Technology Asset Management Global Survey:

Today's Challenges of Device Proliferation

Nlyte Software

Commissioned by Nlyte Software

SAPIO RESEARCH

CONTENTS

FOREWORD

TLAs like 'TAM', and how they keep the business running

The enterprise is full of TLAs (three letter acronyms). Most are important to someone, some are important to everyone - whether they know of them or not.

As organizations digitalize and their compute infrastructure grows, they grow organically. Resources spread, pool and collect in places with gravity. They don't necessarily flow to the places that need them most, where they will - if you'll excuse the metaphor - water the crops the organization depends on for life.

The compute infrastructure for many large organizations is not a happy place. It's complex and inefficient - and the way to fix it is not always clear, easy or simple.

Technology asset management (TAM) - a TLA that many in the business may not yet understand - is a technology that serves the enterprise by bringing order to the chaotically grown compute infrastructure. It functions as a single source of truth for the business to manage the cost, security, compliance, and the operations of its technology.

What kind of technology? From the desktop to data center, the cloud to each remote location, TAM extends beyond facility and compute asset management to the entire Internet of Things. TAM assists the enterprise in the complex task of discovering, cataloguing and assessing everything attached to the network - for compliance, security and efficient operations.

After years of delivering complete asset lifecycle management to the data center, we extend that deep understanding to the TAM landscape and we are sharing our survey insights taken from enterprises across the USA, the UK, and France (and adding it to our global knowledge) so that organizations can make more informed choices by understanding what 'normal' and 'better' look like, and by benchmarking themselves against their peers.

Technology asset management combines and consolidates information from across the organization on the state, location, health, security, and effectiveness of technology. TAM solutions optimize technology, associated software and the combined infrastructure are procured, managed, maintained, secured, and disposed of.

EXECUTIVE SUMMARY

It's not easy to pool the most pertinent points from the brilliant minds of over 1,500 technology asset decision makers in organizations employing over 1,000 people across the US, UK and France. But it's no surprise that almost all of them (96%) think hardware and software asset control is a top five priority for their business.

What is a surprise, though, is that almost one third (31%) of those enterprises are still tracking their asset management control manually! So where is the disconnect?

As ever in all things business, especially when it comes to technology decision-making, the barriers of budget constraints and lack of specific skills are stopping the organization from gaining total asset control. But what happens if you are not 'in control'? Will you be one of those businesses where it takes something seismic to happen that jolts you in to action to put procedures in place for it to never happen again?

> What makes audits worse is that for 34 per cent of organizations, the outcome is a rise in their software licensing costs. Nearly a quarter (21%) even face fines.

Audits are but one way for organizations to evaluate and reconfigure where assets sit. But perhaps unsurprisingly given what enterprises go through with them, 84 per cent of respondents were at least a little concerned about the prospect of vendor software audits. Six per cent of organizations have, incredibly, spent over 500 hours managing the audit process in times past. What makes audits worse is that for 34 per cent of organizations, the outcome is a rise in their software licensing costs. Nearly a quarter (21%) even face fines - an astounding amount that perhaps comes from an inability to manage the processes well rather than any deliberate misdemeanor. There's a strong case for a TAM solution that saves an enterprise significant time and money as we outline on page 16.

So what is the way forward? 'Real-time' is the watchword, and it seems that real-time offers real advantages. 39 per cent of IT managers believe that a real-time (automated) view would save the IT delivery team six to ten per cent time in daily business operations.

61 per cent say a real time view would enhance IT innovation to support business goals. In fact, over a third (37%) believe that they could save 20 per cent of their budget by remediating underutilised software – but only if they had a real-time view of the situation.

Beyond the core time and money aspects of real-time management, the matter of risk looms large. Security risks from un-updated firmware/software is the most concerning risk for businesses and organizations of all types, although it is clear that risks of all types concern decision-makers. Compliance also holds court, with most organizations acknowledging that implementing automated asset management tools would help them improve their compliance performance. But, just one in ten did not adhere to any of the ISO 19770.x standards.

This report concludes that understanding of technology asset management is high, but adoption and discipline needs to be higher across the spectrum for large organizations. As organizations grow they often lose control over their technology assets. Gaining this control back does not need to be the laborious process that it once was.

Of course the whole organization will benefit from TAM, and not just the IT team tasked with securing and running the technology, or the users running more reliable, secure, and optimized technology on high availability platforms... If there is already an asset management team, they are able to stay current and put time and resource to higher level activities that can benefit the business in more innovative ways.

TIME FOR TAM

The research we're dissecting here was commissioned by Nlyte Software and delivered in January 2019. The 1,516 respondents were technology asset decision-makers in organizations employing 1,000 people or more. As such it represents a slice of the US, UK, and French enterprise landscape and should be analogous with how technology asset management is conceived, conducted, and consumed by enterprises across the globe. The interviews were independently conducted online by Sapio Research using an email invitation and an online survey.

Across our global sample (USA, UK, France) 96 per cent say that hardware and software technology asset control is a top 5 priority for the business. It's no surprise!

In the pre-cloud era, tech grew and grew. Desktops, laptops, mobile phones, tablets and other devices... and then the enterprise class backbone technology too: the servers, routers, switches, wireless access points and any or all physical devices from security hardware to the Internet of Things (IoT) sensors, robots, and more.

With the introduction of the cloud and the evolution of software as the primary controller of most business processes, your technology, teams, platforms and assets are spread over a wide network and across disparate locations. It's a challenge to manage it all efficiently - tying it together coherently so that the organization can enable it all to work together effectively to business goals, defined service level agreements (SLAs) and key performance indicators (KPIs).

Ultimately all the applications and data your organization manages collectively depend on a stable and secure physical infrastructure. Whether this is located in your own data centers or in colocation or 'edge' facilities, you must be certain these resources are not compromised, whether intentionally by outside threats to business operations, or unintentionally by misadventure.

Resources can become compromised when personnel make unplanned and/or unrecorded changes to assets. Employees may make well-intentioned modifications such as adding or removing assets such as servers or blades without approval, or without recording the information centrally.

Such events can then open an organization to disruption, either through critical outages or cyber-attack. All too commonly devices can be installed that don't meet corporate or regulatory security and safety standards. Additionally, new security threats are constantly being identified and require the latest firmware and software patches to be applied in order to close such vulnerabilities.

Yet many organizations do not have a comprehensive list of all their hardware, much less the versions of firmware and software running on these assets throughout the network, which results in these systems being at greater risk of cyber-attack, and also makes daily planning and optimizing more challenging. Add in the difficulties the business may face with software asset management (SAM) on top of TAM matters, and there's a case for taking control of the matter to simplify the business challenge, streamline processes and manage technology costs and employee time.

Shining new light on the challenge

Well, on the surface, our new data reveals that TAM appears to be a key business issue for the C-suite - that's what 83 per cent of our 1,516 technology asset decision makers said. All of these were based within organizations employing 1,000+ people. However, almost a third (31%) of organizations are still tracking this manually. That's likely not a state of affairs those involved want to maintain!

> TAM appears to be a key business issue for the C-suite.

As ever in all things business, especially when it comes to technology decision-making, the barriers are budget constraints and lack of specific skills stopping the organization from gaining total asset control.

Let's look into the world of enterprise tech decision makers and how they see the situation, now, and how they see it might change.

THE INTERESTING THING ABOUT INFRASTRUCTURE IS...

What the organization can find and control

The business knows what they should do already! 61 per cent told us that a real-time view of technology and software assets would enhance their IT innovation to support their business goals.

Yet that said, only 45 per cent said that their assets are validated at least daily (30% do this weekly). Moreover, only 50 per cent are tracking assets in their data center. At least a majority of (62 per cent) are doing so for desktop and laptops.

Confusion in the ranks

C-suite respondents believe that assets are being scanned hourly (27%) or daily (35%) - yet those at manager level (presumably the ones at the sharp end) are less confident (8% and 28%, respectively).

As we lengthen the time periods the picture changes, and managers show where they are scanning their assets less regularly than those in the C-suite believe:

Frequency of scan	Total sample	C-suite	Manager
Hourly	13%	27%	8%
Daily	32%	35%	28%
Weekly	30%	25%	31%
Quarterly	17%	11%	20%
Annually	4%	3%	7%
Rarely (only as needed)	3%	1%	6%

Asset validation by team

Daily	Hourly
37 per cent of asset management teams	18 per cent of finance teams
34 per cent of IT teams	14 per cent of IT teams
33 per cent of security teams	10 per cent of asset management teams
29 per cent of compliance teams	7 per cent of compliance team
25 per cent of finance teams	6 per cent of security teams

What's of greater concern is that a whopping 78 per cent of the global respondents claimed that up to 20 per cent of their assets remain undetected from these network scans.

Although most devices are up to date (on average 67% have the latest security software and firmware patches), less than half (49%) have a solution that scans and validates all devices in order to provide an audit trail for security patch management and almost half (48%) of devices are not proactively managed at all! Whilst that 67 per cent figure seems better than average, that means that a third of assets are at risk, outdated, or unmatched. And those are the assets known about - not necessarily the total asset inventory. Clearly, risk from licensing, vulnerability, cyber hygiene and efficiency are still present - and particularly in the case of cyber security - it only takes one breach to upset the whole technology ecosystem. A case might be made that these figures are far from reassuring - in fact, that they are shocking and demonstrate a widespread TAM regime to be compliant with standards and unfit for purpose.

That means that a third of assets are at risk, outdated, or unmatched. And those are the assets known about - not necessarily the total asset inventory.

How teams validate and provide an audit trail for security patch management

The data indicates that generally, about half of organizations have some kind of solution to scan the whole organization, but a reliance on the helpdesk and change management database workflow tickets was almost equally prevalent. Although antidotal to this survey, it is widely believed that Change Management Data Bases (CMDBs) are critically inaccurate and out of date, so depending on these as a trusted source for asset management further exacerbates the asset management gap between reality and inventory.

While most organizations say they audit security patch management, they admit it can take three or more separate tools to approach the picture they need. And more concerning is that three per cent of those surveyed don't have any way to audit security patch management. And when we just look at the answers from security, they double that three per cent average response...

Clearly, if the majority of organizations (78%) are finding that around 20 per cent of their assets are undetected, these solutions and methods in the table above can't be effective enough for the average enterprise. With such a large unknown proportion of devices, the enterprise has an understood but unaddressed risk from possibly unpatched, uncompliant, unlicensed, and uncontrolled devices.

Discovery solutions rely on tools such as 'agents' installed on all hardware assets. However, they don't self-monitor to validate they are installed (ghosting); that they are operational (not deactivated); or that the update process was successful. That is to say, the agents themselves are not a reliable tool for the use that they are intended.

The costs of unpreparedness: Time and money

Perhaps unsurprisingly given the time and resource levy they command, 84 per cent of respondents were at least a little concerned about the prospect of vendor software audits. The IT and security teams both scored the highest for 'very concerned', each at 22 per cent. Somewhat oddly, perhaps, of the Compliance team only seven per cent were 'very concerned'.

The descending scale of concern

It is interesting that the person with the most risk is concerned, but the person most likely responsible for compliance is least concerned, as the figures below state. Clearly to be effective, there needs to be a unified concern and ownership across an organization.

How concerned are you by the prospect of vendor software audits of your business?

- C-Suite - 34%
- Vice President/Senior Vice President - 19%
- Director - 20%
- Manager - 14%

The benefits are there to be taken. On average, enterprises estimated that they can save 22 per cent of their software budget on underutilised software licensing. But still the top blocker or concern about asset management technology is that it is perceived as too costly to implement (28%).

	Total	IT	Finance	Security	Compliance	Asset Management office	Business unit
We have a solution that scans and validates everything including desktop, data center, and mobile devices	49	52	47	40	40	45	47
Rely on helpdesk and change management database workflow tickets	42	42	41	48	40	45	42
Leverage vendor tools like Microsoft SCCM	41	45	36	29	37	38	31
We don't have a way to audit	3	3	2	6	3	5	6

Audits: No one's favourite time

It's hardly a newsflash that vendor software audits eat up company time. Audits are concerning to the majority of organizations, primarily due to the financial implications and time involved. Of those who have had an audit, more than a quarter (27%) spent between 101 and 500 personnel hours getting through the process. In fact, giving staff the required time to manage it is noted as the hardest thing about an audit. Six per cent of organizations have, incredibly, spent over 500 hours managing the audit process in times past. It doesn't matter how well-resourced an organization is - that level of time represents a severe dent in the business operations for any size of business.

What makes audits worse is that for 34 per cent of organizations the outcome is a rise in their software licensing costs. Nearly a quarter (21%) even face fines - an astounding amount that perhaps comes from inability to manage the processes well rather than any deliberate misdemeanor.

Estimating the cost of auditing software in person-hours

The UK jobs board Adzuna, which provides employment data to the UK government executive in Downing Street, states that in February 2019, £36,485 ($48,094) was the national average salary for 'IT jobs' in the UK. Extrapolating (with acknowledgement that this is going to be an inexact calculation), that means that the cost of time might be £8,770 ($11,567) based on that 500 hour figure given above.

Using a TAM solution, a 5,000 person company (with circa 6,000 assets) could expect to amortize the cost of a perpetual license over five years, equating to 7.5 person weeks. A software audit takes 12.5 person weeks, which then equate to weeks gained in productivity if not spent on the audit.

Assumptions:
2080 working hours in the year

Assuming 5,000 laptop/desktops with $300 unused software, it equals $1.5 million savings (ROI).

Spend that time doing something more joyful

Organizations are also quite clear that they know the way forward. 'Real-time' is the watchword. It seems that real-time offers real advantages. Our TAM responders believe that a real time view of assets could save a non-trivial amount of time for the IT delivery team (7% average for both daily business operations and for audit processes). 39 per cent of IT managers believe that a real-time (automated) view would save the IT delivery team 6-10 per cent time in daily business operations.

Furthermore, on average it's estimated that they can make a saving of 22 per cent of software budget on underutilized software licensing. 61 per cent say a real time view would enhance IT innovation to support business goals. Plus, IT spending could be extended by an average of 10 per cent if organizations could re-use that resource to better effect.

Solving this licensing and audit situation is achievable, and the way to do it is through a real-time view of technology and software assets. In fact, 61 per cent of organizations believe that a real-time view of their assets would enhance their IT innovation to support wider business goals.

In addition, over a third (37%) believe that they could save 20 per cent of their budget by remediating underutilised software – but only if they had a real-time view of the situation.

The nitty gritty: Why manage the IT asset lifecycle?

The skills issue / the need for automation

- A lack of software skills
(46% C-suite / 34% managers)
- A lack of technology asset management experience
(32% C-suite / 34% managers)
- A lack of hardware skills (33% C-suite / 30% managers

Undetected assets are compliance and security risks

- 28/29 per cent of C-suite/managers believe that 10 per cent of their assets are undetected and unprotected
- 35/14 per cent of C-suite/managers believe that 20 per cent of their assets are undetected and unprotected

37 per cent of respondents believe that they could recover 20 per cent of their software budget... injecting new resources into more strategic areas.	**35 per cent** of C-suite say data is captured manually as part of an IT asset management process - known to be quickly out of date and prone to human error.
36 per cent of C-suite aren't tracking their edge assets - where the risk of intrusion is highest.	**64 per cent** of managers are tracking assets weekly or less, which means hundreds of change orders unverified.
Software audits can consume **500+ man-hours** of lost productivity/overhead cost.	**77 per cent** have engaged, or have a software audit upcoming: They will happen for most large organizations!
Finance department respondents report negative impacts from audits: • **38 per cent** saw responsible people reprimanded • **28** saw increased licensing costs • **17 per cent** were imposed fines • **15 per cent** faced legal action	**42 per cent** of asset managers were able to negotiate better pricing (and automation helps since continuous monitoring saves money. **29 per cent** of the compliance function believe IT would be more efficient, reducing the burden, because a real-time view through automation would save the IT delivery team 11-15 per cent time in audit business operations.
76 per cent unpatched?! Only 24 per cent of asset managers believe that 80-100 per cent of their devices had the latest security software and firmware patches (a clear security and reliability risk).	**A third,** 33 per cent of devices are infrequently connected to the network, according to asset managers. That missed scanning equates to a greater vulnerability and set of threat vector.
15 per cent of organizations report that somewhere between 80-100% of devices are not proactively managed, which is an open invitation for risk.	**44 per cent** of asset managers believe they could buy more with constant monitoring - saving 20 per cent of software budget on underutilized software licensing.

By optimizing the utilization of IT assets in real-time, it's recognized that there could be a significant financial benefit to the enterprise IT budget, with half (50%) of organizations saying that they could save six to ten per cent of spending. A further 35 per cent could save more than 11 per cent of their spending, it is believed.

From the bottom line to broader benefits, organizations believe that they are most likely to gain the following from a better IT asset management process:

- Business efficiency (41%)
- Overall cost savings (40%)
- Data / corporate security (39%)
- Technology asset/ecosystem reliability (34%)
- Cost savings on reduced software licensing (33%)
- Regulatory compliance (33%)
- Cost savings on reduced maintenance (33%)
- Cost savings on hardware purchasing (31%)
- Meeting customer/business SLAs (28%)
- Environmental concerns (20%)

Beyond the core time and money aspects of real-time management, the matter of risk looms large. Security risks from un-updated firmware/software is the most concerning risk for businesses and organizations of all types, although it is clear that risks of all types concern decision-makers.

- Risks listed as the first-choices by organization
- Security risk from un-updated firmware/software - 18 per cent
- Regulatory risk from data breach - 15 per cent
- Fines, penalties, and legal action from overextended software entitlement usage - 14 per cent
- Reliability risk from un-updated firmware/software - 12 per cent
- Cost risk from potential downtime from unreliable technology assets - 12 per cent
- Reputation risk from data breach - 12 per cent
- Customer risk from service downtime - 11 per cent

Abracadabra! When it comes to the option of magically solving one business challenge to IT delivery, this is where we start to see some differentiation across organizations and their line of business. Overall, however, 'reduce security holes' would be the top option (19%); in a list of 7 other choices, this is a pretty strong metric. Interestingly, the fairly even spread of the other percentages across given answers shows that, aside from the top vexation of security, there's no consensus or stand-out challenge that beats all others. This shows that enterprises and large organizations are beset by many troublesome challenges across the technology asset landscape, more or less equally after the key concern of security, as shown below:

If you could magically solve one business challenge to your IT delivery what would this be?	
Reduce security holes	19%
Improve data sharing between groups and business systems	14%
Leverage Artificial Intelligence (AI) to optimise application workload placement	13%
Increase/predict asset reliability	13%
Work with a single source of truth for all systems	11%
Automate asset discovery and inventory	11%
Automate auditing and reporting	10%
Reduce the vendor and tools needed to manage the compute infrastructure	8%

Interestingly enough, when the results are split out according to seniority of decision-makers, there are encouraging proof points to show that teams are reasonably aligned with what key priorities should be. The only anomaly here is that, according to the stats, VPs and Senior Directors were the only persona group that put the reduction of vendors/tools and the automation of asset discovery and inventory above the aforementioned.

For the security and asset management teams, security is seen as much more of a problem than other areas of business: 27 per cent and 24 per cent respectively, over the 19% general average from respondents across all business departments. Indeed, when it came to the answer 'Increase/predict asset reliability', security saw this as a more pressing problem (their second choice at 17%) versus the Asset Management Office who saw this as their co-equal third choice at the overall total respondent level of 13 per cent. Other sectors that ranked more highly for a security precedence are manufacturing, at 22%, and telecoms, at 19%.

Methods to manage the IT asset lifecycle are varied, with all used by around a third or more of the respondents. However, looking into the responses, it's interesting to see what processes are more or less favored by each controlling department:

Maintaining standards

Standards give guidance and structure to best business practices. GDPR, HIPAA, PCI, SOX, and so on all require asset management tracking and auditing as part of their guidance. ISO 19770.x is one such tool to give structure. 37 per cent of all C-suite respondents acknowledged applying/adhering to some/part/all of the standard. Yet the results of the survey show they are mostly unsuccessful. Most organizations acknowledge that implementing automated asset management tools would help them improve their compliance performance. Just one in Ten. did not adhere to any of 19770.x standards.

19770-1 (a process related standard which outlines best practices for IT Asset Management in an organization)	33%
Vendor standards	32%
19770-4 (allows for standardized reporting of utilization of resources)	29%
19770-3 (a standard which provides a schema for machine encapsulation of entitlements and rights associated with software licenses)	29%
19770-2 (a standard for machine encapsulation of inventory data)	25%
None of the above	10%

	Total	IT	Finance	Security	Compliance	Asset Management	Business unit
Forecasting business needs	41%	41%	33%	24%	47%	47%	49%
Applying a planned maintenance schedule	40%	41%	39%	30%	38%	38%	37%
Proactively scanning and monitoring for errors	38%	39%	37%	24%	36%	33%	38%
Seeking to improve and optimise the cycle	37%	39%	27%	35%	38%	38%	41%
Understand total costs of ownership	35%	38%	30%	17%	25%	31%	34%
Applying intelligence to purchasing and asset management decisions	35%	36%	31%	24%	23%	39%	34%
Purchasing to projected future capacity	32%	33%	38%	29%	23%	26%	31%
Proactively purchasing/storing resources	32%	33%	28%	24%	26%	26%	38%

WHAT WE LEARN

The state of the infrastructure nation

Several of the answers show that large organizations as a whole have no agreement on a clear vision of what their asset management strategy is for.

The survey demonstrated a wide variety of answers as to the methods organizations use to manage the IT asset lifecycle - with no particular consensus - and a lack of success on the best path forward.

Likewise, when presented with the option of magically solving just one business challenge to IT delivery we saw a set of answers spread very evenly across the range: From reducing holes in security (19%) to reducing the vendors and tools needed to manage the compute infrastructure (8%). With an average of 12 per cent, one can see the range between these answers is low, and what that tells us is that there is no one really overriding concern for those looking after the technology assets in large organizations. Or, put another way, those looking after the critical infrastructure for these enterprises are beset with many challenges, and may well be hard-pressed to put out what they may see as multiple fires burning at any one time.

Also, the sense of security and compliance that varies from the C-Suite to the various individuals across organizational groups is concerning, myopic, and shows a false sense of security is prevalent.

One massive point of concern to all manner of organizations should be the fact that most of the industry claims to be adhering to standards such as 19770-1, yet if this was the case, we wouldn't see the 20 per cent of unidentified devices causing such a headache for security, licensing, and compliance.

What's needed is a way to unite the responsible teams and their technology, and make it easier to comply with standards and best practices to achieve the good business outcomes that rely on safe, secure, and reliable technologies.

CONCLUSION

Take some TAM to sort it out

Understanding of technology asset management is high, but adoption and discipline needs to be higher across the spectrum for large organizations. As organizations grow they often lose control over their technology assets. Gaining this control back does not need to be the laborious process that it once was.

Gone are the days of spreadsheets, counting off assets with a clipboard, and keeping a watch on paperwork - cross-referencing dates with a calendar to ensure patches, maintenance, and licensing happened to scedule. Indeed, there is no need for expensive and unreliable hand-scanners and RF-ID systems either, as previous solutions relied on. And all that only if the pressing operational needs of the business allowed for this heads-up and well planned approach.

A lightweight, agentless technology based solution that isn't limited to certain vendor platforms or industry protocols removes these headaches. Such a solution allows for the discovery of any and all types of technology assets, compute, storage, network, software, firmware, IoT and more. A modern TAM solution establishes a Technology Asset Baseline of everything attached to the network. From this baseline all users have the ability to see at a glance via a user-friendly dashboard or tailored reports just what changes are occuring, when and by whom. It removes the headaches and labor intensive audits for the discovery, inventory, and entitlement reconciliation of all technology assets.

What's more, one of the great leaps forward in viability and transparency is the integration that generally comes as standard with modern solutions and allows data to be shared with other business systems such as ERP, fixed asset systems, HR, security, data center infrastructure management (DCIM), IT infrastructure library (ITIL), IT service management (ITSM), configuration management database (CMDB), building management systems (BMS) - and others. Linking assets, locations, usage, and people can reduce hundreds of hours of inventory, audit, and compliance activity, allowing the organization more time to focus on delivering better business value - and even innovation.

The Technology Asset Baseline and ongoing asset monitoring establishes the TAM asset database to be an organization's single source of truth. It contains the most accurate and comprehensive information of every network attached asset's attributes and historical activity. From data center, IoT, cloud, desktop, edge and building systems. Each asset's configuration and relationship is tracked. It becomes the undisputable single source of truth aiding in IT and business communications, providing a comprehensive data engine to make tactical and strategic organizational decisions. Better asset information can then assist in risk management, HR, training, and operational intervention.

Who benefits from TAM?

Of course the whole organization will benefit from TAM, and not just the IT team tasked with securing and running the technology or the users running more reliable, secure, and optimized technology on high availability platforms... If there is already an asset management team, they are able to stay current and put time and resource to higher level activities that can benefit the business in more innovative ways.

> Such a solution allows for the discovery of any and all types of technology assets, compute, storage, network, software, firmware, IoT and more.

TEST YOURSELF

Understand and optimize your organization's TAM

So, if you are convinced that the technology assets across the IT estate might be due some order and top down control and you are are looking to make some changes to optimise the organization's technology and software management process, it can be helpful to ask the business how it fares across a range of key topic areas.

Consider this a useful first-step checklist to understanding, starting, and optimizing TAM performance across your enterprise.

1. Set a strategy and a plan

Most organizations don't start off with a technology asset management plan, but at some stage, they need to create one - once the complexity of the business technology becomes challenging to manage with current resource constraints. Work with stakeholders to develop a strategy and what that looks like translated into actionable plans for the business, IT, users and IT partners and vendors.

There are many sources of guidance from ISO 19770 standards, analyst best practices, and specialist consultants. Leverage any of these as needed - but don't get overwhelmed. Start simple and mature the plan over time, but stay diligent in maintaining the process.

2. Work out your asset landscape

What do you know about your assets in terms of location, security, patch status, health and compliance. It's OK to realise what you don't know, even for it to seem a big obstacle to overcome. By working out where you are the organization is part of the way to getting to where it wants to be.

Your spreadsheets and existing asset databases are going to be out of date. You will need to enlist a modern discovery tool that can collect your technology asset baseline to begin your understanding of the landscape.

3. Understand what the asset lifecycle looks like

Personal tech assets like laptops and mobile phones, and enterprise level assets like servers and routers come into the business. Some travel in and out daily, some might be a higher risk of cyber attack or falling behind in cyber hygiene. When the organization understands how assets should be acquired, managed and decommissioned, it can really start to optimize every part of the life cycle, and what level of management or risk is permissible to maintain the organization's business goals.

4. Understand regulation and risk

Many industries are regulated, and it may not be totally clear what impact that has on IT infrastructure, licensing and technology use. Many have the misconception that regulations only apply to data and access to the applications accessing it. However, these regulations also have mandates around asset management and data portability - servers, storage, network paths, etc.

It's vital to understand how rules and regulations impact the business. Whether it's healthcare, financial, privacy, health and safety or good management - many regulations might have an impact on the organization knowing the health, location and uses and users of its assets. In the event of a crisis being able to demonstrate compliance can make a massive difference to the long-term health of the organization.

5. Set your practices: How do you want to best behave?

Codify best practices and ensure that everyone, from the IT team applying patches and the front-line users using the technology to serve customers, all the way up to the C-suite who must endorse how the business applies the right behaviours. All must understand what is good, safe, and in the best interests of their role and the company strategy.

6. Only measure what matters (but keep an open mind)

Depending on business goals there may be a variety of metrics that matter, from operational efficiency or cost reduction to risk management. If an organization has struggled with compliant licensing of assets, then looking at simple areas like the number of unused licenses, licence expiration, and what the organization's ratio of purchasing to use has been can help all plan a smarter and more cost-efficient business model.

Where it might be optimizing the purchase and maintenance of assets the organization might look to the average cost of assets, the depreciation, maintenance and service costs, numbers of assets in operation vs repair, and how many and of what type are the assets most prone to failure or misuse. With better data, better decisions can be made to optimize the whole process, or step by step improve processes that demand the most urgent attention.

7. Check yourself - learn to love audits

No organization likes a third party audit, but where self-audits are adhered to the organization can be confident that they are always on top of the game - whether that is for software licensing authorities, regulators, or even law enforcement should something untoward happen and the organization need to cooperate. Being able to comply at speed/under stress is a real gift to aid the business in delivering what it needs to prosper, despite whatever else is happening, employing TAM technology that provides constant monitoring and change (delta) reporting by automating the audit process.

8. Stick to the system - it won't let you down

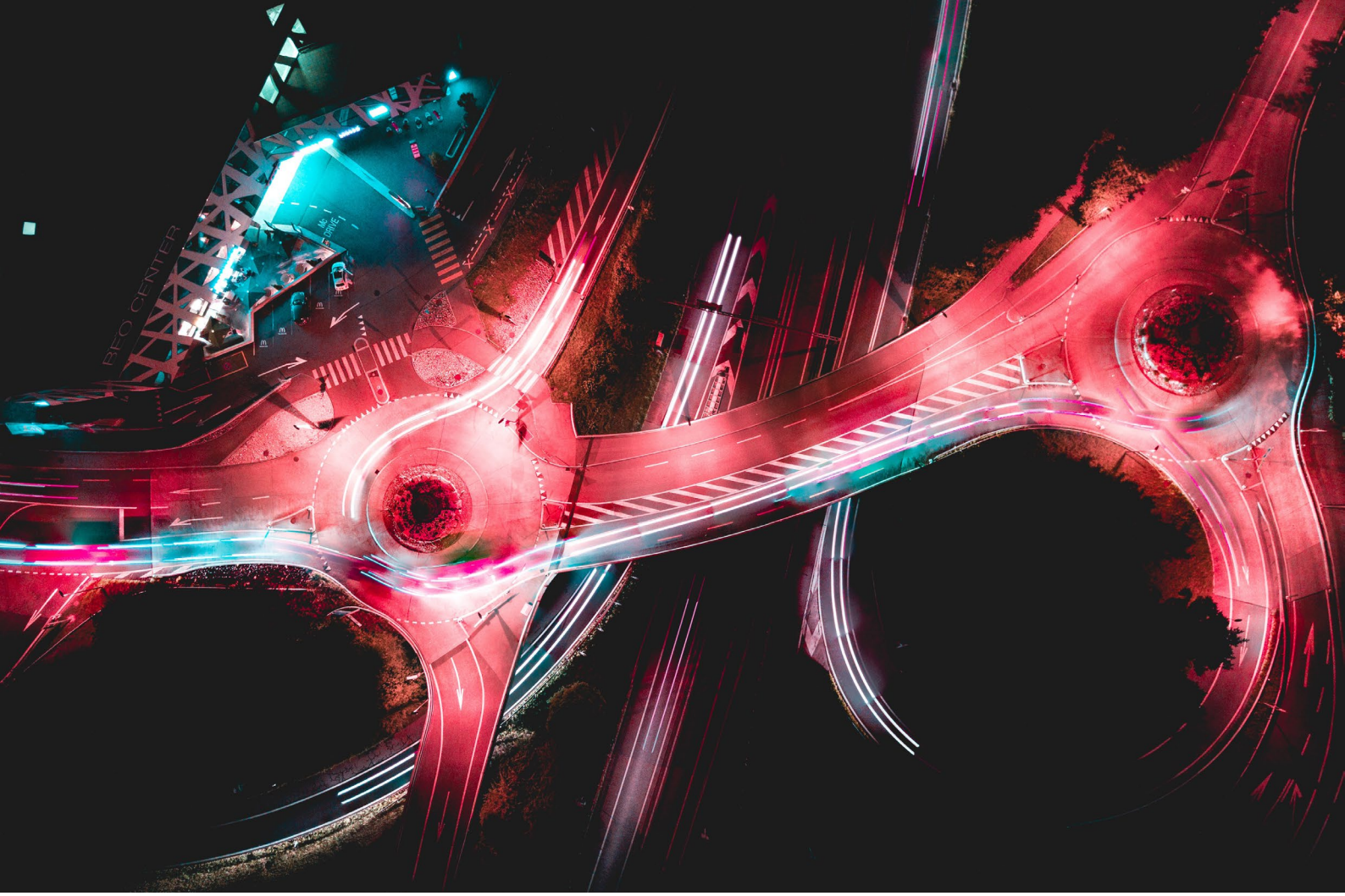
Ensure that the organization keeps to its set systems for improving technology asset management practices. Don't neglect the human component. Many organizations, especially large enterprises, often get into a poor state of technology asset awareness and understanding because talent moves away and new managers don't have historic or organizational knowledge. Slowly the management of the situation changes and people, processes, and assets become invisibly misaligned. Keep the team thinking, talking, documenting, and recording how and why they do what they do.

9. Stay up to date with new developments

New technologies may disrupt the established way the organization conducts business. New regulations may impact how data is stored, or how assets like smartphones and other mobile devices may be managed in and outside of the organization. New practices from industry authorities may replace existing methods or metrics. Staying on top of these external forces is vital to maintain a responsive technology asset mix and ensure the organization is either keeping pace or excelling in its operation.

10. Always be optimizing

The technology environment sometimes changes slowly, but seismically. With the right processes and support in place from partners, vendors, the C-suite, the users and IT management, then the organization can stay on top of change, of risk, and new opportunities as well. It's important to get in the mind-set of business optimization, always looking for new ways to ensure the business delivers on its strategy and seeking to optimize how technology delivers on those strategies.



AFTERWORD

About the research

The research was commissioned by Nlyte Software and delivered in January 2019. The 1,516 respondents were technology asset decision-makers in organizations employing 1,000 people or more. As such it represents a slice of the US, UK, and French enterprise landscape and should be analogous with how technology asset management is conceived, conducted, and consumed by enterprises across the globe. The interviews were conducted online by Sapio Research using an email invitation and an online survey.

About Sapio

Sapio is a full-service market research consultancy that helps brands and agencies produce high quality insight to inform business strategy and drive content generation.

Contact Sapio at sapioresearch.com or on +44 (0) 207 2361 604

About Nlyte Software

Since 2004 Nlyte has been committed to helping organizations optimize the management of their IT infrastructure. Nlyte automates the discovery, workflow management, and reporting across the entire technology stack, physical, virtual, and edge, including software and IoT devices. Nlyte reduces costs and risk while improving efficiency and transparency for the entire organization.

Some of the world's most sophisticated IT organizations use Nlyte's comprehensive out-of-the-box software solutions. Nlyte's commitment to optimizing computing infrastructure, making it easier for people to do their job more efficiently and improve agility across the global organization, continues to develop a loyal following represented by a 98% retention of customers. For more information, visit nlyte.com or follow @nlyte on Twitter.

Nlyte Software

SAPIO RESEARCH