Cigref

Audits de licences logicielles : Charte des bonnes pratiques 2021

Recommandations des membres du Cigref à l'usage des clients et de leurs fournisseurs

Décembre 2021

Audits de licences logicielles : Charte des bonnes pratiques 2021

Recommandations des membres du Cigref à l'usage des clients et de leurs fournisseurs

Mise à jour de la Charte de septembre 2015 du Club Achats Cigref

La présente Charte des bonnes pratiques en matière d'audit de licences logicielles consiste en la mise à jour du document initialement élaboré en 2010 puis actualisé en 2015 dans le cadre des activités du Club Achats du Cigref. Cette dernière mise à jour de 2021 a été réalisée sous la supervision du comité de pilotage du Club Relations fournisseurs du Cigref, avec la contribution active d'une dizaine de juristes, d'acheteurs et de gestionnaires d'actifs logiciels d'organisations membres du Cigref, constitués en taskforce « audit management ».

La présente Charte est assortie d'un clausier comprenant une proposition de clause d'audit type, élaborée par la taskforce, et d'un modèle de protocole d'audit.

TABLE DES MATIÈRES

PROPOS LIMINAIRE

De nombreux grands comptes utilisateurs de licences constatent depuis plusieurs années une tendance à la multiplication des audits de licences de logiciels par les éditeurs. Être conforme à 100 % est impossible pour une entreprise, constat partagé par tous (utilisateurs comme éditeurs). Les audits se déroulent généralement dans des conditions de coopération mutuelle et aboutissent à des conclusions équilibrées. Toutefois, il arrive qu'à l'occasion d'audits, les éditeurs cherchent à maximiser les régularisations, ce qui crée un climat de suspicion entre l'éditeur et le client.

Ainsi, les membres du Cigref constatent que les éditeurs s'appuient parfois sur des clauses contractuelles sujettes à interprétation – d'où un **problème de lisibilité** pour le client – et/ou qui évoluent dans le temps au fil de la relation contractuelle de manière unilatérale – d'où un **problème de prévisibilité**. Ils constatent également que la complexité des modèles de *licensing* des éditeurs rend difficile le **contrôle de la conformité** en amont et encourage la recherche de « failles » par les éditeurs.

Au-delà de ces remarques liées au référentiel contractuel, les membres du Cigref estiment que la méthodologie suivie pendant les audits est souvent très **consommatrice de temps.** Ils regrettent également que le nombre de clauses d'audit insérées dans les différents contrats conduise à un risque de **« droit d'audit permanent »**, avec la nécessité de devoir mobiliser d'importantes ressources internes de manière récurrente.

S'agissant du déroulement des audits à proprement parler, les membres du Cigref observent que les outils de mesure, installés sur leurs systèmes d'information, peuvent poser des **problèmes de transparence, de sécurité et de conformité au regard du RGPD s'agissant des données à caractère personnel.** A cet égard, l'éditeur doit veiller à ce que l'utilisation de ses outils ou scripts d'inventaire ne mette pas en défaut les clients au regard du législateur et des autorités de contrôle. Les membres du Cigref pointent également le risque de conflits d'intérêts lorsque les éditeurs recourent à des tiers auditeurs qui ne sont pas astreints à des **règles de déontologie et de confidentialité** partagées avec le client.

Enfin, sur le plan financier, les clients souhaitent identifier les **situations de bonne foi** où ils n'ont pas connaissance des cas de dépassement des droits acquis, avec le souhait de ne pas devoir acquitter des licences majorées, et de bénéficier des conditions négociées lors des derniers achats.

La charte élaborée en 2010 puis mise à jour en 2015 a servi de référence durant plusieurs années aux membres du Cigref, pour refuser les scripts ou exiger l'assurance/l'engagement de l'éditeur de l'absence de risque ou de collecte de données non nécessaires à l'audit. La charte a ainsi participé à équilibrer le rapport de force entre clients audités et éditeurs dans une période pré-*cloud computing*, où les audits de licences logicielles étaient alors très fréquents.

L'avènement du cloud ne rend pas moins cruciaux les audits pour les fournisseurs, qui peuvent se servir des non conformités identifiées pour inciter leurs clients à migrer dans le cloud. La pratique des audits de licence reste donc répandue et source d'incertitudes économiques et juridiques pour les entreprises. D'autant que les organisations utilisatrices de services numériques s'engagent majoritairement dans une démarche de cloud hybride et que leur trajectoire de migration dans le cloud s'inscrit sur plusieurs années. Il leur faut donc composer avec le SI patrimonial et en particulier, le parc logiciels *on-premise* existant, tout en adoptant les nouveaux modèles de licences et de facturation liés à la consommation de services dans le cloud.

Enfin, contrairement à une idée répandue, la migration dans le cloud ne protège pas entièrement pas le client des audits puisqu'il convient de vérifier la conformité de l'utilisation avec les usages prévus au contrat, y compris dans le cloud.

La préparation du client, et son organisation en amont, pendant et en aval de l'audit reste donc un enjeu important pour les membres du Cigref, qui n'ont pas tous une gestion des actifs logiciels centralisée et structurée. En complément de la présente charte, la taskforce *"Audit Management"* recommande à ce titre la lecture du guide « Software Asset & Cloud Management : de la gestion des actifs logiciels à l'optimisation des services » - Cigref/Elée, mis à jour en octobre 2018 (rapport public).

1. PRINCIPES

Les organisations utilisatrices reconnaissent le droit des éditeurs à vérifier que les usages des licences faits par leurs clients sont conformes aux droits concédés contractuellement. Toutefois, l'usage des audits par les éditeurs doit être encadré contractuellement par des pratiques claires, équilibrées et partagées, et respecter certains principes. Ces principes sont mentionnés ci-dessous. Leur déclinaison opérationnelle figure dans la liste des bonnes pratiques ci-après.

1.1. EN AMONT : LA MISE EN PLACE D'UN SOCLE CONTRACTUEL GARANTISSANT LA CONFIANCE

Le client et l'éditeur doivent se mettre d'accord, en amont et si possible dès la conclusion du contrat de licence, sur un cadre contractuel encadrant l'audit et évitant certaines pratiques source de litiges.

Le cadre contractuel applicable doit exister sur un support durable, non modifiable. Les modèles de *licensing* et les règles d'audit doivent faire l'objet d'un accord par les personnels habilités du client. **Les contrats conclus au moyen d'un clic ou par référence à un lien hypertexte sont à proscrire.**

- Les contrats doivent **permettre une gestion flexible du parc** de licences par le client, notamment en autorisant les réallocations intra-groupe sans surcoût (sous réserve de considérations fiscales ou de règles d'exportation).

- Le contrat de licence doit **envisager les conséquences d'une virtualisation** du parc et/ou le recours à des technologies de *cloud computing*.

- Les contrats doivent **proscrire les options activées par défaut** (qui peuvent être source de non-conformité ultérieure à l'insu de l'acheteur) ou bien contenir un avertissement explicite desdites options afin de permettre au client de gérer son parc en toute connaissance de cause.

1.2. RAPPEL DES PRINCIPES PREVALANT LORS D'UN AUDIT DE LICENCES

Le client et l'éditeur doivent respecter certains principes améliorant la fluidité de l'audit et la coopération des parties :

- L'éditeur dispose d'un droit de vérification de la non-violation de ses droits de propriété intellectuelle. Les modalités d'exercice de ce droit extracontractuel sont à prévoir dans le

contrat. L'audit doit nécessairement **reposer sur des stipulations contractuelles claires, non équivoques et négociées au moment de la conclusion du contrat** plutôt qu'au moment du déclenchement de l'audit**.** En cas d'ambiguïté, l'interprétation restrictive doit prévaloir.

- L'entreprise cliente doit être avertie de l'audit suffisamment à l'avance afin de pouvoir prendre les mesures de nature à **minimiser l'impact et la perturbation** de ses systèmes d'information. Pour les entreprises ayant une activité saisonnière, les périodes occasionnant le moins de perturbation seront privilégiées.

- L'audit doit **être exécuté de bonne foi.** En pratique, il ne peut servir qu'à vérifier la conformité d'utilisation du parc de licences, et n'être motivé que par une exécution de bonne foi du contrat.

- **L'approche d'auto-certification (audits déclaratifs) doit être privilégiée.** Ceci afin d'éviter dans la mesure du possible l'usage d'exécutables par l'éditeur sur lequel le client n'a pas le contrôle et qui peuvent présenter des risques pour son système d'information et/ou créer un climat de suspicion. Ainsi, un audit intrusif ne devrait avoir lieu que si l'éditeur justifie de doutes légitimes sur les conclusions d'un audit déclaratif.

- **Le déclenchement d'un audit doit faire l'objet d'une notification** précise quant à son périmètre (périmètre géographique, licences visées, entités concernées…) et ses modalités de mise en œuvre. En particulier, l'audit par des tiers doit être approuvé contractuellement, les éventuels programmes utilisés par l'éditeur doivent pouvoir être vérifiés par le client.

- **Lors du déclenchement de l'audit, le Cigref recommande la négociation et la signature d'un protocole d'audit** entre l'entreprise auditée et l'éditeur, définissant les modalités d'exécution, de prise en charge et de conclusion de l'audit, susmentionnées.

- **La conclusion de l'audit doit être contradictoire,** c'est-à-dire validée par l'entreprise auditée. Elle ne doit pas servir de support pour une négociation commerciale englobant des sujets différents.

2. BONNES PRATIQUES RECOMMANDÉES EN MATIÈRE D'AUDIT DE LICENCES

La présente Charte pose quelques principes généraux, qui selon les membres du Cigref, devraient présider à tout audit de licences de logiciels. Ces objectifs se veulent équilibrés et respectueux des préoccupations des deux parties.

D'un point de vue pratique, la Charte du Cigref a vocation à :

- **En amont : Être utilisée avant la conclusion d'un contrat de licences, afin de servir de socle à la négociation de clauses d'audit équilibrées et non équivoques ;**

- **En aval : Servir de référentiel pour appréhender le déroulement d'un audit.** Par exemple, le client peut « adopter » la Charte afin qu'elle fasse partie intégrante de sa politique de sécurité, et la signifier à l'éditeur en tant que référentiel lors du démarrage d'un audit.

2.1. PREVENTION DES RISQUES

- Dans le cadre d'une politique préventive de contrôle des usages des actifs logiciels des clients *(Software Asset Management)*, les éditeurs mettent à la disposition de ces derniers des outils leur permettant de s'assurer de la conformité de leurs usages en dehors de toute procédure d'audit.

- Conformément aux clauses contractuelles adoptées d'un commun accord par les clients et les éditeurs de logiciels, ces derniers disposent du droit de vérifier que les licences effectivement utilisées par les clients sont conformes, en nombre comme en périmètre, aux droits acquittés.

- Cette vérification peut prendre la forme d'un audit. Toutefois, les éditeurs et les clients privilégieront les procédures déclaratives, qui permettent de procéder à des régularisations volontaires sans passer par le processus d'un audit mis en œuvre par l'éditeur.

- Si les procédures déclaratives ne permettent pas de conférer une sécurité suffisante à l'éditeur, ou en cas de suspicion établie sur des présomptions justifiées à l'égard du client, une procédure d'audit pourra être mise en œuvre par l'éditeur.

2.2. BONNE FOI

- Le déclenchement d'un audit doit être motivé. Il doit respecter le principe de bonne foi contractuelle.

- L'éditeur ne peut auditer que les logiciels objet du contrat de licence servant de socle à l'audit.

- Une clause d'audit n'est opposable qu'au contractant de l'éditeur. En cas d'accord cadre avec une entité qui passe des commandes pour le compte de sociétés affiliées du même groupe, seule l'entité signataire du contrat cadre peut être auditée, sauf stipulation contractuelle expresse ou accord des parties permettant d'étendre l'audit aux entités qui ne sont pas parties au contrat.

- Toute mise en œuvre d'un outil de comptage doit respecter un principe de transparence et d'information préalable du client.
    - Une entreprise qui accepte de recourir au script de son éditeur de logiciel doit donc avoir accès au code du script qu'elle déploie, en vertu du respect de ce principe de transparence et d'information préalable du client, ainsi que pour des raisons de sécurité et de respect de la protection des données à caractère personnel le cas échéant.
    - Également en vertu de ce principe, les tests effectués par l'éditeur au titre des services de support ne doivent pas servir à mettre en œuvre des scripts de comptage non divulgués.

2.3. LIMITATION DES PERTURBATIONS

- Le nombre d'audits, toutes licences confondues, doit être limité. Un éditeur fera son possible pour regrouper ses demandes d'audits afin de minimiser la gêne pour le client.

- L'éditeur doit centraliser la discussion auprès d'un interlocuteur unique désigné par le client.

- L'audit doit se dérouler dans le respect des règles internes du client et notamment sa politique de sécurité.

- L'audit nécessite un préavis suffisant pour permettre au client de s'organiser afin de diminuer l'impact sur son exploitation.

- Les parties s'accordent sur une enveloppe de « jours.hommes » à mobiliser par le client. Afin d'encourager les approches coopératives, l'éditeur qui impose un audit contradictoire alors que le client a déjà régularisé des droits à la suite d'une vérification unilatérale, devra indemniser le client du nombre de « jours.hommes » mobilisés si l'audit contradictoire ne révèle aucune irrégularité significative.

2.4. PERIMETRE ET MODALITES DE L'AUDIT

- Avant tout audit, l'éditeur doit fournir des informations préalables, qui encadreront le périmètre de l'audit : la liste précise des licences à auditer, les contrats invoqués à l'appui de la demande d'audit et leur interprétation, la métrique de mesure, les entités visées, les moyens mis en œuvre.

- Les outils appartenant au client devront être privilégiés. L'éditeur s'abstient de recourir à des outils de comptage qui impliquent l'exécution de commandes dans le système d'information du client. S'il n'est pas possible de faire autrement, l'éditeur fournit cet outil au client avec un préavis suffisant pour que ce dernier puisse en analyser les risques.

- L'éditeur soumet au préalable au client une méthodologie d'audit. Celle-ci doit privilégier les approches par échantillonnage, de manière à limiter autant que possible la durée et l'étendue de l'audit.

2.5. RECOURS A DES TIERS AUDITEURS

- Le recours à des auditeurs tiers ne doit pas être privilégié. Il doit être limité aux cas où l'éditeur ne dispose pas de structure d'audit en interne.

- L'auditeur tiers doit intervenir exclusivement pour le compte de l'éditeur, et non dans l'intérêt conjoint de l'éditeur et du client.

- Tout auditeur tiers désigné par l'éditeur doit s'engager à respecter (i) la présente Charte, (ii) l'ensemble des conditions et limites contractuellement prévues entre le client et l'éditeur.

- Tout auditeur tiers doit signer un **engagement de confidentialité** qui engage l'entreprise auditrice ainsi que chaque auditeur personne physique.

- L'éditeur recourant à un auditeur tiers ne pourra faire peser le cout de la mission d'audit sur son client.

2.6. CONCLUSION DE L'AUDIT

- L'audit donne lieu à une conclusion validée de manière contradictoire par le client et l'éditeur. Chaque régularisation devra être justifiée en identifiant la règle de *licensing* correspondante au sein des documents contractuels.

- Une fois les régularisations effectuées, l'éditeur doit délivrer quitus au client au terme duquel les cas de non-conformité constatés et régularisés ne pourront faire l'objet d'un nouvel audit dans un délai prévu au contrat.

- Les régularisations sont effectuées au tarif négocié entre le client et l'éditeur. L'application d'un tarif « catalogue » ou majoré n'est possible qu'en cas d'abus intentionnel ou de mauvaise foi démontrée du client.

- Lorsque l'audit porte sur plusieurs filiales au sein d'un groupe, les licences manquantes identifiées dans certaines filiales peuvent être compensées par des licences excédentaires dans d'autres filiales. En cas de limitations liées au contrôle des exportations ou à la fiscalité, cette règle s'applique par région ou par *business unit* du client.

- L'éditeur s'abstient de participer à tout appel d'offres du groupe du client concomitamment à la réalisation et à la conclusion d'un audit, afin d'éviter que l'audit ne devienne un levier de négociation commerciale.

- À l'inverse, l'éditeur ne doit pas conditionner la souscription de nouvelles commandes à la conclusion d'un audit en cours.

Cigref
RÉUSSIR
LE NUMÉRIQUE

Au service de la croissance économique et de la compétitivité de nos membres, grandes entreprises et administrations publiques françaises, utilisatrices de solutions et services numériques, par la réussite du numérique

Le Cigref est un réseau de grandes entreprises et administrations publiques françaises qui a pour mission de développer la capacité de ses membres à intégrer et maîtriser le numérique. Par la qualité de sa réflexion et la représentativité de ses membres, il est un acteur fédérateur de la société numérique. Association loi 1901 créée en 1970, le Cigref n'exerce aucune activité lucrative.

Pour réussir sa mission, le Cigref s'appuie sur trois métiers, qui font sa singularité.

Appartenance

Le Cigref incarne une parole collective des grandes entreprises et administrations françaises autour du numérique. Ses membres partagent leurs expériences de l'utilisation des technologies au sein de groupes de travail afin de faire émerger les meilleures pratiques.

Intelligence

Le Cigref participe aux réflexions collectives sur les enjeux économiques et sociétaux des technologies de l'information. Fondé il y a près de 50 ans, étant l'une des plus anciennes associations numériques en France, il tire sa légitimité à la fois de son histoire et de sa maîtrise des sujets techniques, socle de compétences de savoir-faire, fondements du numérique.

Influence

Le Cigref fait connaître et respecter les intérêts légitimes de ses entreprises membres. Instance indépendante d'échange et de production entre praticiens et acteurs, Il est une référence reconnue par tout son écosystème.

www.cigref.fr
21 av. de Messine, 75008 Paris
+33 1 56 59 70 00
cigref@cigref.fr