Commercial Software Licensing

CHAPTER 9:

Software Self-Audit

Prepared by DoD ESI | January 2013

Chapter Overview

- DoD should insist on Self-Audit if any Contract or License Agreement must include a Software compliance audit provision.
- There are industry best practices DoD should follow in establishing and Conducting Self-Audits and acting upon Results.
- Self-Audits can find situations where DoD is spending more than necessary, and also identify potential compliance issues in a timely manner which will enable DoD to manage any issues within appropriate budget cycles.
- Self-Audits are a good tool to monitor compliance and are an important part of overall Software Asset Management (SAM).

Best Practices for S/W Audit–Publisher Audit

- Publishers' preferred approach for S/W Audits is for the Publisher to audit customer usage with Publisher personnel and tools, reporting findings (often with a bill) to customer.
- Some Publishers abuse the situation, charging list license fees, list maintenance fees, penalties, and interest for all noncompliance situations, including minor or unintended noncompliance.
- Several instances where Software was canceled but accidentally was not removed from servers, have generated significant noncompliance situations.
- Industry analysts (from the S/W User Perspective) strongly recommend against Publisher conducted audits.

Best Practices for S/W Audit–3rd Party Audit

- Some firms, especially if they are not in a strong negotiating position, are still able to deny a Publisher audit and may agree to 3rd Party audit.
- A 3rd Party audit is accomplished by hiring an independent company to perform the audit, under pre-established processes and methods, reporting results to Publisher and User.
- Issues to be addressed with 3rd Party audits include the entity performing the audit, which automated tools they will use, the reporting process, remedy process, who pays for the audit, and whether or not the 3rd Party audit results are binding.

Best Practices for S/W Audit–Self-Audit

- Many large commercial firms, especially those that are significant customers of the Publisher and have a strong negotiating position, have denied Publisher audits and 3rd party audits and instead agreed to self-audit.
- Self-Audit is accomplished by the Software User utilizing internal personnel to perform the audit under pre-established processes and methods, reporting results to the Publisher and to Internal Management. Often senior management is required to certify that the audit was conducted as established, and that the results are accurate.
- DoD License Agreements should contain the DoD friendly and DoD ESI Standard self-audit language referenced on the following pages.

3 Step Approach to Self-Audit

1st Step	What are our existing license rights granted? What Programs, number of users, servers, organizational boundaries, etc. apply?
2nd Step	What is our actual use (including identification of Software on record or on servers not in use)? What Programs, number of users, servers, organizational boundaries, are we using?
3rd Step	What is the comparison of rights granted to actual use?

ESI Proposed Self-Audit Language

DoD Self-Audit Language:

- Audit results will be certified in writing by an appropriate DoD manager designated by DoD for such purposes.
- Publisher will reimburse DoD for the reasonable costs of conducting internal audits requested by Publisher. If the audit results indicate DoD use is 5% or more above license parameters, DoD will absorb its internal costs of the audit. Under no circumstances will DoD reimburse Publisher for Publisher costs.
- Audit results indicating DoD use is 5% or more above license parameters will result in one of the following actions by DoD at DoD's option:
  - *DoD will reduce software use to license parameters within 30 days of reporting audit results; or*
  - *DoD will seek funding to provide an order for the additional software use.*

ESI Proposed Self-Audit Language (cont.)

General. Notwithstanding Publisher audit provisions to the contrary, DoD may perform an internal audit of Software use and will use its best efforts to keep full and accurate accounts that may be used to properly ascertain and verify numbers of licenses, users, or subscription parameters in use.

- Upon Publisher written request, DoD may provide audit reports to Publisher from Licensee's internal audit records as the sole means of satisfying Publisher's requests for audit.
- Publisher must provide a minimum of 30 days written notice when requesting DoD to provide the results of an internal audit.
- DoD will use DoD tools, records, repositories or interviews at DoD discretion to perform its internal audit.
- Audit results will be reported in a form deemed appropriate by DoD for providing compliance information.
- Audit results will be certified in writing by an appropriate DoD manager designated by DoD for such purposes.
- Publisher will reimburse DoD for the reasonable costs of conducting internal audits requested by Publisher. If the audit results indicate DoD use is 5% or more above license parameters, DoD will absorb its internal costs of the audit. Under no circumstances will DoD reimburse Publisher for Publisher costs.
- Audit results indicating DoD use is 5% or more above license parameters will result in one of the following actions by DoD at DoD's option:
  - *DoD will reduce software use to license parameters within 30 days of reporting audit results; or*
  - *DoD will seek funding to provide an order for the additional software use.*

Conducting the Self-Audit

- Self-Audit is accomplished by the Software User using internal personnel to perform the audit under pre-established processes and methods.
- Audit results are reported to Internal Management and to Software Publisher.
- Often, senior management is required to certify that the audit was conducted as established, and that the results are accurate.

Conducting the Self-Audit (cont.)

- Numerous software tools are available to search networks and report software instances/usage.
- Yet only some of these tools are “certified” by certain Publishers.
- The small list of certified tools excludes many recognized, mainstream products.
- Many additional audit tools are well-tested, mainstream products, leaving the Publishers with no logical reason to dispute their use, accuracy, and effectiveness.

Conducting the Self-Audit (cont.)

Issues germane to self-audit and all S/W Audits include:

- who will perform the audit,
- which automated tools will be used for auditing,
- how results will be measured,
- what is the process and timeline for reporting,
- what is the remedy process *(if any is deemed necessary)*,
- who pays for the audit, and
- whether or not audit results are binding *(especially important for Publisher and 3rd Party Audits).*

Typical Results of a Self-Audit

- Comparing actual software use to the rights granted by the terms of the contract generally yields one of the following results:

Common Results from Audit	Consequences/Ramifications
a) Compliance across the entire organization.	None.
b) Software acquired, but not utilized, and with no future plans to utilize.	DoD might be able to save a significant amount of annual maintenance cost, based on the documented under-utilization.
c) Software acquired, but utilized far less than licensed.	
d) Software acquired, but utilized in excess of license grants.	DoD might prevent a complicated situation where the software Publisher could take vigorous actions to charge DoD for improper use. Being proactive, DoD can elect to acquire additional license rights to bring the organization into compliance, or could elect to limit usage within the organization to comply with existing license grants.
e) Software utilized with no record of acquisition or license grants.	DoD needs to determine if license rights exist—from previous organizations or users inherited via reorganization—and then take steps to ensure compliance by acquiring appropriate license rights, or eliminating the software use within the organization.

Software Asset Management

The best practice to employ for avoiding surprises in Software Licensing issues—both under-licensed and over-licensed situations—is to manage the Enterprise's Software Assets proactively. This practice is often called Software Asset Management (SAM) or, if part of overall Information Technology Asset Management, ITAM. The best practice steps in SAM are discussed below:

- Establish Centralized DoD Software Management Policies and Procedures.
- Record Software Licenses and Use Rights.
- Capture and Record Software Information at the Time of Receipt.
- Capture and Record Software Deployment Information at Time of Deployment.
- Manage Compliance with Software Usage Rights Granted.
- Conduct DoD Self-Audits as Necessary.

Software Self-Audit Goal