

WHITE PAPER

Maturity of SAM Practice in the UK Market — Perception and Reality of Risk

Sponsored by: FAST IIS

Frederick W. Broussard Chris Ingle
October 2008

EXECUTIVE SUMMARY

This IDC White Paper, the first in a series of four papers that provide a guide to successful software asset management (SAM), looks at what organisations in the UK are doing and what they can do to improve their use and management of software assets.

Among the main findings of the paper:

- ☒ 80% of organisations procure software to improve their business process and make their workforce more effective. 60% of customers use it to reduce cost. Even though customers see this benefit 40% don't have any process in place to accurately assess costs and hence measure the return on investment.
- ☒ 75% of organisations claim to have a formal SAM strategy and implementation, but the maturity of the practice is often low, resulting in a false confidence about the level of risk facing the business. Low levels of maturity of SAM practice lead to organisations misallocating resource: being over-licenced and overspending on some software assets and being under-licenced for other assets. Much can be done to improve the approach across businesses as very few organisations can truly claim to have a comprehensive SAM strategy.
- ☒ A majority of organisations recognise that poor management of software assets can also bring in risks such as viruses and corruption of data. Despite that, companies are not evaluating the operational, legal and commercial risk from not having a SAM strategy or having a poorly implemented strategy.

IDC recommends that organisations look at three factors in their SAM strategy immediately:

- ☒ Firstly, ensure that responsibility is taken and championed at board level, as this is ultimately where the risk will end up causing potential fiscal, legal and reputation damage to the company and ramifications for directors. Currently, 75% of organisations have non-board members: IT managers, line of business managers and purchasing managers, with responsibility for managing risk in SAM.
- ☒ Secondly, consider implementing a formal SAM training programme for key employees impacting this discipline with regular refresher courses. Currently, only 15% of organisations have this type of training. This programme benefits organisations by enabling staff to effectively manage software licences and tailor a SAM programme consistent with corporate strategic initiatives and goals.

- ☒ Thirdly, consider adopting SAM tools at each key stage to provide a consistent, clear and efficient approach to the subject. The three key areas to review for technology adoption are related to the definition and monitoring of the processes that underpin SAM: discovery of deployed software and tracking actual use, capturing proof of licence entitlement, and reconciliation of the current licence position. Such tools can ease the burden of manual controls and improve the efficiency and decision-making processes inside the organisation to drive down costs and improve compliance. As a minimum starting point, a SAM tool should be used to automate the discovery and tracking of software.

Later papers in the series will look in more detail at the adoption of SAM, adoption of technologies that change how software assets are managed and the technologies and strategies that reduce risk and cost from software assets while ensuring that benefits are realised.

SCOPE AND METHODOLOGY

This paper is the first in a series of four white papers that look at software use and software asset management (SAM), quantifying the risks and benefits of different approaches to managing software assets.

The paper is sponsored by FAST IiS, which has formed the Software Industry Research Board (SIRB) to assist those involved in evaluating, purchasing and managing software by providing a common resource to determine where your approach stands relative to the market and to best practices.

FAST IiS and IDC will carry out this research annually to understand how companies and public sector organisations are responding to the commercial and legal pressures that the fast-changing software industry places on them.

We welcome comments on this paper and input on the direction of future research, which can be sent to:

- ☒ John Lovelock, chief executive, FAST IiS (john.lovelock@fast.org.uk)
- ☒ Chris Ingle, consulting and research director, IDC (cingle@idc.com)

This paper is based on three sources:

- ☒ IDC's ongoing research into SAM and approaches to managing software in business and public sector organisations. IDC defines SAM as the IT practice of acquiring, optimising and retiring software licences throughout the software life cycle. Software asset management provides IT and business executives with the total view of software assets used, including costs, users of the assets, scheduled updates, replacements and retirements in order to optimise software asset use within the organisation to meet company goals and objectives.
- ☒ A 2008 survey of 601 IT executives and buyers of software in the UK. This is representative of the UK business market by size of company and investment in software.

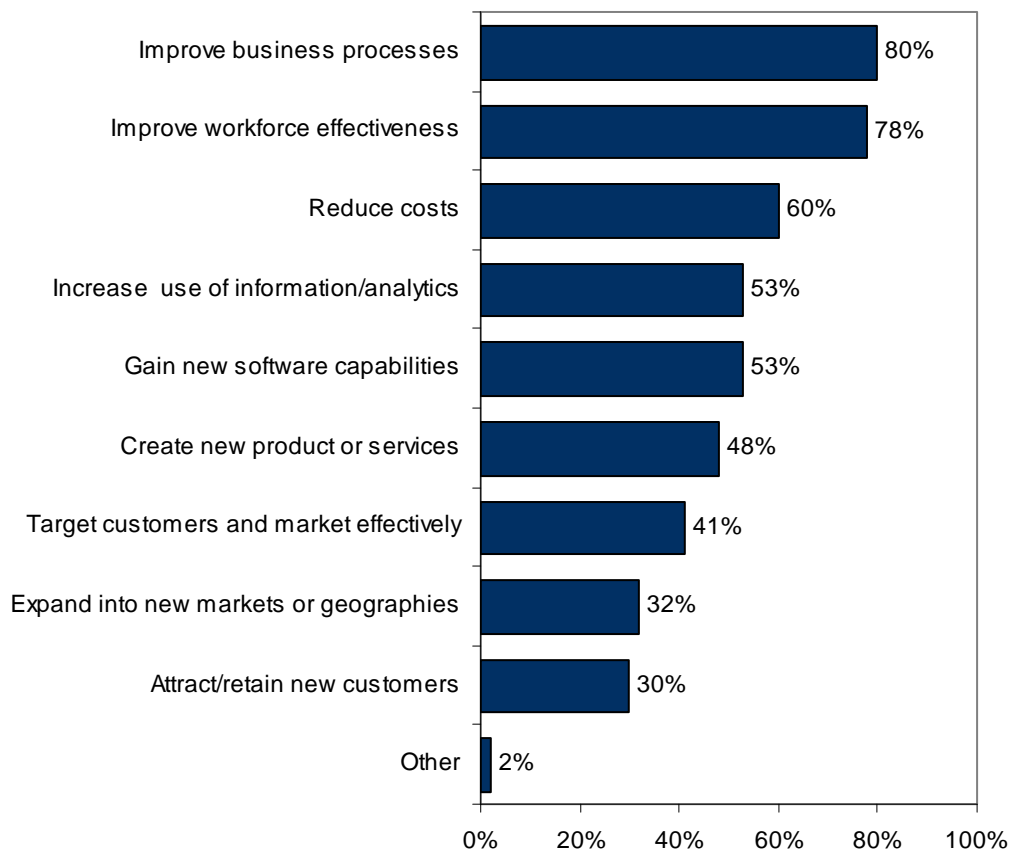
- ☒ SAM Optimisation Model. This recently updated model was developed by Microsoft, based in part on research conducted by IDC, and has been adopted by other organisations. Briefly, it gauges the maturity of a company's IT infrastructure and processes in four levels, as set out below, and provides a framework to self-assess the gaps in current practice needing to be remedied to enable the risks to be reduced and the SAM process to mature:
 - ☐ Basic organisations are the least efficient performers and have high costs and average or below average service levels and agility. These organisations typically have manual processes to identify, track and manage software assets through their life cycle.
 - ☐ Standardised organisations have somewhat better IT costs and service levels and agility when compared with basic organisations. These organisations leverage some of the easier-to-implement best practices regarding SAM.
 - ☐ Rationalised organisations have very low costs, and show modest improvements in service levels compared with the other two groups. These organisations use many IT best practices to automate and standardise SAM processes whenever possible.
 - ☐ Dynamic organisations shift the focus from cost reduction to enabling business with optimal service levels and agility. Dynamic organisations may even choose to accept best practices that increase costs to optimise service levels and agility.

WHAT'S THE MARKET PERCEPTION OF THE VALUE OF SOFTWARE?

There is a disconnect between perception of value of software and effective management of software. Companies interviewed for this survey cite the reasons for deploying software, which are summarised in Figure 1.

FIGURE 1

What are the Benefits of Deploying Software?



Q.: What are the most common reasons for you to buy new software, or adopt new technologies?

Note: Multiple responses accepted, total may exceed 100%.

n = 544

Source: SAM Best Practice Study, IDC, 2008

Reasons for adopting software split into three main groups:

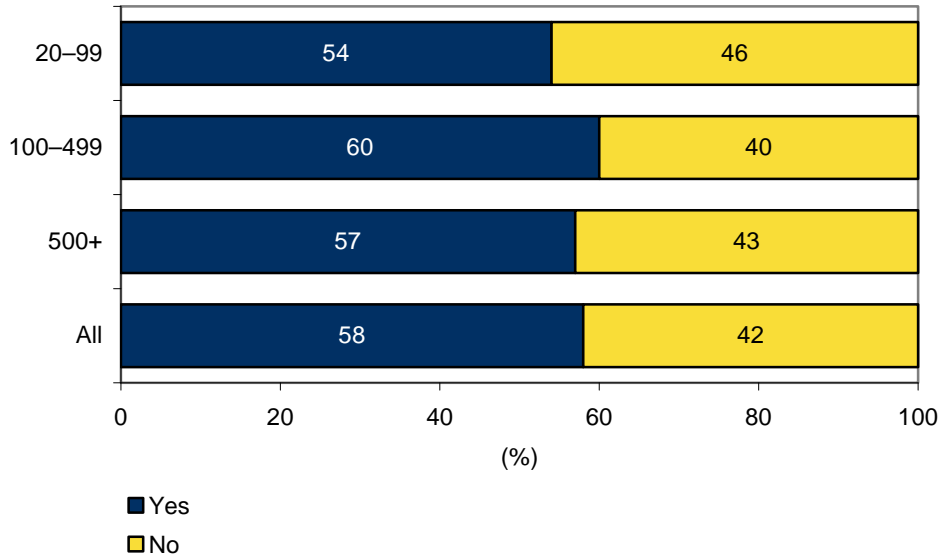
- ☒ Improving management of the business. 80% of companies use software to make their businesses more agile and more effective. Still more are using software to get more information on their business.
- ☒ Improving the productivity of staff. 78% of companies are using software to increase the productivity of their employees. In another survey carried out by IDC, CEOs cited increasing staff (particularly sales) productivity as the main aim for their IT investments.
- ☒ Cost reduction. This was cited by 60% of respondents and there is plenty of evidence that companies can reduce their costs through, for example, automating manual processes or optimising supply chain.

Why then is this value not generally recognised? IDC believes there are a number of reasons why companies face challenges in assessing the value of their software investment:

- ☒ Firstly, the industry does not always clearly demonstrate the full value that customers can see from use of software. Also the full spectrum of licencing options from perpetual to SaaS and volume discounts to OEM can be confusing to the average business buyer.
- ☒ Secondly, many organisations account for software as an expense in the year of purchase rather than as an ongoing or fixed asset, whereas hardware is treated as an asset and placed on the asset register. The use and value of hardware is visible whereas software investment, although often larger, is not.
- ☒ Thirdly, many organisations do not have adequate processes for measuring the value of investment. Software is seen as a necessary expenditure but the full benefits are not always seen or measured. Figure 2 shows how limited measurement can be. Overall, 42% of organisations are not factoring the total cost of their investment into their investment evaluation.

FIGURE 2

Is the Total Cost of Software Investment Measured? Data Split by Number of PCs in Organisation



Q.: When buying software, do you factor in a cost for implementation and ongoing support, technical and user skill updates and the time it will take your staff to become fully conversant with the new software?

Split by number of employees in organisation.

n = 544

Source: SAM Best Practice Study, IDC, 2008

The benefits seen from software use, as well as the challenges, are important but there is a critical factor that has not been given enough consideration: the risks of not managing software properly.

The next section discusses risk and how companies are approaching it.

RISK PERCEPTION AND REALITY

One of our key findings in this research is that despite the importance of software to the business, many organisations fail to implement procedures to manage the risk inherent in using software assets to achieve business benefits.

Risk Perception

We have identified three types of risk:

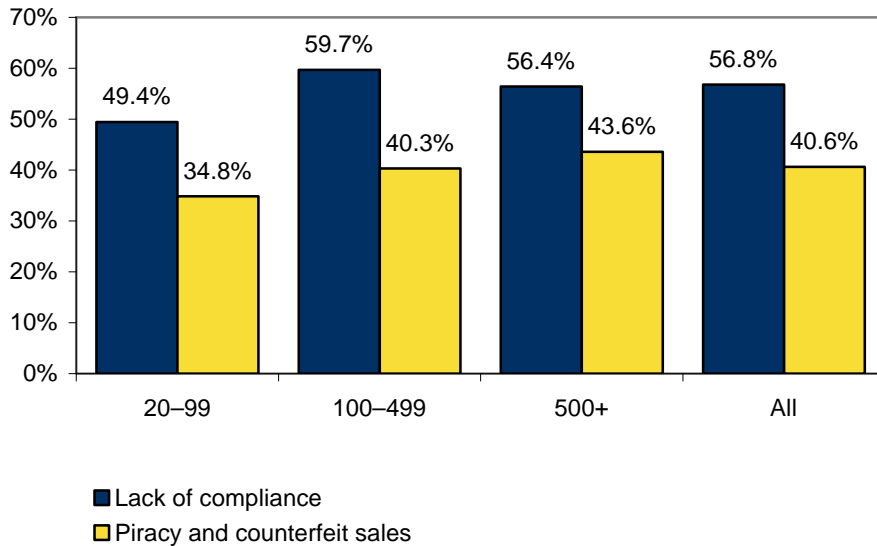
- ☒ Firstly, there is the **commercial** risk that comes with not managing software assets effectively. There are two sides to this: not having sufficient licences to cover use of software; or having too many licences and either spending less than you are contractually obliged to do, under the terms of your licence contract, or more than is required, because you do not have visibility of your software estate. This can have a significant impact on operating costs at a point of reconciliation.
- ☒ Secondly, there is the **operational** risk from software that is not tracked properly through the organisation and consequently could lead to a reduction in the business' ability to function. An example of this is when an employee (maliciously or accidentally through lack of control) introduces malware into the network, which takes over their machine, knocks out a server or the network and has a far-reaching impact on the business.
- ☒ Thirdly, there is the **legal** risk from using unauthorised or pirated software. Organisations expose themselves to legal consequences for allowing employees to use unauthorised software on company hardware resources.

These risks affect any and all organisations that do not practice effective SAM. Piracy covers illegal use of software and use of software which is counterfeited. Lack of compliance covers use of software where the licence agreement does not reflect the use of the software.

As Figure 3 shows, approximately 60% of organisations do not perceive a risk from piracy and 43% do not perceive a risk to their organisation from lack of compliance.

FIGURE 3

Do You See a Risk From Lack of Compliance or Piracy or Counterfeit Software?



Q.: Do you see lack of software compliance as a material risk to your business?

Q.: Do you perceive any risk to your business from software piracy and counterfeit sales?

n = 544

Source: SAM Best Practice Study, IDC, 2008

Clearly this shows that organisations have a growing awareness that lack of compliance is an issue for business. However, their assessment of the immediate risk to the business is arguably lower than the evidence collected in the research would suggest.

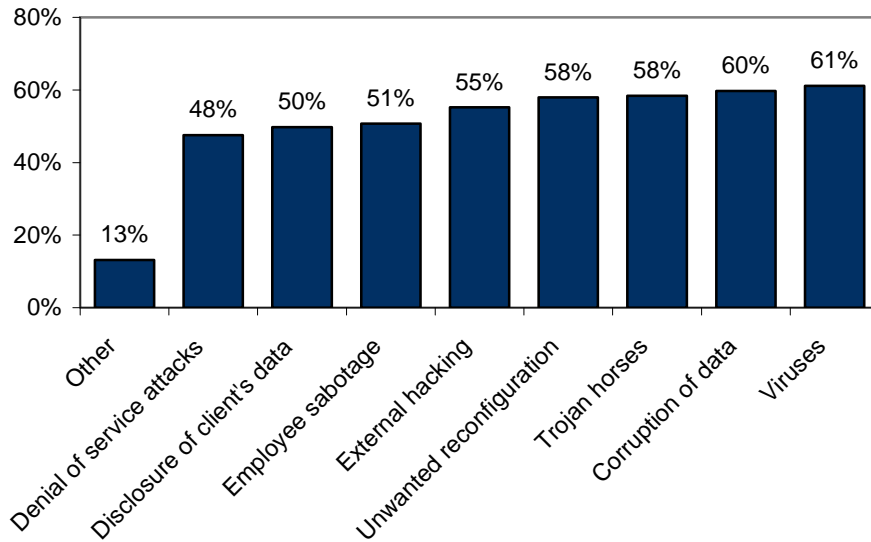
Many of the organisations we interviewed seem to perceive the risks associated with SAM as a problem that affected others rather than themselves. Smaller organisations were among those that perceived the least risk but may in fact be subject to the most risk due to their lack of software management.

Risk Realities

Surprisingly, 60% of organisations do not perceive a risk from piracy or counterfeited software. Ironically, roughly the same percentage identify some of the main risks to their business from pirate software. Figure 4 shows the risks that organisations perceive they can be exposed to from pirate software.

FIGURE 4

Which Risks are Perceived From Pirate Software?



Q.: What potential risks could your business be exposed to from the use of pirated or counterfeit software?

Note: Multiple responses accepted, total may exceed 100%.

n = 183

Source: SAM Best Practice Study, IDC, 2008

Interestingly, very few respondents identified licence compliance (currently rolled up into "other") as a risk from the use of pirated or counterfeit software.

It cannot be overstated how critical these risks are to an organisation. They cover the principal threats to ICT security: untrusted systems, untrusted data and unavailability of data and systems.

Regarding commercial risk, software companies have instituted formal audit processes where a detailed analysis is undertaken to understand whether an organisation is under- or over-paying for its software assets; this may be carried out by a third party or by the software vendor. If the results of the audit reveal that a company is under-licensed it could be faced with a sizeable bill for the additional licences it is using.

Our research shows that 55% of organisations have been subjected to an audit in the last 12 months. It is anticipated that this trend will continue and therefore organisations need to be prepared; 46% of organisations interviewed found the cost of performing a one-off audit much more expensive than they had anticipated.

BEST PRACTICE IN SAM: BENEFITS AND ADOPTION

Later in this white paper and in the series of papers that follow, we will review the key components of best practice in SAM that will help an organisation reduce risk. This section discusses some of the benefits of SAM seen by companies surveyed.

Benefits of SAM

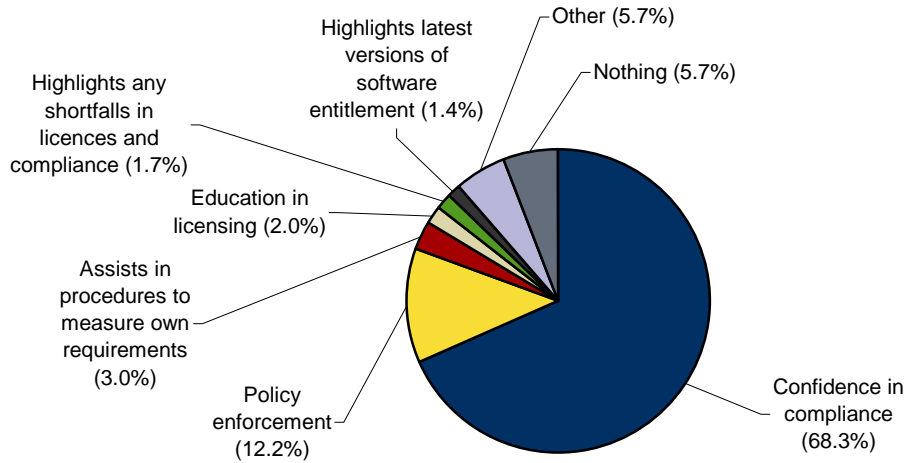
Organisations interviewed for this project cited the following benefits from best practice in SAM:

- ☒ **Reduced commercial risk.** Companies reduce their cost through knowing that they are using all the software they are paying for. SAM enables companies to optimise their expenditure on software in line with the productivity benefits they are gaining from use of that software.
- ☒ **Reduced operational risk.** Organisations that effectively use SAM know which users have access to each resource. This allows them to better monitor access to data and applications and enforce policies so that potentially harmful software is not allowed into the organisation.
- ☒ **Reduced cost of legal compliance.** Companies that have active SAM and licence management practices are able to prove their software deployment and licence entitlement reconciliation. The pre-existence of this audit trail reduces the cost of complying with a formal audit and reduces any exposure to under-licencing. This is an important benefit in response to the fact that 55% of companies questioned had been audited and 46% found the effort and cost of conducting the audit to be significant.
- ☒ **Systems are stable and available and data is more likely to be usable.** In addition companies can identify whether they are using the latest software and have appropriate patch and security processes for that software.

The results of effective SAM can be seen in the responses given by those companies that have been audited. These are shown in Figure 5.

FIGURE 5

Beneficial Outcomes of an Audit



Q.: What was the main factor that was useful in this (audit) process?

n = 296

Source: SAM Best Practice Study, IDC, 2008

The vast majority of benefits are in compliance, with nearly 70% of organisations being more comfortable with their operational risk after audit than before.

Adoption of SAM

Later papers in this series will provide a more detailed guide to the different aspects of SAM. A critical point is that organisations overestimate their use or effectiveness of the SAM best practices they have implemented. 75% of organisations claim to have a formal plan for SAM, but when we look at their adoption of SAM best practices in a sample of categories in the SAM maturity model (see page 3 in the Scope and Methodology section of this document for definitions of these categories) we find that performance varies considerably between category. For example, for inventory accuracy, 38% of companies do not maintain an accurate inventory of their assets. 24% maintain an inventory but may have higher costs than the 25% of organisations that have rationalised their SAM process. Almost all organisations can make cost-effective improvements to their SAM practice.

CONCLUSION — WHAT SHOULD YOU DO FROM HERE?

This paper has shown that many organisations believe they have a reasonable SAM strategy but need to do more to be fully effective. There are clear benefits in doing so, as shown by the companies that have gone through this process in an audit.

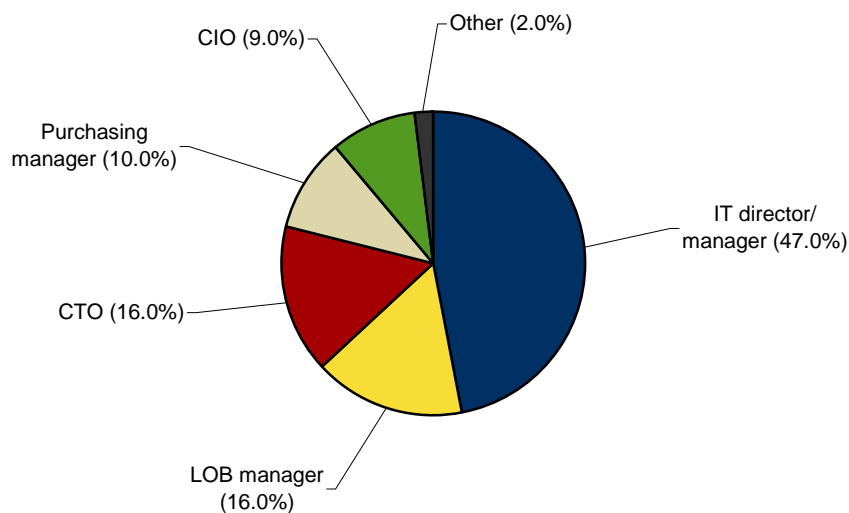
While there are multiple best practices and steps toward a thorough SAM strategy, IDC has identified three simple but fundamental steps for organisations that want to improve their SAM strategy, gain some of the benefits discussed in this paper and avoid some of the risks that we have identified. Clearly much depends on the starting position of your organisation. IDC believes the vast majority of organisations can benefit from assessing these three areas regardless of their current perceptions as to the suitability or otherwise of their current SAM practices.

Step 1: Make SAM (particularly compliance) the Responsibility of the Board

A lack of compliance is a risk in the ways identified earlier. This risk ultimately falls on the board of an organisation. However, the majority of organisations do not assume this risk at a senior level within their companies. Figure 6 shows that in most cases responsibility is not currently a board issue.

FIGURE 6

Responsibility for SAM is Currently Not a Board Issue



Q.: Who is responsible for the SAM strategy and compliance?

n = 544

Source: SAM Best Practice Study, IDC, 2008

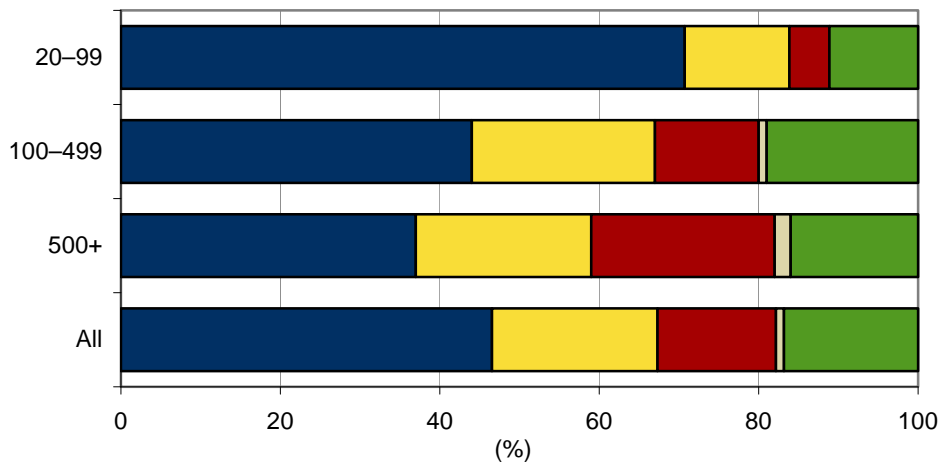
Of course no one would expect the board to manage the operational details of SAM any more than one would expect a board to manage asset registers or set compensation plans for individual sales people. However, at a strategic level the board needs to be assured that the company has minimised its risk and cost in this area and hence needs to ensure that the SAM strategy flows from the board to the procurement and IT staff who manage its daily operation.

Step 2: Ensure That Staff Are Trained on Risks of a Poorly Managed Environment

As Figure 7 shows only 15% of organisations have a training programme for SAM for their staff that includes refresher training.

FIGURE 7

Training Received for Managing Software Licences



- Nothing formal, a training programme was created ad hoc that may include attending industry events or reading literature on Web sites
- We have a formal training programme that was taken a while ago
- We have a formal training programme that includes refresher training
- Other
- None

Q.: What level of training did you, or this person, receive in order to discover, track and manage software licences?

n = 346

Source: Software Usage Survey, IDC, 2008

An immediate, and relatively low cost action, organisations can take is to develop a formal training programme for key personnel responsible for SAM. At a minimum, this should include:

- ☒ The commercial, legal and operational risks from a poorly managed software environment.
- ☒ The responsibilities of the board in respect of the software environment.
- ☒ How those responsibilities are being delegated to staff (for example, in not installing software without permission).
- ☒ The consequences for employees who do not follow these best practices.

Step 3: Use Tools Where Appropriate

Organisations use technologies to identify, manage and track software assets. However, as previously noted, many organisations at a basic level are using manual processes to identify and document software assets, such as spreadsheets. While easy to start with, spreadsheets need constant updating, to track where software assets are located, which employees have authorised licences and how many licences the company may have purchased. With employees that are hired, or those that leave the company, the number of licences can change frequently. Software tends to change more regularly than other assets and can also enter the organisation through many different routes, ranging from a formal purchase to an employee downloading software.

Organisations with significant assets to manage will find that using spreadsheets to track and manage computer hardware and software doesn't scale as the organisation grows. Therefore, IDC recommends that organisations consider the adoption of software solutions that can automatically discover, identify and track software licences over the company's network.

These tools and processes should support three critical areas:

- ☒ **Process.** SAM tools, and the plan underpinning the use of these tools, should estimate the potential return and threats from not implementing an effective SAM strategy. It should show the people responsible throughout the organisations for maintaining the strategy. It should not be a single point of time exercise, it should identify the process to capture change in software use.
- ☒ **Discovery.** The discovery phase should identify all the software running on client devices and on the network. It may do this automatically, or require manual intervention. It should have a process for tracking changes in use and identify who is responsible for doing discovery.
- ☒ **Matching software use with licences.** The tool and process should be able to reconcile software use with licence entitlement. Clearly this requires two inputs, input from the discovery phase and input of licence entitlement for each type of licence (for example, user or server based) and number or terms of licences.

SAM tools are an important part of any SAM strategy and should be evaluated as part of this strategy.

Next Steps

For more details on SAM practice, benefits and strategy please look out for the next white paper in this series. This paper will be available in February 2009 from <http://www.fastiis.org/> and will look at understanding and adoption of SAM in the UK.

Alternatively, you can subscribe to the series of white papers by registering online at www.fastiis.org/subscribeSAM.

Copyright Notice

External Publication of IDC Information and Data — Any IDC information that is to be used in advertising, press releases, or promotional materials requires prior written approval from the appropriate IDC Vice President or Country Manager. A draft of the proposed document should accompany any such request. IDC reserves the right to deny approval of external usage for any reason.

Copyright 2008 IDC. Reproduction without written permission is completely forbidden.



IDC is a **subsidiary** of IDG, one of the world's top information technology media, research and exposition companies.

Visit us on the Web at www.idc.com

To view a list of IDC offices worldwide, visit www.idc.com/offices

IDC is a registered trademark of International Data Group