For SPLA Audits, When Historical Data is Missing, Creativity May Be Required

By Christopher Barnett
Scott & Scott LLP

Most software audits pertaining to products licensed under perpetual licenses (such as licenses acquired under a Microsoft Select Agreement, MPSA or (usually) Enterprise Agreement) incorporate a snapshot-in-time approach, where licenses owned generally are compared to deployments identified through data collected about current-state product deployments. In contrast, audits pertaining to products licensed under a Microsoft Services Provider License Agreement (SPLA) incorporate a strong historical-use element. Since SPLA pricing is based on a monthly reporting model, SPLA audits look at historical usage during the period covered by an audit (often, three years or more), and then compare that historical usage to a licensees' historical usage reports.

And that historical-usage element is where almost all SPLA licensees routinely fall short.

Most companies licensing software under SPLA simply do not keep records regarding their usage quantities for past months. Microsoft's license agreements typically contain requirements to "keep accurate and complete records relating to all use and distribution" of Microsoft's software, but most businesses simply do not make the connection between that obligation and their monthly reporting procedures. As a result, there is a gaping hole in data collection for most SPLA audits.

The SPLA gives Microsoft the right to presume that unreported use identified during an audit month began at the commencement of the end-user relationships associated with that unreported

use, unless a licensee can reasonably demonstrate a different scope and duration. This is where an element of creativity often can bridge the gap to a successful SPLA-audit resolution.

In the absence of historical data, Microsoft and its auditors often are willing to consider alternative approaches for estimating historical usage. For example, if the missing historical data pertain to products licensed per user, then one option could be to estimate changes in user license requirements over time based on changes in the licensee's monthly revenue for the corresponding period. Alternatively, it may be appropriate to estimate historical usage by comparing usage to reporting for the audited month, and then applying the same ratio to reported quantities for previous months. User account creation dates also often are a relevant data point for these purposes.

For products licensed per processor or per core, it often makes sense to use a combination of resource-creation dates and records regarding past changes to the environment. For example, if the licensee can demonstrate through e-mails or other sources of information when it deployed additional infrastructure or server products over time, those records may be used to identify the earliest dates for which certain products should have been reported during the audit period.

In our experience, Microsoft's auditors often are willing to consider different sources of information, but their preference always will be for the explanations that are supported by the most evidence. The stronger the factual basis for arguing in favor of a particular outcome, the better the odds of a successful resolution. In contrast, the more a licensee effectively asks Microsoft to trust it regarding past usage, the more doubtful those odds become.

Of course, the very best way to address the risks associated with SPLA audits is to plan for them. A standard part of any

SPLA licensee’s reporting procedures should be to save an archive of historical usage reports generated by auditable inventory tools. For software and hardware deployments, those tools include System Center, MAP Toolkit, and Lansweeper, among others. Additional sources of information include RVTools (for VMware virtualization data) and Active Directory queries (for information regarding the Organizational Units and Security Groups to which authorized users belong). Well prepared SPLA licensees should be in the habit of preparing their monthly reports accurately and on time based on up-to-date deployment information and then saving that information every month, so that it never becomes necessary to determine the most appropriate, creative approach for filling data gaps.