechtsgeschäftlicher Schuldverhältnisse durch Allgemeine Geschäftsbedingungen gemäß §§ 305 ff. BGB insbesondere dann unwirksam sein, wenn diese nach § 307 Abs. 2 Nr. 1 BGB den Vertragspartner des Verwenders, also den Lizenznehmer, entgegen den Geboten von Treu und Glauben unangemessen benachteiligt.

[16] it-recht-kanzlei.de – „Lizenzüberprüfung, deren Zweck sowie deren vertragliche und gesetzlichen Grundlagen – Teil 1 der Serie zum IT-Lizenzmanagement" – *https://www.it-recht-kanzlei.de/lizenzaudit-softwareaudit-software%C3%BCberpr%C3%BCfung.html*

Empfehlung für die Praxis:
Ob eine solche unangemessene Benachteiligung i.S.v. § 307 Abs. 2 Nr. 1 BGB vorliegt und die Auditklausel damit evtl. unwirksam ist, sollte bei Verwendung eines Standard-Softwarelizenzvertrags des Softwareherstellers Folgendes geprüft werden:
Beinhaltet die Auditklausel beispielsweise keine angemessenen Regelungen über angemessene Fristen zur Anmeldung des Audits, zur Durchführung des Audits zu den üblichen Geschäftszeiten des Lizenznehmers, zur Wahrung der Betriebs- und Geschäftsgeheimnisse des Lizenznehmers und zur Wahrung der Vertraulichkeit und zur Beachtung des Datenschutzes?

24.3.3 Regelungsinhalt von Auditklauseln

Da grundsätzlich allgemein anerkannt ist, dass die Softwarehersteller ein berechtigtes Interesse daran haben, den Nutzungsumfang und die Nutzungsintensität der in den Unternehmen der Lizenznehmer eingesetzten Softwarelizenzen zu überprüfen, und auch in der Regel darauf bestehen, dass Regelungen zum Lizenz-Audit Bestandteil eines Softwarelizenzvertrags sind, wird empfohlen, die den Lizenznehmern gegebenen Möglichkeiten zu nutzen und den Regelungsinhalt der Auditklausel so zu verhandeln, dass die wirtschaftlichen und rechtlichen Interessen der Lizenznehmer gewahrt bleiben.

Empfehlung für die Praxis:
Regelungsinhalt von Auditklauseln sollte, abhängig vom jeweiligen Einzelfall, insbesondere sein:

- *eine angemessene Ankündigungsfrist;*
- *eine Durchführung zu den üblichen Geschäftszeiten des Lizenznehmers;*
- *Dauer, Umfang und Anzahl (beispielsweise höchstens einmal pro Jahr) des Lizenz-Audits;*
- *Festlegung der Auditoren, wie Lizenzgeber, Partner des Lizenzgebers, Wirtschaftsprüfer, Lizenzmanagement-Unternehmen;*
- *Konkretisierung der Prüfungsinhalte;*
- *Wahrung der Betriebs- und Geschäftsgeheimnisse des Lizenznehmers;*
- *Wahrung der Vertraulichkeit und Datensicherheit des Lizenznehmers;*
- *Geheimhaltung der Auditergebnisse;*
- *Übernahme der Kosten;*
- *Haftung des Auditors für potenzielle IT-Performanceprobleme sowie*
- *rechtliche und wirtschaftliche Folgen einer Über- und Unterlizensierung.*

24.3.4 Gesetzliche Grundlagen

Sowohl das Urheberrecht (§§ 101 Abs. 1, 101a Abs. 1 UrhG) als auch das allgemeine Zivilrecht (§§ 242, 809 BGB) gestatten Softwareherstellern als Rechtsgrundlage im europäischen Raum die Durchführungen von Lizenzprüfungen bzw. Audits, welche aber anlassbezogen und sich beispielsweise auf eine hinreichende Wahrscheinlichkeit einer Vertragsverletzung beziehen

müssen. Dabei sind die Maßnahmen zur Prüfung verhältnismäßig auszulegen, was häufig erst einmal eine Besichtigung vor Ort beim Kunden ausschließt und folgerichtig auch mit dem zivilrechtlichen Anspruch auf Auskunft und Besichtigung in Einklang zu bringen ist.

Zivilrechtlicher Anspruch auf Auskunft und Besichtigung

Nach § 809 BGB kann derjenige, der gegen den Besitzer einer Sache einen Anspruch in Ansehung der Sache hat oder sich Gewissheit verschaffen will, ob ihm ein solcher Anspruch zusteht, und wenn die Besichtigung der Sache aus diesem Grunde für ihn von Interesse ist, verlangen, dass der Besitzer ihm die Sache zur Besichtigung vorlegt oder die Besichtigung gestattet.[17]

> *„Da die Anwendbarkeit des § 809 BGB auf dem Gebiet des geistigen Eigentums grundsätzlich unter Berücksichtigung der Grundsätze von Treu und Glauben gemäß § 242 BGB (BGH, Urteil vom 02.05.2002, GRUR 2002, 1046 sog. Faxkartenentscheidung) anerkannt ist, könnte dem Softwarehersteller, um eine Verletzungen seines Urheberrechts feststellen zu können, danach ein Besichtigungsanspruch zur Feststellung einer Urheberrechtsverletzung (beispielsweise wegen Unterlizensierung) gegen den Lizenznehmer zustehen. Da die Tatbestandsvoraussetzungen gemäß §§ 809, 242 BGB nach der Rechtsprechung insofern gewissen Einschränkungen unterliegen, dass eine gewisse Wahrscheinlichkeit bzw. Anzeichen für eine Urheberrechtsverletzung vorliegen müssen und das Geheimhaltungsinteresse des Lizenznehmers sowie der Grundsatz der Verhältnismäßigkeit gewahrt sein müssen, kann ein Anspruch des Softwareherstellers nach §§ 809, 242 BGB auf Besichtigung, etwa von Datenträgern und Hardware, nur in Einzelfällen in Betracht kommen. Darüber hinaus ist in der Literatur strittig, ob durch die Vorschrift von § 809 BGB auch das Vorlegen von Lizenznachweisen, Lizenzverträgen und Rechnungen abgedeckt ist. Unstrittig erscheint jedoch, dass dem Softwarehersteller nach diesen gesetzlichen Regelungen kein Ausforschungs- und Durchsuchungsanspruch zusteht. Selbst, wenn die bisherige „sondergesetzliche" Normierung des § 809 BGB, die – wie oben ausgeführt – durch die BGH-Rechtsprechung nach den Grundsätzen von Treu und Glauben gewissen Einschränkungen unterliegt, durch die Neufassung des § 101 a UrhG (Anspruch auf Vorlage und Besichtigung) mit Inkrafttreten des Gesetzes zur Verbesserung der Durchsetzung des geistigen Eigentums zum 01.09.2008 (sog. Durchsetzungsgesetz) präzisiert wurde, bleibt im Ergebnis festzustellen, dass aus Sicht des Softwareherstellers die Vereinbarung einer vertraglichen Auditklausel unverzichtbar ist, wenn er seinen Anspruch auf eine Lizenzüberprüfung wegen einer (potenziellen) Urheberrechtsverletzung durch den Lizenznehmer durchsetzen möchte."*

In den hier zitierten Ausführungen von RA Matthias Petzold (*it-recht-kanzlei.de*) zum Thema „Lizenzüberprüfung, deren Zweck sowie deren vertraglichen und gesetzlichen Grundlagen" werden noch weitere interessante Aspekte angesprochen, die darauf abstellen, dass Auditklauseln in für Deutschland geltenden Standard-AGB-Formularverträgen häufig unwirksam sind. Auch wenn sich viele weitere Rechtsmeinungen mit dem Thema der „berechtigten oder unberechtigten Einräumung von Auditklauseln in Software- und Lizenzverträgen" auseinandersetzen und zugegebenermaßen recht einleuchtende Argumente finden, die dafür sprechen, dass die Auditklauseln zumindest in Standard-AGB-Formularverträgen unwirksam sind, werden Ihnen solche rechtlich nicht verbindlichen Meinungsäußerungen in der Praxis letztlich nur wenig weiterhelfen. Auch gibt es, soweit mir bekannt ist, zurzeit keinen ausjudizierten Fall in dieser Sachlage.

[17] Original Gesetzestext *https://dejure.org/gesetze/BGB/809.html*

Im Gegenteil: Es könnten recht langwierige Rechtsstreitigkeiten oder auch die Beendigung der Geschäftsbeziehung drohen. Und wenn das in Ihrem Unternehmen ein strategisches Softwareprodukt betreffen sollte, kann dies auf Ihren Geschäftsbetrieb verheerende Auswirkungen haben, da die Hersteller oft am längeren Hebel sitzen. Bei Streitigkeiten könnte ein Hersteller z. B. mit einer einstweiligen Verfügung Ihren Geschäftsbetrieb unter Umständen erheblich einschränken, denn der Richter, der diese anordnet, muss dafür die Gegenseite nicht anhören. Da Sie sich vertraglich für eine lizenzkonforme Nutzung der Softwareprodukte gegenüber dem Hersteller verpflichtet haben, sind Sie faktisch auch daran gebunden, diese einzuhalten. Daher sollte es Sie eigentlich nicht überraschen, wenn dies gelegentlich überprüft wird. Der Gesetzgeber hat festgestellt, dass hier weitere Anpassungen erforderlich sind, und hat im Wege einer weiteren Novellierung im „Gesetz zur Verbesserung der Durchsetzung des geistigen Eigentums (GEigDuVeG)“ den § 101 a UrhG (Anspruch auf Vorlage und Besichtigung) ergänzt und präzisiert (beschrieben unter Artikel 6, S. 1201 ff.). Das Gesetz ist am 7. Juli 2008 in Kraft getreten und hat weitere Paragrafen des UrhG aktualisiert (§§ 97–111c). Trotz der weiteren Stärkung des Schutzes geistigen Eigentums bleibt festzustellen, dass aus Sicht der Softwarehersteller weiterhin eine zusätzliche vertragliche Auditklausel in den Verträgen unverzichtbar ist, wenn Ansprüche wegen einer (eventuellen) Verletzung des Urheberrechts geltend gemacht werden sollen.

24.3.5 Auditklauseln, Hersteller

Nachdem Ihnen ein Software-Audit-Ankündigungsschreiben vorliegt, sollte analysiert und geprüft werden, welche Auditklauseln (aus welchem Herstellervertrag) für diesen Fall Gültigkeit besitzen, ebenso ist zu prüfen, ob mögliche Nebenabreden vereinbart wurden. Die Auditoren beziehen sich normalerweise immer auf die vorliegenden (meist mit einem Verweis auf die aktuellen Weblinks) aktuellen Fassungen der Produktnutzungsrechte, und die können und müssen nicht unbedingt auf ihren Überprüfungszeitraum anwendbar sein. Die Frage, die zu stellen wäre: Welche Version der Produktnutzungsrechte ist auf das Software-Audit anzuwenden? Die aktuelle oder die damals bei Vertragszeichnung gültige?

Es gilt natürlich die damals bei Vertragsunterzeichnung vorliegende gültige Fassung. Also: Es ist wichtig, die Auditklauseln genau darauf zu prüfen, was vereinbart wurde und wozu man verpflichtet ist. Bezugnehmend auf den deutschen Gesetzgeber müssen Klauseln für AGBs klar und verständlich formuliert sein. Wenn diese nicht klar und verständlich formuliert sind bzw. irgendeine Überraschung enthalten, genügen sie per Gesetzesdefinition nicht den Anforderungen einer AGB-Formulierung und können dadurch u. U. auch in Teilen unwirksam sein oder werden.

Betrachten wir uns beispielhaft die Auditklauseln von Oracle aus den aktuellen (deutschen) Vertragsbedingungen.

> *Diese Allgemeinen Vertragsbedingungen (nachfolgend „Allgemeine Vertragsbedingungen“) sind gültig zwischen ORACLE Deutschland B.V. & Co. KG („Oracle“) und der natürlichen oder juristischen Person, die den Auftrag ausgefertigt hat, der diese Allgemeinen Vertragsbedingungen per Verweis einschließt. Durch die Erteilung eines Auftrags, der diesen Allgemeinen Vertragsbedingungen unterliegt, stimmen Sie zu, dass die Anlagen (wie unten definiert), die diesen Allgemeinen Vertragsbedingungen beigefügt sind, in diese Allgemeinen*

Vertragsbedingungen einbezogen werden. Ist eine Bestimmung nur für eine spezielle Anlage relevant, gilt diese Bestimmung nur für diese Anlage, wenn die Anlage diese Allgemeinen Vertragsbedingungen in Bezug nimmt. – https://www.oracle.com/a/ocom/docs/lic-online-toma-de-deu-v040119.pdf

Begeben wir uns zur Seite 14 dieses Dokuments „Anlage P – Programm" und hier zum Punkt „8. Audit":[18]

Nach schriftlicher Vorankündigung mit einer Frist von fünfundvierzig (45) Tagen ist Oracle berechtigt, Ihre Nutzung der Programme zu prüfen, um sicherzustellen, dass Sie bei der Nutzung der Programme die Bestimmungen des zugehörigen Auftrags und des Rahmenvertrags einhalten. Eine solche Prüfung wird Ihren normalen Geschäftsbetrieb nicht unverhältnismäßig stören. Sie verpflichten sich, bei einer solchen Prüfung durch Oracle zu kooperieren sowie, soweit von Oracle in **zumutbarem Umfang** *angefordert,* **angemessene Unterstützung** *und Zugriff auf Informationen zu gewähren. Eine solche Unterstützung umfasst unter anderem den Einsatz* **von Oracle-Datenmesswerkzeugen** *auf Ihren Servern und die Bereitstellung der daraus* **resultierenden Daten** *an Oracle. Die Durchführung der Prüfung sowie dabei gewonnene, nichtöffentliche Informationen und Daten (einschließlich aus der Prüfung resultierender Feststellungen oder Berichte) unterliegen den Bestimmungen in Abschnitt 8 (Geheimhaltung) der Allgemeinen Vertragsbedingungen. Werden bei der Prüfung Verstöße festgestellt, erklären Sie sich damit einverstanden, diese Verstöße innerhalb von 30 Tagen nach schriftlicher Mitteilung darüber zu beheben (was auch die Zahlung von Vergütungen für zusätzliche Programmlizenzen umfassen kann). Wenn Sie die Verstöße nicht beheben, ist Oracle berechtigt, (a) programmbezogene Serviceangebote (einschließlich technischen Supports), (b) Programmlizenzen, die im Rahmen dieser* **Anlage P** *und damit verbundener Vereinbarungen bestellt wurden, und/oder (c) den Rahmenvertrag zu beenden. Sie stimmen zu, dass Oracle keine Kosten übernimmt, die Ihnen durch die Kooperation bei der Prüfung entstehen.*

Auf den Webseiten der DOAG[19] gibt der Rechtsanwalt Dr. Thomas Thalhofer zum Thema „Viele Auditklauseln sind unwirksam, wenn deutsches AGB-Recht Anwendung findet" ein Interview. Im Prinzip könnte man jetzt die (**fett-kursiv**) gekennzeichneten Formulierungen in der Auditklausel einer genaueren Interpretation zuführen bzw. versuchen, diese zu „verstehen", aber wie Dr. Thomas Thalhofer weiter unten in seinen Ausführungen bereits antwortet: „*... Ein Lizenznehmer, der kein Problem hat, braucht die Auseinandersetzung nicht suchen*" – es ist immer auch eine Ermessenssache, ob hier dieses „Goldwaage-Prinzip" einen Audit erfolgreich abwehren könnte, mit all den Konsequenzen, die hier auch bereits in den Ausführungen mit geäußert wurden.

Nachfolgend weitere Äußerungen von ihm zu den Auditklauseln von Oracle.

Die Auditklausel von Oracle beispielsweise ist anlasslos: Sie erlaubt einen Audit jederzeit mit unbeschränkter Häufigkeit, auch wenn es keinerlei Verdacht auf Urheberrechtsverletzung gibt. Auch werden keine Maßnahmen zum Schutz von personenbezogenen Daten und Betriebsgeheimnissen getroffen.

---

[18] License_Online TOMA_v040119_DE_DEU Seite 17, *https://www.oracle.com/a/ocom/docs/lic-online-toma-de-deu-v040119.pdf*

[19] *https://www.doag.org/de/home/news/viele-auditklauseln-sind-unwirksam-wenn-deutsches-agb-recht-anwendung-findet/detail/*

Ist Ihnen ein Fall bekannt, in dem eine Auditklausel aufgrund der von Ihnen beschriebenen anlasslosen Prüfung für unwirksam erklärt wurde?

Wenn Sie sich in der juristischen Literatur umschauen – und ich habe mich mit dem Meinungsstand zur Wirksamkeit von Auditklauseln sehr intensiv beschäftigt –, werden sehr strenge Anforderungen daran angelegt, was in diesen Klauseln enthalten sein muss. Insgesamt gibt es drei Argumente, die gegen eine Wirksamkeit sprechen. Das ist zum einen eine jederzeitige anlasslose Prüfung, d. h. ohne Verdacht auf Urheberrechtsverletzung, was der gesetzlichen Grundregelung im § 101a UrhG widerspricht, dann Gefahr für Betriebs- und Geschäftsgeheimnisse und datenschutzrechtliche Bedenken. Wenn Sie nun aber auf die Praxis schauen, so ist mir kein Fall bekannt, in dem das tatsächlich vor Gericht prozessiert worden wäre. In der Praxis ist es meist so, dass die Kunden die Audits akzeptieren, auch auf Grundlage dieser Klausel, und eben versuchen, mit Oracle irgendwo eine Einigung zu finden, wie der Audit abzulaufen hat. Wie schon gesagt, ein Audit ist als solches auch legitim, weil der Softwarehersteller ein berechtigtes Interesse hat, die rechtmäßige Nutzung seiner Software durch den Lizenznehmer zu überprüfen. Er soll ja auch vergütet werden für die Software, die er entsprechend den vereinbarten Lizenzbedingungen bereitstellt. Nicht zu vergessen ist aber, dass der Lizenznehmer durchaus eine Verhandlungsposition auf Augenhöhe hat, wenn er seine juristischen Positionen hier nutzt. Er muss im Audit nicht zu allem Ja und Amen sagen, was vom Softwarehersteller verlangt wird, sondern kann hier angemessen auf die Berücksichtigung seiner Interessen pochen, da es juristisch durchaus Argumente gegen viele Auditklauseln und die dort niedergelegten Bedingungen gibt – z. B. im Fall von Oracle.

... selbst wenn ein Audit letztlich nicht durchgeführt wird, werden etwaige Ansprüche aus einer Lizenzvertragsverletzung erst einmal nicht wegfallen. Wenn es z. B. tatsächlich einen konkreten Verdacht auf Urheberrechtsverletzung gibt, stehen Oracle immer noch die gesetzlichen Ansprüche wie aus dem § 101a UrhG zur Verfügung, die sie nutzen und geltend machen können. Mit anderen Worten: Ein Lizenznehmer, der kein Problem hat, braucht die Auseinandersetzung nicht suchen, und für einen Lizenznehmer, der wirklich Urheberrechte verletzt hat, ist der Anspruch nicht erloschen, bloß weil ein Audit nicht durchgeführt oder verschoben wird. – Dr. Thomas Thalhofer, *https://www.doag.org/de/home/news/viele-auditklauseln-sind-unwirksam-wenn-deutsches-agb-recht-anwendung-findet/detail/*

Nun, die Thematik um die Wirksamkeit der Auditklauseln resultiert nicht zuletzt auch aus den Schwierigkeiten der Hersteller, ihre Lizenzmodelle auch ausreichend verständlich und „handhabbar“ (für Lizenzgeber und Lizenznehmer) in die neuen Cloud-Gegebenheiten – mit all ihren Komplexitäten – zu transformieren.

24.4 Die Schwierigkeiten der Hersteller

Die verschiedenen Cloud-Liefer- und Servicemodelle, die heute die völlige Normalität abbilden, bringen auch eine Reihe neuer Herangehensweisen, Herausforderungen und Komplexitäten in puncto Softwarelizenzierung und Einhaltung der Lizenzkonformität mit sich. Die cloudbasierten Abonnements und Abrechnungsmodelle sind zwar nicht mehr Neuland, aber auch noch nicht so etabliert, dass diese über Standardverfahren innerhalb der „klassischen" SAM-Life-Cycle-Prozesse gesteuert werden können. Denn nicht nur die eigentlichen Bereitstellungs- und Abrechnungsprozesse sind zu steuern, sondern die verschiedenen Aspekte und Nuancen, die es rund um „IaaS", „PaaS" und „SaaS" zu beachten gilt, sind ebenso in das Risikomanagement mit aufzunehmen. Dies gilt vor allem dann, wenn die Verantwortlichkeiten zur Einhaltung der lizenzkonformen Nutzung der Softwareprodukte nicht immer klar definiert sind. Denn die Haftung für die Einhaltung der Lizenzkonformität verbleibt immer beim Lizenznehmer. Ist dieser nicht bei allen Maßnahmen des Cloud Service Providers so mit eingebunden, dass eine Beurteilung der Lizenzsituation möglich ist, kann das zu erheblichen lizenzrechtlichen Auswirkungen führen.

Durch den sich vollziehenden Paradigmenwechsel beim „Zählen, Messen, Wiegen", hin zu den „IaaS"-, „PaaS"- und „SaaS"-Abrechnungsmodellen, werden die Hersteller nicht mehr lange groß genötigt sein, wie beim bisherigen klassischen „On-Premises"-Modell über Software-Audits nachzuprüfen, ob die erworbenen Lizenznachweise auch den technisch ausgewiesenen Lizenzbedarfen entsprechen. Da die Umstellung auf „SaaS" auf einem Cloud-Hybrid-Betrieb noch eine ganze Weile dauern wird und eben dann auch trotzdem noch „On-Premises"-Lizenzen (BYOL) eine (nur nicht mehr so große) Rolle spielen, werden die Auditaktivitäten nicht ganz verschwinden.

Fragen, die diesbezüglich zu stellen wären:

- Werden „On-Premises"-Lizenzen in die Cloud verschoben, liegt die Einhaltung der lizenzkonformen Nutzung normalerweise beim Lizenznehmer (BYOL), während die Verantwortung für den lizenzkonformen Betrieb beim Cloud Service Provider liegt. Im Fall einer aufgedeckten Diskrepanz durch nicht lizenzkonforme Verwendung von Softwareprodukten, stellt sich die Frage, wer dann die Auditrechnung zahlt. Der Cloud Service Provider oder der Kunde? Und welchen Anteil davon?
- Werden für die Nutzung in einer Public-Cloud die gleichen Lizenzmetriken angewendet bzw. anzuwenden sein, wie bei der Verwendung in einer Private-Cloud?
- Was ist, wenn der Kunde im Servicemodell „IaaS" nicht nur die Kontrolle darüber hat, was in der Cloud-Umgebung ausgeführt wird, sondern möglicherweise auch noch die Kontrolle über Betriebssysteme und bereitgestellte Anwendungen? Welche Regeln zur Verantwortung einer lizenzkonformen Nutzung würden dann für so ein Szenario anzuwenden sein, verantwortet es der Kunde oder der Cloud Service Provider?
- Wie sind die im Unternehmen bestehenden aktuellen „klassischen" Softwarelizenzverträge formuliert? Gibt es hier eventuell schon eine Nutzungserlaubnis der „On-Premises"-Lizenzen in der Cloud?

Die Komplexitäten in der Umsetzung und Steuerung verstecken sich oft, so wie ein Eichhörnchen seine gefundenen Nüsse meistens verstecken möchte. Ehe man sich versieht,

kommt die nächste Nuss, die es zu knacken gilt. Der Cloud-Betrieb erfordert eine Vielzahl an zusätzlichen Dokumenten, statt nur den „klassischen" Lizenznachweis. Auch hier gilt – wie schon im „lokalen" SAM-Betrieb – alles muss richtig interpretiert und über geeignete Risikomanagementkontrollen gesteuert und implementiert werden, um die Einhaltung der Nutzungsbedingungen der Hersteller permanent sicherstellen zu können.

Fazit

Unbestritten ändern sich die klassischen IT-Landschaften und IT-Strukturen und sollten über ein „Cloud Center of Excellence (CCOE)"[20] gesteuert und überwacht werden. Die Cloud-Servicemodelle „IaaS", „PaaS", „SaaS", neue Bereitstellungsformen über Containering, Edge-Computing, Serverless, andere Varianten der App-Entwicklungen wie Low-Code bzw. No-Code, der Einsatz von Open-Source-Produkten wirken sich immer stärker und vielfältiger auf die Art und Weise aus, wie Unternehmen ihre IT-Assets steuern und verwalten müssen. Heutige ITAM-Rollen müssen die neuen Technologien verstehen können, um zusammen mit dem Enterprise-Architekten die erforderlichen Prozesse und Leitplanken implementieren zu können und um den IT-Betrieb lizenzkonform, wirtschaftlich, ressourcenschonend und risikoarm sicherzustellen. Durch die verstärkte Transformation in die Cloud gehen viele Unternehmen umfassend zum Cloud-Servicemodell „SaaS" über. Nun kommen tatsächlich einige Manager in Versuchung, eine Annahme zu treffen, dass doch aufgrund der Abrechnungsmodelle keine SAM-Überwachung mehr erforderlich wäre, da die Kontroll- und Nutzungsdaten doch eher von geringerem Wert sind. Die Realität hat sich aber mittlerweile als völlig gegenteilig erwiesen. Die SAM-Rolle ist jetzt besonders wichtig geworden, um eine „**verbrauchskonforme**" und nicht „**lizenzkonforme**" Nutzung sicherzustellen, damit der Cloud-Betrieb ressourcenschonend und mit weniger wirtschaftlichen und rechtlichen Risiken bereitgestellt werden kann.

24.4.1 Risiken zur Lizenzkonformität variieren

Mit der Transformation der IT-Assets in die Cloud-Modelle können die Risiken der herzustellenden lizenzkonformen Nutzung zwar verringert werden, aber dabei bleiben trotzdem noch Hauptrisiken zu beachten:

- Die lizenzkonforme „Verschiebung" bzw. das lizenzrechtlich saubere Inverkehrbringen der BYOL-Thematik in Public-Cloud Bereitstellungsumgebungen.
- Steuerung und Kontrolle von Zugriffsbeschränkungen, wie z. B. indirekte Zugriffe, Einschränkungen im Hybrid-Betrieb, Mengengerüste bzw. deren Beschränkungen der zugreifenden Geräte.
- Es sind (ähnlich wie bei der Oracle-Thematik) lizenzkostenpflichtige Funktionen in Mehrmandantenebenen (Shared-Umgebung) aktiviert oder diese sind für alle bereitgestellten Benutzer aktiviert, ohne auf die erforderlichen Lizenznachweise zu achten.

Das enorme Wachstum bei den Cloud-SaaS-Modellen (mit seinem Abrechnungsmodell) hat zu einer großen Verschiebung der bisherigen Auditaktivitäten geführt. Beispiele dafür sind u. a. Microsoft und Adobe, deren Umsätze sich in Bezug auf die SaaS-Transformation positiv

[20] cloudcomputing-insider.de – was ist ein Cloud Center of Excellence (CCoE)? – *https://www.cloudcomputing-insider.de/was-ist-ein-cloud-center-of-excellence-ccoe-a-949894/*

entwickelt haben. Beide Hersteller reagieren darauf mit reduzierten Auditaktivitäten – Adobe sogar noch viel umfassender als Microsoft, wenn Sie sich noch einmal die Rangliste in der Tabelle 24.1 anschauen.

Obwohl eine Transformation und Migration hin zum „SaaS"-Modell die Risiken zur Nutzung von unlizenzierten Softwareprodukten vermindert, bleiben komplexe Probleme bestehen. Eine Reduzierung der Auditaktivitäten bedeutet aber nicht, dass SAM-Life-Cycle-Prozesse, -Tools und -Rollen bei Verwendung von „SaaS"-Modellen und entsprechender Abrechnung nicht mehr erforderlich wären. Es muss trotz der vereinfachten Kontrolle der Lizenzkonformität immer noch die Einhaltung der Einschränkungen von „SaaS"-Nutzungsrechten sichergestellt werden. Als Vergleich dazu könnte man in diesem Zusammenhang das Thema „indirekter Zugriff" von SAP anführen. Werden diese nicht ausreichend gesteuert und überwacht, können z. B. Microsofts indirekte Zugriffsregeln erhöhte Haftungs- und Lizenzkosten nach sich ziehen. Vor allem deshalb ist es nach wie vor wichtig, die Integration des Cloud-Services-Managements in die SAM-Life-Cycle-Prozesse voranzutreiben, um damit die Einhaltung komplexer BYOL-Nutzungsrechte lizenzkonform zu steuern und zu überwachen.

Bedingt durch die Motivation der Hersteller, ihren „On-Premises"-Kunden die Cloud-Umgebungen und -Modelle ausreichend schmackhaft zu machen, werden entsprechende Lizenzprogramme aufgelegt, um diese Migrationsszenarien kostenattraktiv abzubilden. Dadurch sind zur Nutzung in Public-Cloud-Umgebungen unbefristete Lizenzen regelmäßig verfügbar, unterliegen jedoch genauso einer lizenzrechtlich detaillierten Bewertung, um Einschränkungen oder zusätzliche Lizenzanforderungen erkennen zu können. Werden im Vorfeld einer Migration mit BYOL-Lizenzen diese Parameter umfassend bewertet, können falsche Annahmen oder auch Erwartungshaltungen rechtzeitig behoben und das optimale Szenario mit den korrekten Optionen aufgezeigt werden.

Wenn ein Software-Audit im Zuge einer anstehenden Cloud-Migration durchgeführt wird, kann dadurch auch das Auditrisiko zunehmen.

Die Auditaktivitäten spiegelten schon immer die Umsätze der Softwarebranche. Aufgrund der erfolgreichen Transformation ihrer Softwareprodukte in die Cloud-Bereitstellungsmodelle reduzieren diese anschließend ihre Auditaktivitäten. Andersherum verstärkt das bei den Softwareherstellern – die mit der Transformation ihrer Produkte noch nicht soweit fortgeschritten sind – die Auditaktivitäten, um damit mögliche Defizite bei den Cloud-Umsätzen zu kompensieren. Für Unternehmen, die noch nicht so starke Ambitionen haben, in die Cloud-Welt zu wechseln und eher noch mit ihrem lokalen IT-Betrieb vorliebnehmen, kann das aber zur Folge haben, dass die Hersteller hier ihre Auditaktivitäten verstärken werden, um damit fehlende Cloud-Umsätze aufzufangen.

Ja, es wird weiterhin Software-Audits geben, aber Cloud-bedingt werden diese möglicherweise schwieriger durchzuführen sein und sehr viel Zeit und Konzentration einfordern (auf beiden Seiten). Das IT- und Software Asset Management wird in jedem Fall stärker an Bedeutung gewinnen, um diese komplette Betriebs- und Compliance-Thematik sicherstellen zu können. Das bedeutet für diese Unternehmen erst recht verstärkte Aufmerksamkeit auf ihre SAM-Strategie und auch ein SAM-Tool zu richten, damit hier entsprechende Transparenz und Sichtbarkeit erzeugt werden kann, wenn denn dann ein Ankündigungsschreiben auf dem Schreibtisch liegt. Mögliche Auslöser dazu stelle ich Ihnen im nächsten Abschnitt vor.

24.4.2 Audit-Auslöser

Sie sollten darauf achten, dass Ihr Unternehmen nicht von sich aus dem Hersteller Anlass bietet, ein Software-Audit durchzuführen. Hersteller können z. B. Anhaltspunkte für eine mögliche Unregelmäßigkeit in Ihren Lizenzbeständen gewinnen, wenn bei Supportanfragen durch den Lizenznehmer Widersprüche entstehen, also beispielsweise Supportanfragen gestellt werden, die nicht zu den vertraglich festgelegten Nutzungsbedingungen passen (z. B. bei der Klärung von IT-Architekturszenarien). Achten Sie auch darauf, was in Ihren Pressemitteilungen publiziert wird. Wenn Sie Meldungen verbreiten wie z. B.: „Als einer der größten Hersteller von ... haben wir mit einer Investition von über 50 Millionen Euro ein neues Rechenzentrum errichtet, welches mehr als 2500 weitere Anwender unterstützen kann.“, wird diese Meldung sicher nicht nur von den Aktionären gelesen. Vertriebsmitarbeiter der Softwarehersteller verwenden unter Umständen auch Informationen aus Gesprächen mit ihren Ansprechpartnern aus den Fachbereichen, um eventuelle Diskrepanzen aufzudecken. Diese Gefahrenstelle können Sie beseitigen, wenn die Fachabteilungen für die Evaluierung von Software keine Befugnisse erhalten, mit externen Herstellern oder Lieferanten allein zu verhandeln, sondern zumindest ein Mitarbeiter aus dem operativen SAM-Betrieb hinzugezogen werden muss.

Erhalten Sie – ohne einen für Sie erkennbaren oder nachvollziehbaren Grund – ein Ankündigungsschreiben zu einem geplanten Software-Audit, könnte es sein, dass Sie entweder wirklich nur zufällig ausgewählt wurden oder es sich um eine reine Routinekontrolle handelt. Ich habe aber auch schon die Situation erlebt, dass ein Service Provider auditiert wurde und anschließend der Auftraggeber des Service Providers gleich mit in den Auditring steigen musste, weil erhebliche Unregelmäßigkeiten festgestellt wurden. Dies hatte dann – wegen fehlender vertraglicher Vereinbarungen mit dem Service Provider für den korrekten Einsatz und die Nutzung der vom Auftraggeber beigestellten Softwareprodukte – erhebliche finanzielle Auswirkungen auf die Lizenzsituation des Auftraggebers (Nachlizenzierung) – Thematik Softwarebeistellungen in „Shared- bzw. dedizierten“ Umgebungen.

Es hängt sehr viel von den geprüften Unternehmen selbst ab, wie Sie ihre Beziehungen zu den Lieferanten oder Herstellern gestalten und ob ihnen eher ein laues Lüftchen oder eine starke Brise entgegenweht, wenn es um die Klärung festgestellter Sachverhalte geht. Versuchen Sie deswegen möglichst, ein ehrliches, von gegenseitigem Respekt getragenes Verhältnis zu den Mitarbeitenden der Softwarehersteller oder Lieferanten aufzubauen und zu unterhalten, um ein eventuelles Software-Audit mit fairen Ergebnissen für alle Beteiligten über die Bühne bringen zu können.

Umsatzsicherung durch Software-Audits

Umsätze zu steigern ist, denke ich, legitim. Softwarehersteller haben hierfür aber nicht nur ihre Vertriebseinheiten zur Verfügung, sondern können auch ihre Umsätze in Bezug auf Softwarelizenzen durch Prüfungen wie über ein Software-Audit steuern.

Schauen wir uns einmal ein paar mögliche Auslöser an, die ein Software-Audit begründen:

- *Starke und massive Verlagerung der Geschäftstätigkeiten in die Home-Office-Nutzung.* Durch die Corona-Pandemie bedingt und den damit einhergehenden gesetzlichen Anordnungen, wurden viele Unternehmen „kalt“ erwischt. Denn es mussten ja jetzt in ziemlich kurzer Zeit die IT-Infrastrukturen auf den „Home-Office“-Betrieb ausgerichtet und erweitert werden.

Problematisch ist dabei, dass sich nicht alle Softwareprodukte einfach so lizenzkonform „umschwenken“ lassen, sei es, dass dafür teilweise andere Lizenzmetriken erforderlich sind, beispielsweise erhöhte Anwender-Remote-Nutzung oder die RZ-Ressourcen (Datenbanken, Prozessoren – andere CPU-Metriken) erweitert werden müssen. All dies, kann in einigen Monaten mitunter eine Ursache sein, dass die Auditaktivitäten wieder anziehen werden, weil geprüft wird, ob die „Erweiterungen“ lizenzkonform durchgeführt wurden.

- *Ursprünglich geplante Investitionen werden verschoben, weil das Budget jetzt für die ungeplanten Ausgaben in Bezug auf die Pandemie verwendet werden müssen.* Aufgrund der unerwarteten Ausgaben im Zusammenhang mit der Pandemie verschieben einige Unternehmen ihre eigentlich geplanten Investitionen in die Zukunft oder sie versuchen, die Aufgabenstellungen mit Hilfe von Open-Source-Produkten zu lösen. Dadurch sehen die Softwarehersteller ihre Umsatzziele gefährdet und versuchen u. U., das mit Auditaktivitäten oder einer Aufforderung zu einem freiwilligen True-Up zu kompensieren.
- *Kunden verzögern oder setzen Vertragsverlängerungen aus.* Immer schon ein beliebter Auslöser für eine mögliche Auditaktivität ist, wenn Kunden ihre Wartungsverträge nicht rechtzeitig oder gar nicht verlängern. Die Softwarehersteller haben diese Umsätze nämlich über Jahre bereits in ihre Umsatzprognosen einkalkuliert. Brechen diese weg, ist das für die Softwarehersteller ein erhebliches finanzielles Risiko. So gilt oft die Maxime, die Supporteinnahmen auf jeden Fall sicherzustellen. Nicht umsonst gehen jetzt die Hersteller oftmals auf einen Re-Instate-Zeitraum von bis zu fünf Jahren, wo dann die Wartung „nachgezahlt“ werden muss.
- *Firmenein- und verkäufe.* Umorganisationen, Zusammenschlüsse, Veräußerungen, Stellenreduzierungen usw., es gibt viele Varianten, wie sich bisherige Softwarelizenznutzungen wandeln können. Meistens kennen die Softwarehersteller beide Seiten und wissen dann auch, wie es dabei um die Compliance-Situation bestellt ist. So können sie anhand eigener Unterlagen erkennen, dass die Softwareverträge nicht so ohne Weiteres zusammengeführt oder angepasst werden können. Dies ist oftmals auch ein erhebliches Risiko, welches beim Verkauf oder Erwerb eines Unternehmens vorher unbedingt zu bewerten gilt. Häufig folgt dann aus diesen Umständen heraus auch recht bald ein Software-Audit.

Um einen plausiblen Anlass für ein Audit zu schaffen (das UrhG kennt kein verdachtsunabhängiges Auditrecht), greifen die Hersteller unter anderem auch auf diese mittlerweile sehr einfach verfügbaren Informationen zurück und gleichen diese mit anderen Daten, beispielsweise aus den herstellereigenen Online-Portalen (Microsoft: „Volume Licensing Service Center (VLSC)“, IBM: „IBM Passport Advantage Online“), ab. Ergeben sich hier Unstimmigkeiten und entsteht der Verdacht einer unlizenzierten Nutzung, wird schon einmal ein freundlicher Brief an den Kunden verschickt, mit der Aufforderung, eine Selbstauskunft (Lizenzbilanz) einzureichen. Unternehmen, die diesen Brief erhalten und sich bis dahin nicht viel um das Thema Softwareasset- und Lizenzmanagement gekümmert haben, werden dann nicht nur einige schlaflose Nächte vor sich haben, sondern auch sehr viel zu tun bekommen. Wird dann das Audit durchgeführt, weil gewisse Umstände seitens des Herstellers dafürsprechen, kann sich dieses über mehrere Wochen oder Monate hinziehen, es bindet in dieser Zeit mindestens eine Vollzeitarbeitskraft und verschlingt noch etliches an weiteren personellen Ressourcen, die u. U. von den einzubindenden Fachbereichen geleistet werden müssen. Umso wichtiger ist es für Sie, sich rechtzeitig bei Bekanntwerden der Audit-Gegebenheiten eine Auditstrategie aufzubauen.

24.5 Auditstrategie festlegen

Mit einer halbwegs guten und strategisch wirksamen Auditverteidigungsstrategie können Sie u. U. erhebliche Erkenntnisse sammeln und Sie sind nicht allein auf die bereitgestellten Informationen des Auditors angewiesen. Viel schlimmer wäre es noch, wenn Sie diesem nichts entgegenzusetzen hätten und alles „glauben" müssen.

1. **Lassen Sie sich extern unterstützen.** Sie sollten sich nicht allein (vor allem nicht ohne Strategie und unvorbereitet) in die Auditsituation begeben, engagieren Sie einen externen, unabhängigen Dienstleister oder ein Rechtsanwaltsbüro, welches sich auf solche Services spezialisiert hat.
2. **Auditanfrage auf Rechtskonformität prüfen.** Prüfen Sie das eingegangene Schreiben, ob es sich hierbei um ein offizielles Herstellerschreiben mit Bezugnahme auf eine anlassbezogene Situation (beispielsweise eine Compliance-Aktion von Oracle License Management Services (LMS)) handelt, oder ob es ein „Angebot" eines Kundenbetreuers, Wiederverkäufers oder Beraters ist, der ein „freundliches Angebot" für eine Lizenzüberprüfung vorlegt. In so einem Fall besteht nämlich keine Verpflichtung, dieser Aufforderungen bzw. Anfrage nachzukommen. Es ist also wichtig zu prüfen und festzustellen, ob durch die Anfrage eine rechtliche Wirksamkeit begründet ist und ob Sie verpflichtet sind, dieser Aufforderung nachzukommen.
3. **Ermitteln der vertraglichen Verpflichtungen zur Einhaltung.** Überprüfen Sie ihre vertraglichen Vereinbarungen in Bezug auf die Anfrage, um festzustellen, ob Sie vertraglich verpflichtet sind, auf diese Auditanfrage zu reagieren. Insbesondere sollten Sie den Prüfungszeitraum und Prüfungsgegenstand umfassend gegenprüfen, falls dieser dem eigentlichen Wortlaut im Vertragsabschluss nicht entsprechen sollte. Zudem ist zu überlegen, ob Sie nicht vielleicht noch einen wirksamen „Schutzzeitraum" in Anspruch nehmen können, weil Sie erst vor kurzem eine Migration durchgeführt haben und sich noch gar nicht alles wieder im produktiven IT-Betrieb befindet.

   Interne Arbeitsgruppe und Stakeholder festlegen, Vorgehensweise abstimmen. Zur Begleitung der Durchführung des Audits sind die verantwortlichen Rollen und Personen zu benennen. Binden Sie das SAM-Betriebsteam und das Lizenzmanagement sowie die entsprechenden Produktverantwortlichen mit ein, schaffen Sie einen Single Point of Contact, über den sowohl intern als auch nach extern (zum Auditor) kommuniziert wird, und zwar **ausschließlich** über diesen SPOC, quasi der „Pressesprecher" zum Software-Audit (siehe auch Abschnitt 24.5.2 „Auditverhaltensregeln – Checkliste"). Stimmen Sie mit Ihrer Arbeitsgruppe – und dem ggf. einzubindenden externen Dienstleister – die Auditstrategie umfassend ab.
4. **Erhalt der Anfrage bestätigen.** Mit dem Vorliegen des Ankündigungsschreibens (siehe Abschnitt 24.6.1.1 „Das Ankündigungsschreiben") werden Sie gleichzeitig dazu aufgefordert, bis zu einem bestimmten Datum den Eingang des Schreibens zu bestätigen. Sie sollten hierbei so wenig wie möglich an „Zusatzinformationen" mit in das Antwortschreiben aufnehmen. Alles, was der Sache in diesem Moment nicht dienlich ist oder Sie eventuell belasten würde, sollte dort nicht aufgeführt sein. Also nur so viel wie nötig und nicht so viel wie möglich an Informationen bereits zu diesem Zeitpunkt preisgeben.

5. **Abklären des Prüfungsgegenstands und Zeitraums.** Verschaffen Sie sich Klarheit über den genauen Auditumfang, den Zeitrahmen und wer die Auditkosten zu tragen hat. Einige Hersteller übernehmen die Auditkosten der Auditoren, wenn die Diskrepanz an „unlizenzierter Software" einen bestimmten Prozentsatz nicht überschreitet. Bei Microsoft sind das ca. fünf Prozent. (Dies ist aber auch immer eine Ermessensfrage des Auditors und abhängig von der jeweiligen Prüfungssituation, es ist keine pauschal anwendbare Regelung.)
6. **Was im Vorfeld angesprochen werden sollte.** Die folgenden Punkte können Sie im Vorfeld ansprechen bzw. auch in das „Audit Execution Agreement" mit aufnehmen lassen, sofern der Hersteller bzw. Auditor auch damit einverstanden ist.

   Einige Dinge, die berücksichtigt werden sollten:

   i. Lassen Sie sich bei einer laut Herstellermeinung vorliegenden unlizenzierten Nutzung aufzeigen, wie sich diese ergeben hat.

   ii. Fordern Sie genaue Informationen zu den Dokumenten und Daten ab, die für den Prüfungsumfang erforderlich und bereitzustellen sind, und verschriftlichen Sie alle Angaben.

   iii. Klären Sie ab, ob eventuelle herstellereigene „Auditprogramme" erforderlich sind oder beispielsweise die Daten aus einem SAM-Tool ebenso qualifizierte Quellen darstellen (siehe auch Abschnitt 21.2.4.3 „Oracle: zusätzliche Optionen und Funktionspacks") und somit die Installation von herstellereigenen Detection-Software-Agenten obsolet sind. Auch hier wieder: Verschriftlichen Sie alles.

   iv. Sollte der angekündigte Prüfungszeitraum unpassend sein oder Sie noch zusätzliche Zeit für die Vorbereitung benötigen, bitten Sie um eine Verlängerung bzw. Verschiebung des Prüfungszeitraums.

   v. Falls es wie unter (iii) akzeptiert wurde, auch andere Quellen als Prüfungsgrundlage zu verwenden, könnten diese (bei ausreichender Qualität) geeignet sein, dem Hersteller die lizenzkonforme Nutzung aufzuzeigen, um somit ggf. das Audit einstellen zu können.

   vi. Sprechen Sie mögliche Rabattstaffeln an, falls eine Unterlizenzierung entstanden ist, um nicht die vollen Listenpreise (unabhängig vom Ausgang des Settlements) zahlen zu müssen. Wenn dem zugestimmt wird, verschriftlichen Sie das entsprechend.

   vii. Es gibt bei einigen Herstellern Verhandlungsspielraum, mögliche überzählige Softwarelizenzen auf Basis einer „Liste-zu-Liste" einzutauschen, um die festgestellte Unterlizenzierung anderer Softwareprodukte auszugleichen (Stichwort: License-Stacking).

   viii. Besprechen Sie im Vorfeld die Vorgehensweise und „Höhe" von Nachzahlungen mit einem möglichen Verzicht seitens des Herstellers auf „Reinstate"-Zahlungen für den Fall, dass Ihnen kein vorsätzliches oder grob fahrlässiges Fehlverhalten oder grobe Fahrlässigkeit vorgeworfen werden kann.

   ix. Bei unklaren Definitionen (was ist ein bestätigter Lizenznachweis?) vereinbaren Sie eine eineindeutige Formulierung, die den Einsatz, den Verbrauch und die Nutzungsrechte für eine Compliance-Sicht regeln, und einigen Sie sich auf entsprechend anzuwendende Kriterien.

   x. Vereinbaren Sie, dass nicht genutzte Softwareinstallationen als „lizenzkostenfrei" betrachtet werden und – für Sie unschädlich – aus dem Audit entfernt werden dürfen.

xi. Der Hersteller sollte Ihnen zusichern, dass Sie für den vorgelegten Abschlussbericht die Möglichkeit erhalten, darauf formell zu reagieren, um so für den Settlement-Bericht ein gemeinsames Ziel verfolgen zu können.

xii. Für den Fall, dass Unstimmigkeiten ausgeräumt werden müssen, bestimmen Sie zusammen die dafür erforderliche Vorgehensweise und den Prozessablauf mit vereinbarten Eskalationsstrecken und -personen.

xiii. Halten Sie schriftlich die Motive bzw. mögliche kommerzielle Interessen von eingesetzten Dritten (Auditor) fest, um möglichen Interessenskonflikten begegnen zu können und im Zweifelsfall darum zu bitten, einen unbefangenen Auditor einzusetzen.

xiv. Schlussendlich sprechen Sie die Möglichkeit einer vorausschauenden „No Audit"-Klausel an, damit Sie nach dem Audit eine gewisse Zeit eingeräumt bekommen, ihre SAM-Life-Cycle- und Betriebsprozesse zu optimieren, um in Zukunft ein stabileres Risikomanagement betreiben zu können.

7. **Richten Sie einen SPOC ein.** Alle beteiligten Personen und Rollen sind grundsätzlich durch den definierten SPOC über jede Kommunikation mit Hersteller bzw. Auditor zu informieren. Der Informationsfluss und -umfang ist dabei eng auf den Auditfall zu beschränken, sodass keine zusätzlichen Informationen freiwillig und vor allem – **nicht unabgestimmt** mit dem SPOC – weitergegeben werden, woraufhin der Hersteller einen Anlass bekommen könnte, den Prüfungsgegenstand und/oder Zeitraum zu erweitern.
8. **Beschaffungen für den Prüfungszeitraum untersagen.** Stellen Sie sicher, dass während des laufenden Software-Audits keine Softwarekäufe mit Bezug zum gerade auditierenden Softwarehersteller erfolgen. Das ist auch so gegenüber dem Hersteller zu kommunizieren.
9. **Abschlussbericht – Ergebnisse überprüfen.** Prüfen Sie den vorgelegten und bereits im Vorfeld abgestimmten Settlement-Bericht noch einmal dahingehend, dass dieser Ihnen vollständig zur Verfügung gestellt wird und zu allen erhobenen Lizenzansprüchen aufgrund etwaiger Lizenzdefizite die jeweiligen Details über den geprüften Softwarebestand enthält. Der Bericht sollte auch Aufstellungen zu den Berechnungen der geforderten Pönalen enthalten und gleichzeitig aufzeigen, dass eventuell vereinbarte ausgleichende Positionen darin enthalten sind (siehe Pkt. vii).

Um die festgelegte Auditstrategie entsprechend umzusetzen und damit diese auch von allen Beteiligten „gelebt" wird, sollten Sie auch einmal einen Blick auf die im Abschnitt 24.5.2 „Auditverhaltensregeln – Checkliste" empfohlenen Verhaltensregeln werfen. Betrachten wir zuvor im folgenden Abschnitt einen groben Auditprozessablauf, hier in diesem Fall für das angekündigte Software-Audit eines Herstellers.

24.5.1 Auditprozessablauf

Wohl dem, der im Fall der Fälle bereits auf einen Ablaufplan bzw. vielleicht sogar auf einen Auditprozessablauf zurückgreifen kann, damit gut vorbereitet ist und sich nicht erst jetzt Gedanken machen muss, wie ein geordneter Prozessablauf aussehen könnte. Von der Sache her sind die ablaufenden Phasen, Aufgaben, Aktivitäten mehr oder weniger immer gleich (bei allen Auditoren), da ja immer wieder ein bestimmter Ablauf eingehalten werden muss, um zu belastbaren Ergebnissen zu kommen, auf die sich dann beide Parteien berufen bzw. einigen können.

In Bild 24.1 habe ich Ihnen einen solchen „grob skizzierten“ Prozessablauf dargestellt. Ich habe auch schon sehr viel umfangreichere und noch viel detailliertere Auditprozess entwickelt, diese hier abzubilden würde allein schon mehrere Buchseiten füllen. Ich hoffe deshalb, dass Ihnen der hier aufgezeigte fürs Erste weiterhelfen wird. Los geht es immer mit dem Ankündigungsschreiben. Dazu finden Sie zwei Beispiele im Abschnitt 24.6.1.1 „Das Ankündigungsschreiben“. Falls die Standardfristen greifen und eingehalten werden sollten, können Sie davon ausgehen, dass nach ca. 30–45 Tage das Audit mit dem benannten Auditor beginnen wird (sofern nicht bestimmte Umstände dem entgegenstehen, weil der Auditor beispielsweise bei Ihnen auch die Bilanzen erstellt und deshalb „ausgetauscht“ werden muss). Im Bild 24.1 habe ich beide Ablaufstrecken visualisiert, denn nicht immer ist es erst ein angekündigtes Hersteller-Audit, das einen Auditprozess startet. Es kann gut sein, dass Ihr Management, Ihre Revision oder andere Stakeholder beispielsweise eine periodische Auskunft verlangen (Risiko managen) oder Vertragsprüfungen anstehen.

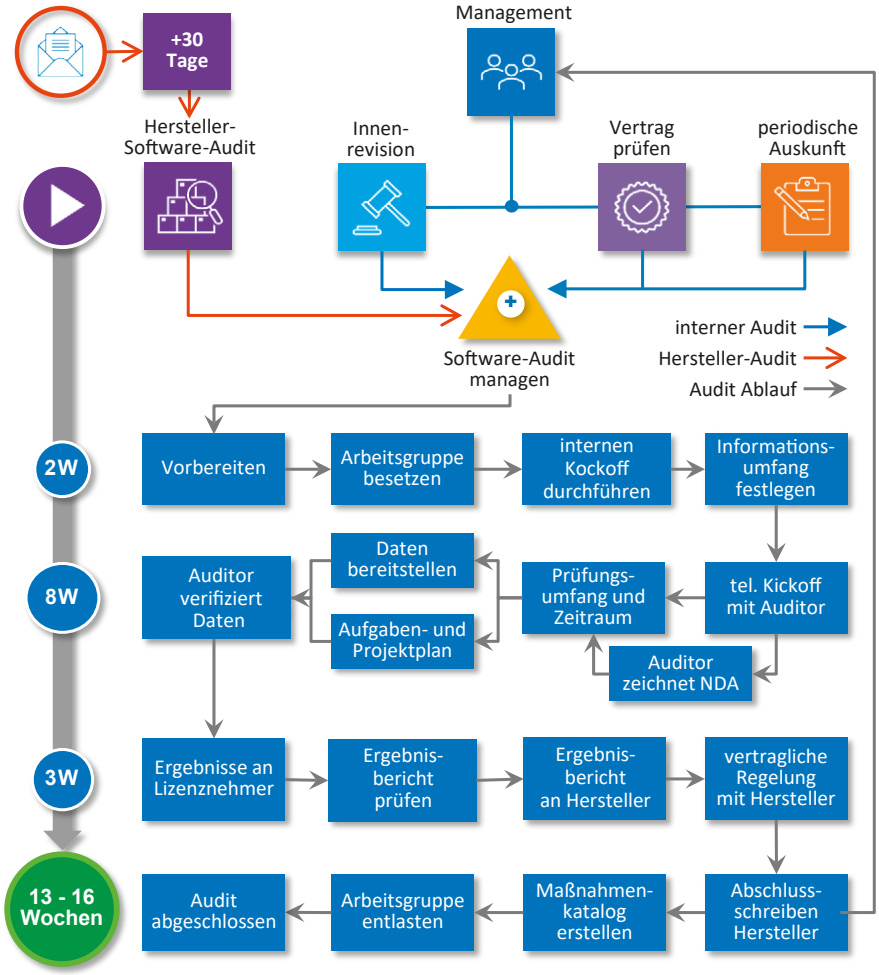

Bild 24.1 Grober Auditprozessablauf

Das wird dann meistens als „Friendly Audit“ oder auch schlicht als „internes Audit“ betitelt. Nach dem Ankündigungsschreiben und dem Fristablauf beginnt schließlich das Software-Audit. Die einzelnen Ablaufschritte können Sie der Grafik entnehmen. Nach ca. 13–16 Wochen sollte dann im Regelfall das gemeinsam verhandelte Ergebnis vorliegen. Es wird dann über einen Maßnahmenkatalog unternehmensintern weiter aufgearbeitet und die „Lesson learned“-Erkenntnisse sind entsprechend umzusetzen.

Zum Prozess gehören auch abgestimmte Verhaltensregeln, damit nur so viel wie nötig und so wenig wie möglich dem Auditor an Informationen herausgegeben wird. Oberste Maxime ist, damit äußerst sparsam umzugehen und keine Flur- bzw. lockere Kaffee-Kommunikation aufzubauen. Denken Sie daran, dass ein Auditor auch bestimmte Zielvorgaben bekommen hat und natürlich auch ein Interesse daran hat, so viele Informationen wie möglich – die seinen Zielvorgaben dienlich sein könnten – zu sammeln.

24.5.2 Auditverhaltensregeln – Checkliste

Das Thema Software-Audit ist so vielfältig und teilweise so individuell ausgeprägt, dass es mitunter schwerfällt, schon im Vorfeld zu wissen, wie man mit einem bevorstehenden Audit umgehen soll. Doch gerade in kleinen und mittelständischen Unternehmen fehlen oft die Ressourcen und das Know-how, um eine lizenzkonforme Nutzung der Softwareprodukte zu gewährleisten. Daher gibt es meist kaum Prozesse und Werkzeuge, die es ermöglichen, Softwarebestände ausreichend transparent zu verwalten, was für die Ankündigung und Durchführung eines Software-Audits die besten Voraussetzungen wären.

Übermitteln Sie allen Beteiligten diese grundlegenden Verhaltensregeln und stimmen Sie das ggf. auch noch enger mit Ihrer Arbeitsgruppe ab.

1. Ohne die verantwortlichen Ansprechpartner in Sachen Softwareasset- und Lizenzmanagement-Themen sind mit dem Auditor keine Termine zu vereinbaren.
2. Es werden keine Softwarelizenzen in einer Ad-hoc-Maßnahme beschafft, falls Kenntnis über eine evtl. Unterlizenzierung besteht. Diese Lizenzen sind nicht für das Audit anrechenbar (Stichtagsregelung) und verursachen nur unnötige Hektik und Kosten.
3. Der Zugang zu den IT-Systemen oder dem internen Netzwerk wird dem Auditor nur mit Genehmigung der Geschäftsführung erteilt.
4. Es werden keine schriftlichen oder mündlichen Aussagen, die den Auditfall betreffen, weitergegeben, wenn diese Informationen im Vorfeld nicht mit den verantwortlichen Ansprechpartnern im Unternehmen abgestimmt wurden.
5. Die Kommunikation mit dem Auditor ist auf den Auditfall zu beschränken, es sollten keine zusätzlichen Informationen freiwillig und vor allem nicht ohne Abstimmung mit den verantwortlichen Ansprechpartnern im Unternehmen weitergegeben werden.
6. Die Vor-Ort-Termine mit dem Auditor sind auf ein Minimum zu beschränken und immer im Vorfeld mit den verantwortlichen Ansprechpartnern abzusprechen und abzustimmen.
7. Alle Termine und Gespräche sind zu protokollieren und bei Nichtteilnahme des verantwortlichen Ansprechpartners im Unternehmen an diesen weiterzuleiten.
8. Dem vom Auditor vorgeschlagenen „Projektablaufzeitplan“ sollte nicht sofort Folge geleistet werden, das erzeugt Hektik und Druck und dadurch entstehen unnötige Fehler.

Der Ablaufzeitplan sollte in Ruhe studiert und mit dem eigenen internen Ablaufzeitplan abgeglichen werden.

9. Es sollten keine persönlichen Auskünfte oder Meinungen (z. B. zu bestehenden Prozessen, dem Qualitätsmanagement, der Qualität der angefragten Daten oder andere den Auditfall betreffende Informationen) ohne Abstimmung erteilt werden.
10. Es sind keine Vermutungen zum Sachverhalt zu äußern. Können Fragen nicht fundiert beantwortet werden, sind diese zurückzustellen und in gemeinsamer Absprache mit den verantwortlichen Ansprechpartnern abzuklären und zu beantworten.
11. Bei auftauchenden Unsicherheiten sollte immer eine Abstimmung mit den beteiligten Personen im Vorfeld erfolgen, bevor Informationen an den Auditor mündlich oder schriftlich übermittelt werden.

Hinweis

Im Verlauf eines Audits sollten immer nur ein oder maximal zwei Mitarbeiter aus Ihrem Unternehmen – sozusagen als offizielle Pressesprecher der Auditarbeitsgruppe – mit dem Prüfer bzw. dem Vertreter des Herstellers (meist der Key-Account-Vertrieb für Ihr Unternehmen) in Kontakt stehen. Diese verantwortliche Position sollte von der entsprechenden SAM-Rolle oder vom Management übernommen werden.

Kommen wir zum Abschnitt, wo ich Ihnen die üblichen Phasen eines Audits etwas näher beschreiben möchte.

24.6 Die Auditphasen

Die Hersteller lassen die vertraglich vereinbarte Einhaltung der Nutzungs- und Lizenzbedingungen prinzipiell von Wirtschaftsprüfungsgesellschaften wie z. B. KPMG AG (Schwerpunkt Microsoft) oder Deloitte & Touche GmbH (Schwerpunkt IBM) überprüfen und die Audits von dem jeweiligen verantwortlichen Vertriebsmitarbeiter begleiten. So steht oftmals bereits im Ankündigungsschreiben auch ein erster „Ablaufplan" – mit den wichtigsten Meilensteinen, wie nachfolgend beispielhaft zu lesen.

The key steps/stages of the compliance review are:

1. *Issue/Receipt of this notification letter.*
2. *Customer appoints a contact person within their organization and provides that person's contact information to „Auditor" within one week.*
3. *Agreement of inspection dates with „Auditor", and discussion of the information and records that will be required.*
4. *Collation, gathering and provision of the information and records needed (two weeks before inspection).*

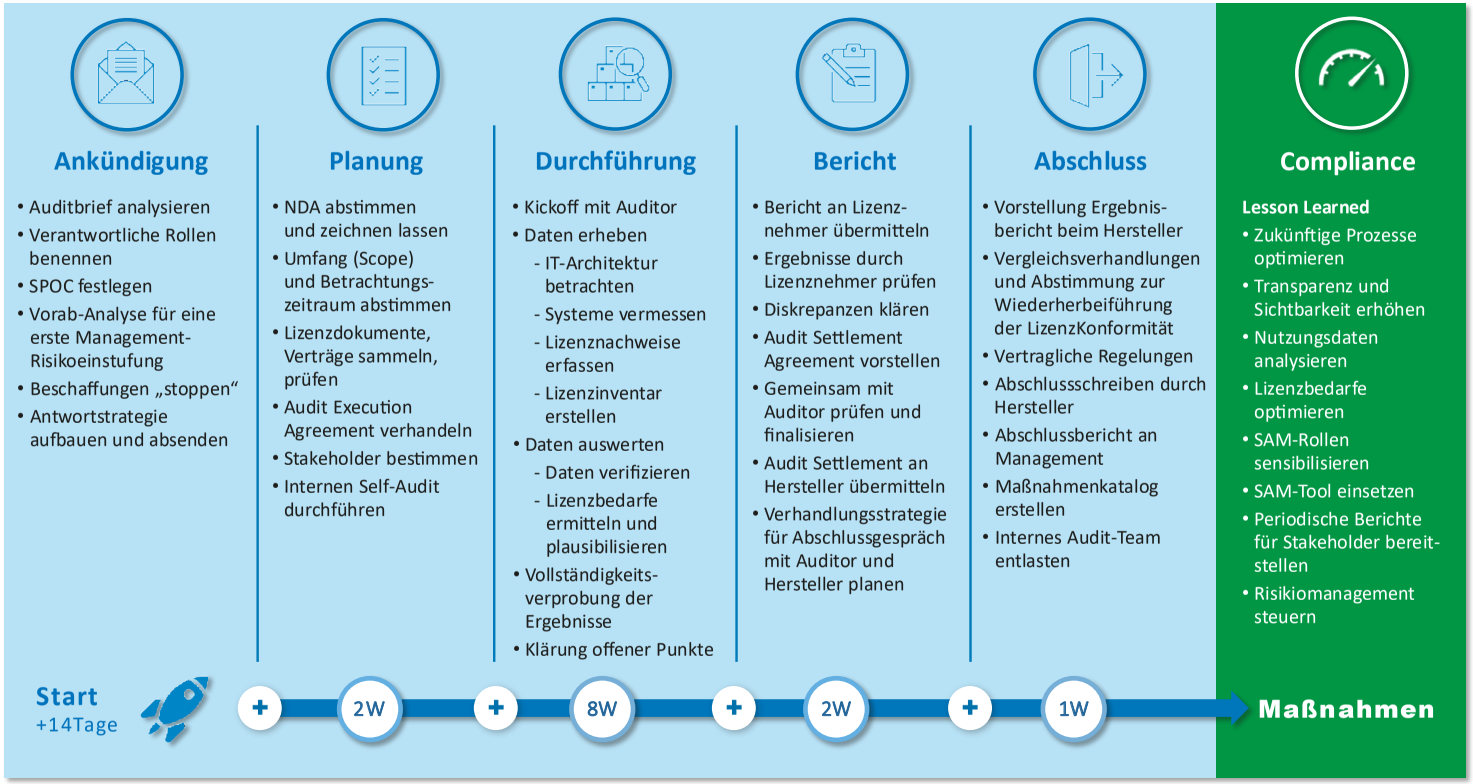

Bild 24.2 Übliche Standardauditphasen

5. *Performance of the inspection by „Auditor“ at your facility.*
6. *Review of the preliminary findings/report with „Auditor“.*
7. *Response by Unternehmen XYZ to those findings. Your response, if any, should be made within 10 days of completion of the inspection and should include all relevant supporting documentation.*
8. *Your review and discussion of the final inspection report.*
9. *Provision of the final inspection report to Microsoft by „Auditor“.*
10. *Settlement meeting, if required, to be arranged by Microsoft.*

Im Bild 24.2 habe ich es Ihnen etwas ausführlicher und verständlicher visualisiert.

Aus dem ganzen Ablaufszenario heraus ergeben sich verschiedene „motivierte“ Sichten zum Ablauf und zur Durchführung des Software-Audits, die Sie im gegenseitigen Gespräch abklären und positionieren sollten.

Auditor zu Kunde

- Ziele, Aufgaben
- Prüfungsumfang, Prüfungsgegenstand
- Zeitrahmen, Phasen, Ablauf, Dauer
- Auditsituation, Komplexitätstreiber

Kunde zu Auditor

- Aufgaben, Mitwirkungen
- Ansprechpartner intern, extern
- Prüfungszeitraum, Prüfungsumfang, Prüfungsbeginn
- Pflichten, Rechte

Das sind Anhaltspunkte, die Sie in einem ersten unverbindlichen Telefoninterview adressieren und abstimmen können. Sie sollten sich aber auch bewusst sein, dass Sie sich eine auf die mitgeteilten Rahmenparameter ausgerichtete Auditstrategie zurechtlegen, die Sie auch umsetzen sollten (so wie es in Abschnitt 24.5 „Auditstrategie festlegen“ bereits ausgeführt wurde). Ein Software-Audit wird immer zuerst mit einem Ankündigungsschreiben angezeigt und leitet damit die Phase „Ankündigung“ ein.

24.6.1 Phase Ankündigung

Im Abschnitt 24.4.1 „Risiken zur Lizenzkonformität variieren“ sind einige Auslöser beschrieben, aus welchen Gründen ein Unternehmen ein Schreiben mit der Ankündigung eines Software-Audits mitunter erhalten kann. Das Schreiben erhalten die Unternehmen mit Bezug auf einen bestimmten zu klärenden Sachverhalt oder auf das vertraglich vereinbarte Auditrecht mit der schon genannten üblichen Ankündigungsfrist von 30 bis 45 Tagen. Spätestens jetzt sollten Sie Ihren Auditprozess aus der Schublade ziehen und „aktivieren“. Die erste Maßnahme wäre dann mal das Zusammenstellen Ihrer Arbeitsgruppe für das Audit.

24.6.1.1 Das Ankündigungsschreiben

Das vom Softwarehersteller – auch „Notification Letter" genannte – schriftlich übermittelte Schreiben besteht aus dem inhaltlichen Teil zur Sache, dem Prüfungsgegenstand und dem Prüfungszeitraum (wie bei einer Betriebsprüfung auch) und mehreren Appendizes (in der Regel mit rechtlichen Hinweisen). Im Schreiben bezieht sich der Hersteller entweder auf konkrete Anlässe, d. h. auf Anhaltspunkte, die aus seiner Sicht einen Lizenzverstoß begründen oder auf eine anlassunabhängige routinemäßige Überprüfung. Wie so ein Anschreiben für gewöhnlich aussieht, sehen Sie beispielhaft (auszugsweise) in den beiden folgenden Bildern (einmal IBM, einmal Microsoft).

Niederlassung München

Unternehmen Muster AG
Abt. Legal / Einkauf
Frau Muster
Hubertus-Strauch-Str. 4
51063 Köln

IBM Deutschland GmbH
Hollerithstraße 1
81829 München
Brief: Postfach 82 03 64
81803 München
Telefon 089 4504-0
***ibm.com**/de*

Eingang

München. 18.02.2016

IBM Softwarelizenzprüfung

Sehr geehrte Frau Muster

wir haben das Unternehmen Muster AG, Köln bereits in 2013 für eine Softwarelizenzprüfung ausgewählt. Eine Kopie des diesbezüglichen Ankündigungsschreibens an Herrn Müller Abt. Legal finden Sie beigefügt.

Prüfungsaktivitäten konnten bis zum heutigen Tag jedoch aus verschiedenen Gründen nur sehr eingeschränkt stattfinden. Mittlerweile haben sich in Ihrem Haus auch die Zuständigkeiten und damit auch unsere Ansprechpartner geändert bzw. haben Ihr Haus mittlerweile verlassen. In Abstimmung mit Herrn Stephanio schreiben ich Sie deshalb an, um den richtigen Ansprechpartner zu finden.

Im nächsten Schritt würden wir Ihnen gerne in einem persönlichen Gespräch aufzeigen, wie die Prüfung ablaufen soll und in welcher Form wir auf Besonderheiten in Ihrem Haus eingehen können. Zur Durchführung der eigentlichen Prüfung hat die IBM die KPMG Wirtschaftsprüfungsgesellschaft AG beauftragt.

Ich feue mich darauf von Ihnen zu hören.

Mit freundlichen Grüßen

Oftmals wird in dem Ankündigungsschreiben auch eine „Möglichkeit" seitens des Herstellers unterbreitet (gesetzt den Fall, man hat eine transparente Sicht auf seine IT-Assets), falls man denn schon weiß, dass man – möglicherweise und überhaupt – unterlizenziert ist, dies doch bitte mitteile. Ein solcher Passus im Schreiben könnte wie folgt lauten:

> *„Sollten Ihrem Unternehmen möglicherweise Abweichungen in der Softwarenutzung bekannt sein, die Sie gerne noch vor Beginn der Lizenzprüfung beheben möchten, helfen wir Ihnen dabei gerne. Benachrichtigen Sie in diesem Fall bitte Herrn Steffen Mustermann (Hersteller). Alle vorab bekannten Abweichungen erforderlicher Lizenzen und zugehöriger Subscriptions sowie Support-Leistungen sind ausschließlich direkt über „Hersteller" zu beziehen.*

Das dazugehörige „Bestellformular“ wird dann natürlich gleich mitgeliefert und ist in etwa so aufgebaut:

Selbstauskunft an die Hersteller Deutschland GmbH

Von Firma (vollständige Firmenbezeichnung):

+ Adresse

Hiermit bestätige(n) ich/wir Folgendes:

Die angefügte Anlage 1 stellt eine Liste von Produkten dar, die wir bereit sind, von „Hersteller“ zu erwerben, um den „Hersteller“-Lizenzbedingungen umfänglich zu entsprechen. Wir haben realisiert, dass die aktuelle Nutzung der aufgeführten Produkte innerhalb unserer Organisation die vorhandenen Nutzungsrechte übersteigt.

Wir garantieren, diese Lizenzdifferenz mittels Direktbestellung bei „Hersteller“ unverzüglich auszugleichen.

_____

Name, Vorname, Titel

_____

Unterschrift, Datum, Ort

Anlage 1

Menge	*Produktnummer und Beschreibung*	*Site*

In den meisten Fällen – falls so etwas von einem zu prüfenden Unternehmen genutzt werden sollte, wovon ich aber abrate, weil es eigentlich einem Offenbarungseid gleichkommt – sind die Zahlungen in einem extrem kurzen Zeitraum (**unverzüglich**) zu leisten und garantieren Ihnen nicht, dass a) das Audit damit beendet wird und dass b) dann nicht doch noch Weiteres „entdeckt“ wird, weil Sie das eventuell aufgrund von Transparenzproblemen so nicht auf dem Plan hatten. Nachfolgend ein Beispielschreiben von Microsoft Ireland an das „ausgewählte“ Unternehmen.

Microsoft Ireland Operations Ltd.
One Microsoft Place
South County Business Park
Leopardstown
Dublin 18

Microsoft

10 January 2020

RE: Compliance review of Software Services provided under Microsoft Business and Services Agreement: U0 including, but not limited to, any Microsoft Services Provider License Agreements (SPLA) for the period from 10th June 2016 (06/10/2016) to the end of the last reporting month prior to the date of inspection.

Dear Uwe ;

Please be advised that we have selected for a formal license compliance review as provisioned for within the terms of the audit clause in the Microsoft Business and Service Agreement. These reviews are managed by the License and Contract Compliance group within Microsoft EOC and are initiated on a regular basis in an effort to help our customers to achieve and maintain license compliance.

U. a. enthält das Schreiben von Microsoft dann Informationen wie die hier zitierten Auszüge:

Mit diesem Schreiben teilen wir Ihnen mit, dass wir beabsichtigen, innerhalb von dreißig (30) Tagen ein Audit durchzuführen, um zu überprüfen, ob das Unternehmen XYZ die Bedingungen der oben genannten Vereinbarung(en) einhält.

Und teilt auch meistens gleich den beauftragten Auditor mit:

It will be performed by an independent, internationally recognized Certified Public Accounting firm. We have selected „Auditor" to perform the audit. „Auditor" is bound by the terms of the confidentiality provision (Section 3) (see Appendix C) of the Microsoft Business and Services Agreement and, therefore, will treat your confidential information with confidence and according to such provision within the scope of its mission.

A representative of „Auditor" will contact you shortly to schedule the audit and discuss the information and records that Unternehmen XYZ will be required to supply. Please provide all supporting documentation and data for „Auditors" review.

In einem ersten zu vereinbarenden Telefoninterview mit dem „Auditor" können dann die organisatorischen Maßnahmen erörtert werden, die für den Beginn erforderlich sind.

Die vier W-Fragen (wann, wer, was und wie), die Sie sich stellen sollten:

- Wann soll das Audit beginnen und über welchem Zeitraum (kalendarische Sicht) ablaufen?
- Wer ist daran beteiligt? Die Ansprechpartner sind für beide Seiten zu benennen.
- Was ist der genaue Prüfungsgegenstand und Umfang, also welche Softwareprodukte oder Systeme sollen Bestandteil der Prüfung sein und worauf bezieht sich der Hersteller (auf den im Betreff aufgeführten Softwarevertrag oder eventuell auf gesetzliche Regelungen)?
- Wie wird der Auditprozess durchgeführt, Remote, per Fragebogen, Excel-Dateien, vor Ort usw.?

Sollte es zu berechtigten Ansprüchen des Herstellers gegenüber Ihrem Unternehmen (dem Lizenznehmer) kommen, sollten Sie folgende Aspekte kennen:

Die Ansprüche nach §§ 97ff UrhG richten sich nicht nur gegen den Vertragspartner, vielmehr kann jeder, der die Software rechtswidrig einsetzt und verwendet, Anspruchsgegner werden. Hierfür wurde in § 100 UrhG die Haftung teilweise erweitert:

- Tochter- und verbundene Unternehmen
- Dienstleister (Service Provider, Outsourcer); hier haftet das Unternehmen auch für die korrekte Nutzung der beigestellten Software beim Dienstleister.
- Haftung des Unternehmens, seiner Organe und der Mitarbeiter
- Bei rechtswidrigem Einsatz von Software haftet grundsätzlich das Unternehmen selbst. Im Rahmen der sogenannten Organhaftung haftet das Unternehmen auch für seine Organe (Geschäftsführung). Eine fahrlässige Handlung besteht beispielsweise, wenn es keine geeigneten Arbeitsanweisungen gibt, um die Einhaltung der Lizenzbestimmungen sicherzustellen. Auch der Inhaber eines Unternehmens kann für Urheberrechtsverstöße, die seine Arbeitnehmer begehen, persönlich haftbar gemacht und im Falle eines Schadens zum Ersatz gegenüber der Gesellschaft verpflichtet werden (§§ 43 GmbHG, 93 AktG, 91 AktG). Als Voraussetzung gilt, dass die Urheberrechtsverstöße in enger Verbindung mit einer nach außen hin dienstlichen Tätigkeit des Arbeitnehmers stehen müssen. Wenn beispielsweise der Arbeitnehmer in seiner Tätigkeit als Administrator unlizenzierte Software verteilt oder zum Einsatz bringt, kann diese Voraussetzung bereits erfüllt sein.

Selbstverständlich kann auch jeder andere Mitarbeiter zur Verantwortung gezogen werden, der selbst wissentlich oder unwissentlich Urheberrechtsverletzungen begeht oder sich an solchen beteiligt, also z. B. eine unrechtmäßige Kopie auf ein IT-System aufspielt oder anderen zur Anfertigung von unrechtmäßigen Kopien Originaldatenträger zur Verfügung stellt bzw. Downloadquellen & Lizenzkeys unberechtigterweise weitergibt.

24.6.1.2 Audit Defense – wie viel ist möglich?

Hinweis: Das Audit können Sie nicht verhindern, eventuell aber den Start des Prüfungsbeginns steuern, um etwas mehr Zeit zu erhalten.

- Kontrollieren Sie das Schreiben, ob Prüfungsgegenstand (Bezug auf den richtigen Vertrag bzw. auch Standort), -zeitraum und -umfang stimmen.
- Prüfen Sie, ob die beauftragte Wirtschaftsprüfungsgesellschaft nicht eventuell bereits bei Ihnen im Unternehmen zu anderen Themen agiert, denn wenn dem so ist, muss ein anderer Prüfer vom Hersteller beauftragt werden. (Oft sind hier Deloitte und KPMG die Hauptakteure bei den Herstelleraudits, aber auch oftmals gleichzeitig bei den Unternehmen als Wirtschaftsprüfer unterwegs.)
- Erfordert der Prüfungsgegenstand Besichtigungen bzw. Stichproben auf DSGVO-relevanten Systemen oder vielleicht auch auf Systemen mit erhöhtem Sicherheitslevel? Dann sollten Sie die Personen bitten, hierfür entsprechende Nachweise bzw. Einstufungen vorzulegen. Das könnte etwas Zeitaufschub bedeuten, bis diese Unterlagen vorliegen.
- Klären Sie mit den einzubindenden Fachbereichen und Rollen ab, inwieweit das Audit den operativen Betrieb beeinträchtigen könnte und welche Auswirkungen damit verbunden sind, ggf. sind dann mit dem Auditor andere Prüfprozesse oder Vorgehensweisen abstimmen.

Empfehlung:

Zögern Sie aber bitte nicht den angesetzten Prüfungsbeginn unendlich hinaus. Ich hatte mal eine Kundensituation, wo der eigentliche Auditstart fast zwei Jahre „verzögert" wurde. Die Konsequenz: Der Hersteller hat dann die üblichen drei Jahre „Rück"-Betrachtung und Nachzahlung auf fünf Jahre erweitert (rechtlich in Ordnung laut den AGBs). Hier hat man sich also mit einer übermäßigen Verzögerungstaktik letztendlich keinen Gefallen erwiesen und der „erkämpfte" Zeitgewinn wurde dann auch nicht so genutzt, dass den Prüfungen mit entsprechend transparenten Daten begegnet werden konnte.

Das ist nur ein Auszug von Aspekten, die einen möglichen zeitlichen Beginn etwas „strecken" könnten, um sich intern besser für das anstehende Audit vorbereiten zu können. Ein möglicher weiterer Zeitgewinn lässt sich erreichen, wenn das eigentlich übliche Standard „Non disclosure agreement (NDA)" aufgrund vielfältiger Aspekte bzw. Argumente kundenspezifisch angepasst werden muss, weil beispielsweise auf Systeme in Hochsicherheits-RZs zugegriffen werden soll, wofür der eingesetzte Auditor eventuell erst eine entsprechende Sicherheitsstufe bzw. -freigabe benötigt. Das dauert in den meisten Fällen mindestens ein paar Wochen und es ist nicht gesagt, ob die Person des Auditors dann auch diese Einstufung erhält. Wie eine Standard-Vertraulichkeitsvereinbarung aufgebaut ist, lesen Sie im Abschnitt 24.6.3.2 „Vertraulichkeitsvereinbarung (NDA)". Kommen wir zur Phase „Planung".

24.6.2 Phase Planung

Das Ankündigungsschreiben ist eingegangen und wurde von Ihnen bestätigt. Sie haben auch schon den ersten telefonischen Kontakt mit dem Auditor gehabt. In dem Telefonat wurde Ihnen dann wahrscheinlich bereits das Datum für das Kick-off-Meeting bekanntgegeben, welches ca. 30–45 Tage nach dem Eingang des Schreibens terminiert sein sollte. Jetzt heißt es für Sie, die nächsten Schritte anzugehen und das Audit intern mit Ihrer Arbeitsgruppe zu planen. Stellen Sie als Erstes die erforderliche Arbeitsgruppe zusammen und bestimmen Sie weitere Stakeholder, die sich aus den folgenden Rollen zusammensetzen sollten:

- Mitarbeitende aus den jeweiligen Fachbereichen, die diese Softwareprodukte oder Systeme, auf denen diese Softwareprodukte im Einsatz sind, verantworten
- Verantwortliche SAM-Rollen, wie z. B. Strategischer bzw. Operativer Lizenzmanager, Produktverantwortlicher
- Leiter Einkauf
- Innenrevision
- IT-Sicherheitsbeauftragter
- Datenschutzbeauftragter
- optional Geheimschutzbeauftragter
- Personalrat, Betriebsrat, weitere Gremien-Rollen

Im Anschluss daran, sollten Sie sich Gedanken über einen groben Projektplan und Zeitrahmen machen, der ja auch für Ihre internen Mitarbeitenden wichtig ist, damit diese Ressourcen rechtzeitig in das laufende operative Tagesgeschäft eingeplant werden können. Es kann Ihnen versichert sein, das wird Sie als Projektleiter/-in mehrere Wochen in Vollzeit beschäftigen und den anderen auch erhebliche zeitliche Ressourcen abfordern.

24.6.3 Im Vorfeld zu erledigen

In dem ersten telefonischen Vorabgespräch mit dem Auditor haben Sie sich bereits über einige grundlegende Dinge abgestimmt. Mit diesen Informationen können Sie beginnen, den groben Projektplan aufzustellen.

24.6.3.1 Groben Projektplan aufstellen

Im Projektplan sollten wenigsten die nachfolgend aufgeführten Aufgaben und Aktivitäten aufgenommen und beplant werden. Wenn Sie sich beispielsweise mit Microsoft Project auskennen, können Sie über die Vorgänger-/Nachfolgerfunktion einen kritischen Pfad aufbauen.

Ganz wichtig: Es wird IMMER vergessen, dass die einzubeziehenden Personen z. B. im Urlaub sind oder eine wichtige Projektarbeit keinen Aufschub duldet. Also bitte mit möglichst entsprechenden Pufferzeiten planen und auch Feiertage berücksichtigen.

Projektplan Software-Audit Herstellername

- Kickoff-Telefoninterview mit benanntem externen Auditor durchführen
- NDA-Erfordernis absprechen und ggf. die dafür erforderlichen organisatorischen Aktivitäten starten

- Projektplan erstellen, Aufgaben festlegen
- Stakeholder/Management/einzubindende Fachbereichsleiter informieren
- Erforderliche Arbeitsgruppe besetzen
- Internen Audit-Kickoff vorbereiten
- Umfang der zu liefernden Informationen bestimmen
- Prüfungsumfang und Zeitraum festlegen
- Unterlagen für Selbstauskunft vorbereiten
- Projektplan mit interner Arbeitsgruppe abstimmen und finalisieren
- Wenn erforderlich, Sicherheitsüberprüfung für Auditor und weitere einzubindende Dritte (z. B. externe Berater) durchführen
- Bei NDA-Erfordernis, „Non disclosure agreement (NDA)“ an Auditor und externe Dritte versenden, Rücklauf auf Rechtmäßigkeit prüfen (siehe im Bild 24.2 „Übliche Standardauditphasen“ in Abschnitt „Phase Planung“)
- Abstimmung Kickoff-Rahmenbedingungen und Termin mit Auditor
- Kickoff mit Auditor planen und durchführen
- Datenbereitstellung durch Fachbereiche
  - technische Daten bereitstellen mit IT-Architekturplänen, Meldelisten zu Verbräuchen usw.
  - kaufmännische Daten bereitstellen (Lizenzdokumente, -nachweise, Softwareverträge)
- Organisation der Freigabe (und erlaubter Weitergabe an den Auditor) der bereitgestellten Daten
- Begleitung der externen Lizenzprüfung und deren Dokumentation (Protokolle schreiben, alles zum Auditablauf Gesagte verschriftlichen!)
- Berichte, Ergebnisse besprechen
- Ergebnispräsentation durchführen
- Vorabinfo der Ergebnisse an Stakeholder
- Audit Settlement Agreement vom Auditor vorstellen lassen
- Diskrepanzen klären
- Gemeinsam mit Auditor prüfen und finalisieren
- Audit Settlement wird vom Auditor an Hersteller übermittelt
- Verhandlungsstrategie für Abschlussgespräch mit Auditor und Hersteller planen
- Vorstellung Ergebnisbericht beim Hersteller
- Vergleichsverhandlungen und Abstimmung zur Wiederherbeiführung der Lizenzkonformität
- Vertragliche Regelungen mit Hersteller
- Abschlussschreiben durch Hersteller
- Abschlussbericht an Management
- Maßnahmenkatalog erstellen
- Interne Arbeitsgruppe entlasten

Im Projektplan haben Sie auch eine Aktivität aufgeführt, die lautet: „Bei NDA Erfordernis, NDA an Auditor und externe Dritte versenden, Rücklauf auf Rechtmäßigkeit prüfen." Diese Aktivität ist auch im Bild 24.1 „Grober Auditprozessablauf" zu sehen. Diese Aktivität müssen Sie aber nur durchführen, wenn es hierzu (entweder mit dem Wirtschaftsprüfer oder dem Dienstleister) noch keine eventuell schon im Vorfeld abgeschlossenen NDAs geben sollte bzw. noch zusätzliche benötigt werden, beispielsweise in Bezug auf Datenschutz, Sicherheitseinstufung usw. Im folgenden Abschnitt sind ein beispielhafter Aufbau und Wortlaut aufgeführt.

24.6.3.2 Vertraulichkeitsvereinbarung (NDA)

Vertraulichkeitsvereinbarung und Sicherheitsvereinbarung beim Auftraggeber für externe Partner (beispielhafte Vorlage)

Zwischen dem Auftraggeber und Auftragnehmer, vertreten durch die folgenden Personen:

Im Rahmen der Zusammenarbeit zwischen Auftraggeber und Auftragnehmer bezüglich des Auftrags einer Softwarelizenzprüfung werden folgende Vereinbarungen geschlossen:

Vertraulichkeitsvereinbarungen

1. Vertrauliche Informationen im Sinne dieser Vereinbarung sind:
   - Alle mündlichen oder schriftlichen Informationen und Materialien, die der Auftragnehmer direkt oder indirekt vom Auftraggeber zur Abwicklung des Auftrags erhält und als vertraulich gekennzeichnet sind oder die sich unmittelbar oder mittelbar auf den Auftraggeber beziehen oder deren Vertraulichkeit sich anderweitig aus ihrem Gegenstand oder sonstigen Umständen ergibt.
   - Die beauftragten Leistungen und sonstige Arbeitsergebnisse.
2. Der Auftragnehmer verpflichtet sich, alle ihm direkt oder indirekt zur Kenntnis gekommenen vertraulichen Informationen strikt vertraulich zu behandeln, nicht ohne vorherige schriftliche Zustimmung des Auftraggebers an Dritte weiterzugeben, zu verwerten oder zu verwenden.
3. Die Verpflichtung zur Vertraulichkeit gemäß Ziffer 2 gilt nicht für Informationen,
   - für die eine Verpflichtung zur Offenlegung der vertraulichen Informationen durch Beschluss eines Gerichts, Anordnung einer Behörde oder ein Gesetz besteht; oder
   - die öffentlich zugänglich sind oder werden; oder
   - von denen der Auftragnehmer bereits vor Abschluss dieser Vereinbarung in zulässiger Weise Kenntnis hatte; oder
   - die dem Auftragnehmer nach Abschluss dieser Vereinbarung bekannt geworden sind, ohne die Verpflichtung aus dieser Vereinbarung verletzt zu haben; oder
   - die von einem Dritten offengelegt werden, ohne dass dieser Dritte gegenüber dem Auftragnehmer diese Vereinbarung zur Verschwiegenheit verletzt hat.
4. Der Auftragnehmer ist für den Auftraggeber auch in anderen Vertragsverhältnissen tätig. Insbesondere ist er seit vielen Jahren mit der Erstellung des Jahresabschlusses betraut. Die Ausnahme zur Vertraulichkeit gemäß Ziffer 3 Spiegelstrich „3–5", gelten ausdrücklich nicht für solche vertraulichen Informationen, die der Auftragnehmer ausschließlich aus seiner Tätigkeit für den Auftraggeber als Wirtschaftsprüfer aus anderen Auftragsverhältnissen, insbesondere denen zur Erstellung der Jahresabschlüsse, erlangt hat oder erlangt („Vertrauliche Informationen aus anderen Vertragsverhältnissen").

5. Über Ziffer 3 hinaus ist der Auftragnehmer berechtigt, diejenigen Daten zugänglich zu machen, welche zur Plausibilisierung der Lizenzprüfung notwendigerweise offenbart werden müssen. Davon ausgenommen sind Daten gemäß Ziffer 4.
6. Der Auftragnehmer wird alle geeigneten Vorkehrungen treffen, um die Vertraulichkeit sicherzustellen. Vertrauliche Informationen werden nur an die Mitarbeiter oder sonstige Dritte weitergegeben, die sie aufgrund ihrer Tätigkeit erhalten müssen. Der Auftragnehmer wird sämtliche Mitarbeiter oder Dritte, die Vertrauliche Informationen erhalten, über Inhalt und Umfang der Rechte und Pflichten aus dieser Vereinbarung informieren. Der Auftragnehmer wird sicherstellen, dass diese die Bestimmungen dieser Vereinbarung einhalten und ebenfalls die vorliegende Vertraulichkeitsvereinbarung unterzeichnen, sofern sie nicht bereits arbeitsvertraglich vom Auftragnehmer entsprechend des beiliegenden Musters zur Vertraulichkeit verpflichtet worden sind.
7. Die Pflicht zur absoluten Vertraulichkeit dauert auch nach Beendigung der Zusammenarbeit an. Auf Verlangen sind ausgehändigte Unterlagen einschließlich aller davon angefertigten Kopien sowie Arbeitsunterlagen und -materialien zurückzugeben. Von der Verpflichtung zur Herausgabe bzw. Vernichtung oder Löschung ausgenommen sind lediglich solche Unterlagen bzw. Daten, zu deren Aufbewahrung der Auftragnehmer gemäß § 51b WPO (Wirtschaftsprüferordnung) gesetzlich oder berufsständisch verpflichtet ist, oder solcher, die im Rahmen automatisierter Datensicherung – auf die nur autorisiertes Personal Zugriff hat – kopiert und archiviert werden.
8. Der Auftragnehmer haftet für alle Schäden in vollem Umfang, die dem Auftraggeber durch Verletzung dieser vertraglichen Pflichten entstehen. Die Haftung für Schadenersatzansprüche jeder Art, mit Ausnahme von Schäden aus der Verletzung von Leben, Körper und Gesundheit, ist bei einem fahrlässig verursachten einzelnen Schadensfall gemäß § 54a Abs. 1 Nr. 2 WPO auf 4 Mio. Euro beschränkt. Jede Haftung für „Hersteller“ oder gegenüber Dritten schließen wir ausdrücklich aus.
9. Die Vertraulichkeitsvereinbarung gilt auch für Rechtsnachfolger der Parteien. Änderungen und Ergänzungen dieser Vereinbarung bedürfen der Schriftform.

Diese Vereinbarung unterliegt dem Deutschen Recht.

Auftraggeber: Datum,

Auftragnehmer: Datum,

<Ende Dokument>

Diese Vertraulichkeitsvereinbarung sollten Sie vor Beginn des Audits ausfertigen und zeichnen lassen, gemäß der in Bild 24.2 beschriebenen Phase „Planung“. In diesem Zusammenhang sollten Sie auch ein sogenanntes „Audit Excecution Agreement“ aufsetzen bzw. verhandeln, um gewisse Spielregeln abzustimmen und festzulegen.

24.6.3.3 Audit Execution Agreement

Mit dem Ankündigungsschreiben einhergehend bekommen Sie nicht nur Pflichten auferlegt, sondern Sie können auch Ihre berechtigten Interessen mit auf den Verhandlungstisch legen. Egal ob Sie eine individuelle Auditklausel vereinbaren oder eine Standardklausel vom Vertragspartner Verwendung findet, es sollten darin mindestens die folgenden Punkte zur Durchführung des Audits angesprochen werden:

- *Organisatorische Punkte*
  - Ablauf und Durchführung des Audits müssen zu den normalen Geschäftszeiten des Unternehmens erfolgen (die Zeiten sind zu vereinbaren).
  - Es sollte festgelegt werden, in welchem Umfang, zu welchem Zeitpunkt und in welcher Periodizität ein Audit stattfindet.
- *Inhaltliche Punkte*
  - Wenn der Hersteller im Vorfeld schon weiß, wen er als Auditor einsetzt, z. B. Wirtschaftsprüfer oder ein Unternehmen, das das Audit durchführt, sollte dies bekanntgegeben werden.
  - Wenn es um bestimmte zu prüfende Nutzungsvereinbarungen für ein bestimmtes Softwareprodukt oder eine bestimmte Lizenzmetrik geht, sollte der Prüfungsgegenstand darauf abgestimmt sein (z. B. die Einhaltung der korrekten Lizenzierung für CPU-basierte Metriken wird geprüft).
- *Juristische Punkte*
  - Es sollte festgehalten werden, dass keine personenbezogene Datenverarbeitung während des Audits stattfindet und nur Daten verarbeitet werden, die für die Prüfung der Einhaltung der Nutzungsbedingungen benötigt werden. Außerdem sollte die Wahrung der Betriebs- und Geschäftsgeheimnisse des zu prüfenden Unternehmens vereinbart sein (siehe Abschnitt 24.6.3.2 „Vertraulichkeitsvereinbarung (NDA)“).
  - Will der Auditor auf Ihren Systemen z. B. eine Batchdatei laufen lassen, um mit bestimmten Parametern die Einhaltung gewisser Lizenzregeln automatisiert zu überprüfen, sollten Sie sich auf alle Fälle eine Verpflichtung (laut neuer Regelung zum Datengeheimnis gemäß Art. 32 Abs. 4 DSGVO[21]) unterzeichnen lassen.
  - Wollen die Prüfer eventuell auch ein Auditprogramm installieren, sollten Sie sich unbedingt vergewissern, dass das Programm zertifiziert ist und wirklich nur die für die Lizenzprüfung notwendigen Parameter abfragt und verarbeitet.
  - Es sind Vereinbarungen und Maßnahmen zu beschreiben (unter rechtzeitiger Hinzuziehung des betrieblichen Datenschutzbeauftragten), um den Datenschutz und die Datensicherheit ausreichend zu gewährleisten, und die erzielten Auditergebnisse unterliegen der strikten Geheimhaltung.
  - Es ist schriftlich zu vereinbaren, dass die mit dem Audit beauftragten Personen bei einer erforderlichen Prüfung an oder in laufenden Produktionssystemen für etwaige Schäden und Performance-Probleme der IT-Umgebungen/-Systeme haften.
- *Kaufmännische Punkte*
  - Es ist festzulegen, wer die Kosten des Software-Audits trägt und unter welchen Prämissen (z. B. ob der Lizenznehmer die Kosten des Audits tragen muss, wenn ein bestimmter Schwellenwert bei einer festgestellten Unterlizenzierung überschritten wird?).
  - Vereinbart werden sollte auch, in welchem Zeitraum nach Bekanntgabe des Auditergebnisses die eventuell entstandenen Nachzahlungen für die nicht lizenzkonforme Nutzung der Software zu entrichten sind (üblicherweise 30 Tage).

[21] dejure.org – Art. 32 DSGVO Sicherheit der Verarbeitung – *https://dejure.org/gesetze/DSGVO/32.html*

- Es ist festzulegen, in welcher Weise eventuell fehlende Lizenzen nachgekauft werden müssen. (Anmerkung: Nicht unüblich sind dann Verrechnungen der zusätzlich zu erwerbenden Lizenzen mit marktüblichen Listenpreisen, also ohne die bestehenden Rabatte, und bei Lizenzen mit Wartung die zusätzliche rückwirkende Erhebung von Wartungsgebühren (Renewal) über einen Zeitraum von ein bis zwei Jahren.)

- *Sonstige Punkte:* In den Auditklauseln werden dann gerne noch Bestimmungen mit aufgenommen, die den Lizenznehmer dazu verpflichten, über vorgefertigte Formulare z. B. alle 30 Tage etwaige Veränderungen an Systemen oder IT-Szenarien zu melden (so etwas kommt beispielsweise bei IBM vor).

Auf alle Fälle sollten Sie den Auditpassus so verhandeln, dass die wirtschaftlichen und rechtlichen Interessen beider Seiten ausreichend gewahrt bleiben und Sie sich auch danach gegenseitig immer noch in die Augen schauen können.

Nachdem Sie den groben Projektplan erstellt und mit Ihrer Arbeitsgruppe abgestimmt haben, sollten Sie – bevor die offizielle Phase der Durchführung mit Datenerhebung und Plausibilisierung beginnt – sich mit einem internen „Testaudit" beschäftigen. So können Sie auch gleich feststellen, wie einfach oder komplex es werden wird, wenn der Auditor fordert, die zu prüfenden Daten und Informationen bereitzustellen.

24.6.4 Audit, internen Test planen

Sie haben ja bereits Kenntnis über die Sachlage (aus dem Ankündigungsschreiben) und können dementsprechend die erforderlichen Daten und Informationen „suchen" bzw. die zuständigen Fachbereiche dazu bereits ansprechen und auffordern, entsprechende Datensammlungen zu initiieren.

Versuchen Sie auch bereits jetzt schon Antworten für die folgenden Fragestellungen zu erhalten:

- Welche Dokumente und Unterlagen werden möglicherweise im Zusammenhang mit dem Auditgegenstand vom Auditor zur Herausgabe oder Einsichtnahme verlangt?
- Wenn u. U. Scripte zum Auslesen von Lizenzinformationen eingesetzt werden, sollte das im Vorfeld schon einmal geprüft werden, vor allem welche Informationen dabei „geloggt" werden.
- Prüfung, ob der Arbeitsgruppe die anzuwendenden Nutzungsbedingungen bekannt sind und diese verstanden werden. Nichts ist peinlicher, wie wenn während der Verifikation mit dem Auditor ein Mitarbeiter mit Halbwissen „glänzt" und eventuell dadurch dem Auditor zusätzliche Informationen preisgegeben werden, weil das Halbwissen vor dem Auditor „diskutiert" werden muss.
- Gibt es Gründe, ein spezielles Augenmerk auf Virtualisierungsinfrastrukturen zu legen?
- Gibt es möglicherweise Softwareinstallationen ohne Nutzung und könnten diese unverzüglich ohne betrieblichen Impact auch deinstalliert werden?
- Möglicherweise ist es bei Ihnen über Prozessabläufe oder eventuell sogar über ein SAM-Tool möglich, eigene Berichte für eine erste Abschätzung in Bezug auf eine Unter- oder Überlizenzierung durchzuführen.

24.6.5 Vorbereitung zur Phase Durchführung

Bevor der eigentliche Auditprozess mit dem Auditor startet, sollten Sie auch diese Punkte in Ihrer Arbeitsgruppe ansprechen:

- Sind die organisatorischen Aktivitäten für die Geheimschutz-Vereinbarungen mit dem Auditor umgesetzt worden?
- Sind noch andere geltende Datenschutzgesetze (z. B. Datenschutzverpflichtung nach Bundes- und Landesdatenschutzgesetz) einzuhalten?
- Gibt es eine Abschätzung zur möglichen Beeinträchtigung des operativen Betriebs im Unternehmen bezüglich der Durchführung der Lizenzprüfung?
- Ist es erforderlich, alle oder nur eine bestimmte Anzahl von Mitarbeitenden zu informieren, dass ein Audit durchgeführt wird?
- Wird ein Eskalations-Prozess benötigt, wer muss über eventuelle Beeinträchtigungen vorab informiert werden?
- Sind möglicherweise Kundensysteme durch die Lizenzprüfungen beeinträchtigt, sind deshalb die Kunden vorab, und wenn, wie lange „vorher“ mit entsprechenden Informationen zu versorgen?
- Wer steuert verantwortlich, dass auch nur tatsächlich der vereinbarte Prüfungsgegenstand in die Prüfung einbezogen wird? Stichwort: Begleitung und Überwachung der Auditoren.
- Wurde festgelegt, wer als Person bzw. Rolle die Aufgaben des SPOC in Richtung Auditor wahrnimmt.

24.6.5.1 Audit, interne Ziele festlegen

Zum Bestandteil einer Auditverteidigungsstrategie (Audit Defense) sollte gehören, sich über die eigenen „Verteidigungsziele“ und die möglichen Ziele des Auditors im Klaren zu sein.

Ziele des Auditors

Das Ziel eines Hersteller-Audits ist es, mit den beauftragten qualifizierten personellen (Auditoren) und technischen Ressourcen sicherzustellen, dass die abgeschlossenen Verträge und deren Bestimmungen lizenzkonform umgesetzt werden und es keine Formen von unlizenzierten Lizenzbedarfen gibt. Dazu gehört auch die Prüfung der Einhaltung von „Melde“-Verfahren (beispielsweise ILMT-Berichte periodisch übermitteln), Herstellerrichtlinien, anzuwendenden Standards und Regeln sowie beispielsweise auf lizenzkonformes Befolgen der Installationsanweisungen (z. B. Oracle Add-ons, die lizenzkostenpflichtig sein bzw. werden können).

Ziele des Kunden (Lizenznehmer)

Wie bei einer Bilanz bzw. Betriebsprüfung auch, haben die beteiligten Parteien meistens gegensätzliche Interessen und Ziele. Die eine Partei möchte beispielsweise mehr Geschäfte erzielen, die andere möchte vermeiden, wegen möglicher kleinerer Verfehlungen – vielleicht aus Unachtsamkeit oder aufgrund fehlender Kontrolle – diese teuer bezahlen zu müssen. Bei dieser Gemengelage sollte dann schlussendlich ein gemeinsamer Konsens gefunden werden.

Ich sage immer: leben und leben lassen. Also, ihr Ziel muss es sein, möglichst wenig bis gar keine Lizenzverfehlungen aufgezeigt zu bekommen, und wenn es welche geben sollte, die so „günstig“ wie möglich nachzuzahlen. An einigen Stellen kann u. U. mit Testsystembetrieb, „falsch“ deklariertes Hot- oder Cold-Stand-by-System oder auch Fehler bei der Durchführung von Migrationen versucht werden, mit dem Auditor ein gemeinsames Verständnis zu finden, wie solche Handicaps (kostenschonend) aufgelöst werden können. Oftmals ergibt sich auch – wie weiter oben schon im Abschnitt 24.5 „Auditstrategie festlegen“ im Punkt 7 (vii) beschrieben – eine Gelegenheit, um überlizenzierte Produkte über „Liste-zu-Liste“ mit „unterlizenzierten“ Produkten einzutauschen und damit das Budget für die möglichen Nachzahlungen zu schonen.

Um „Ihr“ Ziel erreichen zu können, müssen aber auch alle beteiligten Personen und Rollen über den Projektplan, die Auditstrategie, genau im Bilde sein und auch wissen, dass es nur einen SPOC geben kann, der mit dem Auditor kommuniziert, damit es eben nicht zu möglichen Situationen kommt, wo unbeabsichtigt der Auditor Informationen erhält, die das Auditergebnis in Ihrem Sinne negativ beeinflussen könnten. Das ist keine Aufforderung zur Verschleierung, sondern zu einem aufmerksamen und im Rahmen der bestehenden Möglichkeiten einzusetzenden Wissen, denn auch Auditoren können einmal danebenliegen und etwas vergessen oder nicht umfassend beachten, wie in dem folgenden Beispiel von mir in einer Kundensituation persönlich miterlebt.

Beispiel

Bei einem Microsoft-Audit eines Service Providers gab es den Fall, dass dieser es versäumt hatte, bei dem verpflichtenden Wechsel der monatlichen Meldungsform der Windows-Server-Lizenzierung von „pro Prozessor“ auf „pro Core“, diese monatlichen Meldungen dahingehend umzustellen. Es wurde weiterhin ordnungsgemäß „pro Prozessor“ gemeldet, man war aber eigentlich „unlizenziert“, weil ja nicht mehr das korrekt anzuwendende Lizenzmodell (gemäß SPLA-Vertrag) gemeldet wurde. Nun hatte aber im Audit der Auditor diesen Punkt so „abgestellt“, dass ab dem Zeitpunkt des Meldens von „pro Core“ eine unlizenzierte Nutzung erfolgte, obwohl ja weiterhin „pro Prozessor“ zur Abrechnung gemeldet wurde. Das Audit ging am Ende für den Service Provider gut aus, weil durch einen aufmerksamen Dritten festgestellt wurde, dass es bei der Berechnung der „fehlenden pro Core“-Lizenzen versäumt wurde, die bisherigen ordnungsgemäß (aus Sicht des Service Providers) gemeldeten „pro Prozessor“-Lizenzen, hier in die Auditabrechnung entsprechend einzubeziehen. Das wurde zwar erst einmal hin und her diskutiert, letztendlich hat aber dann Microsoft dem sogenannten „License Stacking“-Modell und dessen Anrechnung auf die Lizenzsituation zugestimmt. Das bedeutete, dass die bezahlten „pro Prozessor“-Lizenzen in „pro Core“ umgerechnet wurden und auf den Beginn der eigentlichen Umstellung angerechnet wurden – damit stand dann so gut wie keine Nachzahlung mehr zur Debatte. Wäre dieser Umstand nicht aufgefallen oder auch vom Kunden mit geprüft worden, hätten aus den so noch fälligen ca. 25.000 Euro Nachzahlung schnell ca. 225.000 Euro Nachzahlung werden können. Also, genau hinschauen, Experten einbinden, hinterfragen und im Zweifelsfall auch einmal etwas Basar spielen und verhandeln. Wir sind schließlich alle nur Menschen. Diesen Umstand, genau hinzuschauen und aufmerksam alles mitzuverfolgen und zu hinterfragen, sollten Sie dann auch in Ihrer aufgestellten Arbeitsgruppe thematisieren und den beteiligten Personen und Rollen in ihrem internen Kickoff mitteilen bzw. sie dahingehend sensibilisieren.

24.6.5.2 Agenda interner Audit-Kickoff

Für den internen Auftakt des anstehenden Software-Audits sollten Sie natürlich auch ein Kickoff durchführen, wo Sie schon einmal die wichtigsten Themen ansprechen, organisieren und abstimmen. Falls Sie bereits einen gültigen internen Auditprozess (siehe Bild 24.1) besitzen, haben Sie hierfür eine gute Orientierung, um die erforderlichen Aktivitäten zu beschreiben und zeitlich zu beplanen.

Eine mögliche inhaltliche (Best practise) Aufstellung der anzusprechenden Punkte finden Sie hier:

- **Ausgangsbasis:** Warum haben wir ein Software-Audit?
- **Aufgabe:** Schaffung eines gemeinsamen Verständnisses für das Software-Audit (Ziele, Inhalte, Zeitplan)
- **Arbeitsgruppe & Stakeholder:** einzubindende Personen & Fachbereiche
- **Kommunikation:** Kommunikationsregeln, Definition SPOC (intern & extern), Eskalationsstrecken
- **Planung und Organisation:** Rahmenbedingungen, Arbeitsmodus, Projekt- und Zeitplan abstimmen
- **Handlungsfelder:** Erheben der Daten (kaufmännisch, technisch)
- **Erwartungshaltung:** Abgleichen und Leitplanken festlegen
- **Software-Audit**: Verteidigungsstrategie, Einbindung externer Berater, sind Kunden einzubeziehen, Ergebnisse vom Auditor, Prüfung, Mediation
- **Abschlussgespräch mit Hersteller:** Ergebnisbericht, Kalkulation der Verbindlichkeiten, Vertragliches
- **Lessons learned:** kurz- und mittelfristige Aufgaben und Maßnahmen, Prozesse, Richtlinien, SAM-Tool, Verträge anpassen, IT-Architektur (Change Management), Produktportfolio optimieren, Produkte ausphasen etc.

Im Zuge Ihrer internen Kickoff-Veranstaltung sollte auch (damit beginnend) immer zu allen Aktivitäten ein Ergebnisprotokoll geführt werden. Dies erfolgt am besten durch jemanden, der a) immer in allen Meetings anwesend ist bzw. sein kann und b) auch dem „SPOC"-Team angehört (Sie erinnern sich, nur bestimmte festgelegte Personen sollten die Kommunikation nach innen und außen wahrnehmen).

24.6.5.3 Protokoll interner Audit-Kickoff

Tabelle 24.2 zeigt ein beispielhaftes auszugsweises Protokoll zu einem internen Kickoff eines anstehenden IBM-Audits.

Das avisierte Datum für den Beginn des Software-Audits ist erreicht und der Kickoff-Termin mit dem Auditor steht bald bevor. Damit beginnt jetzt für Ihre Arbeitsgruppe die Phase „Durchführung".

Tabelle 24.2 Beispiel eines internen Kickoff-Protokolls

Thema		Kickoff zum Software-Audit IBM	
Protokoll-Nr.:		1	
Datum/Ort:		4. April 201x/Geb. 1/R31	
Beginn/Ende:		9:00–10:15 Uhr	
erstellt von/am:		Sabine Lutz/01.04.201x	
lfd. Nr.	LG	Aussage	Verantwortlich/Termin
1.	I	*Vorstellung IBM-Audit* Frau Lutz berichtet den aktuellen Status der Vorbereitungen zum angekündigten IBM-Audit und stellt den internen Projektplan vor.	
2.		**Vorgehen und Mitwirkung**	
2.1	I	Im Kickoff-Termin mit dem Auditor wird der Prüfungsgegenstand und Prüfungsumfang konkret benannt und an alle beteiligten Personen übermittelt. Der bestehende Projektplan wird dann auf dieser Basis aktualisiert.	Herr Schneider
2.2	F	*Handlungsfelder* Die Abteilungen AF und ZG können die bestehende lizenzrechtliche Vertragssituation mit den RZ-Kunden nicht abschließend bewerten. Es wird darum gebeten, hier den Fachbereich DF mit einzubeziehen.	Herr Willig
3.	I	*Weitere Fachverfahren* Herr Schulz weist darauf hin, dass im Fachbereich OSE voraussichtlich ab 30.04. bzw. 30.06. ein produktives System ohne erforderliche Wartung im Betrieb sein wird und somit in den Auditprüfungszeitraum fällt.	Herr Schulz
4.	E	*Informationspflicht an unsere Kunden* Es wird geprüft, ob unsere Kunden darüber in Kenntnis zu setzen sind, dass ein Audit auf den bereitgestellten Systemen stattfinden wird.	Frau Wennige
4.1	F	*Dokumentation der IT-Architektur* Bezüglich der Bereitstellung von technischen Informationen (Aufstellung der IT-Architektur) wird es zu Terminschwierigkeiten kommen.	Herr Stollse
4.2	B	*Weitere Aktivitäten* Die Teilnehmer erhalten einen aktualisierten Zeitplan und den jeweiligen Prüfungsumfang nach dem 14.04. und werden um eine kurzfristige Rückmeldung zur Umsetzbarkeit ihrer Aufgaben gebeten.	Frau Lutz

Legende (LG): F = Feststellung, B = Beschluss, A = Auftrag, E = Empfehlung, S = Sonstiges, I = Information

24.6.6 Phase Durchführung

In dem Ankündigungsschreiben wird u. a. auch aufgeführt, dass der Hersteller regelmäßige Lizenzprüfungen durchführt, mit dem Ziel, die Nutzung und Installation der vorhandenen Software sowie die damit verbundenen Subscriptions und Supportleistungen gemäß den gültigen Lizenzbestimmungen festzustellen. Ebenso wissen Sie ja bereits, von wem (Hersteller) das Ankündigungsschreiben ist, und demzufolge auch, welche Softwareprodukte in die Prüfung einbezogen werden. Damit Sie dem Audit nicht ganz unvorbereitet gegenüberstehen, sollten Sie die Zeit bis zum angekündigten Prüfungsbeginn nutzen und versuchen, sich jetzt einen Überblick über die Sachlage zu verschaffen:

- Sichten Sie die vorhandenen Verträge und möglichen Informationen (wie z. B. E-Mails, Protokolle zu den Verhandlungen der Softwareverträge, wo eventuell weitere Absprachen oder Nebenabreden festgehalten wurden).
- Lassen Sie sich von den verantwortlichen Mitarbeitern eine aktuelle Aufstellung über die Hard- und Softwareumgebung geben, die die zu prüfenden Softwareprodukte betreffen. Sind User-gebundene Lizenzmetriken mit im Spiel, sollten Sie auch schon einmal die Fachbereiche ansprechen, die z. B. das Active Directory betrieblich verantworten, damit hier bereits eine Prüfung auf aktive/inaktive Benutzer erfolgen kann.
- Suchen Sie die für den Prüfungszeitraum (ab Ankündigungsschreiben zwei Jahre zurück) relevanten Lizenznachweise und -meldungen heraus (z. B. Microsoft True-Up-Meldungen oder bei IBM die ILMT-Berichte).
- Haben Sie bereits ein SAM-Tool im Einsatz, ziehen Sie sich dort schon einmal erste Berichte bzw. beginnen Sie mit einer umfassenden Aufstellung der Lizenzbedarfe und prüfen Sie schon einmal, ob die in den Verträgen vereinbarten Nutzungsbedingungen in Ihren IT-Szenarien richtig umgesetzt wurden (anhand der aktuellen Bebauungspläne Ihrer IT-Architektur).

Im ersten Zusammentreffen (dem Kickoff) werden organisatorische Aspekte geklärt und abgestimmt sowie u. a. der Prüfungsablauf und es werden dabei dann auch die Prüfungsdokumente vorgestellt und erläutert, die der Kunde in Form einer Selbstauskunft auszufüllen hat.

24.6.6.1 Kickoff mit Auditor

Als Erstes wird meistens noch einmal auf die Begriffsdefinition des Charakters der Prüfung hingewiesen.

Disclosure

Prüfungsumfang: „Hersteller“ nimmt das ihm vertraglich zustehende Prüfungsrecht aktuell in Form einer Plausibilisierung wahr. Der im Folgenden verwendete Begriff Prüfung steht daher nicht für eine vollumfängliche Prüfung im berufsrechtlichen Sinn nach der Wirtschaftsprüfungsordnung, sondern nur für eine eingeschränkte Überprüfung in Form einer Plausibilisierung.

Über die vom Auditor vorgelegte Agenda werden dann die Rahmenbedingungen und Prüfungsschritte vorgestellt und besprochen. Eine solche Agenda könnte die folgenden Punkte enthalten:

- Übersicht Hersteller-Lizenzprogramm
- Projektorganisation und Ablauf
- Betrachtungszeitraum
- Projektphasen erläutern
  - Planung (Prüfungsinhalte, Betrachtungsumfang, Vorgehensweisen)
  - Datenerhebung (Softwareinventar, Lizenzinventar, Lizenznachweise)
  - Auswertung (Übersicht der Lizenzbedarfe versus Lizenznachweise bzw. Meldungen)
  - Bericht (Entwurf, Abstimmung)
  - Abschluss (Settlement-Bericht mit Hersteller, Mediation, Auflösung der Diskrepanzen)
- Ansprechpartner, Kommunikationsfluss, SPOC, Eskalationsprozess
- Nächste Schritte

Weitere Hinweise des Auditors während des Kickoff-Termins sind beispielsweise die hier aufgeführten Aspekte, die Sie auch gewissenhaft mit in Ihren Protokollen vermerken sollten, denn diese Informationen bzw. die Kickoff-Dokumente zählen bereits mit zu den offiziellen Software-Audit-Unterlagen.

Hinweis 1: Kauf von Software während der Lizenzprüfung

Lizenzkäufe während der Lizenzprüfung (beginnend mit dem Ankündigungsschreiben bis zum Abschlussschreiben)	
Lizenzkauf für Neuprojekte oder für zukünftige Erweiterung bestehender IT-Umgebungen	Lizenzkauf zur Abdeckung einer bereits bei Beginn der Lizenzprüfung durch den Kunden intern identifizierten Unterlizenzierung
Sollte der Kunde Lizenzen für ein neues Projekt benötigen, wird „Hersteller" den Kauf unterstützen, jedoch werden die Lizenzen **nicht** in den für die Lizenzprüfung relevanten Lizenzbestand einbezogen. „Hersteller" bzw. der „Hersteller" Business-Partner, über den ein Auftrag abgewickelt wird, wird eine separate Klausel in den Angeboten, Bestellscheinen hierzu aufnehmen.	Ein solcher Auftrag sollte nach einer Besprechung mit Ihrem Hersteller Licensing Manager erfolgen, weiterhin sollte eine schriftliche Bestätigung des Sachverhalts erfolgen. Der Lizenzkauf wird in dem für die Lizenzprüfung relevanten Lizenzbestand berücksichtigt.

Hinweis 2: Betrachtungszeitraum der laufenden Lizenzprüfung

- Die eingesetzte Software muss zu jedem Zeitpunkt ausreichend lizenziert sein.
- Der Hersteller beschränkt die rückwirkende Betrachtung innerhalb dieser Prüfung auf zwei Jahre vor dem „Notification Letter".
- Der Betrachtungszeitraum der Prüfung erstreckt sich bis zum Auditor-Bericht an den Hersteller.
- Für jedes einzelne Produkt sollen sich Nutzungsdaten und Lizenzbestand auf den gleichen Zeitpunkt beziehen (Datum des Wartungsvertrags, unter dem die Software betrieben wird).
- Dieser Zeitpunkt kann für unterschiedliche Produkte variieren.

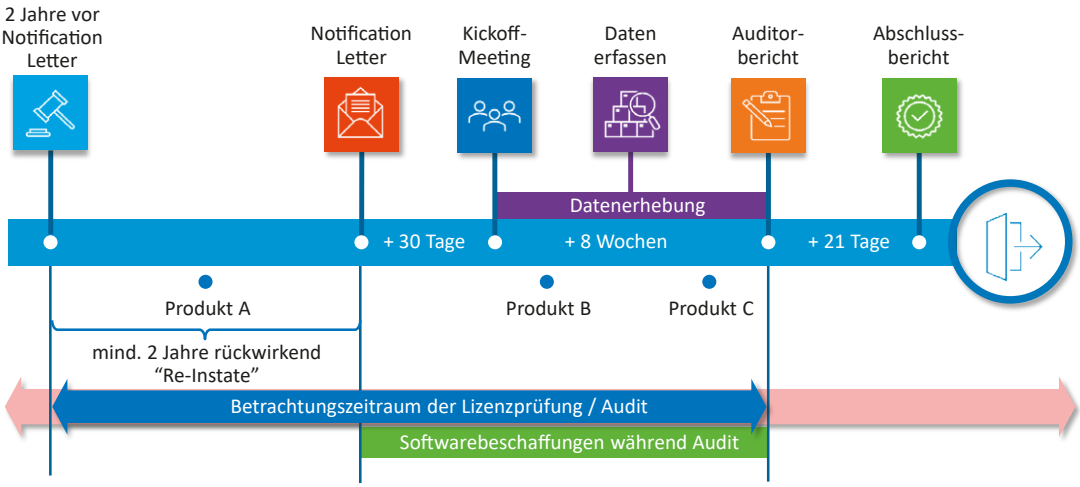

Bild 24.3 Zeitstrahl Betrachtungszeitraum bei einer IBM-Lizenzprüfung

Im Bild 24.3 habe ich einen Zeitstrahl mit dem Betrachtungszeitraum visualisiert, wie er typischerweise für IBM-Lizenzprüfungen angewendet wird. Lassen Sie sich aber bitte nicht „täuschen", denn die dort aufgezeigten „mind. zwei Jahre (rückwirkend) Re-Instate" können, wenn es wirklich „krachen" sollte, auch einmal fünf Jahre umfassen. Der Hersteller ist laut den Nutzungsbedingungen auch befugt dazu. Ich habe es bisher nur einmal erlebt, dass IBM hier bei einem Audit die Fünf-Jahres-Karte gezogen hat, ohne Einbeziehung vereinbarter Rabattstaffeln.

Nach dem ersten Kickoff und der damit verbundenen Vorstellung und Erläuterung der auszufüllenden Prüfungsdokumente liegt der Ball wieder im Spielfeld des Kunden. Dieser Abschnitt der Datenerhebung in der Phase „Durchführung" ist nicht nur vom Arbeitsaufwand her, sondern auch vom zeitlichen Aspekt (bis zu zwei Monate oder sogar noch mehr, je nach Komplexität) der umfangreichste im gesamten Prüfablauf.

24.6.6.2 Welche Informationen sind zu erheben?

Die zu erhebenden Daten von unterschiedlichen Herstellern sind von der Sache her gleich, allerdings unterscheiden sich u. a. die bereitgestellten Auditunterlagen. So haben z. B. KPMG und auch Deloitte ihre eigenen Templates und jeder verwendet für die Datenanalyse und Verifikation auch jeweils andere Prozesse im Hintergrund. Beide haben aber als Ziel, den Status der Lizenzkonformität im Namen der Hersteller zu ermitteln.

- **Beispiel Microsoft:** Der Auditor erstellt einen sogenannten Report mit dem Titel „ELP – Effective License Position", in dem folgende Daten erfasst werden:
  - Product Family, Version, Type of license, Licenses (MLS Volume Licenses, OEM Licenses, other), Preliminary License Entitlement, Deployments (Identified by Inventory Discovered Tool, Identified Manually), Total Software Deployment, Software Deployment vs. License Entitlement, License Allocation (+/-), (Downgrades, Upgrades, Virtualization, Parallel Installations, Training Licenses, Test Installations), Total License Allocation, Licensing Delta, Upgrade Licenses (Upgrade Licenses Quantity, Upgrade Licenses Quantity (w/Maintenance), Comments).

- Um diese Fülle an Informationen überhaupt auswerten zu können, werden Unterlagen und Informationen aus dem Volume Licensing Service Center (VLSC) mit Inhalten aus den aktuellen Select-, Open- und Enterprise-Agreement-(EA)-Verträgen und aus der Vergangenheit gesichtet (z. B. die erfolgten TrueUps während der Laufzeit). Falls diese Informationen ungenügend sein sollten, können weitere Unterlagen vom Kunden verlangt werden, z. B. die Lizenznachweise von Einzelhandelspaketen (FPPs) oder OEM- und System-Builder-Softwareprodukten (hier oft Betriebssysteme).

Soweit es mir bekannt ist, gibt es die Möglichkeit, wichtige Informationen für das ELP-Formular schon aus dem VLSC-Portal zu exportieren, sodass der Auditor oder der Kunde nicht ganz von vorne anfangen muss, um die Informationen in das ELP-Sheet einzutragen. Anschließend wird ein Abschlussbericht erstellt und an Microsoft weitergeleitet. Die weiteren Maßnahmen koordiniert dann ein Vertriebsmitarbeiter von Microsoft in Zusammenarbeit mit dem zuständigen Lieferanten.

- **Beispiel IBM:** Zur Erfassung der für die Prüfung notwendigen Informationen werden Excel-Formulare verwendet, bei Deloitte nennt es sich beispielsweise „IBM Customer Workbook“, hier werden alle zu erfassenden Daten zusammengeführt. Bei KPMG werden beispielsweise zwei Excel-Formulare „DR1“ und „DR2“ verwendet, in denen Daten vom Kunden erfasst werden und auf die ich in den folgenden Abschnitten beispielhaft eingehen werde.

Sicherlich müssen Sie für Ihre Vorbereitungen auch noch auf andere Bereiche zugehen, wie Einkauf, Recht, Finanzen oder eventuell sogar noch auf den Dienstleister, der Ihre Serverfarm betreibt. Achten Sie also darauf, die benötigten Informationen möglichst schnell und effizient aufbereitet zu erhalten. Wichtig ist dabei, dass Sie sämtliche Produktverantwortlichen und Ihre IT-Architekten mit den verantwortlichen Systembetreuern ins Boot holen. Nur sie können Ihnen eventuelle Szenarien richtig erläutern und darstellen und die verwendeten Lizenzmetriken erklären, um die Dokumente und Daten entsprechend „unschädlich“ auszufüllen.

24.6.6.2.1 Auditvorlagen – Beispiel IBM

Die Excel-Formulare sind in der Regel nach den folgenden Schemata aufgebaut.

Dokument I: Vertrags- und Produktinformationen

Registerblatt Produktnutzung

- **Übersicht**
  - Titel der Maßnahme, beispielsweise IBM-Lizenzprüfung, (Produktnutzung)
  - Beschreibung der Maßnahme
  - Kontaktdaten der Ansprechpartner des Auditors
  - Kundenname, der geprüft wird
- **1. Vorgabeliste für die Benennung der installierten Produkte**
  - Herstellername/Bezeichnung
  - Produktname

- Metrik
- Installiert (J/N)
- Kommentarspalte

- **2. Vorgabeliste für die Benennung weiterer installierter Produkte**
  Hier werden Produkte aufgelistet, die entweder einen anderen „Brand-Namen" bekommen haben, also irgendwann umbenannt wurden, wie beispielsweise Lotus Notes, was sich jetzt Collaboration Solutions nennt, oder „Advanced Information Management (ehem. WebSphere) oder „Cloud & Smart Infrastructure (ehem. Tivoli) etc.
- **2.1 Übersichtsliste weiterer sonstiger Produkte aus dem Herstellerproduktportfolio**
  Hier werden meistens noch weitere Produktnamen aufgeführt, die vom Hersteller (hier IBM als Beispiel) akquiriert wurden und demzufolge natürlich jetzt auch mit in den Prüfungsumfang einzubeziehen sind.

Registerblatt Verträge und Organisation

Unter dieser Registerkarte werden die Verträge bereits aufgelistet sein, die für die Prüfung und den Prüfungszeitraum relevant sind, beispielsweise Passport Advantage.

1. **IBM-Verträge (z. B. ESSO, IPAA, IPAA Express) sowie Verträge mit von IBM akquirierten Softwareherstellern.** Vertragstyp, Kundenname, Vertragsnummer, Site-Nummer, Kundennummer, Details

Also hier auch bitte schon einmal genau prüfen, ob die angegebenen Daten soweit stimmen. Sind Optionen zu betrachten, dass Sie beispielsweise die zu prüfenden Softwareprodukte wiederum ihren Kunden bereitstellen oder diese die Produkte von Ihnen (Ihr Unternehmen ist beispielsweise ein Service Provider) beziehen, müssen auch hierzu Angaben gemacht werden. Das nennt sich dann:

2. **Einzubeziehende Organisationen.** Organisation, Unternehmen (vollständige Firmierung), Ort, Land

In einem weiteren Dokument sind die Daten zur Software-Nutzungserhebung der installierten Softwareprodukte zu erfassen. Bleiben wir bei dem Beispiel mit IBM, wären in dieser Liste jetzt die folgenden Informationen zu erfassen:

Dokument II: Datenermittlung zur Softwarenutzung

Registerblatt Übersicht

„IBM führt zurzeit in Ihrem Haus eine Softwarelizenzprüfung durch. Bitte machen Sie auf den folgenden Blättern Angaben zu den Installationen und der Nutzung der aufgeführten IBM-Produkte (unabhängig davon, ob diese produktiv eingesetzt werden).

Die untenstehenden IBM-Produkte wurden von Ihnen als installiert angegeben. Falls Sie darüber hinaus weitere IBM-Produkte installiert haben, lassen Sie uns das bitte gesondert wissen."

- *Informix Enterprise Edition,*
- *Security QRadar Core Appliance XX05, Security QRadar SIEM All-in-One 31XX, Security QRadar SIEM All-in-One 31XX Failover,*
- *Spectrum Protect Suite Entry,*
- *WebSphere MQ*

Greifen wir beispielhaft das Produkt „**Informix**“ heraus.

- **Produktname aktuell:** Informix Enterprise Edition
- **D- und E-Partnr. (aktuell):** D0D1QLL (SKU[22]-Lizenz), E08SLLL (SKU-Wartung)
- **Produktname (alt):** Informix Dynamic Server Enterprise Edition Unlimited Users SubCapacity bzw. Informix Dynamic Server Enterprise Edition Unlimited Users
- **D- und E-Partnr. (alt):** D59M6LL, D55QQLL, E0323LL, E023HLL
- **Metrik:** Processor Value Unit

Das **Registerblatt für Informix** wäre wie folgt aufgebaut:

A. Angaben zum Produkteinsatz

A1. Bitte stellen Sie uns für jeden Server die angefragten Hardwareinformationen vollständig zur Verfügung und geben Sie in der Tabelle alle aktiven Informix-Server an.

- **Allgemeine Angaben:** Server-Name, Informix-Instanz-Name, eingesetzte Version, produktiv (J/N), Art des Servers (phys., virtuell), Standort des Servers
- **Angaben zum physischen Host:** Servermodell des physischen Hosts, Prozessorname und Modellnummer, Anzahl der belegten Prozessor-Sockets, Anzahl der Kerne pro Socket, Gesamtzahl der Prozessorkerne
- **Angaben zu virtuellen Servern:** Name des physischen Hosts, Anzahl der zugewiesenen vCPUs
- **Angaben zu Clustern:** Ist der physische Host Teil eines Clusters, Name des Clusters, Gesamtzahl der physischen Host-Server innerhalb des Clusters
- **Weitere Angaben, falls erforderlich (insbesondere begründen, falls keine Lizenzkostenpflicht besteht)**

Weitere Fragestellungen (am Beispiel des IBM-Templates), die es zu beantworten gilt:

A2. Stellen Sie uns die unten aufgelisteten Outputs/Screenshots für jeden Server zur Verfügung.

Hier kommen Kommandozeilen-Scripte zum Einsatz, die dann bestimmte Log-Daten auswerfen und per Screenshots zu dokumentieren sind.

B. Dokumentation des Produkteinsatzes

Bitte erstellen Sie einen Output oder Screenshot, aus welchem die eingesetzte Version/Edition der Software hervorgeht. Sollten Sie verschiedene Versionen der Software einsetzen, stellen Sie Screenshots aller eingesetzten Versionen zur Verfügung.

C. Sub-Capacity Reports

Bitte stellen Sie uns die Sub-Capacity Reports für die vergangenen vier Quartale zur Verfügung.

<Ende des Dokuments>

Sie haben mit ihrer Arbeitsgruppe die technischen Daten vor Ort oder über Remoteverbindungen (auf Server) erhoben sowie die erforderlichen zusätzlichen Informationen und Dokumente (wie z. B. Screenshots von Versionsständen, Sub Capacity-Reports) zusammengestellt und ebenso die erforderlichen kaufmännischen (beispielsweise Rechnungen) und

[22] SKU = Stock Keep Unit (eigentlich sollte es sich dabei um eine eineindeutige Nummer handeln, was aber oftmals nicht der Fall ist).

Lizenznachweisdokumente (beispielsweise Berichte aus dem Herstellerportal) und die damit zusammenhängenden Dokumente des Herstellers. Mit diesen Informationen wurden die Auditdokumente befüllt und an den Auditor zur weiteren Bearbeitung übermittelt, damit dieser jetzt „seine" Datenanalyse und Verifikation der von Ihnen zugesendeten Daten und übermittelten Informationen vornehmen kann.

Aufgaben des Auditors

Im nächsten Schritt sind die Unterlagen an den Auditor oder an die mit der Prüfung beauftragten Personen weitergeleitet. Basierend auf den von Ihnen übermittelten Daten und Informationen wird der Auditor die Dokumente einer ersten Überprüfung unterziehen und dazu auch die Informationen verwenden, die er zuvor vom Hersteller übermittelt bekommen hat. Das sind meistens Informationen und Zahlenmaterial über die abgeschlossenen Verträge und deren vereinbarte bzw. erworbene Stückzahlen. Die Auditoren verlassen sich aber nicht nur auf die Angaben des Prüflings, sondern recherchieren zusätzlich an bestimmten Punkten, wie z. B. die Anzahl der aktiven Mitarbeiter im Active Directory bzw. im Adressbuch vom Exchange-Server etc., um damit (meistens stichprobenartig) die Korrektheit der abgegebenen Zahlen und Informationen prüfen zu können. Ebenso lassen sie sich IT-Architekturpläne vorlegen oder gehen vor Ort in das Rechenzentrum, um bestimmte auf Papier angegebene Konstellationen zu überprüfen. Sie erinnern sich: Eine rechtswidrige Nutzung kann auch vorliegen, wenn das im Einsatz befindliche IT-Szenario nicht auf die erlaubten Nutzungsbedingungen der Software ausgerichtet ist (ein klassisches Problem bei Virtualisierungsumgebungen). Meisten ergeben sich (zwangsläufig) aber Situationen, wo es Klärungsbedarf bzw. Verständnisfragen geben wird. Hierfür sollten Sie sich mit dem Auditor abstimmen und den primären Kommunikationskanal und den Zeitraum/Zeitbedarf abstimmen, üblicherweise wird das über vereinbarte wöchentliche Jour fixe geregelt. Sind die ersten Ergebnisse erarbeitet, geht es in den nächsten Schritt, zur gemeinsamen Verifikation und Plausibilisierung der Daten. Hierfür wird üblicherweise auch ein Termin (meistens vor Ort) oder per Remote-Verbindungen anberaumt.

24.6.6.3 Datenanalyse und Verifikation

Oftmals wird eine Abdeckungsrate von 100 Prozent aller Maschinen im Betrachtungsumfang gefordert, die ggf. unter Zuhilfenahme von Scan-Agents, anderen Inventory-Quellen, ITSM-Tools, CMDBs oder über Software-Asset-Management-Tools bereitzustellen sind. Nicht nur, dass 100 Prozent im IT-Betrieb völlig utopisch sind, ist dieses Ansinnen auch rein ressourcentechnisch in der Kürze der Zeit nicht umsetzbar.

Weiterhin wird oftmals gefordert:

- Jegliche Lücken in der Abdeckung oder Datenlieferung müssen durch den Lizenznehmer geschlossen werden.
- Zusätzlich wird eine Plausibilisierung der Maschinen durch den Auditor bei einem Vor-Ort-Besuch durchgeführt.
- Ist kein SAM-Tool verfügbar, muss der Lizenznehmer Skripte, Befehle, Managementkonsolen etc. für die Datenerhebung verwenden und die Ergebnisse im Vor-Ort-Besuch aufzeigen.

Damit wären wir beim nächsten Schritt, dem Vor-Ort-Besuch. Das Ziel ist hierbei, eine Verifizierung der zuvor erhaltenen Informationen durchzuführen.

Der Termin umfasst meistens die folgenden Punkte:

- Über geführte Interviews mit den Produktverantwortlichen und Systemadministratoren wird ein allgemeines Verständnis zum Aufbau der IT-Infrastruktur mit den betriebenen Softwareprodukten und deren Nutzungen erarbeitet.
- Im nächsten Schritt werden die zuvor übersandten Daten am Live-System gegengeprüft.
- Im Fall von noch fehlenden oder unklaren Informationen werden diese jetzt noch erhoben und dokumentiert.
- Eventuell offene Punkte werden auf Basis der „neuen" Ergebnisse geklärt und es wird versucht, einen gemeinsamen Konsens zu erarbeiten.

Die Systemadministratoren des Kunden werden die Erhebung und Verifizierung der benötigten Installationsinformationen in Anwesenheit des Auditors eigenverantwortlich durchführen.

Lassen Sie uns nachfolgend einen Blick auf einen solchen „Vor-Ort-Termin" werfen und betrachten wir beispielhaft das zu diesem Termin erstellte Ergebnisprotokoll (in Auszügen).

lfd. Nr.	Aussage
1.	**Agenda zum Ablauf der Verifikation**
2.	**Verifikation der Daten**
2.1	Die Verifikation erfolgt mit Fragen und Systemprüfungen ▪ *Informix:* Auf allen Systemen wurden die Angaben zur Hardware und zu den eingesetzten Versionen von Informix zu den bereits in DR2 übersandten Daten gegengeprüft. Der Auditor erläutert die Sub-Capacity-Lizenzbedingungen und insbesondere die Anforderungen zum Einsatz des IBM License Metric Tools (ILMT). Der Auditor teilt mit, dass nach aktueller Lage von einer Full-Capacity-Lizenzierung ausgegangen werden muss. ▪ *Tivoli Storage Manager (Spectrum protect):* Es wurde seitens des Kunden die IT-Architektur und die Historie zum Einsatz der Software erläutert. Zur Auswertung der Speichervolumen werden auf den gemeldeten Systemen die Daten erhoben und mit anonymisierten Systemnamen in eine Excel-Tabelle überführt und an den Auditor zur weiteren Bearbeitung und Verifizierung übermittelt.
3.	**Vollständigkeitsverprobung**
	Erläuterung der Vorgehensweise zur Vollständigkeitsverprobung. a) Der Kunde stellt eine Serverliste bereit, um stichprobenartig Server zu prüfen, was aber abgelehnt wird, da dies im Vorfeld vertraglich nicht vereinbart wurde. b) Bereits benannte Systeme werden einer teilweisen Vollständigkeitsverprobung unterzogen. c) Vom Auditor wird geprüft, ob eine vom Kunden vorzulegende schriftliche Vollständigkeitserklärung über die Korrektheit der Serverliste ausreichend ist. Szenario b) wurde im Vor-Ort-Termin durchgeführt, Szenario c) ist vom Auditor noch abzuklären, es wird dazu eine Rückmeldung an den Kunden geben.

lfd. Nr.	Aussage
4.	**Weiteres Vorgehen zur Abstimmung des Ergebnisberichts**
	Nach Fertigstellung des vorläufigen Abschlussberichts wird in der KW 12 dem Kunden der Bericht vorgestellt und erläutert, in der KW 13 wird der Bericht dem Hersteller vorgestellt, der Kunde kann dazu Anmerkungen und Erläuterungen einbringen. In der KW 14 wird ein telefonischer Abstimmtermin zur Mediation zwischen Hersteller und Kunde vereinbart.
5.	**Nachtrag zum Termin**
5.1	*WebSphere MQ:* Zu diesem Sachverhalt gibt es aus Sicht des Auditors und der internen Qualitätssicherung keine Beanstandungen.
5.2	*Spectrum Protect Suite Entry (ehem. Tivoli Storage Manager Suite for Unified Recovery Entry):* Es werden zwei Windows Server mit der Entry-Version betrieben, beide Unix Server sind als Backup-Server klassifiziert und lizenzrechtlich abgedeckt. Systeme werden demnächst abgebaut, die gesicherten Datenvolumina sind weit unter Lizenznachweis in Höhe von 23 TB.
5.3	*Informix Dynamic Server Enterprise Edition Unlimited Users Sub Capacity.* Aussage Auditor: ILMT unterstützt bereits seit Ende 201x „HP-UX“ für eine Sub-Capacity-Überwachung. Somit hätten die manuellen Sub-Capacity-Meldungen durch einen ILMT-Bericht ersetzt werden müssen. Dadurch ist laut Auditor eine „Non-Compliance“-Situation entstanden. *Auditor ergänzt mit E-Mail vom 27.1x.1x:* Im Zuge der Befüllung der „DR2-Liste“ wurden die angeforderten manuellen Sub-Capacity-Berichte zur Verfügung gestellt und dadurch wurden die genutzten Sub-Capacity-Werte sauber dokumentiert. Mit der erfolgten regelmäßigen Übermittlung des Worksheets zum „Virtualization Environment – Group of Servers (Cluster)“ ist ein konkludentes Handeln vollzogen worden. Aus diesem Sachverhalt heraus hat der Kunde die angegebenen Nutzungsberechtigungswerte nicht überschritten.
5.4	*In der E-Mail vom 27.1x.1x wird außerdem darauf hingewiesen, dass die Protokollabschnitte, die die Sicht des Kunden darstellen und nicht vom Auditor kommentiert wurden, keine konkludente Bestätigung dieser Ansichten seitens des Auditors darstellen.*

In der Phase „Durchführung“, die sich unterteilt in „Datenerhebung“ und „Datenauswertung“, ist dann auch einmal der Zeitpunkt gekommen, wo Sie eine erste Version des Ergebnisberichts vom Auditor übermittelt bekommen, auch um darin dann ggf. Ihre Sicht der Dinge anzumerken. Es kann ja durchaus sein, dass bestimmte Situationen vom Kunden anders betrachtet bzw. interpretiert werden. Zur letztendlichen Konsensfindung mit dem Hersteller sollte das dann auch wahrgenommen werden, eventuell noch durch fachliche externe Expertise unterstützt.

24.6.7 Phase Bericht

Der Abschlussbericht des Auditors (z. B. unter dem Titel „Software-Plausibilisierungs-Settlement bei …“) stellt die Ergebnisse für den Hersteller zusammen. Darin wird für jedes geprüfte Softwareprodukt ein Steckbrief in der folgenden Form erstellt:

- Übersicht Lizenzbestand Ist/Soll des zu betrachtenden Softwareprodukts,
- Beschreibung der Situation, die dargestellte Kundensicht zu diesem Softwareprodukt,
- Prüfungsergebnis mit Darlegung der verwendeten Quellen, Daten, Zahlen und Anmerkungen,
- Pseudonymisierung der Daten (beispielsweise Servernamen) für den Hersteller durch den Auditor.

Im Folgenden eine kurze Darstellung eines pseudonymisierten „Abschlussberichts“ an den Hersteller und wie sich dieser aufbaut:

- **Deckblatt:** Berichtstitel, Kundenname
- **Inhaltsverzeichnis:** Zusammenfassung, Anlagen, Anhänge
- **Allgemeine Informationen:**
  - Rahmendaten der Lizenzprüfung, Kontaktdaten Hauptansprechpartner des Kunden, Einbezogene Unternehmen, Einbezogene Plattformen
  - Hinweis zum Bericht
    Beispieltext: *„Auditor hatte keine Möglichkeit, die Vollständigkeit der vom Lizenznehmer gemachten Angaben im Rahmen einer stichprobenhaften Plausibilisierung zu überprüfen. Stattdessen hat der Lizenznehmer eine Vollständigkeitserklärung bezüglich der IBM-Nutzungsangaben abgegeben.“*
  - Art der Durchführung
    Beispieltext: *„Der vorliegende Ergebnisbericht beruht auf den von Lizenznehmer bereitgestellten Informationen und dem dazu vorliegenden Sachstand im Rahmen der Plausibilisierung zum Einsatz der aufgeführten Softwareprodukte. Möglicherweise hätte die Vorlage weiterer Informationen zu einer anderen Darstellung geführt. Das Dokument ist nur für den internen Gebrauch des Lizenznehmers und Herstellers bestimmt und ist nicht zur Weitergabe an Dritte zugelassen. Die abschließende Berichterstattung erfolgt ausschließlich an den Hersteller. Gemäß Beauftragung wurden die vom Lizenznehmer übermittelten Daten über Interviews mit Mitarbeitern des Kunden plausibilisiert.“*
- **Quellenübersicht (der erhaltenen Daten vom Kunden):** Datenlieferung zur Produktnutzung, Datenlieferung mittels Auditor-Datenanfrage zur Softwarenutzung, Vor-Ort-Besuch, Datenlieferung im Nachgang zum Vor-Ort-Besuch
- **Nicht eingesetzte Produkte:** Aufstellung (in Listenform), welche der zu prüfenden Softwareprodukte beim Kunden nicht installiert sind
- **Lizenzstatus (zu den geprüften Softwareprodukten):** Produkt, Metrik, Lizenzbedarf, vorhandene Basislizenzen, Abweichung, aktive Wartung, Abweichung (Reinstatement), Produktnummer (SKU), Basislizenz Produktnummer (SKU), Reinstatement Produktnummer (SKU), Wartung Produktnummer (SKU)

- **Begriffsdefinitionen (Erläuterungen von verwendeten Schlüsselbegriffen):** Prozessorchip, Core, Socket, Aktiver Socket, Unbelegter Socket, Maximale Socketanzahl, Hyper-Threading, Processor Value Unit („PVU"), Host, Virtueller Server, Full-Capacity, Sub-Capacity, Sub-Capacity-Berichtsmethoden, ILMT

Haben die Auditoren die Überprüfung der Angaben abgeschlossen, wird das Prüfungsergebnis in einem Bericht festgehalten und zur abschließenden Validierung noch einmal an den Kunden übermittelt.

24.6.7.1 Validierung der Prüfergebnisse

Nicht nur rein hypothetisch, sondern tatsächlich ernst gemeint sind diese Fragestellungen hier, die es dabei zu beantworten bzw. zu berücksichtigen gilt:

- Plausibilitätsprüfung der übermittelten vorläufigen Prüfberichte, ob eine korrekte Zusammenführung und Interpretation der bereitgestellten Auditdokumente durch den Auditor erfolgten

  Diese sollten kritisch hinterfragt werden, denn unter Umständen gibt es einen Interpretationsspielraum bei der Bewertung der Ergebnisse (siehe dazu auch mein Praxisbeispiel zum Thema „License Stacking" im Abschnitt 24.6.5.1 „Audit, interne Ziele festlegen").
- Nochmaliges Einbeziehen und Sichten von aktuellen Verträgen und lizenzrechtlich relevanten Dokumenten und Unterlagen als Grundlage für die Beurteilung der Qualität und Stimmigkeit der vom Auditor ermittelten Ergebnisdaten.
- Schaffen eines gemeinsamen Verständnisses zum Ergebnis der Lizenzprüfung, um diese als einen definierten Ausgangspunkt für die nachfolgende Mediation mit dem Hersteller zu nutzen.

Bei größeren Diskrepanzen kann es durchaus vorkommen, dass das Auditverfahren nicht seinen gewohnten üblichen Standardverlauf nimmt, weil erhebliche erforderliche Rahmenbedingung für eine Plausibilisierung fehlen. Auch so etwas würde dann mit in dem Ergebnisbericht des Auditors aufgenommen werden, damit sich der Hersteller darüber selbst ein Bild machen kann. Beispielhaft könnte das sein:

- Die vom Kunden übermittelten Lizenzdaten können durch den Auditor nicht ausreichend schlüssig dargestellt werden (erforderliche Transparenz fehlt).
- Die originären Lizenznachweise liegen dem Auditor nicht im erforderlichen Umfang vor.
- Aufgrund der fehlenden Lizenznachweise ist eine historisierende Plausibilisierung von Basislizenzen zu den bestehenden Upgrade-Ketten nicht nachvollziehbar.
- Die vom Kunden übermittelten „Deployment"-Zahlen können seitens des Auditors nicht eindeutig zugeordnet und bestätigt werden.
- Das beim Kunden eingesetzte SAM-Tool konnte keine ausreichende Unterstützung bei der Analyse und Bewertung der Daten liefern.
- Aufgrund einer intransparenten Vorgehensweise zur Darstellung der IT-Architektur kann keine eindeutige Aussage für den lizenzkonformen Einsatz der zu prüfenden Softwareprodukte getroffen werden.

Spätestens in so einem Prüfszenario muss und sollte rechtzeitig mit dem Auditor zusammen das Gespräch mit dem Hersteller gesucht werden, um ggf. über Herstellerdokumente eine

„bessere“ Klärung der Lizenzierungssituation herbeiführen zu können. Dass das dann auch anderweitige Konsequenzen, nicht nur seitens des Herstellers gegenüber dem Kunden, nach sich zieht, denke ich, ist dann jedem bewusst. Denn es würde bedeuten, dass (wenn vorhanden) die bisherigen SAM-Rollen und -Prozesse sowie die damit verbundene Risikosteuerung mehr oder weniger komplett versagt haben.

Hinweis

Auch Wirtschaftsprüfer sind nicht vor Fehlern gefeit. Deswegen sollten Sie bei der Vorstellung der Abschlussprüfberichte die Zahlen genau kontrollieren und ggf. auch kritisch hinterfragen, wenn Sie gewisse Darstellungen nicht verstehen oder Ihnen diese nicht plausibel erscheinen.

Ziel der Validierung der Prüfergebnisse ist es, die getroffenen Absprachen und Sichten in den relevanten Punkten zu bestätigen und so die Übermittlung des Ergebnisberichts an den Hersteller vorzubereiten.

24.6.8 Phase Abschluss

Der mit dem Kunden abgestimmte Ergebnisbericht wird nun an den Hersteller übermittelt. Gleichzeitig wird dazu ein gemeinsamer Termin (Auditor, Kunde, Hersteller) vereinbart. An diesem Termin wird der Auditor dem Hersteller den Ergebnisbericht vorstellen und erläutern. Dabei werden u. a. auch die folgenden Aspekte betrachtet:

- Behandlung etwaiger Abweichungen
- Das vom Hersteller aufzubereitende Settlement wird auf der aktuellen Preisstaffel (Entitled Preis) des Lizenznehmers basieren.
- Hersteller berechnet Subscription und Support rückwirkend für 24 Monate. Diese Berechnung kann ggf. auf den tatsächlichen Installationszeitraum beschränkt werden, sofern die benötigte Dokumentation im Rahmen der Prüfung vorgelegt worden ist.

Aus diesem Termin heraus, mit den dort getroffenen Absprachen und Vereinbarungen, wird vom Hersteller der Abschlussbericht erstellt und in einem weiteren Termin, wo der Auditor nicht mehr mit anwesend sein wird, dem Lizenznehmer als Verhandlungsbasis vorgelegt.

24.6.8.1 Audit-Abschlussbericht an Lizenznehmer

Der Abschlussbericht des Herstellers an den Lizenznehmer kann ein umfangreicher Settlement-Bericht sein, beispielsweise in Form einer PowerPoint-Datei, aber auch schlicht und ergreifend nur ein Excel-Tabellenblatt, wo bereits die monetären Aspekte aufgestellt sind. Es kommt auch immer ein Stück weit darauf an, wie man in dem vorhergehenden Abstimmungstermin auseinandergegangen ist. Wenn nämlich bereits ein Konsens gefunden werden konnte, um die beiderseitigen Interessen zu wahren, wird der Abschlussbericht mehr oder weniger nur noch die Höhe der Pönalen enthalten. Diese können aber meistens auch noch einmal etwas „verhandelt“ werden, denn der Hersteller hat auch ein berechtigtes Interesse daran, dass seine Produkte weiterhin langfristig vom Lizenznehmer eingesetzt werden.

Ergebnispräsentation durch den Hersteller

- Hersteller erstellt den Abschlussbericht inklusive einer monetären Bewertung und der Höhe der Pönalen.
- Nach Annahme durch den Lizenznehmer erwartet der Hersteller eine zügige Begleichung des ausgewiesenen Fehlbetrags (meistens innerhalb von 30 Tagen).

Im Kern enthält dieser Abschlussbericht vom Hersteller die folgenden Punkte:

- Produktnummer (SKU)
- Produktbezeichnung
- Preisstaffel
- Produkt-Basispreis
- Produkt-Wartungspreis
- Reinstatement-Preis
- Abweichung (Mehrbedarf)
- Summe der Verbindlichkeit
- Preis für fünf Jahre Reinstatement
- Gesamtpreis

Diese Auflistung dokumentiert damit alle Defizite in den Lizenzberechtigungen für installierte und/oder in Gebrauch genommene Software mit den Berechnungen der möglichen Lizenzgebühren für den erforderlichen Defizitausgleich der Lizenzbedarfe für die Basislizenzen und Wartungsgebühren.

Die Lizenzprüfung endet mit dem Versand des Abschlussschreibens durch den Hersteller an den Lizenznehmer.

Nun wird (von beiden Seiten) nicht die Erwartungshaltung eingenommen, dass das erste Settlement-Angebot vom Hersteller auch gleich vom Lizenznehmer in Gänze akzeptiert wird. Nicht selten wird dann im Rahmen einer Mediation ein endgültiges Ergebnis in einer Art Vergleich verhandelt.

24.6.8.2 Auditmediation

Nachdem der Abschlussbericht dem Lizenznehmer übermittelt und von diesem einer ersten Prüfung unterzogen wurde, wird oftmals vom Lizenznehmer – in der Regel bei einer Unterzahlung – ein möglicher Vergleich angestrebt, da die zu leistenden Pönalen sicher nicht unerheblich sind und auch von den wenigsten in das Jahresbudget eingeplant wurden. Da in der Regel bei den Pönalen der nichtrabattierte Listenpreis angesetzt wird, versuchen die Lizenznehmer zu erreichen, dass wenigstens der bisherige rabattierte Listenpreis für die Kalkulation der Nachzahlungen zur Anwendung kommt. Das liegt aber immer im Ermessensspielraum des Herstellers, da dieses Vorgehen eigentlich der Strategie zuwiderläuft, auch hier auf die Kunden ein Stück weit erzieherisch einzuwirken, um die lizenzkonforme Nutzung der Softwareprodukte sicherzustellen. Denn würden dann immer „nur“ die rabattierten Listenpreise vom Hersteller angesetzt, könnte das möglicherweise bei der Einhaltung der Lizenzkonformität zu einem sehr laxen Verhalten unter den Lizenznehmern führen.

Nach der Evaluierung einer einvernehmlichen Lösung für eine mögliche Reduzierung der Pönalen würden dann die vertraglichen Aktivitäten beidseitig veranlasst, um damit dann auch das Software-Audit offiziell zu beenden. Die dann bestehende Compliance-Situation, ist der neue zukünftige Software- und Wartungsbestand, auf dem dann bei einem weiteren zukünftigen Audit wieder aufgesetzt werden würde bzw. dessen Datenlage dann als Ausgangspunkt dient. Damit wird nun auch offiziell das Software-Audit beendet.

24.7 Was kommt nach dem Audit?

Nach dem Audit ist vor dem Audit. Sicherlich kann davon ausgegangen werden, dass in den Unternehmen, die unvorbereitet ein Audit erleben durften und dabei erhebliche Nachzahlungen zu leisten hatten, die Verantwortlichen spätestens jetzt aufgewacht sind und sich dem Thema SAM und dessen Risikomanagement nicht mehr verschließen werden. Abgesehen davon, wäre jetzt zu empfehlen, die vergangenen Erfahrungen in einer Nachschau zu bewerten und, wie es so schön heißt, als „Lessons Learned“[23] aufzunehmen und umzusetzen.

Mögliche To-dos

- Analysieren Sie mit allen am Audit beteiligten internen Mitarbeitern den Ablauf des Audits und halten Sie diese Ergebnisse in einem Abschlussprotokoll fest.
- Erstellen Sie daraus einen Abschlussbericht für das Management und für die Revision.
- Erstellen Sie daraus einen Maßnahmenkatalog mit kurz- und mittelfristigen Aufgabenstellungen.
- Erstellen Sie einen Risikobericht über die eingesetzten Softwareprodukte, um eventuell schon den nächsten potenziellen Software-Audit-Kandidaten zu bestimmen.
- Prüfen Sie, ob die Vertragsunterlagen in Ihren Systemen vollständig und aktuell sind.
- Prüfen Sie, ob es klare Anweisungen an die Mitarbeiter bzgl. des Umgangs mit urheberrechtlich geschützter Software gibt (Open Source ist hier nicht von Belang).
- Sensibilisieren Sie noch einmal Ihre Mitarbeiter und erstellen Sie ggf. neue Richtlinien zum Umgang mit Software.
- Überprüfen Sie Ihre eigenen internen Richtlinien und Verfahren und optimieren Sie diese. Prüfen Sie vorhandene Kontrollmechanismen, um sicherzustellen, dass die Probleme, die zu Ihrer Gefährdung geführt und/oder diese vergrößert haben, nach bestem Wissen und Gewissen behoben werden.
- Überprüfen Sie Ihre bisherigen SAM-Prozesse und -Rollen – und wenn Sie noch kein SAM-Tool im Einsatz haben, eine Evaluierung und Implementierung eines solchen.

In einigen Fällen vergessen Kunden, die gemachten Erfahrungen und Problemstellungen aufzuarbeiten und mit geeigneten Maßnahmen zu begleiten, und befinden sich ein paar Jahre später wieder in derselben Ausgangslage, weil keine umfassende Ursachenanalyse durchgeführt und mit entsprechenden Maßnahmen gegengesteuert wurde.

[23] Lessons Learned – Wikipedia – *https://de.wikipedia.org/wiki/Lessons_Learned*

Mögliche weitere Arbeitspakete und Folgeaktivitäten wären

- Bewertung des aktuellen Lizenzmanagements, der aktuellen Lizenzadministration und der aktuellen lizenzrechtlichen Umsetzung der IT-Architektur.
- Die Lizenzierungshistorien von Softwareprodukten – hier zuerst von den Herstellern mit einem erhöhten Lizenzrisiko, dann weitere – sollten aufgearbeitet werden.
- Überlegen Sie, eine nachhaltige kaufmännische Lizenzadministration aufzubauen, mit entsprechenden Prozessen und Strukturen.
- Instanziieren Sie eine permanente Kommunikation zwischen SAM-Betrieb und den IT-Betriebs-Fachbereichen, um die Einhaltung lizenzkonformer Nutzung der Softwareprodukte zu gewährleisten.
- Sorgen Sie dafür, dass die operativen SAM-Rollen rechtzeitig mit in die Change-Management-Prozesse der IT-Architektur einbezogen werden.

Weitere Maßnahmen

- Erstellen Sie einen Auditprozess mit flankierenden Richtlinien, Aufgabenstellungen und verantwortlichen Rollen, um eine einheitliche und vom Risikomanagement mitgetragene Vorgehensweise im Fall eines Hersteller-Software-Audits aktivieren zu können.
- Führen Sie mit dem Auditprozess öfter (vor allem bei Herstellern mit einem erhöhten Lizenzrisiko) interne „eigene“ Software-Audits durch, damit proben Sie gleichzeitig die Abläufe und sind beim nächsten Mal viel besser darauf vorbereitet.
- Ermöglichen Sie umfangreichen Wissenstransfer für die SAM-Rollen und Produktverantwortlichen mittels Aus- und Weiterbildungsangeboten bzw. Zertifizierungen.
- Machen Sie eine Reifegradanalyse über Ihre bestehenden SAM-Life-Cycle-Prozesse und bewerten Sie diese, am sinnvollsten über die Norm ISO/IEC 19770-1:2012 und :2017, um mögliche Defizite in den SAM-Life-Cycle-Prozessen und im IT-Asset-Management aufzuzeigen.
- Binden Sie die Bereiche Enterprise-Architektur und Risikomanagement auch in die Belange des operativen SAM-Betriebs mit ein.

Die Erfahrung lehrt, dass recht schnell das nächste Software-Audit eines anderen Herstellers ins Haus stehen kann. Dafür sollten Sie nun auf der Basis Ihrer neuen Erfahrungen besser vorbereitet sein.

Die oft gestellte Frage: In welchem Zeitrahmen sind die „Lessons learned“ umzusetzen?

Die Beziehung zwischen Zeit, Entfernung und Geschwindigkeit ist in der Mathematik gut etabliert. Geht es jedoch um die Belange des wirtschaftlich Machbaren, werden oftmals Annahmen getroffen – wie wahrscheinlich ist es, dass wir ein Software-Audit angekündigt bekommen, und wie wahrscheinlich ist es, dass wir jedes Jahr ein Software-Audit angekündigt bekommen? Klar, ein begrenzender Faktor in diesem Wahrscheinlichkeitstheorem sind die einem Hersteller zur Verfügung stehenden Ressourcen. Gerade weil das auch bisher ein limitierender Faktor gewesen ist, um die Schlagzahl der Software-Audits erhöhen zu können, wollen die Hersteller so schnell wie möglich ihre „On-Premises“-Lizenzmodelle in die Abonnement- und Subscription-Modelle transformieren. Hier sind Sie nämlich dann Ihrem Controller gegenüber in der Verpflichtung, wirtschaftliche und ressourcenschonende Softwarenutzungen zu steuern, und nicht mehr gegenüber dem Hersteller, denn der hat

ja bereits über die Abonnements und Subscription-Pläne seine Umsätze erzielt und spart außerdem zukünftig auch noch die Kosten zur Beauftragung von Software-Audits. Um die Eingangsfrage wieder aufzunehmen: Aus diesem Grund ist es wichtig, den erforderlichen Umfang zur Steuerung und Umsetzung Ihrer SAM-Ziele zu kennen, denn das unterstützt Sie dabei, mit abgestuften Prioritäten den Zeitrahmen für das Erreichen bestimmter Meilensteine zu bewerten und festzulegen. Bedenken Sie dabei aber auch, dass die möglicherweise erforderlichen, zu durchlaufenden Lernkurven fairerweise auf die Schultern mehrerer zu besetzenden Rollen verteilt werden sollten.

Fazit

Mit der extremen Beschleunigung der Transformationen von „On-Premises"-Lizenzmodellen hin zu Abonnements und Subscription ändern sich auch die Zielsetzungen der Hersteller, um die Einhaltung ihrer Nutzungsbedingungen lizenzkonform sicherzustellen. Die Hersteller, die bereits ihre Lizenzmodelle (umsatzträchtig) transformieren konnten, auditieren auch weniger (siehe Tabelle 24.1 Rangliste der Hersteller). Hier liegt beispielsweise Adobe ganz hinten, auditiert also nur noch wenig. Andererseits erhöhen sich die Komplexitäten bei dem Thema Bring-your-own-license (BYOL) für die Unternehmen. Das ist wiederum ein möglicher Aspekt für die Hersteller, dann doch die Auditaktivitäten zu erhöhen, um bei Unstimmigkeiten zur lizenzkonformen Nutzung von „On-Premises"-Lizenzen ein weiteres Vertriebs- und Verkaufsargument für die Cloud-Lizenzen (mit Subscription) anführen zu können und zu versuchen, die Kunden über die Durchführung von Audits zu den „neuen" Cloud-Angeboten zu bewegen, da diese stabilere Umsätze versprechen. Nicht ohne Grund steht deswegen – laut der Studie von Gartner – Oracle ganz oben auf der Rangliste. Haben Sie also beispielsweise noch keine größeren bzw. umfangreichen Migrationsprojekte in die Cloud geplant, könnte es durchaus sein, dass zukünftig die Abstände der Hersteller-Software-Audits kürzer werden. Im Umkehrschluss bedeutet diese Erkenntnis, dass Sie eine proaktive Vorbereitung auf solche Auditsituationen notwendigerweise und sinnvoll in Betracht ziehen sollten, zumindest bei den Softwareprodukten der Hersteller, die in der aktuellen Rangliste auf den vorderen Plätzen stehen. Besondere Aufmerksamkeit sollten Sie dabei auf Ihre bestehenden Verträge legen, da mittlerweile die für Sie wichtigen Softwareprodukte oftmals nur noch als Cloud-Produkt mit sehr eingeschränkten „On-Premises-Rechten" verfügbar sind. Sollte das der Fall sein und Sie können oder wollen noch nicht in die Cloud migrieren, müssen Sie rechtzeitig agieren und die bestehenden Verträge so verhandeln, dass Sie weiterhin auch „On-Premises"-Lizenzen aktiv einsetzen dürfen.

Durch das anhaltend dramatische Wachstum der Cloud-Services werden ein Monitoring und das Messen von Softwarenutzung als Grundlage für eine wirtschaftliche Verwaltung und Optimierung zu einer unausweichlichen Anforderung. Die Geschäftsprozesse sollten die Cloud-Services in den Anwendungsbereich des SAM-Betriebs und seiner Rollen mit einbeziehen, um den Nutzungsbedarf und den Nutzungsverbrauch effektiv steuern zu können, damit ein risikoarmes und ressourcenschonendes IT- und Softwareassetmanagement gelingt.

Die Rolle des IT- und Softwareassetmanagements ist komplexer als je zuvor geworden. Weil die Daten überall, ob lokal und oder in verteilten Cloud-Umgebungen, zu finden sind, benötigen die Unternehmen heute mehr denn je die SAM-Experten und ihre Tools, um die Integration von lokalen und Cloud-Daten in die Geschäftsprozesse zu unterstützen. Um Transparenz und Sichtbarkeit über die gesamte Technologielandschaft zu gewährleisten und somit die erforderlichen technologischen Informationen bereitzustellen, sind optimierte SAM-Life-Cycle-Prozesse und Rollen sowie moderne und effektive SAM-Tools ein wichtiger Baustein für die Geschäftsprozesse. Um Kosten- und Risikomanagement in lokalen und Cloud-Umgebungen voranzutreiben, ist die Einbindung von ITAM-Führungskräften sowohl in die Audit- als auch in die Cloud-Welt eine unabdingbare Voraussetzung, damit zukünftig die Risiken für Software-Audits so gering wie möglich bleiben. ■