ARTICLE

Are audit clauses fit for purpose?

Audit clauses provide a mechanism through which software publishers protect the use of billions of dollars of intellectual property and ensure that their customers comply with the terms on which software is licensed to them. They are surprisingly brief.

The software compliance business has grown enormously since the mid-1990s. Thousands of audits take place every year and roughly $10 billion is paid to publishers as a result. Those of us involved at the very beginning of this activity confidently expected that within a few years customers would be largely compliant with terms and audit activity would be a routine, non-controversial background activity. We could not have been more wrong.

The audit industry is now opposed by an audit-defence industry, tool providers have grown substantially, significant sums are spent on software asset management, technology has changed and software is increasingly delivered in ways that were not envisaged then – through the cloud or on a SaaS basis. But through this change auditing has continued and become more significant rather than less.

Despite this evolution, the contractual basis upon which auditing and software compliance takes place is largely unchanged. It may be argued over daily, but it is seldom challenged in court.

One often-cited case is the 118 Data Resources case.[1] This was an interim application for specific performance. In the judgment the audit process was compared to a "search and seizure" process[2] and to the provision of information on disclosure. Neither of these is a good analogy in our view and these comparisons overlook the fact that there is well-established market activity in this area which, whilst there are variations, has a broadly similar and well-understood shape. Nevertheless, the fact that the request for an audit can be misunderstood in those terms suggests that more expansive drafting in audit clauses might be important: what should they cover?

63 publisher audit clauses

The shape of that market activity is defined by the audit clauses in software publishers' license agreements. We have looked at 63 of these from amongst the 100 or so largest software publishers. These are the clauses we could most easily find. They are also individual examples of clauses that may vary over time and between jurisdictions, and to some degree between customers. We picked only English language examples.

1 118 Data Resources Ltd v IDS Data Services Ltd [2014] EWHC 3629 (CH)
2 Ibid., paragraph 23

Taken together, these clauses have a high degree of commonality. There is a clear set of terms that are usually present addressing:

1. Who may carry out audits – usually the publisher and/or an authorised representative.
2. Frequency – not more than once every 12 months is usual.
3. Notice period – seven business days is pretty common, but Microsoft and Aveva offer 30 days (not business days) and Oracle give 45 days' notice.
4. The audit rights – as a minimum to inspect and to receive copies of documentation, sometimes spelled out in more detail, and usually subject to not unreasonably interfering with the customer's business.
5. The subject matter – usually customer's records, systems and facilities; sometimes with brief additional specifics.
6. The purpose of the audit – typically to verify that the customer's use of software is in conformity with its licenses, sometimes very widely drawn.
7. The customer's obligations – to provide the necessary information within a specified period, and sometimes couched in more general terms around cooperation.
8. Who bears the cost of the audit and commonly the basis on which costs may be imposed on a customer if under-licensing is identified.

It is noteworthy that the audit clause at issue in the 118 case did not address items 4 and 5 above, and this omission was clearly a factor, especially given the judge's concerns about the widely drawn purpose.

There are a number of fairly common additions to these, largely standard, terms. These include a requirement that the customer certify its compliance with the license terms, requirements to produce documents or reports upon request (outside the audit process) and the basis of settlement of any shortfalls.

There are also some very important omissions:

- Only five publishers make any explicit mention of completeness. This is odd given completeness is a central issue in software audits. Completeness is the issue of whether, for example, software is being used in different environments or on different servers or by different people from those identified by the customer, i.e. it is the search for customer mistakes. It is one of the biggest risks for the auditor and publisher and one of the least welcome aspects of the audit for customers. We have probably had more discussions with customers on this than any other topic around audits. This is often put along the lines of "don't you trust us?", which is unhelpful because audits are there to check, not simply to accept, assertions by customers: something Lord Denning made clear in in the House of Lords in the Fomento Sterling Area case[3] in 1958.
- Confidentiality was also discussed in the Fomento case in 1958, but only eight of the audit clauses we examined make any reference to it. Again, this is surprising since in practice almost every audit starts with a discussion between auditor and customer about a non-disclosure agreement, and audits often require the collection of information likely to be considered protected under data protection legislation. These discussions are a frequent source of delay and disagreement and at least two publishers have thought to address this in the audit clauses by stating that (in effect) no further NDA will be required. The failure to address confidentiality was a factor in the 118 Data Resources decision.
- 62% of the audit clauses refer to the use of third parties to conduct audits on behalf of the publisher. That is not, however, a fair reflection of the proportion of audits done by third parties as two of the largest vendors – SAP and Oracle – almost always use their own personnel. In other fields this is relatively unusual, but perhaps because of the volume of audits in software, for some vendors it makes sense to sustain internal teams for this. Where third party auditors are envisaged, in only a third of clauses is there any requirement that these be independent. Perhaps that is understandable if the alternative is an internal team, clearly not independent, but this is an area where there is room for misunderstanding. There seems no clear market view on what degree of independence is intended (when it is intended) and this is an issue often raised by customers if matters progress to a formal dispute.

3 Formento (Sterling Area) Ltd v. Selsdon Fountain Pen Company Ltd and Others [1958] 1 All ER 11

- In our experience access to people is a critical aspect of efficiently conducting a software audit. It is not essential, but a documents only process is likely to be significantly longer and more expensive. Sometimes this has been used as a delay tactic, but the downsides fall as much on the customer as the publisher, especially when there are findings sufficient to trigger a cost transfer clause. It is surprising that only three of the 63 clauses make any reference to the customer making personnel available in addition to documents.
- Increasingly, information on software use is capable of being collected remotely. This can be through the customer running particular commands or scripts, as is the case for SAP for example, but it can also be by automated reporting to the publisher of a customer's license and configuration data in particular circumstances or in response to remote requests: Avaya is an example. Automated systems and embedded software are especially used by publishers whose products are frequently subject to software piracy and download and use by organisations with no entitlements at all. Exactly a third of publishers referred to the possibility of remote audits and/or remote collection of data in this way.

The audit process inevitably captures large amounts of data about customers' IT environments and usage. Some of this may be sensitive from a commercial point of view, much of it is sensitive from a security point of view and some of it may amount to personal data. It is surprising that there is little in the clauses which addresses the data handling and data privacy aspects of audits: only McKesson's and Opentext's audit clauses reference data protection and privacy at all, although others may address this elsewhere.

The cases that have ended up in the courts, in the UK and the US primarily, have sometimes focused on the purpose and scope of the audit clause, with customers seeking to describe these in narrow terms. The argument put is that the clauses are too thin on detail to be capable of specific performance (in the 118 case) or that they are not sufficiently specific to be capable of enforcement under the law of X or Y country.

Alignment around a model clause?

Audit clauses are generally brief, between 100 and 200 words: the shortest we looked at was 21 words. The conduct of audits is by and large well understood and there is a significant degree of industry custom and practice, but this sits almost entirely outside the drafting of the clauses and is largely undocumented and by agreement. This can cause problems when the conduct of audits is challenged and especially when international practice meets local contracts, local jurisdiction and local law.

There are important variations too, as indicated above, and with customers exposed to perhaps two or three audits a year by different publishers and different auditors, there is clearly room for misunderstanding.

It is tempting therefore to propose a long and comprehensive clause covering every possible issue. In theory this might pre-empt disputes when audit rights are exercised but it also increases the likelihood that aspects of the clause may age badly if, as is not unusual, the clause is exercised many years after it is put in place: simplicity provides a degree of flexibility, especially with rapidly changing technology and business models.

With that in mind, the elements that we would look for in a strong audit clause include the following:

1. Who may conduct the audit, especially any use of third parties and whether they are to be independent.
2. The frequency of the audit and the period to be covered.
3. The notice period.
4. What the auditor is empowered to do, for example to talk to people, to run audit tools and to retain information.
5. What the auditor may see, including the right to verify that information excluded is correctly excluded, ie the completeness check.
6. The purpose of the audit, and the breadth of terms that may be considered by the auditor.
7. Customer obligations, around the provision of access to people, places, records and devices, and addressing access to third parties who hold relevant information on behalf of the customer.
8. Who bears the cost, usually the publisher unless there are significant findings.
9. Confidentiality of information provided by customer, publisher and auditor, and the limited purposes for which it may be used.
10. Remote audits, including any requirements on the customer to provide information on request, or to self-audit, and/or the use of dial-home technology.
11. Data protection and obligations to comply with data legislation.
12. Reporting processes and the customer's right to comment on audit findings.
13. Settlement arrangements, ie the basis upon which any license shortfalls will be addressed, including back maintenance, pricing, interest and so on.

Even as a list this amounts to over 200 words, longer than most audit clauses.

In other industries some clauses and/or entire contracts have been largely standardised – the use of JCT contracts in construction for example. Software audit rights are not usually positioned as a source of competitive advantage: some alignment of these between publishers would be beneficial to customers and would help mature an activity that surprisingly lacks formalisation.

The views expressed in this article are those of the author(s) and not necessarily the views of FTI Consulting, its management, its subsidiaries, its affiliates, or its other professionals.

DAVID EASTWOOD
Senior Managing Director
Economic & Financial Consulting
+44 203 727 1292
david.eastwood@fticonsulting.com

GARETH COFFEY
Senior Director
Economic & Financial Consulting
+44 203 727 1714
gareth.coffey@fticonsulting.com

ANDY JACKSON
Senior Director
Economic & Financial Consulting
+44 203 727 1436
andy.jackson@fticonsulting.com

0000 - 07/20