

Deloitte.

**Are you getting the Software Asset Management
services you pay for?**

Conducting a contractual compliance inspection of your
SAM third party suppliers

A Deloitte SAM Bulletin



Bulletin 2

Authors

Peter Kunorubwe
Alex Martin

Contributors

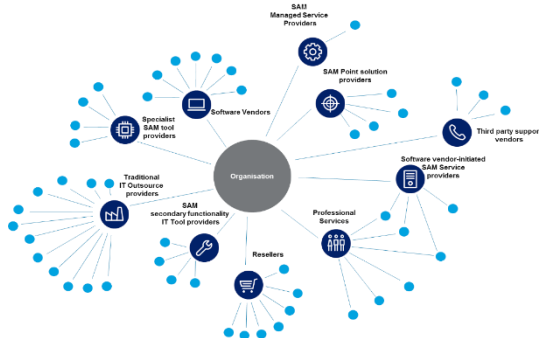
Kristian Park
Laurianne Bourg
Nicola Hicks

Introduction

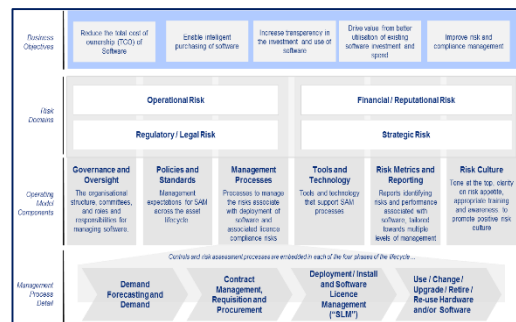
Welcome to the second in our series of bulletins exploring Software Asset Management (“SAM”) from alternative angles. Previously, we explored the third party SAM services marketplace, the benefits and risks of using a third party SAM service provider, and highlighted how organisations can establish third party risk management practices to manage the risks of using an extended SAM supply chain:

Extracts from Deloitte SAM Bulletin 1: “Managing the risks and realising the opportunities of using third party Software Asset Management (SAM) providers”

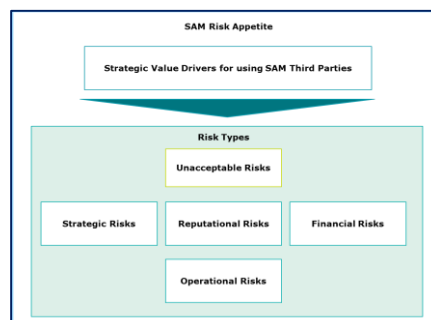
Understand the marketplace



Create a SAM Framework



Define the Risk Appetite and KRIs



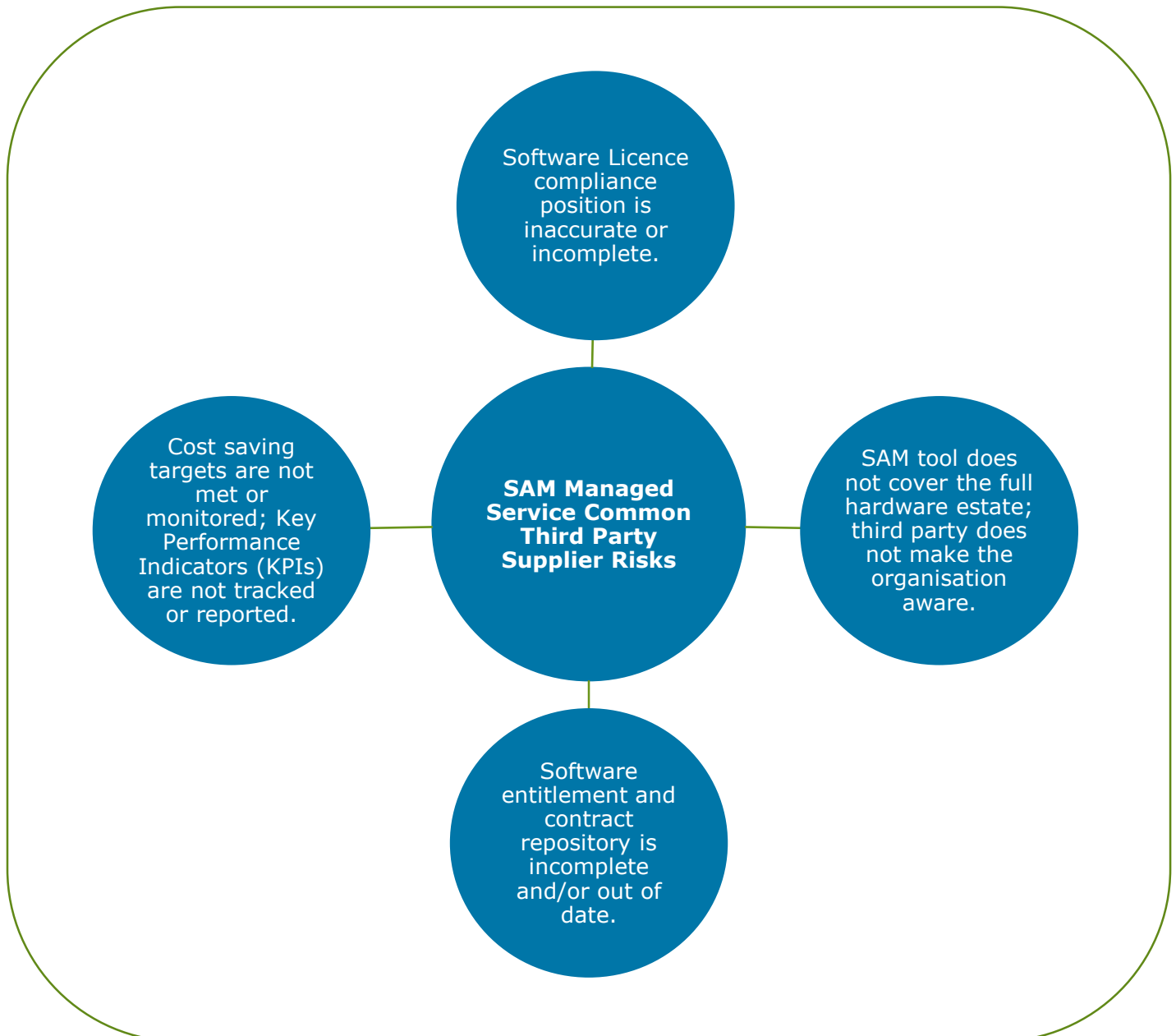
But what about **once an organisation has entered into a third party SAM services partnership?** How does an organisation **monitor their third parties to confirm they are providing the services that have been paid for?** Given the amount of resource and effort required to perform operational SAM activities, it can be challenging to maintain oversight of third parties that are providing support on those activities. However, it is important to perform compliance assessment activities on these third parties, as failing to sufficiently monitor the services that they deliver can prove costly. If a SAM third party fails to perform contracted SAM activities or the quality of data falls short of required levels of accuracy, the result can mean software licence non-compliance and unplanned financial penalty.

As such, once a service contract has been agreed with a third party SAM service provider, a core activity in any organisation’s third party risk management activities should be ensuring that the supplier (or suppliers) comply with the terms of the agreed contract. As with any contract, third party SAM agreements may include many complex clauses. To ensure full value for money from third party SAM relationships, it is important that organisations regularly confirm that their SAM partners are fulfilling their contractual obligations.

In this second bulletin, we will explore the common contractual risks that are present in a typical SAM third party services agreement and touch on how to perform an inspection of a SAM supplier against their contractual obligations to deliver SAM.

Key SAM supplier contractual compliance risks

The risks that third party SAM relationships pose to an organisation vary both according to the type of third party relationship that has been established and by the organisations' risk appetite and risk priorities. In our previous bulletin, we explored how to establish a risk appetite for SAM services and to define Key Risk Indicators, based on potential risks that may impact an organisation's SAM objectives. The following illustrates some of the key risks that may present themselves for a common SAM third party relationship - that of a supplier providing a SAM Managed Service:



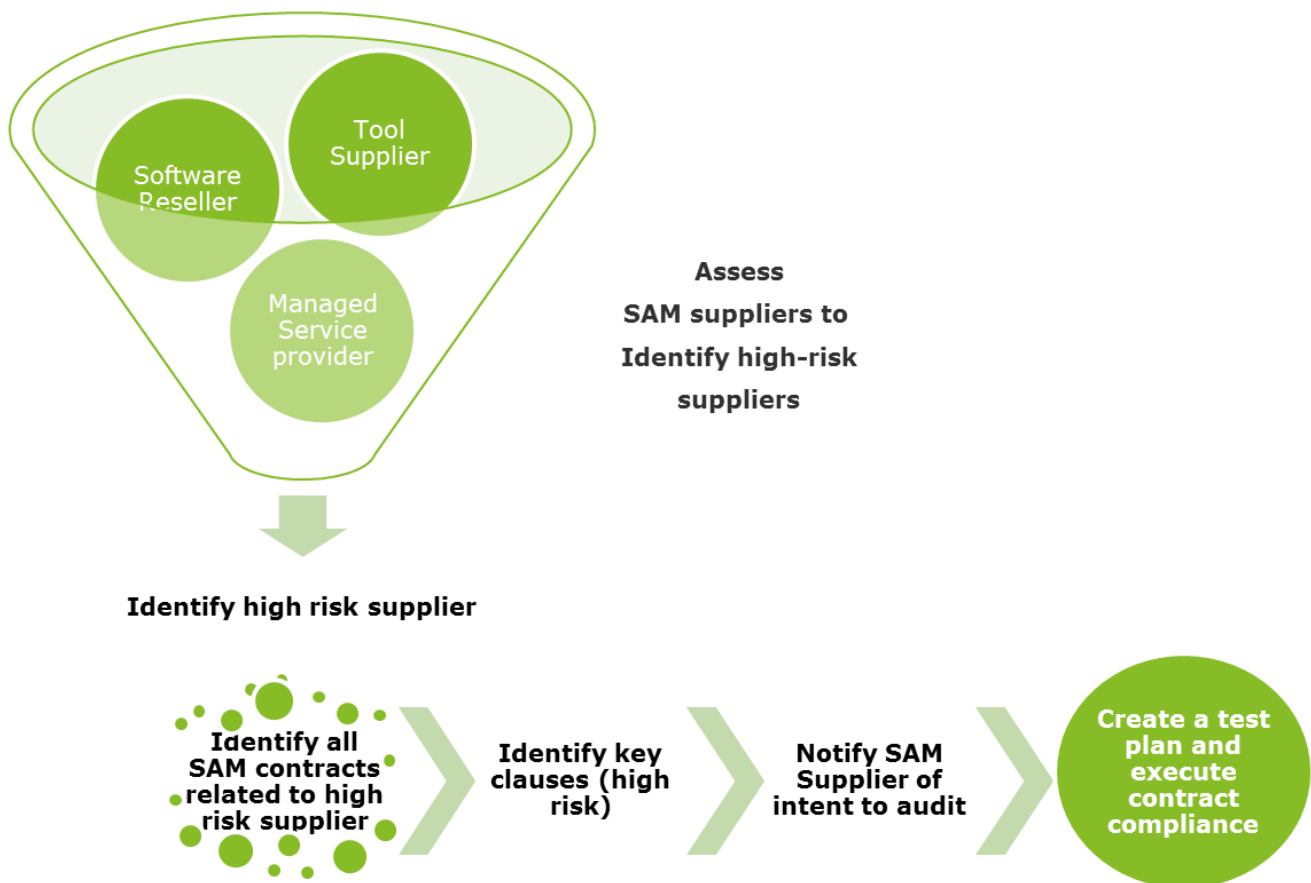
Other non-software specific contract risks that Deloitte have observed include potential errors in invoices raised for services, a failure to apply volume licence discounts for purchases made on behalf of the organisation and missed service credits in event a delivered service misses an agreed Service Level Agreement (SLA).

Assessing SAM Third Party Suppliers for their Contractual Compliance

How to Assess SAM Third Party Suppliers

Conducting an assessment of SAM third party suppliers can be broadly divided into the following main phases:

- Assessing the different SAM suppliers (where more than one is used) to identify any suppliers whose services may be higher risk to the organisation, and to identify the supplier that is the highest priority to be assessed for contractual compliance (Aligning this assessment to organisational Key Risk Indicators ensures that the risks that are of priority to the organisation are fully considered);
- Identifying all the contracts related to SAM for the target supplier;
- Analysing the contract(s) to identify the key clauses for which the supplier will be assessed for compliance;
- Notifying SAM suppliers that the organisation intends to perform an audit of their compliance;
- Creating a test plan that effectively assesses the supplier's compliance with the contractual clause; and
- Initiating the plan and performing the compliance testing.



Step 1: Identify SAM Suppliers to Assess

The first step in performing a SAM service compliance assessment, where multiple third parties are used, is to identify the suppliers whose services are critical to the organisation's software licence compliance or are high-risk as defined within the organisation's risk appetite. In the event that a single SAM third party supplier is used, this task is simple. However, increasingly Deloitte has observed that, in order to realise the benefits of a wide breadth of experience, subject matter expertise and to capitalise on the competitive marketplace, many organisations employ more than two third party suppliers to provide aspects of their SAM services. As such, it is important to understand which third party SAM supplier performs services which represent a high risk to the business, as illustrated below.

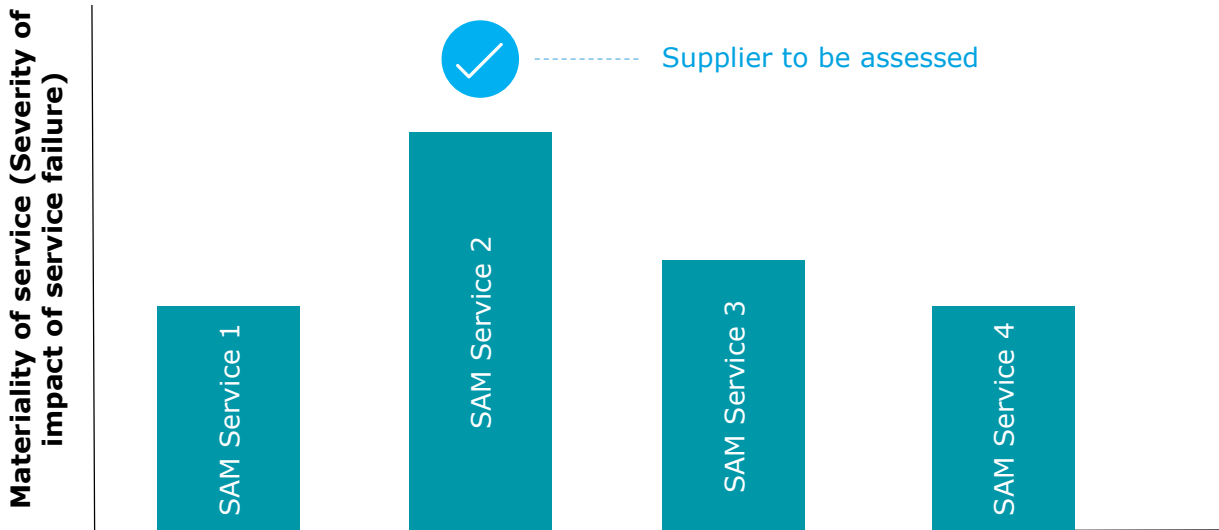


An organisation should define what their key risks are and the weighting they have when performing an assessment priority. A key risk may, for example, be either:

- A service provided that is integral to the operating functionality of an organisation, (for example procurement and install of software) without which, an organisation may not be able to function properly); or
- An activity, such as software licence compliance reporting, which if not performed, may result in risks not being identified properly or on a timely basis.

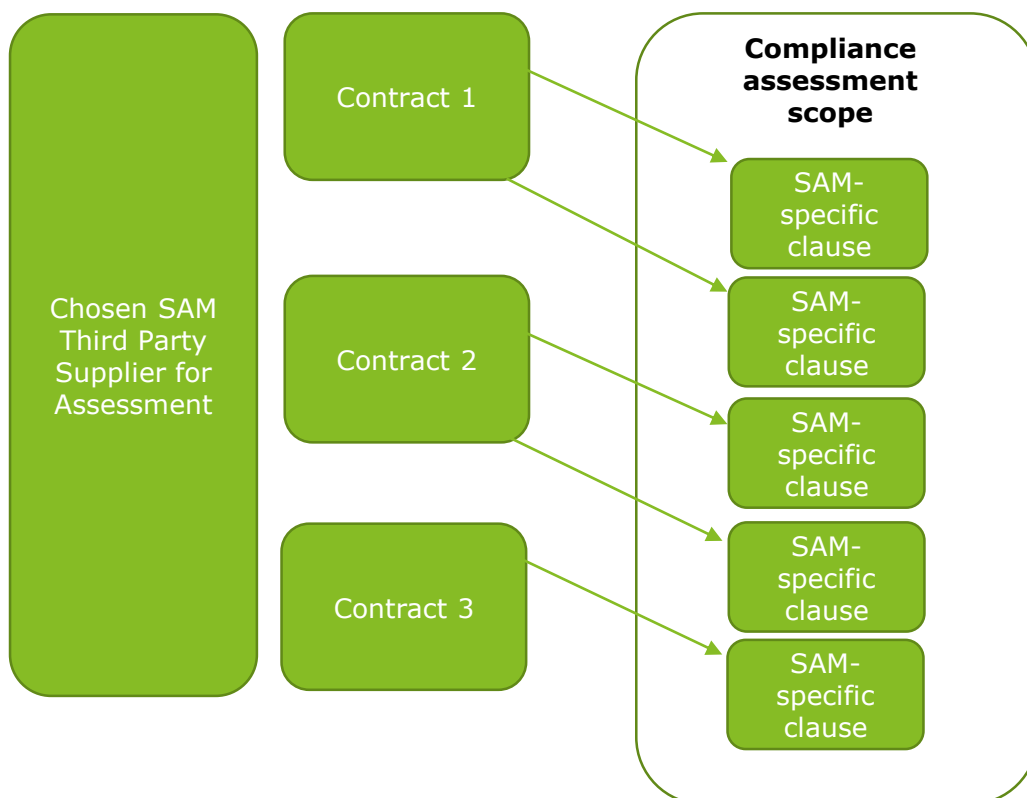
Other risks may be services being performed which are not critical to the operational running of an organisation, but nevertheless may subsequently represent a lower level risk to the organisation if not completed.

An example method that may be used to prioritise the SAM suppliers to be assessed is to measure each outsourced SAM service against the materiality of that service – i.e., the impact that the failure of the services would have to the business. By performing this exercise, a view of the services that may be of priority for assessment begins to become apparent:



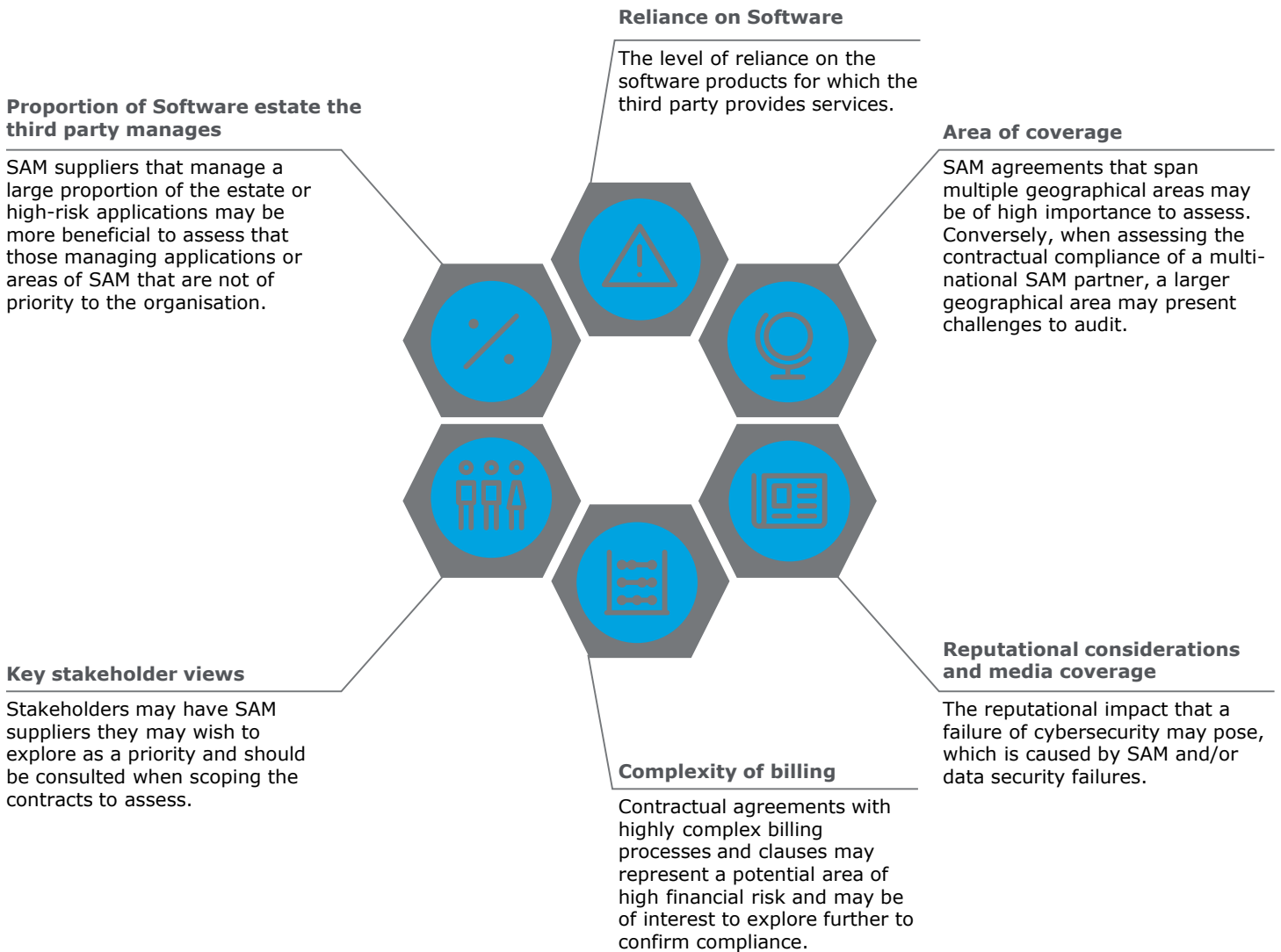
SAM Services outsourced to a third party

This method of assessment clearly highlights the highest-risk SAM suppliers to an organisation. Within some organisations, there may also exist multiple contracts for a single supplier and this process may be repeated at a more granular level, to identify what contracts are of the highest priority to be assessed:



Step 2: Agree Key Objectives and Priorities for an Assessment

The assessment needs a clear objective to ensure that the inspection is performed in a co-ordinated fashion and that the information obtained in the assessment is relevant and can be quantified to identify supplier compliance. An organisation should identify what it is they are looking to obtain or understand from the assessment. We have outlined a number of key areas that may be of consideration:



In addition to identifying what KRIs are aligned to each supplier, organisations must also consider these other key factors and a scoring method should be defined, with a high and low threshold of risk for each risk factor agreed. By performing an initial assessment of these factors against financial risk and assigning a rating to each of them, an overall level of risk can be determined and plotted against other SAM third party supplier contracts. This can provide a clear indication of the risk levels that each supplier and contract represents to an organisation and thus, the priority for each assessment.

Approaching the SAM Third Party Supplier

Step 3: Confirm Audit Rights

Before an assessment of a SAM third party can even be started, it is important to understand what rights have been agreed with the supplier to perform such an assessment. Generally, these rights are detailed within the terms of the contract in an 'audit clause'. The terms of this clause may have a bearing on what activities can be performed and whether an inspection can even be conducted.

Where a right to audit is in place, the supplier should be approached to notify them of the intention to audit, in line with any audit notification clauses in the contract. In the event that no audit clause is in place within the contract, organisations may be in a position to leverage their relationship with the supplier to agree for an assessment to be conducted.

Once a dialogue has been established, a scope and plan can be agreed between the organisation and third party as to how the assessment will be performed.

Step 4: Agree Activities and Topics to be Covered

For every SAM service that is outsourced, there are a number of activities or topics that represent a greater risk and/or area of preferred focus for an organisation than others. As such, an agreed scope should be drawn up that outlines the topics that are to be assessed and the activities that are to be performed for each topic, to verify compliance. As each topic may require a different type of analysis, creating a working plan and scope will help to set up the terms of the assessment. Some of the key clauses that may be considered as part of a SAM third party contractual compliance assessment include:

Cost Savings and Return on Investment

The delivery of cost savings is especially prevalent within SAM Managed Services. An assessment may be performed to understand what return on investment the organisation has obtained so far through the supplier's activities and performance.

Service Credits and Incentives

The supplier's performance may be assessed to understand how well they are delivering the agreed services and whether any agreed incentives have been achieved.

Reporting

Tests of a sample of reports provided by the supplier can be performed to verify their completeness and accuracy.

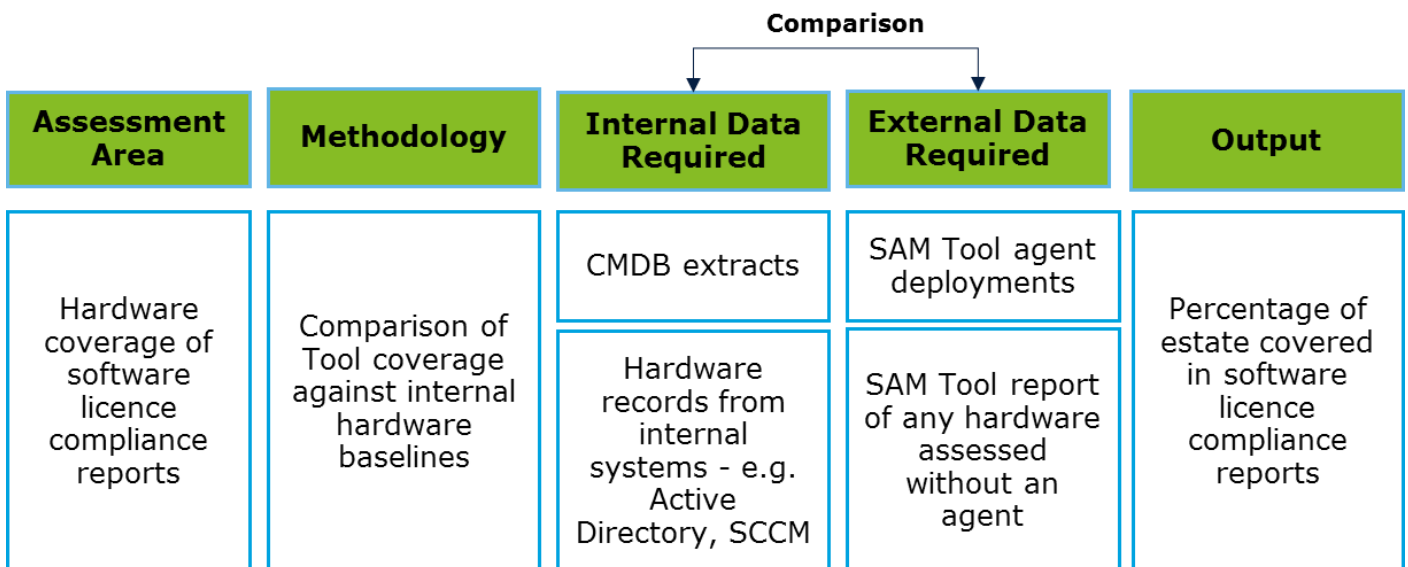
Administration, Logistics and Payments

Assessments may wish to focus on how well the supplier administers the services they provide. This could include, for example, the invoices billed to the organisation and/ or any issues with resourcing the services.

Step 5: Measuring a Supplier's Compliance

By this point, key SAM suppliers will have been identified and the contracts and clauses to be assessed agreed. But how does an organisation test the supplier's compliance against these contractual requirements? Firstly, it is necessary to determine what analysis can be performed using data that is available internally to the organisation, and what information and activities may require input from the SAM third party.

In some instances, relevant data may be already available internally, for example, where regular internal reporting on SLAs is already being performed. As such, it is important to discuss the audit with key stakeholders internally, to understand what monitoring is in place and the data that is collated, to support the compliance assessment. Further, the type of testing to be performed will depend on the nature of the SAM work that the supplier is providing and the clauses agreed to be assessed, which will then inform the data required. For example, in a SAM Managed Service, in the event a supplier is contracted to report on software licence compliance across an organisation's hardware estate using a SAM tool:



The key to testing the third party's contractual compliance is to have in mind at all times what the desired outcome of the testing is. What information are you trying to find out by doing the testing? What kind of output are you looking for? Will the data provided be qualitative or quantitative, and will this influence the type of testing that can be performed?

When the type of data that is required to be provided by the SAM third party supplier is identified, a request to the supplier can then be created. The supplier's response to this request can provide useful information to the assessment in itself, in the event that data cannot be supplied or is not available in a timely manner, in line with any Service Level Agreements in the contract.

Once the compliance assessment has been performed, the testing conducted and a report created of the findings, in the event that non-compliance has been identified, it will be necessary to discuss the observations with the third party supplier. It is useful to refer back to the contract with the supplier, as it is possible that procedures for reimbursement or obtain service credits have already been agreed. This point is also a good opportunity to assess and discuss with the SAM supplier any opportunities for improving processes to avoid such instances from re-occurring. In the event any non-compliance has been identified internally, the same exercise can be applied to the organisation's own processes. We will be exploring the subject of performing internal audits in relation to SAM in a future bulletin.



Conclusion

Monitoring of SAM third party suppliers is an important activity for any organisation leveraging the skills and expertise of SAM third parties to deliver SAM services. Only by performing such compliance exercises on an iterative basis can a level of assurance be gained on the effectiveness of the third parties' activities.

Consequently, by verifying that all contractual obligations are being conducted in line with expectations, an organisation gains a greater reassurance that its software is being managed appropriately, that it is compliant with the terms of its software licensing agreements, and that it is realising the full value that SAM third party suppliers offer. A supplier compliance inspection provides valuable data not only on the effectiveness of the third party supplier, but on the effectiveness and completeness of a SAM function as whole. They may also serve to highlight potential gaps in controls and processes, and the overall SAM framework and identify areas where additional verification and validation is required on third party contributions to a SAM function.

Contact

If you would like to speak to Deloitte regarding our SAM services, please feel free to reach out to us:

Kristian Park – Partner
+44 7920 591507
krpark@Deloitte.co.uk

Peter Kunorubwe - Director
+44 7715 853811
pekunorubwe@Deloitte.co.uk