

DISCUSSION DRAFT (VERSION 1.02) – APRIL 2021




Software License Audits: Code of Conduct

— Table of Contents

Introduction	5
Scope	6
Objectives and Principles	7
Terminology	8
Code of Conduct	9
Audit Ethos	9
Clear Communications	9
Acting in Good Faith	9
Project Governance	9
Notification	10
Appointment of auditors.....	10
Scoping.....	10
Identification of Key Stakeholders	10
Planning	10
Managing the Audit	11
Entitlement Records.....	11
Consultants and Service Providers	11
Confidentiality during an Audit	11
Non-Disclosure Provisions.....	12
Confidentiality of Sensitive Data	12
Usage of Data	12
Data Security.....	12
Data Collection Utilities and Documentation	12
Data Collection.....	12
Scope of Data Collected from Customers.....	13
Use of Tools and Utilities.....	13
Act of Collection	13
Data Transmission.....	14
Completeness and Accuracy	14
Reporting and Audit Resolution	14
Report Format.....	14

Factual Accuracy 14
Explanation of the Findings..... 15
Customer Feedback 15


This document represents an initial draft for discussion purposes. Comments can be sent to [code of conduct feedback@fticonsulting.com](mailto:code_of_conduct_feedback@fticonsulting.com).

If there is interest in developing this further it will need, at a minimum, input from publishers, customers and auditors, and their advisers. This input is required not just in respect of detailed drafting but on the substantive issues of the balance of rights and obligations, the standing of the Code, how it might be kept up to date and what, if any, sanctions might be contemplated for non-compliance. We look forward to receiving comments on the draft and suggestions as to how best to take this forward.

Version control

1.02 This version is made public for consultation.

Introduction

1. Most software used by enterprises is licensed subject to terms which commonly include a right for the software publisher to conduct an audit of the customer's compliance with the license. It has become increasingly common for publishers to invoke these rights, both on an ad hoc, occasional basis, and on a programmatic basis. The number of such audits has grown significantly over the last 20 years and in any given year thousands of these audits take place.
2. The license agreement is the source of the right to audit but this rarely sets out much detail as to the way in which the audit rights should be exercised. There is therefore considerable variation in the approaches taken by publishers and customers to audits. Some audits are conducted by specialist teams within the publishers, but it is very common for publishers to appoint third-party auditors to conduct audits, some of whom may be subject to professional standards but many of whom are not.
3. This variation creates difficulty for publishers, customers and auditors in conducting audits consistently in accordance with the terms of license agreements. Agreements vary in detail, publishers may approach things differently, customers' software estates are very different, software products are licensed in different ways and all parties may have different attitudes to the expected rigour of the work, the acceptable time, cost and resource requirements and to privacy and similar matters. These expectation gaps can create significant tensions between publisher and customer to the detriment of both parties.
4. This code of conduct for software audits ("the Code of Conduct" or "the Code") is intended to help alleviate this situation by clarifying expectations on all parties as to how a software audit should be conducted. The Code is not intended to address the conduct of any parties to a license agreement outside the specific context of a software audit.
5. It reflects the views of publishers, customers and auditors. It is proposed to apply on a voluntary basis when both publisher and customer agree and to be in all respects subordinate to the specific terms set out in the license agreement.

Scope

6. The Code of Conduct applies only to the exercise of software license audit rights by publishers in relation to their customers. It does not address conduct outside this specific context, for example the sale or licensing of software or the ongoing management of software by either publishers or their customers.
7. Similarly, the Code does not apply to audits or reviews or inspections, however described, that are conducted other than under the terms of an audit clause, for example voluntary audits, self-declarations, requests for information outside an audit context.
8. The Code does not apply when the entity which is subject to audit is not a customer of the publisher, for example when an audit is conducted pursuant to allegations of software piracy.
9. Within the context of a software audit, the Code sets out expectations on all parties to the audit; these include:
 - The publisher, including any in-house auditors
 - The customer
 - Any third-party auditors engaged by the publisher to conduct the audit (if applicable)
10. Any third parties engaged by the customer to respond to the audit (if applicable)
11. The Code of Conduct is subordinate to the rights set out in the licence agreement between a publisher and its customer.
12. Compliance with the Code is voluntary. The Code will apply only if both the publisher and the customer agree at, or shortly after, notification of the audit by the publisher.
13. If, during the audit, either party considers that the premises under which the parties chose to comply with this Code of Conduct no longer apply then that party should notify the other to this effect. The parties should discuss this and, absent any re-commitment to comply with the Code, the Code will no longer apply.

Objectives and Principles

Objectives

14. The Code of Conduct aims to:
 - i. Address customer concerns about the audit process.
 - ii. Promote greater certainty and consistency as to the audit approach taken by software publishers, reducing the risks and costs for customers in responding.
 - iii. Enable smoother and more efficient audits at lower cost and with less disruption to customer relationships, making it easier for publishers to understand how their software is being consumed.
 - iv. Improve transparency and trust in the relationships between software publishers and their customers.
 - v. Promote improvements in the conduct of software audits to the benefit of all parties.

Principles

15. An audit is a governance tool to enable a software publisher to satisfy itself that terms in software licences have been complied with by a customer. The information exchanged is to be used only for that purpose.
16. Audits are to be conducted in a fair and transparent manner on all sides and in accordance with the licence agreement.
17. The auditor's role is to conduct the audit on behalf of the software publisher, which is its client. It is not the auditor's role to provide advice to the customer. Nevertheless, there are benefits to all parties from the greater understanding of license terms and use that flows from an audit.
18. The role of the third-party auditor is to be a fact finder; it is not the third-party auditor's role to determine the contractual terms of the software license agreements but it is entitled to proceed in accordance with its understanding of the terms.
19. A necessary part of an audit is to establish a complete understanding of the usage of the publisher's software; this means that testing may be required in relation to devices, locations and business units which the customer believes do not use the software publisher's products as well as those that do.

Terminology

20. The following definitions are used in this Code of Conduct.

Audit | Compliance Audit | Software Compliance Audit

21. A project conducted to establish a reconciliation between software licenses owned and software licences in use at a customer, and the customer's compliance with the terms and conditions of those licences, in accordance with the terms of an audit clause in a software license agreement or other contract between the customer and software publisher.

22. An audit in this Code is not the same as a financial or statutory audit, nor an internal audit for governance purposes.

Software Publisher | Publisher

23. The party to the audit which is the licensor of the software being audited.

Customer

24. The party to the audit which is the licensee of the software being audited.

Auditor

25. The party to the audit which conducts the audit. This can either be:

- i. A third-party auditor which conducts the audit on the software publisher's behalf, or
- ii. An in-house auditor employed by the software publisher.

26. Where the term "auditor" is used in the document, both cases above are intended to be addressed. Where distinction needs to be drawn, the terms "third-party auditor" or "in-house auditor" are used.

Consultants

27. External parties engaged by the customer to be involved in the audit on a consulting basis, for example to assist with data collection.

Service Providers

28. External parties engaged by the customer who provide services that are relevant to the activities undertaken during the audit, such as hosting or IT estate management services. Service Providers may need to be involved in the audit to provide data.

Code of Conduct

Audit Ethos

29. The aim of an **audit** is to calculate for those products, entities and geographies in scope a complete
30. and accurate view of the licenses owned and used by the **customer** (an “Effective Licensing Position” or “ELP”), including whether the customer’s use complies with the terms and conditions of the license agreements. The report should be a complete and accurate view of the position at the time of the **audit**, with license requirements calculated, and use assessed, according to contractual terms.

Clear Communications

31. All parties should be clear and transparent in communications in respect of the **audit**.

Acting in Good Faith

32. The **audit** should be conducted in accordance with the terms of the license agreement and in a timely manner.
33. **Auditors** should approach the **audit** as objective finders of fact.
34. **Customers** should not seek to alter their usage of the publisher’s software after notification of the **audit** so as to present a misleading or atypical impression of their use.
35. A **third-party auditor** should disclose to both parties, in general terms, the relationships which it has with the **software publisher** and the **customer**.
36. The **auditor** should be prepared to explain its findings, in writing or face to face, to both the **customer** and the **publisher**.
37. Where an **auditor** is subject to the standards of conduct of a professional or regulatory body, those standards should be adhered to in the conduct of the **audit**.

Project Governance

38. Setting accountability and ground rules for how the **audit** will be conducted is an important step to achieving an efficient process. Investing time in the planning and scoping of the **audit**, with a clear project plan accompanied by escalation routes, sets the tone for an effective **audit**.

Notification

39. An **audit** commences when the **customer** is formally notified by a **software publisher** under the terms of an **audit** clause in a license agreement. Notifications must refer to, and be in accordance with, the applicable clauses and should be in writing (including email).

Appointment of auditors

40. The **auditor** should meet all qualifications set out in the audit clause.

Scoping

41. The **software publisher** should clearly define the product, organisational and geographic scope of the **audit** at the outset, or as early in the process as possible. If products by the **publisher** which were not contemplated in the initial scope discussions are unexpectedly identified during the **audit**, the **software publisher** should, after informing the **customer**, be entitled to extend the scope to include these.

Identification of Key Stakeholders

42. The **software publisher** should identify the person responsible for the **audit**, and their line manager for escalation purposes.
43. The **software publisher** should explain the role, if any, of the account team and of any reseller or partner which may be involved in the resolution of any **audit** findings.
44. A **third-party auditor** should identify the lead for the work and their line manager for escalation purposes.
45. The **customer** should identify the sponsor and project manager for the **audit** at the outset. The project manager should have sufficient seniority and knowledge of the organisation to be able to effectively manage the collection of data.
46. The **customer** should identify any consultants appointed to advise the **customer** in relation to the **audit**.

Planning

47. All parties should conduct the **audit** in line with the terms set out in the license agreement and the **audit** notification communication.
48. All parties should come to a consensus on a project plan, with timeframes, at the start of the **audit**. This should be documented in writing and should make clear the respective responsibilities of the parties.
49. The **customer** should make the **software publisher** and **auditor** aware of any business activity and known resource restrictions that may affect the **audit** at the outset of the **audit**, for

example planned change freezes, data centre migrations, planned annual leave of key contacts. All parties should work collaboratively to minimise the impact of this activity on the **audit**.

Managing the Audit

50. All parties should make every effort to meet the timeframes set out in the project plan and to work collaboratively to complete the **audit** within a reasonable timeframe and minimising disruption to the business of the **customer**.
51. **Customers** should accept that resources, time and effort will be required to facilitate the **audit**.
52. The **software publisher** and **auditor** should be sensitive to the needs of the **customer's** business and to **customer** requests around resource availability and timescales.
53. Clear escalation procedures should be established at the outset of the **audit**, on both the **software publisher** and **customer's** sides.

Entitlement Records

54. The **software publisher** should provide license entitlement records to the **customer** early in the **audit** process to allow for review.
55. The **customer** should review and validate the completeness of license entitlement records provided by the **software publisher** or the **auditor** and work collaboratively to provide evidence of any additional entitlements held.

Consultants and Service Providers

56. **Service Providers** engaged by the **customer** to host IT infrastructure or any software within the scope of the **audit** should be identified by the **customer**. It is the **customer's** responsibility to facilitate the involvement of such **Service Providers** as may be necessary to enable the **customer** to fulfil its role in the **audit**.
57. **Consultants** may be engaged by the **customer** to assist it during an **audit**. The **customer** remains responsible for any information provided by such consultants to the **auditor** and/or the **software publisher**.

Confidentiality during an Audit

58. An **audit** can involve the collection and analysis of data that is considered confidential, with associated concerns around the transmission, storage, access, and usage of that data. This section sets out some principles as to the collection and handling of confidential data.

Non-Disclosure Provisions

59. Unless the license agreement otherwise addresses this, the **customer** may request that any **third-party auditor** puts in place a non-disclosure agreement. No non-disclosure agreement will be required with **in-house auditors** which will be covered by the obligations of the parties in the license agreement.
60. Where a separate non-disclosure agreement is required, the **customer** and the **third-party auditor** should endeavour to agree the terms as quickly as possible.
61. The **customer** should undertake that any **Service Providers** and **Consultants** that are assisting with the **audit** are subject to the same confidentiality terms as the **customer**.

Confidentiality of Sensitive Data

62. The **auditor** should ensure that data that could be considered sensitive for privacy or security reasons is redacted in the report prior to the release to the **software publisher**, unless agreed otherwise by the **customer** in writing.

Usage of Data

63. All parties should ensure that any data shared during an **audit** is only used for the purposes of an **audit**.
64. An **in-house auditor** will confine information received to the in-house audit team until the **auditor's** report is finalised.

Data Security

65. All parties should ensure that sufficient controls are in place to ensure that confidential data can only be accessed by individuals directly involved with the **audit**.

Data Collection Utilities and Documentation

66. The **customer** should ensure that any tools and/or documentation provided to assist with the data collection are only used for the **audit** and are not distributed to other parties or used for any other purpose without the prior written consent of the party which provided the tools and/or documentation.

Data Collection

67. The data requested as part of an **audit** should be rationalised and collected in the most efficient manner possible: this may be an iterative process. Data already existing at the **customer** should be used as far as possible to minimise effort, but with adequate testing to ensure completeness and accuracy. Where a **customer** does not have the necessary tools or data to hand, utilities or methodologies provided by the **publisher** or **auditor** should be used to fill the gaps.

Scope of Data Collected from Customers

68. As far as possible, data collected should be limited to that which is relevant to the **publisher's** programs and licensing metrics and necessary for the audit. All parties should accept that there may be instances where incidental data is gathered that does not directly relate to the **publisher's** programs or licensing metrics. This should be treated as **customer** confidential.
69. When collecting data, the **auditor** should be able to explain where requested the rationale for the data required. The **customer** should not unreasonably withhold requested data, for which the rationale has been explained.
70. Where the **customer** has data sources that already fulfil some or all the data points requested, this should be used as far as possible.
71. Data provided by the **customer** for the purposes of the **audit** should be tested for completeness and accuracy by the **auditor**. The **customer** should expect that if there are gaps in the completeness or accuracy of the data, additional work will be required to gather missing information or to assess its likely significance.

Use of Tools and Utilities

72. Where the **auditor** requires tools or utilities to be run to collect data, and these tools or utilities do not form part of the software deployed by the **customer**, the **customer** should be given adequate time to test the execution of these tools or utilities.
73. When agreeing a project plan at the commencement of the **audit**, all parties should build in sufficient time to allow testing of tools and utilities, taking guidance from the **customer** regarding relevant change control policies.
74. The **customer** should endeavour to ensure that testing and change control formalities are completed as swiftly as possible.
75. The **customer** should not unreasonably restrict the use of tools or utilities by the auditor.
76. Where data is collected through tools and similar mechanisms, a copy of the data should be provided to the **customer**.

Act of Collection

77. The **auditor** should not directly interact with the **customer's** IT systems.
78. The **customer** should cooperate with requests for data and provide the requested data in a timely manner, including provision of sufficient access to personnel.
79. Where the **auditor** identifies that further data is required, the **software publisher** or **auditor** should inform the **customer** of this additional requirement as soon as it becomes apparent.

The **customer** should cooperate with the requests from the **software publisher** or **auditor** to provide any such additional data.

Data Transmission

80. Data should be transmitted between the **customer**, the **auditor** and the **software publisher** via means appropriate to the sensitivity of the data.

Completeness and Accuracy

81. All parties should take reasonable care to ensure that the data provided during the **audit** is complete and accurate.
82. The **auditor** should be prepared to explain to the **customer** the reason for completeness and accuracy testing on data provided by the **customer**, including data created following the **software publisher's** or **auditor's** instructions.
83. The **auditor** should be prepared to explain to the **customer** the steps taken to validate the completeness and accuracy of the data, as well as any material limitations to the testing.

Reporting and Audit Resolution

84. The report can have significant financial consequences for **customers and publishers**; it should be clear how data has been used to draw conclusions, and **customers** should have the opportunity to check the facts before submission to the **software publisher**.

Report Format

85. The **auditor's** report should be clear, accurate and easily understood to enable the **publisher** and the **customer** to understand the position.
86. Assumptions should be clearly stated in the auditor's report.
87. The **software publisher** or the **auditor** should ensure that when producing a report, the resulting license position is clearly linked to the source data to allow for efficient and timely review of the report by the **customer**.
88. If the **audit** report includes any data which has been extrapolated, the report should describe the approach to extrapolation and the assumptions upon which it is based, as well as the effect of the extrapolation on the resulting numbers.

Factual Accuracy

89. The **software publisher** should allow the **customer** adequate time to review and provide commentary on the factual accuracy of the report and allow for a right of reply.

90. The **auditor** should provide the **customer** with the opportunity to provide feedback/points of mitigation, preferably throughout the course of the **audit**, or allow adequate time after delivery of the report.
91. The **customer** should endeavour to review the report and provide feedback within the period allocated by the **software publisher**.

Explanation of the Findings

92. The **auditor** should be prepared to explain the **audit** findings to the **customer**, including the **audit** methodology.

Customer Feedback

93. A **third-party auditor** should ensure that any commentary that the **customer** requests to be included on any items in the **audit** report are included in the final report to the **publisher**.

DAVID EASTWOOD

Senior Managing Director

+44 7802 636079

david.eastwood@fticonsulting.com

ANDY JACKSON

Senior Director

+44 7970 202566

andy.jackson@fticonsulting.com

GARETH COFFEY

Senior Director

+44 7976 989060

gareth.coffey@fticonsulting.com

EXPERTS WITH IMPACT™

FTI Consulting is an independent global business advisory firm dedicated to helping organizations manage change, mitigate risk and resolve disputes: financial, legal, operational, political & regulatory, reputational and transactional. FTI Consulting professionals, located in all major business centers throughout the world, work closely with clients to anticipate, illuminate and overcome complex business challenges and opportunities.

©2021 FTI Consulting, Inc. All rights reserved. www.fticonsulting.com

