Cigref

Software licensing audits: Charter of best practices 2021

Recommendations from Cigref members for the use of customers and their suppliers

December 2021

Software licensing audits: Charter of best practices 2021

Recommendations from Cigref members for the use of customers and their suppliers

Update to the September 2015 Charter of the Cigref Purchasing Club

This Charter of best practices in software licensing audits is an update to the document initially produced in 2010, then updated in 2015, as part of the activities of the Cigref Purchasing Club. This last update of 2021 was carried out under the supervision of the steering committee of the Cigref Supplier Relationship Club, with the active contribution of around ten lawyers, purchasers and software asset managers from Cigref member organisations, set up as an "audit management" taskforce.

This Charter is accompanied by a set of clauses comprising a proposal for a standard audit clause, drawn up by the taskforce, and an audit protocol template.

TABLE OF CONTENTS

INTRODUCTION

Many large account licence users have, for several years, noticed a trend of increasing software licensing audits by publishers. 100% compliance is impossible for a company, a finding shared by all parties involved (users as well as publishers). Audits generally follow a process of mutual cooperation, leading to balanced conclusions. During audits, however, IT suppliers can seek to maximise adjustments, creating a climate of suspicion between the publisher and the customer.

Cigref members therefore note that suppliers sometimes rely on contractual clauses open to interpretation - resulting in **problems of understanding** for the customer - and/or clauses which change unilaterally over time in the course of the contractual relationship - resulting in **problems of anticipation**. They also find that the complexity of suppliers' licensing models makes it difficult to **inspect compliance** in advance, and encourages suppliers to search for "faults".

Beyond these remarks regarding the contractual reference framework, Cigref members believe that the methodology followed during the audits is often very **time-consuming.** They also lament the fact that the number of audit clauses inserted into the various contracts leads to a risk of **"permanent audit rights"**, resulting in a need to dedicate significant internal resources to the matter on a recurring basis.

In terms of the actual conduct of the audits themselves, Cigref members observe that the measurement tools, installed on their information systems, can lead to **problems of transparency, security and compliance with the GDPR with regard to personal data.** Here, the supplier must ensure that the use of its inventory tools or scripts does not put customers at fault in the view of the legislator and the supervisory authorities. Cigref members also point out the risk of conflicts of interest when publishers use third-party auditors who are not subject to the **rules of ethics and confidentiality** shared with the customer.

Lastly, in financial terms, customers want to identify **situations of good faith** in which they are unaware of having exceeded the acquired rights, not wanting to have to pay for increased licenses, and wanting to benefit from the conditions negotiated during the last purchases.

The charter drawn up in 2010 and then updated in 2015 served as a reference for Cigref members for several years, allowing them to refuse scripts or to require the supplier's assurance/commitment regarding the absence of any risk or the collection of data not necessary for the audit. The charter thus helped to ensure a balance of power between audited customers and suppliers in a period before the existence of cloud computing, where software licensing audits were very frequent.

The advent of the cloud does not make audits any less crucial for suppliers, who can use identified non-compliances to encourage their customers to migrate to the cloud. The practice of licensing audits therefore remains widespread and a source of economic and legal uncertainty for companies, especially since organisations using digital services mostly engage in a hybrid cloud approach, with their trajectory for migration to the cloud covering several years. They therefore have to deal with the legacy IS and in particular, the existing on-premise software base, while adopting new licensing and invoicing models relating to the use of cloud services.

Finally, contrary to popular belief, migration to the cloud does not fully protect the customer from audits since it must be checked that the use is compliant with the terms of the contract, including in the cloud.

Customer preparation, and their organisation before, during and after the audit, therefore remains an important issue for Cigref members, who do not all have centralised and structured software asset management. In addition to this charter, the *"Audit Management"* taskforce therefore recommends reading the "Software Asset & Cloud Management: from software asset management to services optimisation" - Cigref / Elée guide, updated in October 2018 (public report).

1. PRINCIPLES

User organisations recognise the right of suppliers to verify that their customers' use of licenses complies with the rights granted by the contract. However, contractual guidelines must be in place for the use of audits by suppliers, with clear, balanced and shared practices, respecting certain principles. These principles are set out below. Their operational breakdown is included in the list of best practices below.

1.1. IN ADVANCE: THE ESTABLISHMENT OF A CONTRACTUAL BASIS ENSURING TRUST

The customer and the suppliers must agree, in advance and if possible from the conclusion of the licence agreement, on a contractual framework governing the audit and avoiding certain practices that are a source of disputes.

The applicable contractual framework must exist on a durable, non-modifiable medium. The licensing models and the audit rules must be agreed by the authorised personnel of the customer. **Contracts concluded by clicking a mouse or by reference to a hypertext link are to be prohibited.**

- Contracts must **allow flexible management of the software park** by the customer, in particular by authorising intra-group reallocations at no additional cost (subject to tax considerations or export rules).
- The licence agreement must **consider the consequences of virtualisation** of the park and/or the use of cloud computing technology.
- Contracts must **prohibit options enabled by default** (which may be a source of subsequent non-compliance without the purchaser's knowledge) or else contain an explicit warning of said options in order to allow the customer to manage their park with full knowledge of the facts.

1.2. REMINDER OF THE PREVAILING PRINCIPLES DURING A LICENSING AUDIT

The customer and the supplier must respect certain principles to ensure the smooth running of the audit and improve cooperation between parties:

- The publisher has the right to check that their intellectual property rights are not violated. The procedures for exercising this extra-contractual right are to be set out in the contract. The audit must **be based on clear, unequivocal contractual stipulations negotiated at the time**

the contract is agreed rather than when the audit is triggered**.** In the event of any ambiguity, preference must be given to the restrictive interpretation.

- The customer company must be given sufficient notice of the audit to be able to take any measures to **minimise the impact and disruption** to their information systems. For businesses with seasonal activity, preference shall be given to the periods causing the least disruption.

- The audit must **be carried out in good faith.** In practice, it can only be used to check compliant use of the software park, and be justified only by a good faith execution of the contract.

- **Preference should be given to the self-certification approach (declarative audits).** This is so as to avoid, as far as possible, the use of executables by the publisher over which the customer has no control and which may present risks for their information system and/or create a climate of suspicion. An intrusive audit should therefore only take place if the publisher can justify legitimate doubts about the conclusions of a declarative audit.

- **Precise notification must be provided when triggering an audit,** regarding its scope (geographical scope, licences covered, entities concerned, etc.) and its methods of implementation. In particular, audits by third parties must be contractually approved, and the customer must be able to check any programs used by the supplier.

- **When the audit is triggered, Cigref recommends negotiating and signing an audit protocol** between the audited company and the supplier, defining the procedures for carrying out, handling and concluding the audit, as mentioned above.

- **The audit must come to a joint conclusion,** in other words validated by the audited company. The conclusion must not be used in support of commercial negotiations encompassing different subjects.

2. RECOMMENDED BEST PRACTICES IN LICENSING AUDITS

This Charter sets out some general principles which, according to Cigref members, should govern any software licensing audit. These objectives are intended to be balanced and respectful of the concerns of both parties.

From a practical point of view, the Cigref Charter is intended to:

- **Beforehand: Be used before agreeing a licence contract, as a basis for negotiating balanced and unambiguous audit clauses;**

- **Afterwards: Serve as a reference to understand the progress of an audit.** For example, the customer can “adopt” the Charter to form an integral part of their security policy, and provide it to the publisher as a reference on triggering an audit.

2.1. RISK PREVENTION

- As part of a preventive policy to check customer software asset use (Software Asset Management), publishers provide them with tools allowing them to ensure compliant use outside of any audit procedure.

- In accordance with the contractual clauses adopted by mutual agreement between the customers and the software publishers, publishers have the right to check that the number and scope of the licences actually used by the customers are compliant with the rights for which they have paid.

- This verification can take the form of an audit. However, publishers and customers will give preference to declarative procedures, which allow voluntary adjustments without going through the process of an audit implemented by the publisher.

- If the declarative procedures do not provide sufficient security to the publisher, or in the event of suspicions established based on justified suppositions with regard to the customer, an audit procedure may be implemented by the publisher.

2.2. GOOD FAITH

- The triggering of an audit must be justified. It must respect the principle of contractual good faith.

- The publisher can only audit software covered by the licence agreement which serves as the basis for the audit.

- An audit clause is only enforceable against the publisher's contractor. In the event of a framework agreement with an entity which places orders on behalf of affiliated companies of the same group, only the entity signing the framework agreement can be audited, unless expressly stated in the contract or in the event of an agreement by the parties allowing the audit to be extended to entities that are not parties to the contract.

- Any use of a counting tool must respect the principle of transparency and prior information to the customer.
    - A company that agrees to use the script of its software publisher must therefore have access to the code of the script that it deploys, in accordance with this principle of transparency and prior information to the customer, as well as for security reasons and to respect the protection of personal data where applicable.
    - Also as a result of this principle, tests performed by the supplier for support services must not be used to implement undisclosed count scripts.

2.3. LIMITATION OF DISRUPTION

- The number of audits, for all licences, must be limited. A supplier will do its best to consolidate its audit requests in order to minimise inconvenience to the customer.

- The supplier must centralise discussions with a single point of contact designated by the customer.

- The audit must be carried out in accordance with the internal rules of the customer, and in particular its security policy.

- The audit requires sufficient notice to allow the customer to organise itself in order to reduce the impact on its operations.

- The parties agree on a number of "man-days" to be used by the customer. In order to encourage cooperative approaches, suppliers who insist on a joint audit when the customer has already adjusted the rights acquired following a unilateral verification will have to compensate the customer for the number of "man-days" used if the joint audit does not reveal any significant irregularity.

2.4. SCOPE AND METHODS OF THE AUDIT

- Before any audit, the supplier must provide preliminary information establishing the scope of the audit: the precise list of licences to be audited, the contracts invoked in support of the audit request and their interpretation, the measurement metrics, the targeted entities and the resources implemented.

- Preference should be given to tools belonging to the customer. Suppliers shall refrain from using counting tools which involve the execution of commands in the customer's information system. If this cannot be avoided, the supplier shall provide this tool to the customer with sufficient notice to allow them to analyse the risks.

- The supplier first submits an audit methodology to the customer. This methodology should favour sampling approaches, so as to limit the duration and extent of the audit as much as possible.

2.5. USE OF THIRD-PARTY AUDITORS

- The use of third-party auditors should preferably be avoided. It should be limited to cases where the supplier does not have an internal audit structure.

- The third-party auditor must act exclusively on behalf of the supplier, and not in the joint interests of the supplier and the customer.

- Any third-party auditor appointed by the supplier must undertake to comply with (i) this Charter, (ii) all the conditions and restrictions contractually established between the customer and the supplier.

- Any third-party auditor must sign a **confidentiality agreement** which is binding both for the auditing company and for each individual auditor.

- Suppliers using a third-party auditor will not be able to charge their customer for the cost of the audit mission.

2.6. CONCLUSION OF THE AUDIT

- The audit gives rise to a conclusion validated jointly by the customer and the supplier. Each adjustment must be justified by identifying the corresponding licensing rule within the contractual documents.

- Once the adjustments have been made, the supplier must issue a full discharge to the customer, after which cases of non-compliance noted and rectified cannot be the subject of a new audit within a period stipulated in the contract.

- Adjustments are made at the rate negotiated between the customer and the supplier. The application of a "catalogue" or increased price is only possible in the event of intentional abuse or demonstrated bad faith on the part of the customer.

- If the audit covers several subsidiaries within a group, the missing licences identified in certain subsidiaries may be compensated for by excess licences in other subsidiaries. In the event of restrictions related to export control or taxation, this rule applies by region or by business unit of the customer.

- Suppliers shall refrain from participating in any call for tenders from the customer's group during the performance and conclusion of an audit, in order to prevent the audit from becoming a lever for commercial negotiation.

- Conversely, the suppliers must not make new orders a condition for the conclusion of an ongoing audit.

Achieving digital success to help promote the economic growth and competitiveness of its members, who are major French corporations and public administrations, and users of digital solutions and services

Cigref is a network of major French corporations and public administrations set up with a view to developing its members' capability to acquire and master digital technology. It is a unifying player in the digital society, thanks to its high-quality thinking and the extent to which it represents its members. Cigref is a not-for-profit body in accordance with the French law of 1901, created in 1970.

To achieve its mission, Cigref counts on three business units, which make it unique.

Belonging

Cigref speaks with one voice on behalf of major French corporations and public administrations on the subject of digital technology. Its members share their experiences of the use of technology in working groups in order to elicit best practices.

Intelligence

Cigref takes part in group discussions of the economic and societal issues raised by information technologies. Founded nearly 50 years ago, making it one of the oldest digital associations in France, it draws its legitimacy from both its history and its understanding of technical topics, giving it a solid platform of skills and know-how, the foundation stones of digital technology.

Influence

Cigref ensures that its member companies' legitimate interests are known and respected. As an independent forum in which practitioners and actors can discuss and create, it is a benchmark recognised by its whole ecosystem.

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