auditprotect®
SOFTWARE LICENSING + LEGAL

AUDIT-GUIDELINE

Umgang mit Software-Lizenz-Audits in Anwenderunternehmen

Dr. Robert Fleuter Peter Wesche

www.auditprotect.de

Edition 2023

Inhaltsverzeichnis

1. Einleitung 4
1.1 Zweck dieser Audit-Guideline - Wer kann davon profitieren? 4
1.2 Neue Editions dieser Audit-Guideline 4
1.3 Welche Belastungen bringt ein Software-Audit? 5
1.4 Welche Chancen kann ein Audit mit sich bringen? 5
1.5 Effiziente Handhabung - Wie profitieren Sie maximal von der Guideline? 5
1.6 Qualitätssicherung dieser Audit-Guideline 6
2. Kommerzielle und juristische Grundlagen für Audits 7
2.1 Auslösende Anlässe / Kommerzielle Motive 7
2.2 Rechtliche Basis (Deutschland) 8
3. Maßnahmen im Audit-Vorfeld 10
3.1 Briefing interner Akteure / Hinterlegung der Audit-Guideline 10
3.2 Benennung der Akteure 11
a. Interne Akteure 11
b. Koordinator 12
c. Stellvertreter der Akteure 12
d. Template Akteure 13
3.3 Implementierung der Standardaktionen 13
3.4 Audit Readiness 15
4. Sofortmaßnahmen beim Audit Call 17
4.1 Implementierten Prozess auslösen gemäß Template 17
4.2 Hilfsweise improvisierten Prozess auslösen ohne Template 17
4.3 Analyse des Audit Call 17
4.4 Erste Reaktion an Vendor 18
4.5 Tabelle Ablaufplan 19

Copyright auditprotect 2017

5. Durchführung der Software-Vermessung On-Premise 20
5.1 SAP 20
a. Verfahrensgrundlagen 20
b. Programmgestützter Audit-Prozess für SAP-ERP und S/4HANA (Selbstauskunft) 22
c. Behandlung des SAP Audit-Reports 23
d. Besonderheiten ‚Indirekte Nutzung' 24
5.2 Oracle 27
a. Verfahrensgrundlagen 27
b. Programmgestützte Vermessung der Technology-Produkte 28
c. Behandlung des Oracle Audit-Reports 29
d. Besonderheiten, Entwicklungen 30
e. Audit von Oracle-Java-Installationen 31
5.3 Microsoft 34
a. Verfahrensgrundlagen 34
b. Programmgestützte Vermessung Microsoft 35
c. Behandlung des Microsoft Audit-Reports 36
6. Reaktion auf Audit-Report des Vendors 37
6.1 Vorläufiger Audit-Report 37
6.2 Audit-Abschlussbericht 37
7. Kaufmännische Lösung 38
7.1 Herstellung der Compliance 38
7.2 Preisverhandlungen / Konditionen 38
7.3 Umgang mit nutzlosen Lizenzen 39
7.4 Kosten des Audit 40
7.5 Bestätigung der Compliance 40
8. Anmerkungen zu Audits für Cloud-Software 41
9. Weitergehende Vendor-Informationen 42

Copyright auditprotect 2017

Edition 2023 vom 18.09.2023

Alle Fotos shutterstock.com

Autoren:

Dr. Robert Fleuter ist Mitgründer von BLC Rechtsanwälte. Zuvor war er in Rechtsabteilungen von Industrieunternehmen tätig, u.a. bei Oracle und bei einem SAP-Partner, dort in der juristischen Gesamtverantwortung. Seine über 20-jährige Expertise im Softwarerecht gibt er auch als Dozent an Hochschulen weiter, wo er berufstätige Fach- und Führungskräfte in den Studiengängen Wirtschaftsinformatik und IT-Management (MBA) weiterbildet.

Peter Wesche ist Gründer von Doctor-License und war zuvor als Lead-Analyst für Software Asset Management bei Gartner tätig, mit über 3500 Kundengesprächen seit 2004 weltweit. Davor arbeitete er über 16 Jahre bei der SAP AG in Walldorf, zuletzt als Bereichsleiter und Projektleiter für die IoT Infrastruktur. Seine Spezialität ist die Optimierung von Softwareinvestitionen, die sich aufgrund der komplexen Lizenzregeln und der individuellen Einkaufshistorie einer einfachen Systematik entziehen.

Copyright auditprotect 2017

1. Einleitung

1.1 Zweck dieser Audit-Guideline - Wer kann davon profitieren?

auditprotect möchte mit dieser Audit-Guideline eine Orientierungshilfe für Anwenderunternehmen bei Lizenz-Audits durch Vendoren von Standard-Software anbieten. Das können u.a. SAP, Oracle oder Microsoft sein, die Audits in verschiedenen Formen und Intensitäten verlangen, etwa Selbstauskunft, Remote-Audit, On-Site-Audit oder Mischformen. Etliche Funktionsträger in Anwenderunternehmen können damit in Berührung kommen, wie Lizenzmanager, System-Administratoren, IT-Einkäufer, Juristen, Compliance Officer, CIOs, Finanzmanager und die Geschäftsleitung.

Die betroffenen Akteure in Unternehmen sollen befähigt werden, zunächst intern einige Weichenstellungen vorzunehmen, um Risiken zu reduzieren. Diese Audit-Guideline kann aber nicht sämtliche Aspekte und alle denkbaren Szenarien erfassen und kann insbesondere keine individuelle Beratung ersetzen. Die Akteure sollen mithilfe der Guideline verantwortlich beurteilen können, in welcher Phase sie weitere Expertise zur Audit-Begleitung hinzuziehen.

1.2 Neue Editions dieser Audit-Guideline

auditprotect hat diese Guideline auf der Basis von über 20 Jahren Erfahrung mit Software-Audits erstellt und kann weiterführende Erkenntnisse aus der ständigen Projektbearbeitung in Nachfolge-Editions dieser Audit-Guideline einbringen. Darin werden hilfreiche Erfahrungen aus

Copyright auditprotect 2017

der Audit-Praxis sowie aktuelle Fortentwicklungen in juristischen oder technischen Bereichen einfließen. Zudem ist zu berücksichtigen, dass Vendoren ihre Regelwerke ständig verändern. Eine solche aktualisierte Edition ist im 2-Jahresabstand vorgesehen.

1.3 Welche Belastungen bringt ein Software-Audit?

Belastender Faktor ist zunächst die Unsicherheit, die beim Erhalt des Aufforderungsschreibens vom Vendor entsteht, mit welchem er ein Audit ankündigt (Audit Call). Was für den Vendor tägliche Routine ist, präsentiert sich für das Unternehmen als seltene oder erstmalige Ausnahmesituation.

Eine weitere Belastung – auch mit Kostenrelevanz - tritt hinzu, weil die Erledigung des ungeplanten Projekts das Tagesgeschäft stört, Ressourcen bindet und oft erheblicher Zeitaufwand für Mitwirkungshandlungen anfällt. Schließlich das finanzielle Risiko: Der Vendor könnte Nachzahlungen in ungeahnter Höhe fordern und androhen, bei Eskalation wegen angeblicher Lizenzverstöße den Rechtsweg zu beschreiten und Funktionsträger in die Haftung zu nehmen.

1.4 Welche Chancen kann ein Audit mit sich bringen?

Allerdings sind Chancen aus einem Audit denkbar, wenn es gelingt, diesen eigentlich lästigen Anlass unter einigen Aspekten zum Nützlichen zu wenden. Denn wenn das Unternehmen ein Audit professionell mitgestaltet, können sich wertvolle neue Erkenntnisse z.B. zum Lizenzbestand ergeben.

So können möglicherweise überflüssige Lizenzen und sinnlose Support-Aufwendungen identifiziert werden. Einspareffekte durch Bereinigung von User-Zuordnungen in Anzahl und Kategorie sind genauso denkbar wie der ggf. anzuratende Wechsel auf vorteilhafte Metriken. Das Unternehmen kann ggf. günstigere Gestaltungen der System-Landschaft oder des Nutzerverhaltens vornehmen (Vermeidung Indirekter Nutzung etc.), um eventuell Kostensenkungen in der Zukunft zu erreichen.

1.5 Effiziente Handhabung - Wie profitieren Sie maximal von der Guideline?

Diese Audit-Guideline kann ihre präventive Wirkung am besten entfalten, wenn Unternehmen bereits weit im Vorfeld eines Audits und ohne konkreten Audit-Anlass bestimmte Vorbereitungen und Festlegungen treffen. Die dafür erforderlichen Aktivitäten sind unten in Ziffer 3 hinterlegt. Dazu gehört etwa die vorbereitende Benennung der Akteure und Festlegung der Standardaktionen für den Ernstfall.

Essentiell ist auch die jederzeitige Aktualität der empfohlenen Festlegungen. Daher sollte ein zu bestimmender Verantwortlicher im Unternehmen die Pflicht zur regelmäßigen Überprüfung

Copyright auditprotect 2017

übernehmen, etwa zu einem fixen Termin im Kalenderjahr. Er sollte ggf. Aktualisierungen in den Festlegungen/Standardaktionen veranlassen, z.B. bei erheblichen Änderungen bzgl. Personal, Organisation oder IT-Landschaft.

1.6 Qualitätssicherung dieser Audit-Guideline

Es ist im Sinne einer ständigen Qualitätsverbesserung dieser Audit-Guideline sinnvoll, wenn der Koordinator bzw. dessen Stellvertreter sich die Zeit nimmt, die vorbereitenden Festlegungen / Templates regelmäßig – vielleicht zu einem festen Zeitpunkt im Kalenderjahr – zu überprüfen und ggf. zu aktualisieren. Das ist eine lohnenswerte Investition in Audit Readiness, die sich beim nächsten Ernstfall auszahlt. Denn nur dann ist das Unternehmen schnell genug wieder auf Augenhöhe mit dem Vendor, wenn dieser zu einem unerwarteten Zeitpunkt erneut ein Audit ansetzt.

Copyright auditprotect 2017

2. Kommerzielle und juristische Grundlagen für Audits

2.1 Auslösende Anlässe / Kommerzielle Motive

Warum wird ein Unternehmen Ziel eines Audits? Wie erfolgt die Selektion beim Vendor?

Indizien für ein finanziell einträgliches Audit erhält der Vendor direkt aus öffentlich zugänglichen Quellen wie etwa der Website des Unternehmens und der Fachpresse. Von dort dargestellten unternehmerischen Entscheidungen und geschäftlichen Entwicklungen wird auf die dafür technisch vorhandene bzw. die erforderliche IT-Struktur geschlossen.

Auch dritte Unternehmen, die für das Audit-Zielunternehmen Leistungen erbracht haben, können mit Projektberichten und Referenzangaben auf ihren Websites Audit-Anlässe bieten. So könnte ein Dritt-Unternehmen werbemäßig herausstellen, die IT-Landschaft beim Audit-Zielunternehmen um bestimmte Systeme erweitert zu haben, was beim Vendor den umsatzträchtigen Verdacht auf Indirekte Nutzung auslösen kann.

Die Vendoren erhalten aber auch Indizien in indirekter Weise, und zwar durch Informationen ihrer Geschäftspartner, die für das Audit-Zielunternehmen tätig sind (z.B. Reseller der Vendoren). So lassen geschäftliche Erfolge sowie getätigte Änderungen und Zukunftsplanungen des Unternehmens auf Lizenzrelevanz schließen, etwa bei Personalbestand, technischer Ausrüstung und Prozessen, Investitionsvorhaben oder bei M&A-Maßnahmen. Ein prüfender Abgleich mit dem

Copyright auditprotect 2017

Kundenkonto (Lange nichts mehr gekauft!?) setzt dann die Umsatzphantasie beim Vendor in Gang.

Offiziell, vordergründig und freundlich verpackt heißt es vom Vendor, die Lizenz-Compliance solle partnerschaftlich überprüft, also ein Soll-Ist–Vergleich angestellt werden zwischen den vertraglich eingeräumten Nutzungsrechten und dem tatsächlich praktizierten Nutzungsverhalten im Anwender-Unternehmen (Check auf Unterlizenzierung). Sicherlich ist der offiziell vorgebrachte Zweck, der Schutz des Urheberrechts an der Software (Verbot unzulässiger Vervielfältigung), ein valides Motiv für ein Audit.

Doch im Hintergrund geht es in Wirklichkeit oft um mehr:
Eine möglichst ausgedehnte Reichweite und Detailtiefe des Prüfungsverlangens – teils verstärkt durch mehrfach nachgeschobene Zusatzfragen – kann dem Vendor umfassende Erkenntnisse über Infrastrukturen, Geschäftsprozesse und unternehmerische Entscheidungen bzw. Planungen liefern. Das kann am Rande dessen liegen, was vernünftigerweise zum Schutz des Urheberrechts objektiv erforderlich ist. Der Vendor durchleuchtet das Unternehmen und erhält Einblicke, die ihm neben der umsatzträchtigen Behauptung „Indirekte Nutzung“ z.B. auch erlauben, neue Produkte, Technologien oder Vertragsformen zu forcieren (Mietmodelle, Migrationen, etc.).

Das Audit hat damit auch die Funktion einer tieferen Account-Qualifizierung, zusätzlich zur üblichen Sales-Aktivität der Account Manager. Denn als angestrebter Zusatzeffekt sollen Kundenbindungen erhöht und Investitionsentscheidungen zwecks Umsatzgenerierung beschleunigt werden.

2.2 Rechtliche Basis (Deutschland)

Mit welchem Recht darf der Vendor überhaupt ein Audit verlangen?

Gesetzliche Bestimmungen bieten sehr selten eine tragfähige Rechtsgrundlage für ein Audit. Zwar können §§ 101, 101a Urheberrechtsgesetz (UrhG) wegen der Anzahl oder Schwere von Rechtsverletzungen dem Lizenzgeber einen Anspruch auf Auskunft, Vorlage von Unterlagen und Besichtigung von Sachen gewähren.

Das kommt jedoch nur in Betracht bei hinreichender Wahrscheinlichkeit einer Rechtsverletzung. Ein verdachtsunabhängiger anlassloser Kontrollanspruch besteht danach nicht. Zudem müssen weitere Voraussetzungen erfüllt sein. Für ein routinemäßiges jährliches Audit, wie Vendoren es üblicherweise handhaben, geben die gesetzlichen Bestimmungen jedenfalls keine Befugnis.

Vertragliche Bestimmungen als Rechtsgrundlage für Routine-Audits finden sich häufig in Gestalt von Audit-Klauseln in den Lizenzverträgen zur Software-Überlassung. Von der Rechtsnatur her sind das regelmäßig Allgemeine Geschäftsbedingungen (AGB). Sie unterliegen – die Geltung deutschen Rechts vorausgesetzt - zwecks Überprüfung ihrer Rechtswirksamkeit der sogenannten AGB-Kontrolle, etwa am Maßstab von § 307 BGB:

 Copyright auditprotect 2017

Danach können AGB wegen unangemessener Benachteiligung unwirksam sein, wenn sie mit wesentlichen Grundgedanken der gesetzlichen Regelung, von der abgewichen wird, nicht zu vereinbaren sind. Abgewichen wird von den gesetzlichen Grundgedanken aus den o.g. §§ 101, 101a UrhG, die einen verdachtsunabhängigen Kontrollanspruch gerade ausschließen. Die Abweichung vom gesetzlichen Leitbild könnte möglicherweise ein Indiz für Unwirksamkeit von üblichen Audit-Klauseln sein. Aber auch wegen ihrer Intransparenz oder ihres überraschenden Charakters können Audit-Klauseln unwirksam sein.

Hinweis:
Den verantwortlichen Akteuren und Lesern dieser Audit-Guideline sollte bewusst sein, dass die rechtliche Befugnis für ein Audit zweifelhaft sein kann, selbst wenn der Wortlaut der Klausel im Vertragstext vordergründig für den Vendor zu sprechen scheint. Es ist gut möglich, dass der Vendor weder den behaupteten Anspruch auf das Audit selbst hat, noch auf die im Audit Call konkret gewünschten Maßnahmen und Mitwirkungshandlungen des Unternehmens (Remote-Audit, On-Site-Untersuchungen, verlangte Informationstiefe über Geschäftsabläufe etc.). Es kann sich für die Akteure im Zweifel lohnen, zwecks anfänglich richtiger Weichenstellung externe Audit-erfahrene Experten zu kontaktieren.

Copyright auditprotect 2017

3. Maßnahmen im Audit-Vorfeld

Der Vendor ist naturgemäß immer im Vorteil: Denn allein er bestimmt mit dem Audit Call dessen Zeitpunkt, Umfang, Intensität und Methode. Im Unternehmen wird das Ereignis dagegen stets als überraschend empfunden. Es kommt zusätzlich zum stressigen Tagesgeschäft und damit immer ungelegen. Man fühlt sich überrannt, unvorbereitet und angesichts einer unangenehmen Angelegenheit in der schwächeren Position.

Um sofort auf Augenhöhe mit dem Vendor zu agieren, empfiehlt sich ein vorinstalliertes, automatisiertes und strukturiertes Vorgehen. Denn bereits implementierte Prozesse bringen Sicherheit und wertvollen Zeitgewinn im Ernstfall. Dazu dienen die vorbereitenden Maßnahmen weit im Vorfeld eines Audit, die das Unternehmen sofort umsetzen sollte, wie hier nachfolgend ausgeführt.

3.1 Briefing interner Akteure / Hinterlegung der Audit-Guideline

Primäre Empfänger innerhalb eines Unternehmens, an die der Vendor ein Audit-Anschreiben (Audit Call) per Briefpost adressiert, sind häufig Lizenzmanager, Mitglieder der Geschäftsleitung oder CIOs. Ob bzw. welche weiteren Funktionen/Personen als Erst-Adressaten in Betracht kommen (IT Service Manager o.ä.), sollten verantwortliche Akteure individuell – ggf. anhand früherer Audits - feststellen.

Alle Funktionsträger, die potentielle Erst-Adressaten eines Audit Call sein können, sind über die Existenz und Wirkung dieser Audit-Guideline im Unternehmen in Kenntnis zu setzen.

Die Audit-Guideline ist bei den genannten Stellen (potentielle Erst-Adressaten und deren Assistenz) zu hinterlegen und muss dort im Ernstfall direkt verfügbar sein, um Sofortmaßnahmen starten zu können. Dazu werden im Folgenden Templates zur Verfügung gestellt, und zwar hinsichtlich der Akteure und hinsichtlich der Prozesse.

Copyright auditprotect 2017

3.2 Benennung der Akteure

a. Interne Akteure

Essentielles Anliegen dieser Audit-Guideline ist eine zu erstellende Liste der Personen/Funktionen, die im Ernstfall, also unmittelbar nach Eingang des Audit Call, zu involvieren sind. Zumindest nachfolgende Funktionsträger empfiehlt es sich als Akteure in einem Template zu listen und bei Eingang eines Audit Call sofort zu informieren:

- IT-zuständiges Mitglied der Geschäftsleitung bzw. CIO (falls noch nicht als Erst-Adressat des Audit Call ohnehin informiert), da signifikante Nachforderungen und Streitigkeiten mit einem großen Vendor die unternehmerische IT-Planung tangieren können.

- Lizenzmanager, da dort das Know-how zum Softwarebestand bzw. zu Schwachstellen vorhanden ist. Teilweise hat der Lizenzmanager den Lead für die Durchführung des Audits, weil bei ihm das Querschnittswissen über das Zusammenspiel aller Beteiligten konzentriert ist.

- Finanzverantwortlicher (CFO, Kaufmännischer Leiter), da finanzielle Risiken drohen durch Nachforderungen bei Unterlizenzierung und ggf. auch Investitionen anfallen können.

- Rechtsabteilung / Unternehmensjurist, da Lizenzvertragsrecht, Software-Recht, IT-Recht, Urheberrecht etc. immer die entscheidende Rolle spielen bei Argumentationsaufbau / Forderungsabwehr und dort die Maßnahmen zum juristischen Gefahrenmanagement, eventuell durch externe Audit-Expertise, koordiniert werden.

Je nach Organisation des Unternehmens kann die zusätzliche Aufnahme weiterer Funktionen in das Template nützlich sein, wie beispielsweise

- Compliance Officer, da mit der vom Vendor hinterfragten Software Compliance ein Teilbereich seiner Zuständigkeit betroffen ist und Vendoren teils strafrechtlich relevante Compliance-Verstöße behaupten.

- IT-Einkauf, da dort kommerzielle Konditionen mit dem Vendor bei erforderlichen Zukäufen zu verhandeln sind.

- System-Administratoren, da dort das technische Know-how für die konkret betroffenen IT-Systeme vorhanden ist und dort der technische Einsatz der Vermessungsprogramme des Vendors erfolgt.

- Fachbereiche, die Ist- und Planzahlen liefern können für aktuelle IT-Projekte, Nutzungsänderungen oder besondere Nutzungsszenarien (z.B. Sondernutzer, indirekte Nutzer) und so die inhaltlichen Nutzungsthemen beratend in das Audit einbringen.

Copyright auditprotect 2017

- Vertragsmanagement, da es für die Frage eines korrekten Lizenz-Status oft maßgeblich auf eine lückenlose Vertragshistorie ankommt. Kleine Details können in historischen Vertragstexten oder in der Pre-Sales-Kommunikation für die Abwehr von Nachforderungen entscheidend sein.

Ergänzende Expertise sollten die Akteure im Bedarfsfall von außen anfragen, etwa

- Externe IT-Provider, welche die unmittelbare Kontrolle und Einsicht in die Ablaufumgebung der fraglichen Software innehaben (z.B. bei Outsourcing-Szenario).

- Lizenzberater/Softwarejurist, welche den Akteuren bei komplexen Lizenzportfolios beratend zur Seite stehen.

b. Koordinator

Aus dem Kreis der Akteure auf dem Template ist ein Koordinator festzulegen, welcher zusätzlich zu seiner Fachfunktion in der Verantwortung steht, alle anderen Akteure und sämtliche Maßnahmen bis zum Audit-Abschluss zu koordinieren, etwa der IT-Leiter. Oft übernimmt auch der Lizenzmanager diese Koordinationsaufgabe. Angesichts knapper interner Ressourcen, die für ein überraschendes Audit gebunden sind, kann es sinnvoll sein, ein hinzugezogenes externes Expertenteam (Lizenzberatung/Softwarerecht) mit der Koordination zu beauftragen.

c. Stellvertreter der Akteure

Stellvertreter für sämtliche o.g. Akteure / Funktionen sind in der Check-Liste ebenfalls zu hinterlegen. Sie sind lediglich hilfsweise als Ersatz einzubinden bei Verhinderung der betreffenden Primärperson.

Copyright auditprotect 2017

d. Template Akteure

Im Ergebnis könnte eine Check-Liste etwa so aufgebaut sein (jeweils mit Zeile für Stellvertreter):

Name	Funktion	Kontaktdaten	Rolle
nn	Geschäftsleitung IT	Tel, E-Mail	Adressat/Information
nn	CIO	Tel, E-Mail	Adressat/Information
nn	Lizenzmanager	Tel, E-Mail	Adressat/Koordinator
nn	CFO/Kaufm. Leiter	Tel, E-Mail	Information
nn	Interner Jurist	Tel, E-Mail	Beratend
nn	Compliance Officer	Tel, E-Mail	Beratend
nn	IT-Einkauf	Tel, E-Mail	Information
nn	System-Administrator	Tel, E-Mail	Support
nn	Fachbereich User I, II	Tel, E-Mail	Beratend
nn	Vertragsmanagement	Tel, E-Mail	Support
nn	Externe IT-Provider	Tel, E-Mail	Support
nn	Lizenzberater	Tel, E-Mail	Beratend

3.3 Implementierung der Standardaktionen

Rollenprofile der Akteure sowie Vorgaben zur effizienten Ausgestaltung von Standardaktionen sollten in einem Template für den Ernstfall übersichtlich dokumentiert sein. Es ist bei allen Akteuren zu hinterlegen. Folgende Anregungen zur Gestaltung der Standardaktionen können einfließen:

Erst-Adressat

Direkt nach Erhalt des Aufforderungsschreibens vom Vendor muss der Erst-Adressat des Audit Call (z.B. Geschäftsleitung, CIO) die zu involvierenden Akteure gemäß Template darüber in Kenntnis setzen. Insbesondere ist dabei der benannte Koordinator für die Audit-Abwicklung sofort zu informieren. Idealerweise ist das Aufforderungsschreiben des Vendors in Kopie an die Akteure im Verteilerkreis zu geben.

Koordinator

Der Koordinator sollte möglichst zusammen mit der Info-Email an den Verteilerkreis ein zeitnahes erstes Meeting oder eine Telefonkonferenz der involvierten Akteure einberufen.

Copyright auditprotect 2017

Kommunikation intern mit Akteuren

Bei sämtlicher Email-Kommunikation innerhalb des Teams empfiehlt es sich, stets und automatisiert eine bestimmte zentrale Email in cc zu verwenden, welche diejenige des Koordinators sein kann. Denn dann ist der Koordinator zu jedem Zeitpunkt über den Informationsfluss zwischen allen Akteuren und damit über den Stand der Dinge informiert. Er kann daraus im Ernstfall mögliche Optionen der Positionierung gegenüber dem Vendor ableiten.

Kommunikation extern mit Vendor

Wichtig ist folgendes festzulegen: Wer von den Akteuren ist berechtigt, mit dem Vendor über Audit-Themen zu kommunizieren? Die Info-Ströme sollten von vornherein klar kanalisiert ablaufen.

Denn ein konsistentes und durchdachtes Verfügbarmachen von Compliance-relevanten Informationen an den Vendor (technische Abläufe, juristische Bewertungen etc.) nur durch dafür vorgesehene Akteure erleichtert den Aufbau von schützenden Argumentationslinien, um Nachforderungen gering zu halten. Die Kommunikationsberechtigung zum Vendor ist häufig beim IT-Leiter / CIO gut aufgehoben. Es empfiehlt sich, andere Lizenz-relevante Stellen im weiteren Umfeld ausdrücklich auf diese Kommunikationsregelung zu verpflichten. So wird der Vendor den kommunikationsbefugten Akteur nicht umgehen können.

Dieser fungiert im Anwenderunternehmen während des gesamten Audit-Prozesses als maßgeblicher Ansprechpartner für das Audit-Team auf Vendorenseite. Mit diesem kann z.B. verabredet werden, welche Personen bei jeglicher Email-Korrespondenz jedenfalls stets in cc gesetzt werden sollen, z.B. CIO und Lizenzmanager.

Copyright auditprotect 2017

3.4 Audit Readiness

Nicht erst mit Eingang des Audit Call, sondern zeitlich weit im Vorfeld sollten die Bereiche Lizenzmanagement und System-Administration die Basis für ein gutes Gelingen legen (Herstellen von Audit Readiness):

Lizenzmanager

Eine Kernaufgabe des Lizenzmanagers ist die Aufstellung bzw. Aktualisierung der Lizenzbilanz, d.h. die Dokumentation des aktuell genutzten bzw. verfügbaren Lizenzportfolios. Hierbei wird stets zwischen Soll- und Istbestand unterschieden. Das ist die Differenz zwischen der vertraglich eingeräumten Nutzungserlaubnis - einschließlich ihrer jeweils vereinbarten Metrik - und der tatsächlichen Intensität der Software-Nutzung in der Unternehmenspraxis. Wenn die Nutzung über das zulässige Maß hinausgeht, sie also nicht mehr vom eingeräumten Lizenzumfang gedeckt ist, kommt es zur problematischen Unterlizenzierung.

Da der eigentliche Zweck eines Software-Audits die Verifizierung der Lizenzbilanz ist, steht das Lizenzmanagement insofern beim Audit-Prozess im Mittelpunkt. Denn eine vielleicht nicht immer perfekte, aber dennoch belastbare Lizenzbilanz hilft bei der Vermeidung unangenehmer Überraschungen im Ernstfall. Dazu bedarf es sowohl des Abgleichs mit Beschaffungen des IT-Einkaufs als auch regelmäßig proaktiver interner Vermessungen, um etwaige Verschiebungen des Nutzungsverhaltens in der Lizenzbilanz abzubilden.

Copyright auditprotect 2017

System-Adminstratoren

Die technischen Systemverantwortlichen (Administratoren) betreuen die Systeme und stellen ihr Funktionieren sicher. Sie sind verantwortlich für eine Vielzahl von Aufgaben, die Einfluss auf das Gelingen einer Vermessung haben. Hier nachfolgend sind beispielhaft einige Aufgaben gelistet, die sowohl routinemäßig anfallen, als auch anlassbezogen in einer konkreten Audit-Situation dringlich werden können (situative Beispiele in Klammern):

- Systemeinstellungen vornehmen (unzulässige Virtualisierung vermeiden)
- Updates einspielen (aktuelle Vermessungsroutinen zwecks Fähigkeit zur Selbstauskunft)
- Systeme ändern (Anzahl benutzter Server reduzieren)
- Personaleinsatz planen (Ressourcen vorhalten für typische Audit-Zeiten, GJ-Ende bei Vendor)
- Kurzfristige taktische Maßnahmen für Sonderaufgaben ergreifen (Migration vor Start des Vermessungstools abschließen)
- Alternative Vermessungstools austesten

System-Administratoren setzen zudem im Audit die Vermessungsmaßnahmen technisch um (Einsatz der Vermessungstools des Vendors).

Copyright auditprotect 2017

4. Sofortmaßnahmen beim Audit Call

4.1 Implementierten Prozess auslösen gemäß Template

Der implementierte Informationsprozess ist unmittelbar nach Eingang des Audit Call in Gang zu setzen, s. oben Ziffer 3.3 „Implementierung der Standardaktionen".

4.2 Hilfsweise improvisierten Prozess auslösen ohne Template

Falls entgegen den Empfehlungen in Ziffer 3 oben die Templates bezüglich der Akteure und Prozesse nicht implementiert sind, so sollte der vom Vendor angeschriebene Erst-Adressat des Audit Call (z.B. Geschäftsführer) mindestens folgenden Akteuren das Aufforderungsschreiben des Vendors sofort zur Kenntnis geben:

- Für IT zuständiges Mitglied der Geschäftsleitung
- Lizenzmanagement
- Rechtsabteilung / Unternehmensjurist

Ein Koordinator für das Audit ist festzulegen, ebenfalls ein berechtigter Akteur für abgestimmte Kommunikation mit dem Audit-Team des Vendors. Auch in allen weiteren Schritten sollte sich das improvisierte Vorgehen – soweit eben im Ernstfall noch möglich – in analoger Weise an den Empfehlungen für die zu implementierenden Standardaktionen orientieren.

4.3 Analyse des Audit Call

Zunächst ist die juristische Korrektheit des Anschreibens selbst sowie der Audit Scope (Inhalt und Reichweite des Prüfungsverlangens) klar zu analysieren. Es geht um Kriterien der rechtlichen Zulässigkeit generell (auch der Audit-Klausel selbst, s. Ziffer 2.2 oben), um die Konkretisierung der prüfungsrelevanten Produkte und Systeme (Vermessungsplan) sowie um die Bewertung der verlangten Formen wie Selbstauskunft, Remote Audit, On-Site-Audit oder andere. Nicht vermessbare Bereiche wie Sonder-User oder spezielle Metriken sind ggf. zu identifizieren und separat zu berücksichtigen.

Weitere Anhaltspunkte für eine Analyse:

- Sind die Formalien des Audit-Anschreibens eingehalten?
- Ist die Schriftform gewahrt, soweit die Audit-Klausel das verlangt?
- Hat der Absender/Vendor den richtigen Adressaten angeschrieben? Oder nur eines der anderen Konzernunternehmen?
- Ist die korrekte Audit-Klausel als Berechtigungsbasis für den Audit Call in Bezug genommen?
- Sind in der Audit-Klausel Fristen vereinbart, die dem Unternehmen zustehen?

Copyright auditprotect 2017

- Ist die Verhältnismäßigkeit der verlangten Mittel/Methoden gewahrt bzw. sind sie dem Informationszweck nicht angemessen?
- Existieren Bedenken bzgl. überzogener sachfremder Auskunftsverlangen? Geschäftsgeheimnisse? Datenschutz?
- Verbleibt beim Einsatz des verlangten Vermessungstools ausreichende Transparenz und Kontrolle bzgl. der übermittelten Daten?
- Ist ggf. ein Dritter korrekt legitimiert, der im Auftrag des Vendors auftritt („Auditor")?

Damit gleich zu Anfang die entscheidenden Weichen vorteilhaft gestellt werden, sollte die Rechtsabteilung eingebunden sein, die im Rahmen ihres juristischen Gefahrenmanagements ggf. spezielle Audit-Expertise (Lizenzberatung und Softwarerecht) von außen hinzuzieht und bei den anderen Akteuren einbindet.

4.4 Erste Reaktion an Vendor

Nach der fachgerechten Analyse des Audit-Anschreibens, welches oft auch schon eine vom Vendor gewünschte Prozessbeschreibung samt Projektplan mit bereits datierten Milestones beinhaltet, ist eine erste Reaktion zu formulieren. Dafür ist ein stets passender Standardtext kaum geeignet, sondern eine Antwort ist in Abhängigkeit von den Erkenntnissen, offenen Fragen und möglichen Problemen situationsadäquat zu individualisieren. Vendoren sehen oft einen Kontakt zur Terminvereinbarung innerhalb von zwei Wochen vor, um den Prozessbeginn in einem anzusetzenden Kick-off-Meeting zu besprechen.

Das Antwortschreiben an den Vendor kann je nach Sachlage und Detailtiefe des Ersuchens u.a. diese Aspekte beinhalten:

- Eingang bestätigen
- Kooperationsbereitschaft signalisieren
- Terminverschiebung wünschen und begründen (relevantes Team nicht vollständig anwesend, Urlaub, betriebliche Dringlichkeiten, laufende Projekte etc.)
- Bitte um Darlegung der Audit-Berechtigung und des Anlasses

Copyright auditprotect 2017

- Frage nach Konkretisierung von Umfang und Reichweite (Produkte, Systeme)
- Bitte um Audit-Methode, die den laufenden Betrieb möglichst wenig beeinträcht
- Dokumentation bewerten zur Handhabung von Vermessungstools und zur Transparenz der übermittelten Inhalte

Eventuell sind Vereinbarungen über den Gesamtkomplex anzuregen, einschließlich o.g. Punkte, der Zeitschiene, Kostenverteilungen, Beschränkungen und weiteren Besonderheiten. Unter Umständen bietet die schiere Menge der zu übermittelnden Daten Anlass dazu, vom Vendor eine Audit-Vereinfachung zu fordern, um die Prüfungserfordernisse in Grenzen zu halten.

4.5 Tabelle Ablaufplan

Der Prozess beim Audit Call lässt sich etwa so tabellarisch skizzieren:

Klärungen vor Vermessungsbeginn	C-Level	Lizenz-manager	Jurist	Fachbereich	IT-Einkauf	Admini-strator	Provider	Lizenzber.
Korrekte Adressierung	I	K	V	-	B	-	-	-
Fristen im Audit Call	-	K	V	-	-	-	-	-
Zulässigkeit der Verfahren	I	K	V	-	S	-	-	I
Priorisierte interne Belange	I	K	I	V	S	-	-	-
Erste Reaktion an Vendor	I	V	S					
Angemessenheit des Verfahrens	-	V	S	-	-	S	S	B
Prüfung technischer Voraussetzungen	-	K	I	-	-	V	V	S
Geforderte Compliance-Erklärung des Vendors	I	K	V	-	-	-	-	B
Datensicherheit/Datenschutz	I	K	V	S	-	S	S	S
Probelauf der Vermessung	-	K	I	-	-	V	V	S
Bewertung des Probelaufs	I	V	S	S	S	S	-	S
Aufstellung eines Ablaufplans	-	V	I	S	S	S	S	S
Zweite Reaktion an Vendor zum Vermessungsablauf	I	V	S	-	-	-	-	-
Abstimmung des Ablaufs mit Vendor	I	V	S	-	-	-	-	-
Durchführungsfreigabe	V	K	S	I	I	I	I	I

Legende:
I = Information
K = Koordination
V = Inhaltlich verantwortlich
B = Beratend
S = Support und Durchführung
- = Unbeteiligt

Copyright auditprotect 2017

5. Durchführung der Software-Vermessung On-Premise

Ein Audit für On-Premise-Software besteht immer aus den drei Elementen Audit Call (s. auch oben Ziffer 4), der programmgestützten bzw. manuellen Vermessung der tatsächlichen Nutzung sowie der Präsentation der Vermessungsergebnisse im Audit-Report. Hieraus resultierende kaufmännische Konsequenzen sind unten in Ziffern 6. und 7. behandelt. Nachfolgend werden zunächst tragende Aspekte für die Audit-Durchführung einiger prominenter Vendoren beleuchtet, nämlich SAP, Oracle und Microsoft.

5.1 SAP

a. Verfahrensgrundlagen

Das Betreiben von Audits erfolgt durch die zentrale Einheit „SAP Global License Auditing Services“, in Deutschland auch erscheinend unter der Bezeichnung „License Compliance & Audit“.

Nachfolgend soll die Struktur der Audit-Bestimmungen der SAP im Überblick dargestellt werden:

Struktur Audit-Klausel SAP, z.B. manifestiert in AGB 2016, Ziffer 3:
https://www.sap.com/docs/download/agreements/general-terms-and-conditions/ops/sap-general-terms-and-conditions-on-premise-germany-german-v5-2016.pdf
Zunächst verlangt SAP für jede Nutzung, die über den vertraglich vereinbarten Nutzungsumfang hinausgeht, dass sie im Voraus schriftlich angezeigt wird.
SAP ist berechtigt, die Nutzung in Übereinstimmung mit den SAP-Standardverfahren durch Vermessung zu überprüfen:
https://support.sap.com/keys-systems-installations/measurement/information/Documentation.html

Copyright auditprotect 2017

Der Zugriff auf die aktuelle Dokumentation ist nur mit der Berechtigung zum Zutritt auf den Service-Marktplatz der SAP möglich. Deshalb ist die Registrierung des verantwortlichen Lizenzmanagers für diese Quelle angeraten.

Auditformen und ihre Voraussetzungen:

- Selbstauskünfte unter Einsatz der von SAP zur Verfügung gestellten Vermessungstools (siehe Abbildung in Ziffer 5.1b)
- Remote-Vermessungen — Selbstauskunft verweigert oder
Selbstauskunft keine aussagefähigen Ergebnisse und
Objektive Anhaltspunkte für Rechtsverletzung
- Vermessungen vor Ort — Remote-Vermessung verweigert oder
Remote-Vermessung keine aussagefähigen Ergebnisse und
Objektive Anhaltspunkte für Rechtsverletzung

Für die Umsetzung des SAP Standardverfahrens sind Skills aus der Administration und der allgemeinen SAP-Anwendungsbetreuung erforderlich. SAP bietet für die Umsetzung der Standardverfahren auch einschlägige Trainingskurse bzw. Videos an.

Neben der Vermessung des SAP-ERP Systems sind auf dem Service-Marktplatz auch die Vermessungsmethoden für folgende Systeme zugänglich:

- SAP HANA Datenbank
- SAP Unwired Platform
- SAP Core Metric
- SAP Sybase Legacy License
- SAP BusinessObjects über https://support.sap.com/en/my-support/systems-installations/system-measurement/businessobjects-bi-measurement.html

Copyright auditprotect 2017

b. Programmgestützter Audit-Prozess für SAP-ERP und S/4HANA (Selbstauskunft)

Quelle: SAP

Abb 5.1: Die ERP-Selbstauskunft auf Basis des SAP-Standardverfahrens

Copyright auditprotect 2017

Das oben illustrierte SAP-Standardverfahren für die Vermessung von SAP-ERP bzw. S/4HANA verläuft zweistufig:

- Vermessung der Produktiv- und Entwicklungssysteme durch die Transaktion USMM
- Konsolidierung der einzelnen Vermessungsergebnisse über den Konzentrator LAW (License Administration Workbench)

Wahlweise kann SAP die Einzelergebnisse konsolidieren. Dies hat allerdings den Nachteil, dass das Anwenderunternehmen keine Übersicht mehr über das effektive Vermessungsergebnis hat, weil es die Effekte dieser Konsolidierung nicht zu sehen bekommt.

Zu allen Elementen der USMM-basierten Vermessung (entspricht im Weitesten den Funktionsmodulen mit ihren Metriken) gibt es eine betriebswirtschaftlich orientierte Dokumentation im Service-Marktplatz, jedoch mit unterschiedlicher Qualität und Aktualität.

Das Standardverfahren wurde aus Sicht der User-basierten Lizenzierung entwickelt und ist nicht geeignet, die SAP-Engines für alle Metriken programmgestützt zu vermessen. Diese nicht vermessbaren Engines muss das SAP-Anwenderunternehmen durch Selbstauskunft erklären. SAP informiert über die im Einzelfall erforderlichen Selbstauskünfte zusammen mit der Versendung des Vermessungsplans (siehe Ziffer 4.3) an das Unternehmen.

Das Vermessungsprogramm kann alle typischen Eigenschaften bzw. Mängel von Software aufweisen:

- Versionierung
- Unvollständigkeit
- Programmierfehler
- Eingeschränkte Dokumentation
- Fragliche Geeignetheit bzgl. der konkreten Lizenzvertragsbedingungen.

Selbst wenn das Verfahren vollständig konform mit den verfügbaren SAP-Hinweisen durchgeführt wird, sind die Ergebnisse häufig unzutreffend bzw. erklärungsbedürftig. Insofern ist anzuraten, die Vermessungsergebnisse stets durch Plausibilitätschecks zu validieren. Im Zweifel sollten die Akteure spätestens an dieser Stelle eine erfahrene externe Beratung involvieren.

Zu beachten ist, dass SAP in späteren Versionen des Vermessungsprogramms auch früher nicht vermessbare Engines bzw. erweiterte Nutzungsrechtsprüfungen durch neue Vermessungs-routinen messbar machen kann. So leitet SAP ggf. bei zukünftigen Audits auch Lizenzverletzungen für die Vergangenheit her.

c. Behandlung des SAP Audit-Reports

SAP kann sowohl die Ergebnisbesprechung als auch die betriebswirtschaftliche Bewertung des Audits unterschiedlich behandeln:

- Übersendung eines Vertragsangebots
- Mündliche Vorverhandlung

Copyright auditprotect 2017

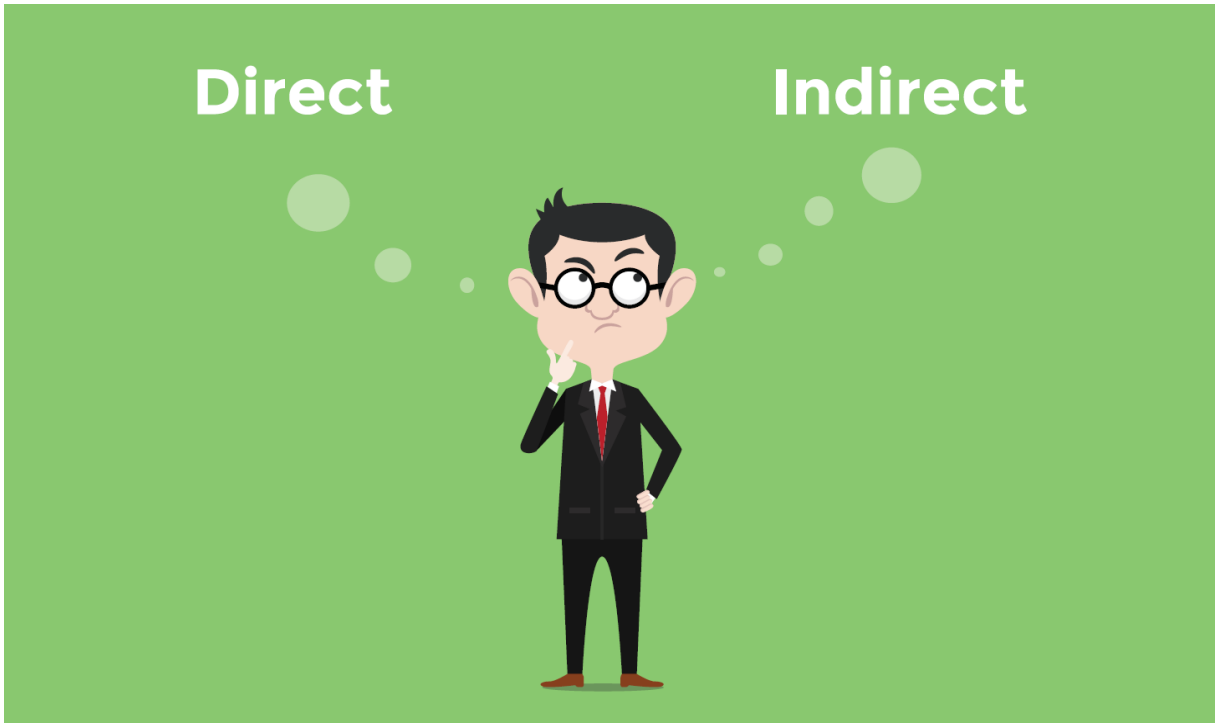
- LAW-basierter Kurzreport
- Mehrseitiger detaillierter Audit-Report mit Grundsatzaussagen zur Compliance.

d. Besonderheiten ‚Indirekte Nutzung'

SAP hat ein neues Lizenz- und Preismodell entwickelt, welches seit April 2018 angeboten wird.

Was ist der Anlass für die Neuerungen?

Im Schwerpunkt adressiert das Modell das konfliktträchtige Thema „Indirekte Nutzung" der SAP-Software. Dabei ist die Frage, ob für Nicht-SAP-Nutzer von angebundenen Drittsystemen ebenfalls SAP Lizenzen erforderlich sind, wenn diese Nutzer - also indirekt über das Drittsystem - auf das SAP ERP-System zugreifen. Die Nutzung kann also sowohl herkömmlich seitens einer natürlichen Person ausgelöst werden (Human Access) wie auch automatisiert (indirekt) als Digital Access von irgendeinem Gerät / Maschine im Rahmen des IoT (Digital Economy).



Für derartige Nutzungen hat SAP bisher die Anschaffung von User-Lizenzen nach unterschiedlichen Modellen verlangt (z.B. Platform User). Das hat oft zu unangemessenen Härten, zu Schieflagen im Leistungsäquivalent und zu Vertrauensbelastungen bzgl. SAP als Geschäftspartner geführt. Bei Audits ist nämlich manches Anwenderunternehmen völlig überraschend mit Nachforderungen konfrontiert worden.

Für den direkten Zugriff einer natürlichen Person auf das SAP-System als Human Access soll es bei der herkömmlichen User-basierten Lizenzierung bleiben.

Copyright auditprotect 2017

Was ist neu?

SAP will ihr Vergütungsinteresse bei indirekter Nutzung nicht mehr zugriffsbezogen, sondern ergebnisabhängig im Sinne von Wertschöpfungskomponenten realisieren (business outcome). Neun typische Leistungsergebnisse, die Anwender mit dem SAP-System üblicherweise für ihre Geschäftsabläufe generieren, bilden die Anknüpfungspunkte für Lizenzgebühren. Es geht um die Benutzung des SAP-Systems für das Kreieren von folgenden neun SAP-Belegen („documents"):

- Sales Order
- Invoice
- Purchase Order
- Service Order & Plant Maintenance
- Production Orders (Manufacturing)
- Quality Management
- Time Management
- Material Document
- Financial Document.

Die Herstellung darüber hinausgehender Dokumententypen ist vorläufig nicht vergütungspflichtig. Lediglich das initiale Generieren eines der genannten neun gelisteten Belege soll eine Vergütung auslösen, nicht aber die Änderungen. Das Entstehen weiterer Belege, die als Folge der Erst-Generierung resultieren, bleibt ebenso vergütungsfrei.

Beispiel: Ein initiales Auftragsdokument (etwa Sales Order) entsteht vergütungspflichtig. Jedoch sollen die in der Folge für diesen Vorgang produzierten Belege, z.B. Auftragsänderung, Lieferung oder Invoice gemäß bisheriger SAP-Darstellung vergütungsfrei sein. Ebenfalls vergütungsfrei sind auch spätere Zugriffe für Lesen, Updaten oder Entfernen des Primärdokuments. Dabei soll es unerheblich sein, wie viele Drittprogramme, Bots oder Internet Services auf diese Informationen zugreifen oder wie oft diese geändert werden.

Wie wird abgerechnet?

SAP will die neun gelisteten Belegtypen je nach ihrem wirtschaftlichen Wert vergütungsmäßig unterschiedlich gewichten und Mengendiscounts gewähren je nach der Anzahl vergütungspflichtig hergestellter Initialdokumente. Zusätzlich wird das Verfahren dadurch kompliziert, dass für manche Belegtypen nicht der Beleg, sondern jede Position des Belegs zählrelevant ist.

Beispiel: Bei einer Bestellung wird jeder gekaufte Artikel einzeln gezählt. Nach bisheriger Verlautbarung will SAP die vergütungsrelevanten Mengen in 12-Monats-Perioden messen und abrechnen. Demnach wäre die Metrik für dieses Lizenzmodell die Anzahl Belege bzw. Belegpositionen pro Jahr.

Copyright auditprotect 2017

Für wen gilt das neue Modell?

Das neue Modell gilt für Neukunden. Für Bestandskunden sollen drei Möglichkeiten offenstehen:

- Sie können unverändert im bisherigen Modell verbleiben.
- Zwecks Erledigung/Neugestaltung des Konfliktthemas „Indirekte Nutzung" können sie für diesen Aspekt auch ihre Lizenzen auf das neue Modell migrieren und im Übrigen im bisherigen Vertragskonstrukt bleiben (Vertragsänderung mittels Addendum). Das soll unter teilweiser Anrechnung („up to 100% credit for their prior investments") ihrer bisher getätigten Lizenzinvestitionen geschehen. Hierbei entstehen komplexe Bewertungsfragen mit Blick auf eine kommerziell akzeptable Leistungsäquivalenz.
- Diese Fragen stellen sich auch bei der dritten Option der Bestandskunden, nämlich dem vollständigen Umstieg von SAP-ERP auf S/4HANA (Contract Conversion).

Wie wird vermessen?

Nach dem Konzept von Sender und Empfänger: SAP basiert die Vermessungstechnik auf der Identifikation von sendenden und empfangenden Systemen. Damit sollen Belege bzw. deren Generierungsquellen aus Digital Access unterscheidbar werden von solchen, die durch natürliche User im Wege des Human Access entstehen. Dabei können nach dem neuen SAP Digital-Access-Modell Lizenzierungserfordernisse auf beiden Systemseiten entstehen. Diese Systeme können SAP-Systeme wie auch Drittsysteme sein. Laut SAP werden seit August 2018 die Sender von automatisierten Zugriffen mit Identifiern ausgestattet, während die Empfänger (das buchende SAP-System) Anfang 2019 solche Identifier erhalten.

Vorläufige Bewertung

Unter kommerziellen Gesichtspunkten und aus dem Blickwinkel einer fundierten Lizenzberatung besteht bei den eingeräumten Optionen zu Vertragsumstellungen die Gefahr einer Unterbewertung der bisherigen Investitionen zulasten des Anwenderunternehmens. Manches angeblich „Neue" könnte auch nur in der Gestalt einer Neuverpackung durch Rebundling oder Renaming daherkommen.

Ob eine geänderte Metrik für das jeweilige Unternehmen besser ist, steht in Frage. Wird die indirekte Nutzung zum Thema im Audit-Report, sind die Vorschläge zur Implementierung der neuen Metrik ‚erzeugte Belege' intern sorgfältig zu prüfen, z.B. durch Hochrechnungen der zukünftigen Nutzung über die nächsten fünf Jahre.

Gerade bei den zahlreichen individuellen Vertragsverhandlungen zwischen SAP und änderungswilligen Anwenderunternehmen, die aufgrund des neuen Modells absehbar sind, ist eine absichernde Unterstützung durch Expertise von außen für eine vorteilhafte Neuorientierung anzuraten.

 Copyright auditprotect 2017

5.2 Oracle

a. Verfahrensgrundlagen

Das Betreiben von Audits erfolgt durch die dortige Einheit LMS (License Management Services).

Oracle macht Audit-Vorgaben in „Allgemeine Vertragsbedingungen", die auch mit „Rahmenvertrag" bezeichnet sind, und auf die Oracle im „Auftragsdokument" in Bezug nimmt:
http://www.oracle.com/us/corporate/contracts/lic-online-toma-ph-de-de-3936864.pdf

Die Audit-Klausel findet sich auf S. 15 dieses Dokuments und lautet:

8. Audit
Oracle darf Ihre Nutzung der Programme prüfen, vorausgesetzt, Oracle kündigt die Prüfung 45 Tage im Voraus schriftlich an. Sie erklären, dass Sie bei derartigen Audits durch Oracle kooperieren, zumutbare Hilfe leisten und Zugriff auf Informationen gewähren. Ihr normaler Geschäftsbetrieb wird durch ein derartiges Audit nicht unverhältnismäßig gestört. Zudem verpflichten Sie sich, für Ihre nicht von Ihren Lizenzrechten gedeckte Nutzung der Programme anfallende Vergütungen innerhalb von 30 Tagen nach schriftlicher Aufforderung nachzuentrichten. Wenn diese Zahlung nicht erfolgt, ist Oracle berechtigt, (a) programmbezogene Serviceangebote (inklusive Technische Unterstützung), (b) bestellte Programmlizenzen unter dieser Anlage P und allen zugehörigen Verträgen und/oder (c) den Rahmenvertrag außerordentlich zu kündigen. Sie erklären sich damit einverstanden, dass Oracle nicht für Kosten einzustehen hat, die Ihnen durch Ihre Mithilfe bei einer Prüfung durch Oracle entstehen.

Zudem gibt die „License Compliance Policy" aus Sicht des US Headquarters einen kurzen generellen Überblick zu den Pflichten des Anwenders samt möglicher Konsequenzen bei Non-Compliance:
https://www.oracle.com/corporate/license-management-services/policy.html

Das Regelwerk „Software Investment Guide" in Form eines ‚White Paper' formuliert die wichtigsten Lizenzregeln, enthält aber auch Disclaimer über die Unverbindlichkeit der dargelegten Prinzipien:
http://www.oracle.com/us/corporate/pricing/software-investment-guide/index.html

Oracle Software-Audits unterscheiden sich stark nach den jeweiligen Audit-Objekten:

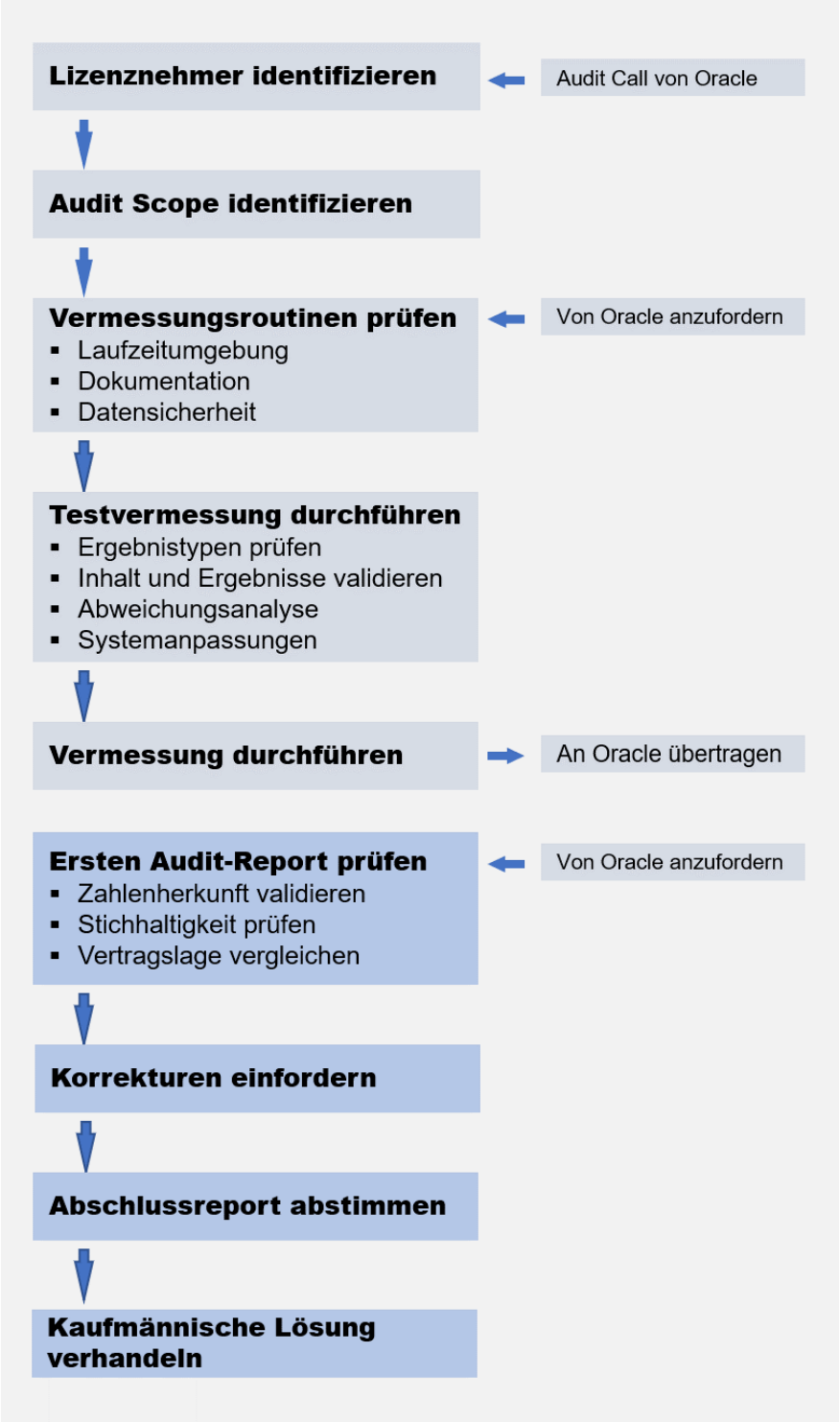
- Für die Technology-Produkte (Datenbanken, Middleware, bzw. Business Information) gibt es strukturierte und seit Jahren geübte Verfahren.
- Für die Produkte der verschiedenen Anwender-Software (E-Business Suite, Siebel, Peoplesoft, etc.) sind teilweise die ursprünglichen Vermessungsverfahren der Hersteller noch im Einsatz.

Oracle überträgt die Durchführung des Audits häufig an Auditoren (regionale Dienstleister), abhängig von der Größe des Audit-Zielunternehmens und dem Audit Scope. Auditoren bieten im Vorfeld von Audits eine Reihe von Schulungen an.

Copyright auditprotect 2017

b. Programmgestützte Vermessung der Technology-Produkte

Die Vermessung für die Oracle-Produkte der Sparte ‚Technology' ist der häufigste Fall und weist die größte Standardisierung auf. Hier ein Ablaufdiagramm zur Vermessung von Oracle Technology:



Quelle: auditprotect

Abb 5.2: Ablaufdiagramm zur Vermessung von Oracle Technology

Copyright auditprotect 2017

Direkt im Anschluss eines Audit Call wirkt Oracle routinemäßig darauf hin, den Adressaten auf fixe Termine (Meilensteine) zu verpflichten zwecks Begrenzung der Audit-Laufzeit. Mit dieser Vereinbarung entsteht ein gewisser Druck auf die Akteure/Fachabteilungen zur termingerechten Lieferung eines Ergebnisses. Zur Erhöhung der Prüfungsqualität im Sinne eines Schutzaufbaus und zur Vermeidung von Compliance-Risiken ist es angeraten, sich diesem Druck durch Einbindung externer Experten zu entziehen. Oftmals liegen nämlich die Gründe von Verspätungen in der verzögerten Kommunikation seitens Oracle oder in ihrer unklaren Lizenzregelung.

Vielen Anwenderunternehmen ist nicht bewusst, dass die konkreten Modalitäten für Software-Audits durchaus verhandelbar sind. Auch während der Durchführung von Audits sind die genauen Maßgaben häufig durch Verhandlung dem aktuellen Umfeld anpassbar.

c. Behandlung des Oracle Audit-Reports

Oracle (ggf. beauftragter Auditor) erstellt den Audit-Report auf Basis der übermittelten Ergebnisse der Vermessungsroutinen, und zwar i.d.R. zunächst als vorläufigen Report zur Abstimmung mit dem auditierten Unternehmen.

Folgende Besonderheiten sind im Falle von Oracle-Technology-Audits zu beobachten:

- Oracle‘s Regelwerke enthalten eine Vielzahl von Bedingungen, deren Verletzung für den Lizenznehmer nicht offensichtlich, aber leicht behebbar ist. Dies erkennt das Anwenderunternehmen häufig nicht, z.B. bei den Parametern zur Virtualisierung.
- Oracle bedient sich zur Begründung von Vermessungsergebnissen regelmäßig ‚erweiterter Tatbestände‘ (Beispiel: indirekte Nutzung), deren Geltung behauptet, aber ggf. nicht vereinbart oder nur in nachträglichen Regeländerungen (Policy) veröffentlicht ist.
- Oracle droht gelegentlich mit Folgen aus fortgesetzter Non-Compliance, die sich auch auf die Versagung zukünftiger Supportleistungen oder gar der Kündigung von Nutzungsrechten erstrecken.

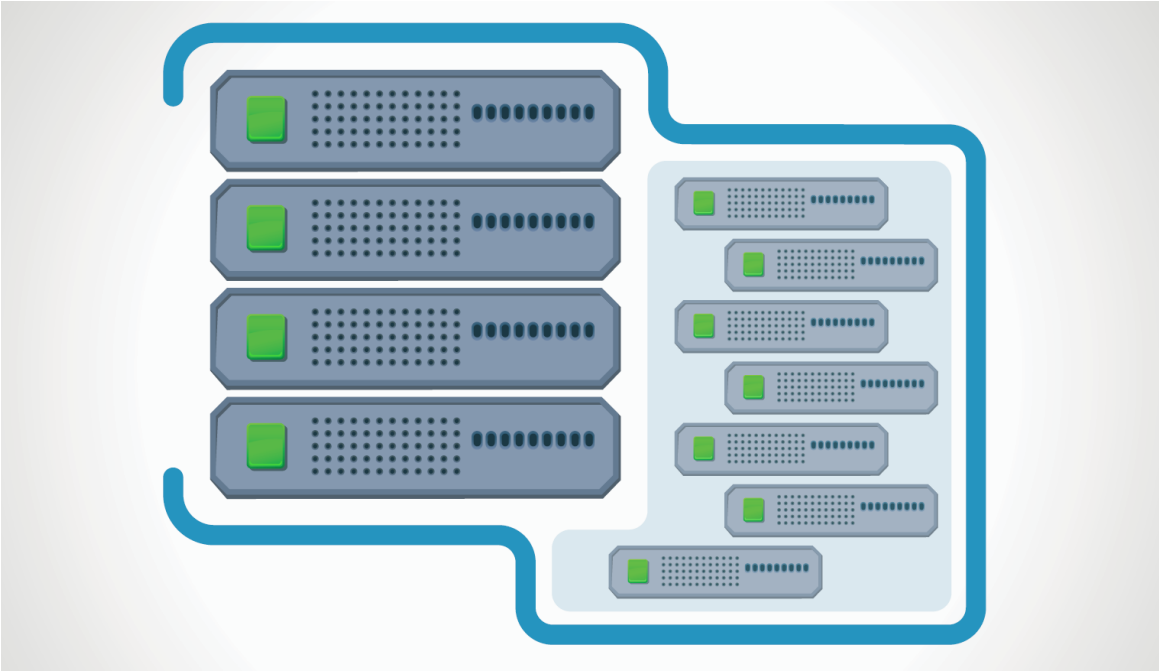
Hinsichtlich der Qualität speziell von Oracle Audit-Reports ist folgendes kritisch anzumerken (s. auch allgemeine Kritik in Ziff. 6.1 unten):

Mitunter drängt sich der Eindruck auf, dass die Oracle-Einheit LMS wenig sorgfältig agiert, wenn es um fundierte, plausible Begründungen für vorgeworfene Non-Compliance geht. So wird anstatt des technischen und softwarerechtlichen Tiefgangs, der für eine überzeugende Herleitung von angeblichen Verstößen für das Unternehmen wichtig ist, einfach seitenweise Zitate aus historischen Vertrags- und Policy-Dokumenten angehäuft. Das erfolgt in Reports und in nachfolgenden PP-Presentations, ohne auf den ersten Blick einen punktgenauen Zusammenhang zum Vorwurf herzustellen. So ist die Relevanz der kopierten Textpassagen als Beleg für die Behauptungen im individuellen komplexen Fall teils nicht transparent. Weit hergeholte Textmassen, mit denen Anwenderunternehmen wiederholt bombardiert werden, können nicht zweifelhafte oder fehlende Sachargumente ersetzen.

Copyright auditprotect 2017

d. Besonderheiten, Entwicklungen

Beim Thema Virtualisierung gibt es seit Jahren Konflikte, die in letzter Zeit zugenommen haben. Es geht um die Frage der Lizenzvergütung von Oracle-Produkten in virtualisierten Umgebungen. Dabei unterscheidet Oracle zwischen den beiden Ansätzen Soft-Partitioning und Hard-Partitioning. Nur letzteres ist für das Unternehmen vorteilhaft. Die Einordnung von fraglichen Prozessen/Technologien behält Oracle sich vor.



Der Einsatz von Virtualisierungstechnologien wie etwa VMware, die Oracle als Soft-Partitioning klassifiziert, führt – aus Oracle-Sicht - zu einer Lizenzierungspflicht für sämtliche Prozessoren beim Unternehmen, auf denen potentiell die Software laufen könnte. Bei bestimmten Versionen des VMware-Produkts vSphere wäre danach nicht nur das gesamte Cluster bzw. das gesamte vCenter zu lizenzieren, sondern alle Prozessoren sämtlicher Server in allen vCentern. Tatsächlich erhöht sich zwar dadurch nicht die Nutzungsintensität der Oracle-Software selbst, was ggf. höhere Gebühren rechtfertigen könnte, aber die Lizenzkosten steigen stark. Das Äquivalenzverhältnis zwischen Vergütungsinteresse und Nutzen beim Unternehmen gerät aus den Fugen.

Auch nach Verlautbarungen der User-Vereinigung DOAG ist die Wirksamkeit der rechtlichen Grundlage stark in Zweifel zu ziehen. Nach vertraglichen und technischen Analysen seien die Anspruchspositionen von Oracle im Ernstfall kaum haltbar. Ein nur fallweiser individueller Genehmigungsprozess durch Oracle (sog. VLAN-Approval) ist verhandlungsaufwändig und bleibt unsicher angesichts fortlaufender Änderungen in der IT-Architektur.

Die Fremdhersteller von Virtualisierungstechnologien stellen Monitore zur Verfügung, welche die geforderte Abgrenzung der verwendeten Ressourcen im Betrieb ermöglichen und den Oracle-eigenen Kontrollmechanismen gleichzusetzen sind. Durch geeignete Detail-Argumente erfahrener Lizenzberater und Anwälte für Softwarerecht sind die Oracle-Positionen durchaus angreifbar.

Copyright auditprotect 2017

e. Audit von Oracle-Java-Installationen

Bis Januar 2023 war die kommerzielle Nutzung von Oracle-Java durch eine Lizenzmodell geprägt, welches die nutzenden Client-User und die Server differenziert in Ansatz brachte.

Im Januar 2023 hat Oracle eine neues Lizenzmodell in die Welt gesetzt, dass am ehesten mit einer Site-License vergleichbar ist: Wenn auch nur eine einzige Person in einem Unternehmen mit z.B. 10.000 Arbeitskräften Java-Software von Oracle benutzt, dann richtet sich der Preis nach dieser Gesamtzahl von 10.000. So, als ob diese alle Nutzer wären, obwohl es in Wirklichkeit nur einen einzigen Java-User gibt.

Die Lizenzgebühren berechnen sich nach der Anzahl von Arbeitskräften in jeglicher Beschäftigungsform, egal ob in Festanstellung, in Teilzeit und mit Befristung, also inklusive Aushilfen und Saisonkräfte. Dieser Personenkreis mag im Umfeld der eigenen Kernbelegschaft mit einigem administrativem Aufwand noch eingrenzbar und erfassbar sein.

Kontrollverlust durch ausufernde Preisbemessung?

Aber es wird noch komplizierter: Vollends ausufernd und undurchsichtig wird die Preisbemessung durch Einbeziehung eines zusätzlichen Personenkreises außerhalb des Anwenderunternehmens. Denn auch bei dessen Geschäftspartnern wie Vertreter, Auftragnehmer, Outsourcer und Berater werden die entsprechenden Arbeitskräfte mitgezählt. So sagt es die weitgreifende Definition der neuen Mitarbeiter-Metrik in der Oracle Global Price List, mit dem sperrigen Namen "Oracle Java SE Universal Subscription".

Auf den Punkt gebracht heißt das für IT-Finanzmanager: Die Lizenzkosten richten sich auch nach der Mitarbeiteranzahl ganz anderer Akteure, nämlich nach fast der Gesamtheit der Geschäftspartner, wenn sie in irgendeiner Weise die internen Geschäftsabläufe unterstützen. Wohlgemerkt, das ist alles unabhängig davon, ob die extrem weitgezogenen Personenkreise die Java-Software überhaupt nutzen.

Eine Menge ungeklärter praktischer Probleme bei Definition, Eingrenzung und Abgrenzung liegt auf der Hand. Das Ergebnis ist eine bemerkenswerte Unschärfe und Intransparenz der Preisbemessung, was die Position des Anwenders verwässert. So sind Räume für Willkür und letztlich Verhandlungsmacht eröffnet, die Oracle gegenüber dem Anwender ausspielen kann.

Explodieren die Lizenzkosten?

Veröffentlichte Kalkulationsbeispiele von Beratern zeigen eine explosionsartige Vervielfachung der künftigen Lizenzkosten im Vergleich zum bisherigen Preissystem. Dieses richtete sich nach der Anzahl von Clients und Servern beim Anwender. Auf Basis der neuen Preispolitik nach Personenanzahlen wird jetzt teils eine Vervierfachung der Java-Lizenzgebühren errechnet, und je nach Konstellation sogar eine Verdreißigfachung!

Geraten strategische Planungen von Budgets und Software-Landschaften ins Wanken? Viele IT-Finanzmanager fühlen sich jedenfalls mit einer fragwürdigen und bedrohlichen Preisbemessung konfrontiert.

Copyright auditprotect 2017

Ständiger Entscheidungszwang

Das Problem stellt sich für den CFO nicht einmalig punktuell, sondern immer wiederkehrend, falls der Weiterbetrieb von Java gewollt ist: Mit Ablauf der jeweiligen Mietzeit („Subscription") entfällt das Nutzungsrecht des Anwenders automatisch. Zudem lässt Oracle für jedes Java-Release von Zeit zu Zeit die in der Subscription enthaltenen Support-Leistungen auslaufen. Damit endet die betriebsnotwendige Versorgung mit Sicherheits-, Performance- und Bugfix-Updates. Nur gegen Zusatzkosten – und auch dies nur zeitlich limitiert - erhält der Anwender weiteren Support.

Zwar stellt Oracle auch kostenfreie Java-Releases zur Verfügung. Aber das ist oft nicht der praktikable Ausweg für die Unternehmen. Denn auch das Ausweichen auf ein aktuelleres kostenfreies Release ist intern mit Zeitaufwand, Kosten und Risiken aufgrund der Migration verbunden, einschließlich möglicher Umstellungen in Technik und Abläufen.

Das Dilemma: Diese Wahl zwischen erdrückenden Lizenzpreisen und belastenden Migrationsfolgen müssen Budgetverantwortliche für jeden neuen Mietzeitraum und bei jedem Nachfolge-Release erneut treffen.

Sind IT-Finanzchefs voll informiert?

Das Problem verschärft sich dadurch, dass den Verantwortlichen oft gar nicht bekannt ist, ob eine Java-Nutzung im Unternehmen stattfindet, geschweige denn deren Art, Umfang und Umstände. Welche Verträge mit ggf. unterschiedlichen Regelungen und Laufzeiten wurden in der Vergangenheit abgeschlossen? Ist eine vielleicht vorhandene Lizenz zu verlängern oder ist sie überflüssig?

Fortführung nach alter Metrik oder Zwang zu neuem Preismodell? Gibt es Unternehmensbereiche, wo die Software durch einzelne Personen unautorisiert zum Download und so „inoffiziell" in Nutzung kam?

Das alles können IT-Finanzchefs zeitlich weit vor den nächsten Software-Lizenz-Audits abklären lassen. Diese werden generell von großen Software-Anbietern wie Oracle und SAP regelmäßig bei ihren Kunden durchgeführt. Spätestens beim Audit kann es zu Nachforderungen kommen, deren Höhe niemand erwartet und eingeplant hat.

Neue Preispolitik: Ein systemwidriger Fremdkörper?

Wer mit Software-Budgets zu tun hat, weiß: Software-Metriken reflektieren regelmäßig das wirtschaftliche Partizipationsinteresse der Lizenzgeber/Vendoren. Maßstab dafür ist die Nutzungsintensität beim Anwender. Je höher der wirtschaftliche Nutzen für das Unternehmen - ausgedrückt etwa durch die User-Anzahl -, desto mehr soll der Vendor durch die Höhe der Vergütung partizipieren. Bei Software-Miete ist die Vergütung verbrauchsabhängig gestaltbar, etwa mittels der Anzahl oder der zeitlichen Dauer von Nutzungsvorgängen / Zugriffen.

Copyright auditprotect 2017

Anders jedoch das neue Oracle-Lizenzmodell:
Die Mitarbeiter-Metrik stellt gar keinen Anknüpfungspunkt zur tatsächlichen Nutzungsintensität von Java mehr her. Denn der Preis ist ja gerade nicht nutzungs- bzw. verbrauchsabhängig, sondern er richtet sich nach einer ganz anderen, sachfremden Kategorie: Nämlich nach der Mitarbeiteranzahl unterschiedlicher Marktakteure, die niemals User waren und auch künftig niemals Zugriffe tätigen werden. Das stellt alles auf den Kopf, das ist ein Systembruch. Entsprechend finden etliche Oracle- Kunden die neue Preispolitik unfair und wandern ab.

Darf Oracle das denn überhaupt?

Das fragen sich alle Beteiligten zu Recht. Darf man denn jahrelang das Vertrauen von treuen Kunden in die fortlaufende Java-Lizenzierung auf Mietbasis in Anspruch nehmen und dann plötzlich die Preisgrundlage kippen, auf die sich alle in ihren Dispositionen verlassen haben?

Haben Vendoren denn ein willkürliches „Metrik-Erfindungsrecht“, wie hier die weite Einbeziehung von Personenkreisen auch ganz anderer Marktakteure? So wie der Staat ein Steuererfindungsrecht nach Beliebigkeit hat, etwa für Hundehaltung, Vergnügung, Kaffee, Zweitwohnsitz, und zwar ohne seine Leistungen speziell dafür zu erbringen?

Ausweg: Nutzung von kostenfreien Releases?

Mit welchen Methoden lässt sich denn die Beschränkung auf kostenfreie Releases nachweisen?

Hierzu ist eine Vermessungssoftware erforderlich, welche

1. sämtliche Vorkommen von Oracle-Java Editions in einem Firmennetzwerk entdeckt,
2. alle Parameter zur Identifikation der jeweiligen Edition vollständig detektiert und
3. die parallele Nutzung von Oracle Java Commercial Features ausschließt.

Wenn eine vollständige Eigenvermessung mit entsprechender Zuverlässigkeit vorgelegt werden kann, so kann das die Zulässigkeit weiterer Auditmaßnahmen in Frage stellen.

Daher ist die detaillierte Vermessung eine erforderliche Voraussetzung für die Audit-Abwehr.

Gefahr verdeckter Audits

Oracle erhält über seine eigenen Download-Server Informationen über die Zielsysteme der Downloads. Dies kann nicht mit Sicherheit durch Cyber-Security-Tools verhindert werden. Daher sollte sich jedes Anwenderunternehmen darüber klar sein, dass Oracle über Informationen verfügen kann, welche frühere Downloads noch heute nachweisbar machen.

Daher ist zu prüfen, ob durch eine permanente Bestandsüberwachung durch geeignete Scanner-Tools die Vermeidung jeglicher Compliance-Verletzung glaubhaft gemacht werden kann und so Oracle das Interesse an Audits verliert.

Copyright auditprotect 2017

5.3 Microsoft

a. Verfahrensgrundlagen

Das Betreiben von Audits erfolgt i.d.R. durch beauftragte Dienstleister/Auditoren und wird intern überwacht von der Einheit Software Asset Management (SAM).

Quellen für Audit-Rechte von Microsoft können sich z.B. ergeben aus den Ausführungen zur *Nachprüfung der Vertragserfüllung* in Microsoft Business Agreement bzw. MBSA, Microsoft Business & Service Agreement.

Oft lassen sich einschlägige Audit-Klauseln schwerer identifizieren, wenn alternative Beschaffungswege mit speziellen Agreements genutzt werden. Es steht nämlich jedem Unternehmen frei, Lizenzen über den von Microsoft vorgesehenen Standardvertriebsweg im Inland, über freie Händler international oder auch direkt von anderen Anwenderunternehmen zu erwerben. Letztere auch als Gebrauchtsoftware bezeichnete Variante bietet sich insbesondere dann an, wenn die erforderlichen Lizenzen nicht mehr über den Standard-Vertriebsweg zu erhalten sind.

Liegt eine Mischbeschaffung vor, z.B. aus Altlizenzen, Volumenverträgen und Zukäufen über Drittmärkte, so gilt es insbesondere, die Nutzungsrechte gut zu dokumentieren und die Auditoren geeignet zu informieren.

Microsoft auditiert die Anwenderunternehmen nicht regelmäßig, sondern legt mehr Wert auf die Vertiefung der Kundenbeziehung. Daher hat Microsoft in der Vergangenheit diverse Schritte unternommen, die Aufgabe der License Compliance Verifizierung auf die Anwenderunternehmen bzw. ihre jeweiligen Microsoft-Reseller zu verlagern.

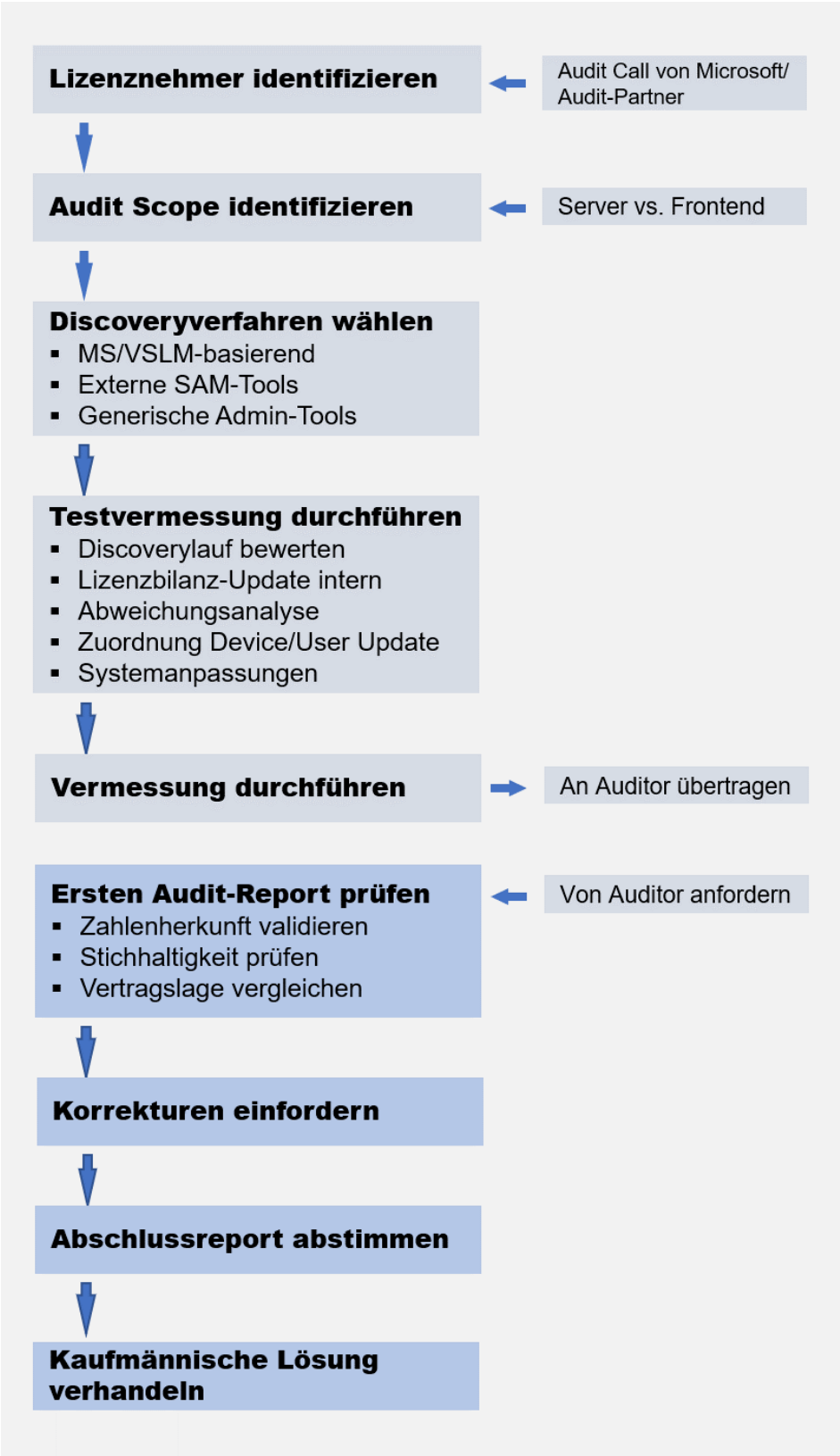
Allein die Vielzahl von beteiligten Stellen, welche in die Umsetzung von Audits eingebunden sein können (Microsoft-Reseller, Auditoren, Microsoft selbst über interne SAM-Einheit), verkomplizieren die Rechtsbeziehungen und Maßgaben im Rahmen des Audit zusätzlich. Daher ist es vor Beginn einer Vermessung ratsam, die genauen Microsoft-Grundlagen mit externer Softwarerechts- und Lizenzexpertise zu prüfen und Einfluss auf die Anwendung fairer Verfahren zu nehmen.

Diese Audit-Guideline behandelt keine spezifischen Verfahren zur Vermessung von weiteren Microsoft-Produkten, wie z.B. Microsoft Dynamics (ERP und CRM).

Ebenso bleiben die Cloud-basierten Angebote von MS 365 bzw. Office 365 unbehandelt, da diese über das Microsoft-Lizenzportal bestellt werden und keinen Audit in der On-Premise-Umgebung mehr erfordern.

Copyright auditprotect 2017

b. Programmgestützte Vermessung Microsoft



Quelle: auditprotect

Abb 5.3: Ablaufdiagramm Microsoft-Audit

Copyright auditprotect 2017

c. Behandlung des Microsoft Audit-Reports

Für einen Großteil der Frontend- und Server-Produkte nimmt Microsoft eine technische Verankerung der Lizenzspezifikation in die Laufzeitumgebung vor, z.B. über die Registry. Dies erlaubt dem Administrator, über das Auslesen dieser Informationen (‚Discovery') einen ersten Überblick über die installierten bzw. genutzten Lizenzen zu erhalten. In der Folge der Interpretation dieser Informationen und mittels Vergleichs mit den zugehörigen Lizenzregeln kann für interne Zwecke oder für das laufende Audit ein Audit-Report erstellt werden.

Setzt das Anwenderunternehmen eigene Tools zur Überprüfung der Compliance ein (SAM-Tools), so ist der Auditor oftmals mit der Übermittlung der entsprechend gefertigten Lizenzbilanz zufrieden. Im gegenteiligen Fall bieten solche Tools zumindest eine einfache Basis für die Verifikation der Microsoft-Audit-Ergebnisse.

Copyright auditprotect 2017

6. Reaktion auf Audit-Report des Vendors

Der Audit-Report des Vendors dient eigentlich dem Zweck, dem Anwenderunternehmen seine Unterlizenzierung und die Notwendigkeit zum Lizenznachkauf aufzuzeigen. Der Vendor wird die Darstellung i.d.R. so gestalten, dass seine Schlussfolgerungen und Forderungen nicht in Frage gestellt werden.

Es ist wichtig, auf die vorgelegten Audit-Reports mit Sorgfalt und Entschlossenheit zu reagieren, denn sie stellen die Grundlage für die anschließend geltend gemachten kommerziellen Forderungen dar. Dabei ist die Vendor-Sicht kritisch zu hinterfragen. Leitlinien sollten dabei einerseits das Verständnis der Rechtslage sowie die Wahrung der kommerziellen Unternehmens-interessen sein.

Folgende technischen, softwarerechtlichen sowie kommerziellen Erfahrungswerte sind aufzuarbeiten:

6.1 Vorläufiger Audit-Report

- Die Form des Reports ist nicht selten unbefriedigend.
  Je nach Tiefe der Lizenzprüfung stellen die Vendoren ihre Ergebnisse in einer Form dar, die einen Zukauf nahelegen. Dieser initiale Bericht enthält oft nicht die notwendige Tiefe und Transparenz, die zur überzeugenden Begründung eines Nachkaufs erforderlich sind.
- Die Herangehensweise der Vendoren/Auditoren ist von unterschiedlicher Qualität.
  Im ersten Report sind nicht selten fehlerhafte Darstellungen oder Interpretationen enthalten, es fehlt gelegentlich an notwendiger Fachkenntnis zur Bewertung von Vermessungsergebnissen im weiteren Kontext.
- Es mangelt nicht selten an der korrekten Interpretation der individuellen Softwareverträge.
  Die Vendoren/Auditoren haben Zeitdruck und verfügen nicht immer über eine tiefere Kenntnis der konkreten Nutzungsbedingungen aus einschlägigen Verträgen.
- Die Übersicht über die Vertragshistorie ist mitunter begrenzt.

Alle Aspekte von unrichtigen Bewertungen seitens der Vendoren/Auditoren sind sorgfältig zu widerlegen, damit für den Abschlussbericht auf Basis des korrekten Sachverhalts daraus resultierenden Nachforderungen abgeleitet werden können.

6.2 Audit-Abschlussbericht

- Der Abschlussbericht (finaler Audit-Report) sollte eine Aussage über die bestehende bzw. zu erreichende Compliance, bezogen auf den Audit Scope, enthalten.
- Maßnahmen zur Beseitigung von etwaigen Non-Compliance-Tatbeständen werden benannt. Das kann verschiedene Varianten einschließen, die vorher diskutiert wurden, z.B. Kulanz, Stilllegung/Parken von Lizenzen etc.
- Der Abschlussbericht sollte im geeigneten Projektgremium, bestehend aus den relevanten Akteuren ggf. samt externer Audit-Experten, bewertet werden und erst dann als akzeptierte Grundlage für die kommerzielle Lösung gelten.

Copyright auditprotect 2017

7. Kaufmännische Lösung

Das Audit ist erst abgeschlossen, wenn die identifizierte und beidseitig anerkannte Non-Compliance behoben ist, bzw. die Verpflichtung zur Behebung vertraglich feststeht. Die finale kaufmännische Lösung entsteht aus der Betrachtung mehrerer miteinander verbundener Themenkomplexe:

7.1 Herstellung der Compliance

Im Fall von festgestellter Non-Compliance - dokumentiert im finalen Audit-Report (Abschlussbericht) - erstellt der Vendor eine Stückliste für weitere erforderliche Lizenzen, die das Unternehmen zur Behebung des Defizits beschaffen muss. Der Zukauf erfolgt auf Basis eines abzuschließenden Softwarekaufvertrags. Dieser beinhaltet oftmals eine Transaktion, die über die minimal erforderliche Herstellung von Compliance hinausgeht. Denn der Deal kann bereits auch zukünftige Bedarfe berücksichtigen, die das Unternehmen anlässlich des Audits erkannt hat (teils mittels vertrieblicher Überzeugungsarbeit des Vendors) und vorausschauend sofort mit erledigen möchte.

7.2 Preisverhandlungen / Konditionen

Mit dem Wunsch nach bereits zukünftiger Bedarfsdeckung kann sich das Umsatzvolumen für den Vendor erweitern, was einen größeren preislichen Verhandlungsspielraum zugunsten des Unternehmens eröffnet. Wird dieser Verhandlungsspielraum vom Vendor nicht im Sinne des Unternehmens berücksichtigt, so könnte eine verbesserte Ausgangslage durch Einbindung von externer Softwarerechts- und Lizenzexpertise herbeigeführt werden.

Copyright auditprotect 2017

Jedenfalls ist das Bestehen des Vendors auf Listenpreise zum Ausgleich von Non-Compliance (ohne sonst üblicher Rabatte) schon vor Beginn der Preisverhandlung aus dem Weg zu räumen. Denn das ist als Strafkomponente rechtlich zweifelhaft.

Zur wertmäßigen Beurteilung und Verhandlung der Transaktion sind die üblichen Themen der Beeinflussung von Preis und Rabatt zu bemühen. Ein wichtiger Bestandteil dieser Preisdiskussion sind die historischen Bestpreise, als auch Preis-Benchmarks vergleichbarer Unternehmen. Solche Preis-Benchmarks werden von spezialisierten Beratungspartnern wie auditprotect mit Vendor-spezifischen Vergleichsdaten auf Basis von License12.com, einem Tool als Internetplattform, angeboten.

Hinzu tritt typischerweise ein zeitliches Thema, nämlich der Quartalsabschluss des Vendors, der die Handlungsweise seiner Vertriebsbeauftragten im Sinne einer schnellen Einigung prägt (Interesse an Umsatzsteigerung). Um den Zeitdruck beim Vendor zum eigenen Vorteil zu nutzen, sollte das Unternehmen den Zeitpunkt des Quartalsabschlusses (z.B. beginnt bei Oracle das Geschäftsjahr mit Juni) frühzeitig in die verhandlungstaktische Planung des Audit-Ablaufes einbeziehen. Denn je großzügiger sich der Vendor auf die Interessen des Unternehmens einlässt, desto eher beschleunigt er den Einigungsprozess in seinem eigenen Abschlussinteresse.

7.3 Umgang mit nutzlosen Lizenzen

Ein Ergebnis der Audit-Reports kann die Aufdeckung nutzloser Lizenzen sein, also existierende Nutzungsrechte an Software, die in der Installation keinen betrieblichen Wert entfalten können, weil sie z.B. veraltet, inkompatibel, höherwertig als benötigt oder durch ihre Metrik für die Unternehmenspraxis ungeeignet sind.

Copyright auditprotect 2017

In einem solchen Fall ist es gängige Praxis, die betreffenden Lizenzen zu migrieren. Das bedeutet, dass die Werte der nutzlosen Lizenzen gegen neue, gewünschte Produkte in kaufmännisch akzeptabler und geeigneter Weise verrechnet werden. Was hier unter ‚akzeptabel' verstanden wird, ist oftmals Verhandlungssache.

Eine kaufmännische Lösung sollte jedenfalls beinhalten, dass keine nutzlosen Lizenzen fortgeschrieben werden, wenn sich auch in der künftigen IT-Planung keine neue Nutzungsoption für diese abzeichnet.

7.4 Kosten des Audit

Audit-Klauseln können vorsehen, dass das Anwenderunternehmen im Fall festgestellter Non-Compliance Audit-Aufwendungen des Vendors tragen soll. Umgekehrt wäre auch denkbar, den Vendor mit internem Projektaufwand aufgrund extensiv geforderter Mitwirkungshandlungen zu belasten. Beides wird aber kaum praktiziert.

Dies könnte im Rahmen der ersten Reaktion an den Vendor Teil einer Vereinbarung über den Gesamtkomplex (siehe Ziffer 4.4) werden.

7.5 Bestätigung der Compliance

Eine etwaig gewünschte Bestätigung der Compliance handhaben die Vendoren i.d.R. sehr restriktiv und wollen dies auch nur auf Anfrage überhaupt diskutieren. Sie argumentieren, dass die jeweiligen Vermessungsverfahren immer nur eine unvollständige Momentaufnahme seien. Insoweit sind die Vermessungen für die Anwenderunternehmen lediglich von begrenztem Nutzen.

Sofern eine Compliance-Bestätigung erfolgt, bezieht sie sich oft nur auf die im Verfahren untersuchten Lizenzierungssachverhalte, die untersuchten Systeme und auf den Untersuchungszeitpunkt. Eine weitere Einschränkung kann in der Behauptung des Vendors bestehen, man habe nicht sämtliche übermittelten Vermessungsergebnisse zur Kenntnis genommen.

Copyright auditprotect 2017

8. Anmerkungen zu Audits für Cloud-Software

Zum Wesen der Nutzung von Cloud-Software gehört ihr Installationsort, der nicht wie üblich On-Premise beim Anwenderunternehmen liegt. Die Installation – erreichbar für eine Vielzahl von weiteren Anwendern - liegt in der Betriebsverantwortung des Providers an einem Ort seiner Wahl. Aufgrund seiner Verfügungsgewalt ist insofern der Provider für die Überprüfung und Sicherstellung der vertragsgemäßen Nutzung verantwortlich, und nicht mehr das Anwenderunternehmen. Dessen neue Nutzer müssen sich vor Beginn der Nutzung den Zugriff vom Provider autorisieren lassen. Dieser hat dabei alle Möglichkeiten, den Zugriff nur bei ausreichender Lizenz zu erlauben.

Dieses vereinfacht dargestellte Szenario wirft allerdings eigene Fragestellungen beim Anwender auf:

- Wie prüft man die Nutzungsaufzeichnungen des Providers (Abrechnungsgrundlage)?
- Können sich die Nutzer ebenso einfach abmelden, und sind diese Lizenzen sofort wieder für andere verfügbar?
- Wie ist die Nutzung generell kündbar, gibt es ein einheitliches Ausstiegsdatum?
- Wie verfährt man bei Gebührenerhöhungen seitens des Providers?
- Wird die vereinbarte störungsfreie Verfügungsbereitschaft eingehalten?
- Sind die Unternehmensdaten auch ohne die Cloud-Anwendung verfügbar (aktuelle Sicherungskopien)?

Insbesondere der erste Punkt ist kritisch, denn nur der Provider kennt die Nutzungsprotokolle. Es ist demnach folgerichtig, bei Cloud-Anwendungen über eine Umkehrung der Audit-Berechtigung nachzudenken: Wie kann also der Provider dem Unternehmen nachweisen, dass die bei ihm aufgezeichneten Nutzungshandlungen tatsächlich vom Anwender vorgenommen wurden?

Dabei werden auch im Cloud-Bereich die Lizenzregeln immer komplizierter, z.B. durch Verknüpfung einzelner Lizenztypen und durch innovative Berechnungskonzepte für den Ressourcenverbrauch. Es zeichnet sich damit ab, dass zwar die Rollen wechseln mögen, aber nicht

Copyright auditprotect 2017

die Problemstellung: Zukünftig wird das Anwenderunternehmen eine Kompetenz vorhalten müssen, um die Nutzungsberichte der Provider vollständig validieren zu können!

9. Weitergehende Vendor-Informationen

Folgende Quellen von Vendoren können zur weiteren Erläuterung der Themen dienen (Stand 01.12.2018):

Microsoft:
Standardverträge
https://www.microsoft.com/en-us/licensing/licensing-programs/licensing-programs.aspx
Lizenzregeln
https://www.microsoft.com/en-us/download/confirmation.aspx?id=11091
Auditverfahren
https://www.microsoft.com/en-us/licensing/learn-more/compliance-verification-faq.aspx
Service-Provider-Bezugsmöglichkeiten
https://www.microsoft.com/de-de/Licensing/lizenzprogramme/spla.aspx

Oracle:
Standardverträge
http://www.oracle.com/us/corporate/contracts/index.html
Lizenzregeln
http://www.oracle.com/us/corporate/pricing/sig-070616.pdf
Auditverfahren
https://www.oracle.com/corporate/license-management-services/index.html

SAP:
Standardverträge
https://www.sap.com/about/agreements.html
Lizenzregeln
https://www.sap.com/docs/download/agreements/product-use-and-support-terms/sur/sap-list-of-prices-and-conditions-sap-software-and-support-sur-german---germany-v10-2018.pdf
Auditverfahren (verlangt Zugang zum SAP Service Marktplatz)
https://support.sap.com/en/my-support/systems-installations/system-measurement/system-measurement-information/documentation.html

Copyright auditprotect 2017