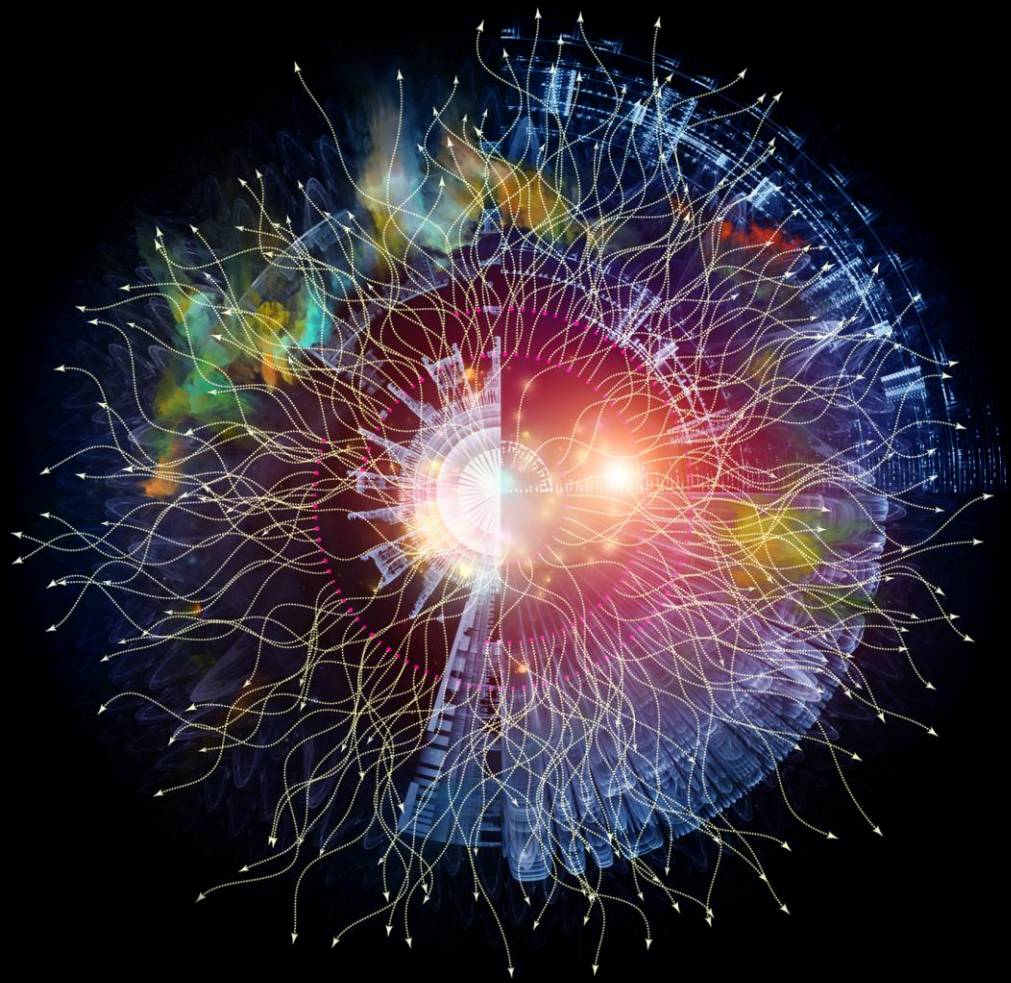
Deloitte.



IT Asset Management (ITAM)

Global Survey 2022-23

Bridging the gap between aspiration and capability

MAKING AN IMPACT THAT MATTERS since 1845

Foreword

I am pleased to share with you the results of our second global survey on IT Asset Management (ITAM).

In 2021, our first survey looked at the current state of ITAM in organizations. It showcased how they need to change their focus and investment priorities in governing IT assets to reflect the changing technology landscape, and more specifically, newer ways of licensing hardware and software.

This landscape has continued to evolve, perhaps even faster than we had ever imagined, amid increased uncertainty and complexity in the business and macro-economic environment. This, in turn, has further elevated the demands and aspirations from ITAM and software asset management (ITAM) teams from a widening range of stakeholders in most organizations that participated in the current survey.

The objective, as earlier, has been to align better to strategic opportunities that would help maximize value from IT investments, this time with a much stronger desire for advancement and getting tangible results.

"Despite this enhanced ambition to get more out of ITAM, most organizations represented in this survey acknowledged their failure to establish an appropriate level of capability supported by a framework and operating model to manage IT assets that remains fit-for-purpose in this rapidly changing environment."

A more powerful and empowered ITAM team is required, one that can use their expertise to develop a holistic response to these growing demands. These aspirations include, for instance, addressing the many implications of embracing multiple facets of the cloud in multi-cloud environments, supporting IT security teams more efficiently and effectively as required in the current disruptive environment – all this in a sustainable and responsible manner as typically required by organizational sustainability initiatives. It is however heartening to note that help continues to remain at hand as external assistance for ITAM also continues to evolve to ensure efficiency and culture of cross-functional collaboration, mirrored by the rise of a FinOps culture in organizations.

Key findings

ITAM maturity and inability to develop fit-for-purpose operating models

Despite growing desire and maturity, most organizations acknowledge their failure to establish an appropriate level of capability and a fit-for-purpose ITAM framework and operating model amid a complex and rapidly changing business, regulatory and technological environment.

Multiple facets of the cloud

Rapid adoption and evolution of multiple facets of the cloud is increasingly impacting various aspects of ITAM with only some organizations starting to respond with help from their employees. Data security continues to remain a major area of concern, primarily due to challenges in ensuring shared responsibility between the cloud service provider and the user organization.

Cyber security alignment

The lack of cyber security alignment is now considered the greatest concern for ITAM. Respondents believe that lack of visibility of IT assets and weaknesses within existing ITAM tools possibly represents the greatest limitation that organizations face in achieving better alignment with their IT security teams.

Green IT and other sustainability considerations

Many ITAM teams acknowledge lack of attention to the “invisible materiality” of information technology in organizational sustainability initiatives.

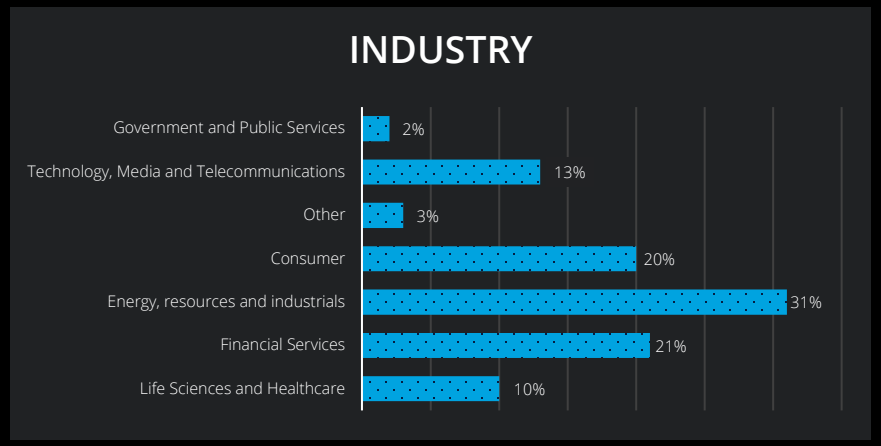
External assistance and FinOps

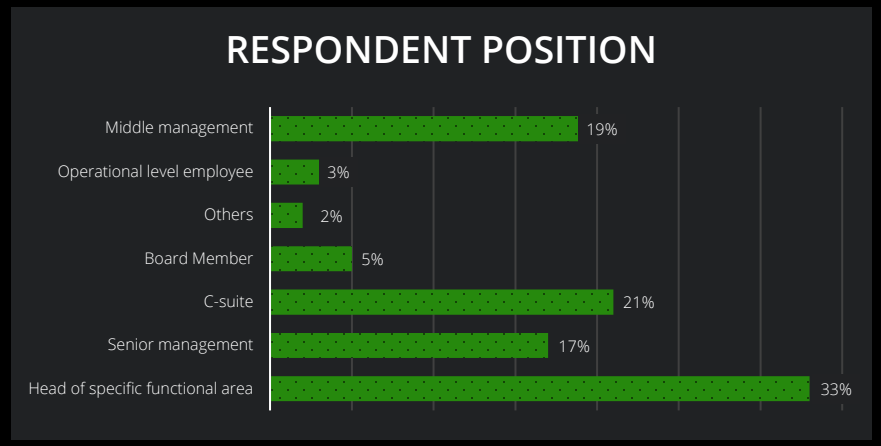
Delivery of managed services and other forms of external assistance in ITAM are rapidly evolving to ensure efficiency and culture of collaboration, mirrored by the rise of a FinOps culture in organizations.

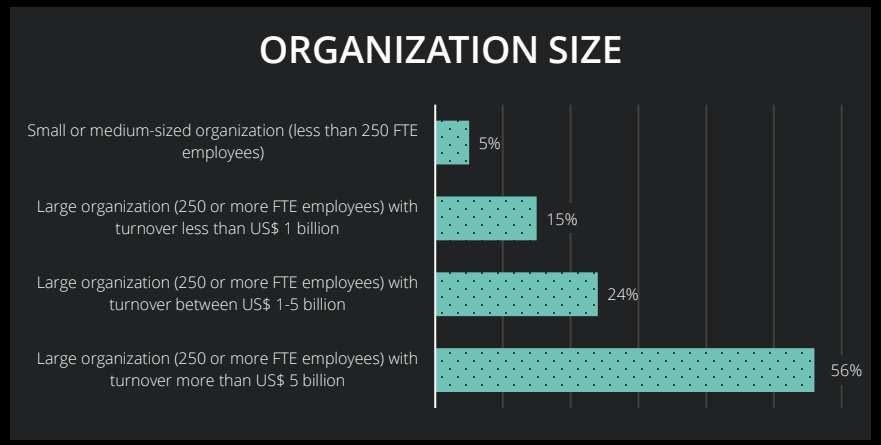
Key findings

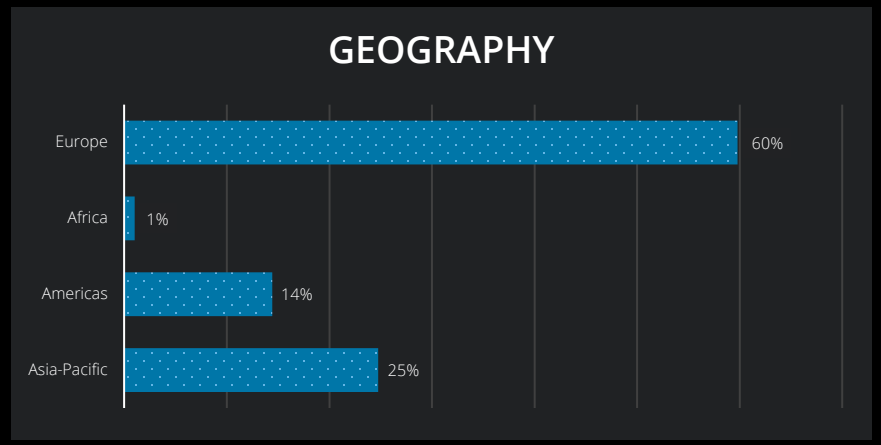
We invited over 3500 participants in over 20 countries to participate in this survey, covering all major industry sectors. These individuals either led or played a key role in relation to ITAM initiatives in smaller and larger organizations (figure – 1).

Figure 1: Demographic profile of respondents









Key findings

I hope you enjoy reading this report as you explore the various opportunities in ITAM that lie ahead. As always, I would welcome your feedback on what trends you're seeing in the marketplace—or if you would like us to benchmark anything different in future reports.

Our ITAM and ITAM professionals across the globe can help you understand how this survey's findings reveal distinctive opportunities for your organization. To learn more, please contact your local expert.

Diederik Van Der Sijpe

Lead Partner

IT & Software Asset Management

01

ITAM maturity and inability to develop fit-for-purpose operating models

Key findings

ITAM maturity and inability to develop fit-for-purpose operating models

Despite growing desire and maturity, most organizations acknowledge their failure to establish an appropriate level of capability and a fit-for-purpose ITAM framework/ operating model amid a complex and rapidly changing business, regulatory and technological environment.

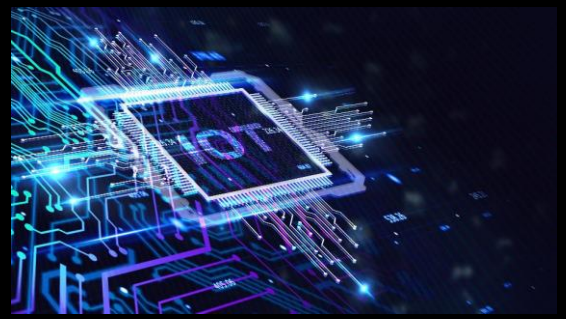
The need to invest in the strategic transformation of ITAM has become increasingly urgent.

Our previous ITAM survey report had predicted that more progressive and astute organizations will increasingly recognize ITAM as a long-term strategic investment that creates ongoing value across the entire organization going far beyond just their IT team. This would be in sharp contrast to the more traditional and tactical mindset aimed merely to invest as little as possible to minimize or rationalize the ownership and operating costs of IT assets (i.e., just managing licensing risk).

As indicated in our previous report, there is no doubt that ongoing transformation (enabled by continued investment) in ITAM is increasingly becoming unavoidable due to the rapidly evolving technology landscape amid shifting paradigms in the business environment. *For example, the struggle to simply have full visibility of all the technology-related elements in today's technology-enabled digital enterprises has significantly challenged ITAM mechanisms in* ***more than eight out of ten organizations.*** *Such technology-related elements include hardware and software components, whether deployed in-house, on-premise, or off-premises on the cloud or in any other way*.

Yet there is hope around ITAM being able to drive efficiency and cost-effectiveness going forward.

We had also anticipated that new technologies, including the cloud and Internet of Things (IoT), would reinforce the emphasis on cost optimization as the primary driver for such organizational investments with a continuous focus on risk reduction and resilience related to IT assets.



Key findings

ITAM maturity and inability to develop fit-for-purpose operating models

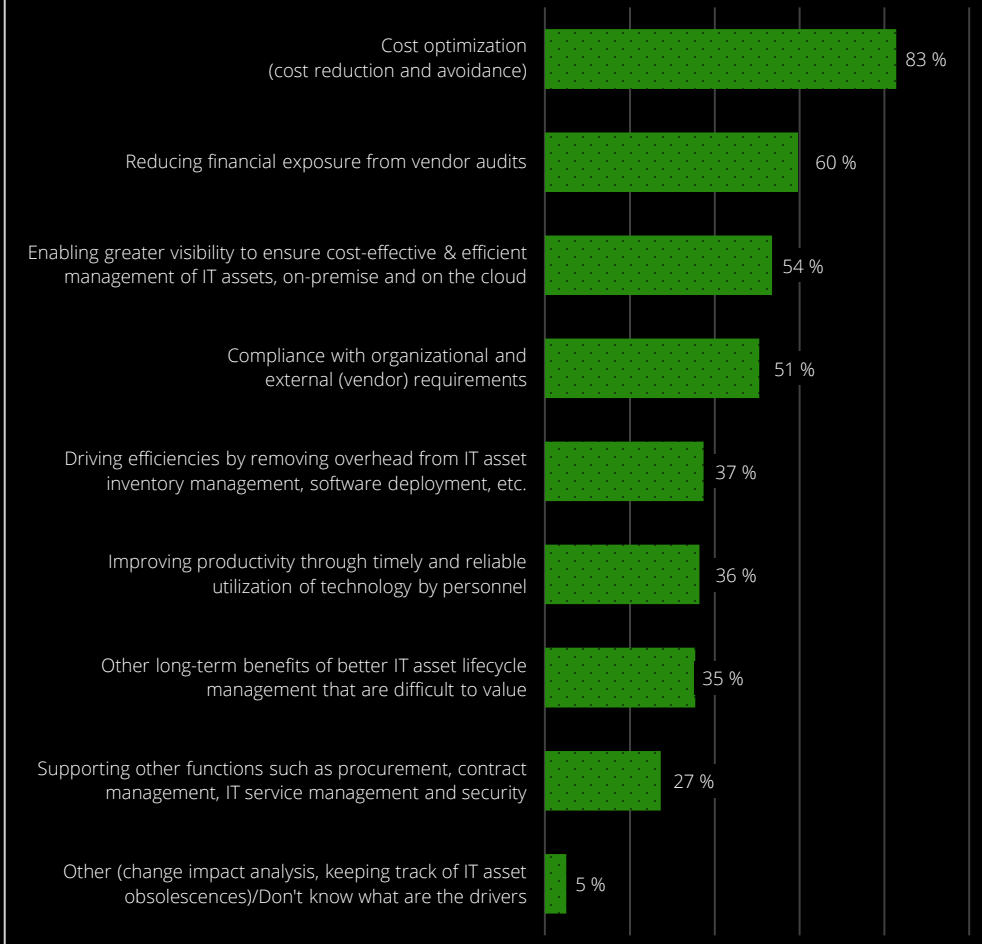
Data from our current survey data validates this prediction (figure – 2).

83% of our 2022 respondents rate cost optimization (both reduction and avoidance) as the strongest driver for investment in ITAM initiatives, up from 74% last year.

At the same time, reducing exposure from vendor audits (particularly in those organizations that have ignored the need for ITAM transformation) is a significantly higher concern that is worrying six out of ten respondents this year, up from 47% last year. We expect this will stimulate the focus and investment on ITAM.

More than half the respondents are specifically concerned about the lack of visibility of IT assets in their organizations. These respondents recognize that end-to-end IT visibility is not only required for proper mapping of IT assets and related dependencies in their organizations. Such visibility can also provide meaningful insights to other functions such as procurement and cyber-risk management to increase their effectiveness using ITAM data.

Figure 2: Drivers for investment in ITAM

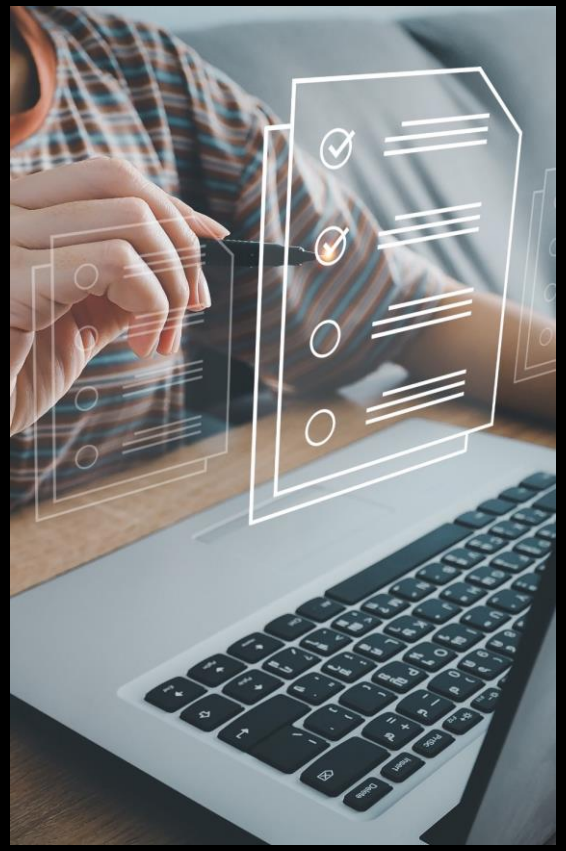


Key findings

ITAM maturity and inability to develop fit-for-purpose operating models

Bridging the capability gap to emerge as a strategic function

Our current survey enabled us to drill-down into the capability of these organizations in managing specific aspects of ITAM risks (figure -3).



Capability development in ITAM teams since our last survey appears to have continued to focus on the **core licensing component**. It is heartening to note that 84% of respondents believe that their current ITAM program allows them to **appropriately focus on and manage licensing risks, with a broader approach and perspective** (in contrast to just worrying about getting through their next vendor audit).

However, the proportion of respondents who believe their current ITAM program allows them to focus on **other areas that create strategic value for their organizations**, such as software spend optimization or IT security risks drops sharply to 53% and 30% respectively, implying their constraints to create ongoing value across the entire business, going far beyond just their IT teams, although some of them are clearly starting to get there.

This is in a context where 81% of respondents this year continue to believe that the **rapidly changing business, regulatory and technological environment is making it more challenging to enhance ITAM maturity**. This is also giving rise to the need for higher degrees of collaboration and cross-working within the organization with a widening of team capability beyond core licensing.

Key findings

ITAM maturity and inability to develop fit-for-purpose operating models

These data points indicate that the aspiration to evolve as a long-term mechanism for strategic investment extending beyond IT is still a distant dream for many.
Yet there is no doubt that some progress has been made.

Nearly three-quarters of respondents (71%) believe that dependency mapping has a significant role in their ITAM strategy. They believe that their ITAM team having an overview of which configuration items are supporting business applications and what happens if one of them fails is critical. We see this as a reaffirmation of strategic intent to gain better control over IT assets.

Sadly, only 53% of respondents have consistent business processes related to ITAM that are continually refined. It is here that we begin to see the gap between aspiration and capability.

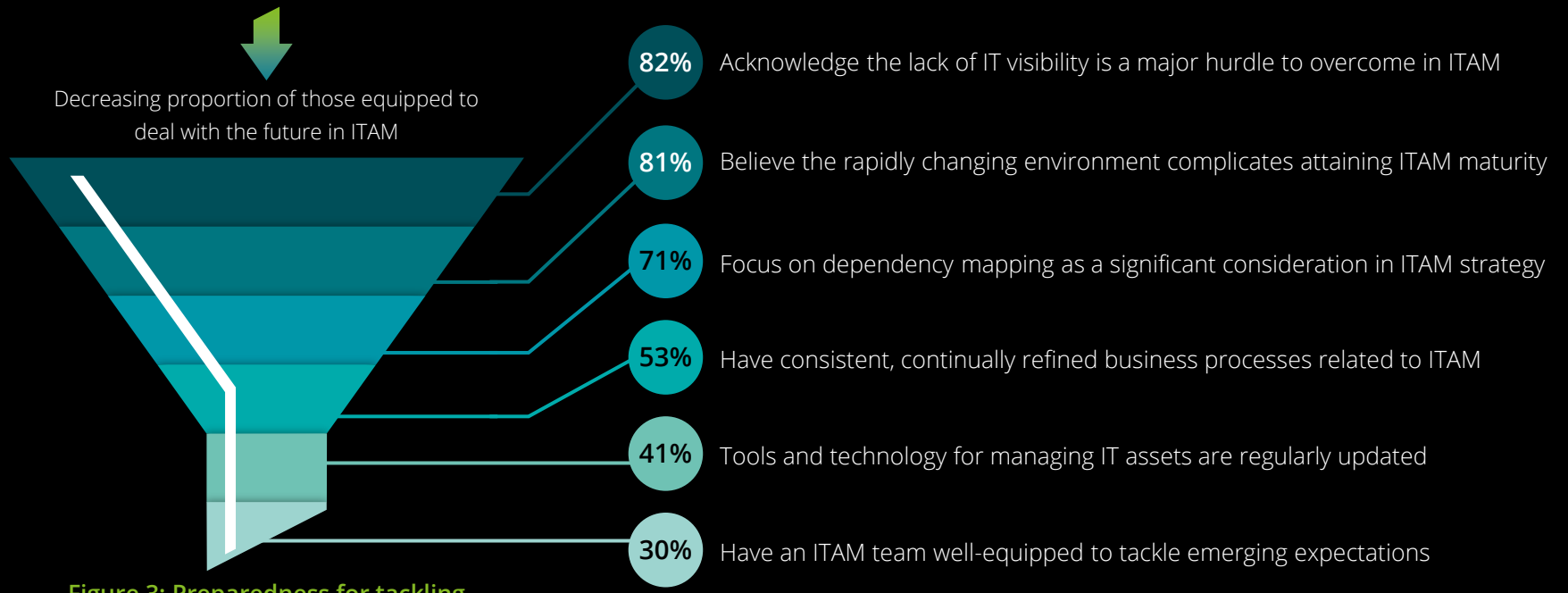


Figure 3: Preparedness for tackling emerging ITAM expectations

Key findings

ITAM maturity and inability to develop fit-for-purpose operating models

IT continues to be at the heart of ITAM initiatives but with growing co-ownership of budgets

The growing technical complexity of emerging and evolving solutions and architectures is still keeping IT departments at the heart of ITAM initiatives with IT departments owning ITAM budgets in three-quarters of organizations, a proportion that is unchanged from last year.

However, it is encouraging to note the spirit of growing involvement of procurement and finance.

This year's survey data shows that 17% of procurement teams have started owning budgets of organization-wide in ITAM initiatives, up from only 8% last year.

Similarly, an encouraging 27% of finance teams in participating organizations owned or co-owned ITAM budgets, also up from only 7% last year.

Another bit of good news is that the proportion of respondents who believe that increasing value from ITAM is being derived from teams other than IT is increasing. This reconfirms that the organizational journey to evolution is moving in the right direction.

This year, 18% of respondents believed that the maximum value from ITAM initiatives is being derived by IT security teams, a sharp increase from 7% last year.

Similarly, the proportion of organizations where the most value derived by finance and procurement teams has also increased from 7% and 8% respectively last year to 12% and 13% in the current year.

But despite this increase, only 30% believe that their ITAM teams are well-equipped to deal with emerging expectations including closer involvement/collaboration with business on topics such as cyber-security, amid the growing dominance of cloud-based IT infrastructure and applications, hybrid working propositions, environmental, social and governance (ESG) matters.

Key findings

ITAM maturity and inability to develop fit-for-purpose operating models

Enabling cross-functional teams drive enforcement is emerging as a common area of focus

Despite the relative lack of capability in areas outside of the core licensing risk management, the top priority areas of action (figure – 4) seem to cluster around working with cross-functional teams within organizations, assisting them in more value-added ways. These include:

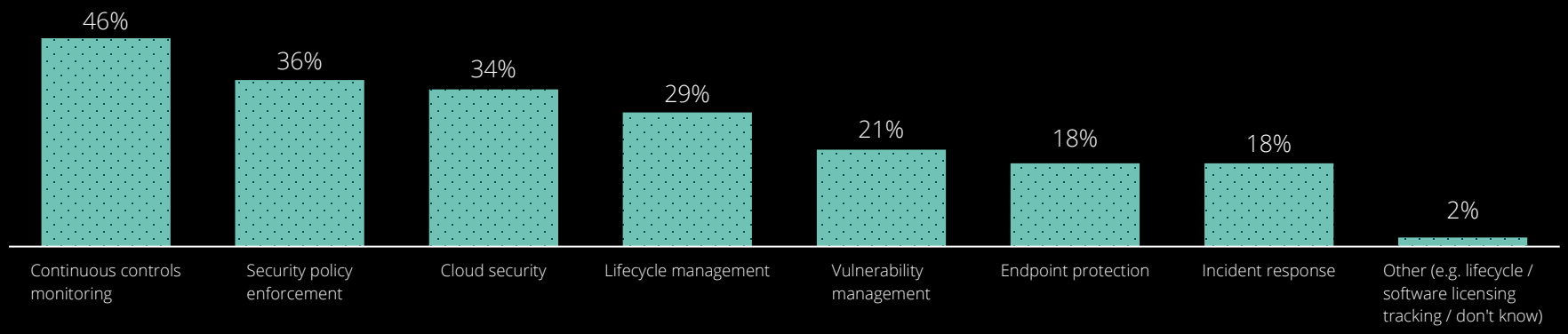
Introducing continuous controls monitoring automatically identifying assets that stops adhering to the organizational security policies (46%)

Security policy enforcement: helping in automatically addressing IT assets that don't adhere to organizational security policies (36%)

Cloud security: helping find cloud instances not being scanned for vulnerabilities, those that are misconfigured, or not adhering to industry benchmarks like CIS Foundations Benchmarks (34%)

Lifecycle management: helping manage IT assets through the entire lifecycle from forecasting and pre-acquisition analysis to disposal including decommissioning, recycling etc. (29%).

Figure 4: Priority areas of focus for ITAM



Key findings

ITAM maturity and inability to develop fit-for-purpose operating models

Supplementing the enforcement of organizational or industry standards, the ability to cover all phases of the IT asset lifecycle indicated above is also expected to become an important consideration.

ITAM teams have traditionally been focused primarily on procurement, deployment and appropriate usage of IT assets and ongoing IT asset discovery and license compliance monitoring.

However, in the transformational journey ahead, managing issues related to IT asset decommissioning/recycling (e.g., privacy, license optimization, etc.) is going to be a top area of focus, particularly given the growing sustainability and environment focus of ITAM teams of the future. Additionally, ITAM could make a significant contribution to processes related to IT asset forecasting and pre-acquisition analysis.

Deloitte's point of view and predictions

Understanding and overcoming the reluctance to invest in transforming ITAM

Overcoming the reluctance to invest in ITAM transformation initiatives requires the reasons for such reluctance to be understood in the first place before they can be addressed. Our research and analysis revealed that ITAM processes in many of these organizations surveyed had typically been designed to mitigate basic software licensing risks by IT teams with the least possible investment.

While this may have been a sensible approach at that time, most of these organizations were slow or reluctant to shift gears when their business and IT environments drastically changed.

An excessive focus on cost-cutting has no doubt further aggravated the problem over the last few years, redirecting investment away from ITAM, ignoring the instrumental role that ITAM itself can potentially make in an IT cost reduction play. This has also often been combined with an "optimism bias" where business leaders have lacked sufficient foresight about potential losses they could face, for instance, through IT asset-related incidents including financial/reputation loss through security exposures, lack of clarity around shared responsibilities in multi-cloud settings or even through lack of due focus on sustainability in IT as a key component of organizational ESG initiatives.

We predict that ITAM will increasingly be a critical competitive differentiator for those organizations where members of executive leadership are ultimately accountable for driving ITAM transformation initiatives (with active oversight by the Board).

Such organizations recognize that transformed ITAM can deliver tangible benefits only by involving an increasing number of "business side" stakeholders including key functional teams such as finance, procurement, risk management, security, cloud teams etc. as well as the business units themselves which utilize the various organizational IT elements. With this stakeholder group getting bigger and more complex, the ITAM team of the future should comprise of a group of smart specialists who can tie everything together in a more collaborative setting, where a critical source of competitive advantage arises from technology as well as insights shared by others. Stakeholders' buy-in can be harnessed in newer and cleverer ways, leveraging sweet spots such as the ability to provide full visibility of the IT estate across all types of technology deployment.

Like all other organizational transformation projects, ITAM transformation will also require project management input to create and track the ITAM transformation roadmap, following up and coordinating with involving everyone in this expanded group of stakeholders.

02

Multiple facets of the cloud

Key findings

Multiple facets of the cloud

Rapid adoption and evolution of multiple facets of the cloud is increasingly impacting multiple aspects of ITAM with only some organizations starting to respond with help from their employees. Data security continues to remain a major area of concern, primarily due to challenges in ensuring shared responsibility between the cloud service provider and the user organization.

Most of our survey respondents rightly believe that rapid adoption of cloud technologies is directly related to driving business transformation in their organizations. However, the assumptions that are often made in relation to lowering Total Cost of Ownership (TCO) of organizational IT assets are not always correct. This is primarily because an exponential increase in adoption of cloud technologies in context of a growing business will no doubt increase TCO. However, a strong cloud cost management function (see also discussion in section 5 on FinOps) can manage, optimize and effectively reduce the incremental cost with predictability and control.

Findings from our current survey echo this perspective. Reducing and controlling such incremental IT cost is the top reason for embracing multiple facets of cloud technologies; yet this can be achieved only if organizations develop stronger ITAM teams (with larger and more realistic budgets) to manage rising costs and address other drivers of investment related to higher cloud-technology adoption across multiple facets, modes of deployment and nature of application.

Key findings
Multiple facets of the cloud

Figure – 5 reiterates growth in multiple facets of cloud adoption in respondent organizations.

Overall, a hybrid approach will be dominant moving forward.

The vast majority of participants in this survey (87%) envision a hybrid IT environment in their organization with both on-premise systems and off-premises cloud/hosted resources in an integrated fashion.

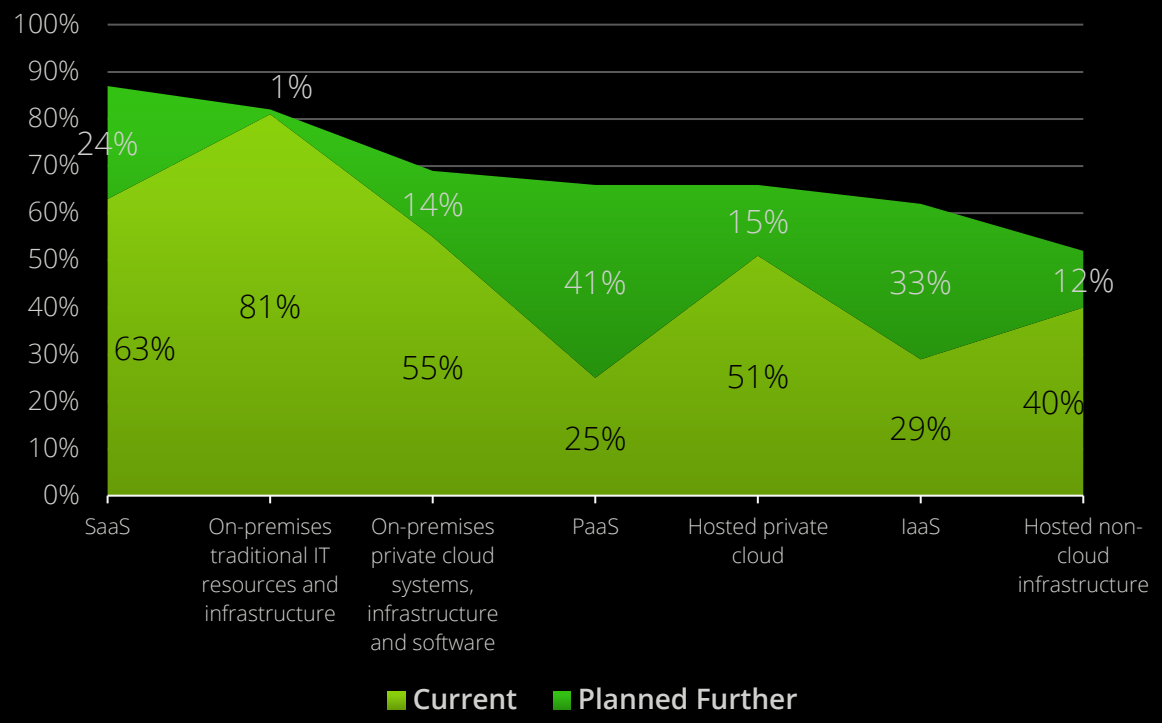
While this will significantly enhance dependencies on the cloud, yet some element of on-premise systems are here to stay. Only a small minority (8%) however envisage moving to a completely off-premises IT environment.

SaaS is and will be the most popular mode of cloud deployment for the foreseeable future.

While 81% of respondents reported that they have some form of on-premise (traditional) IT resource and infrastructure, the use of SaaS has so far been the most popular form of cloud usage that has so far been adopted by respondents (63%).This is followed by the adoption of other on-premise private cloud systems, infrastructure, and software (55%) and hosted private cloud (51%), that are managed more by cloud project teams rather than ITAM/ITAM teams. PaaS and IaaS are still at relatively lower levels of adoption, at 25% and 29% of respondents, respectively.

Despite the related concentration risk, as many as 56% of respondent organizations are opting to remain with a single critical (i.e., primary) cloud provider, with closer monitoring, instead of gearing their cloud strategy towards a multi-cloud environment. This 31%, representing the minority, are working with a larger number of vendors to address concentration risks arising from sole-supplier dependency levels. The remaining 13% are not yet sure about their stance as yet.

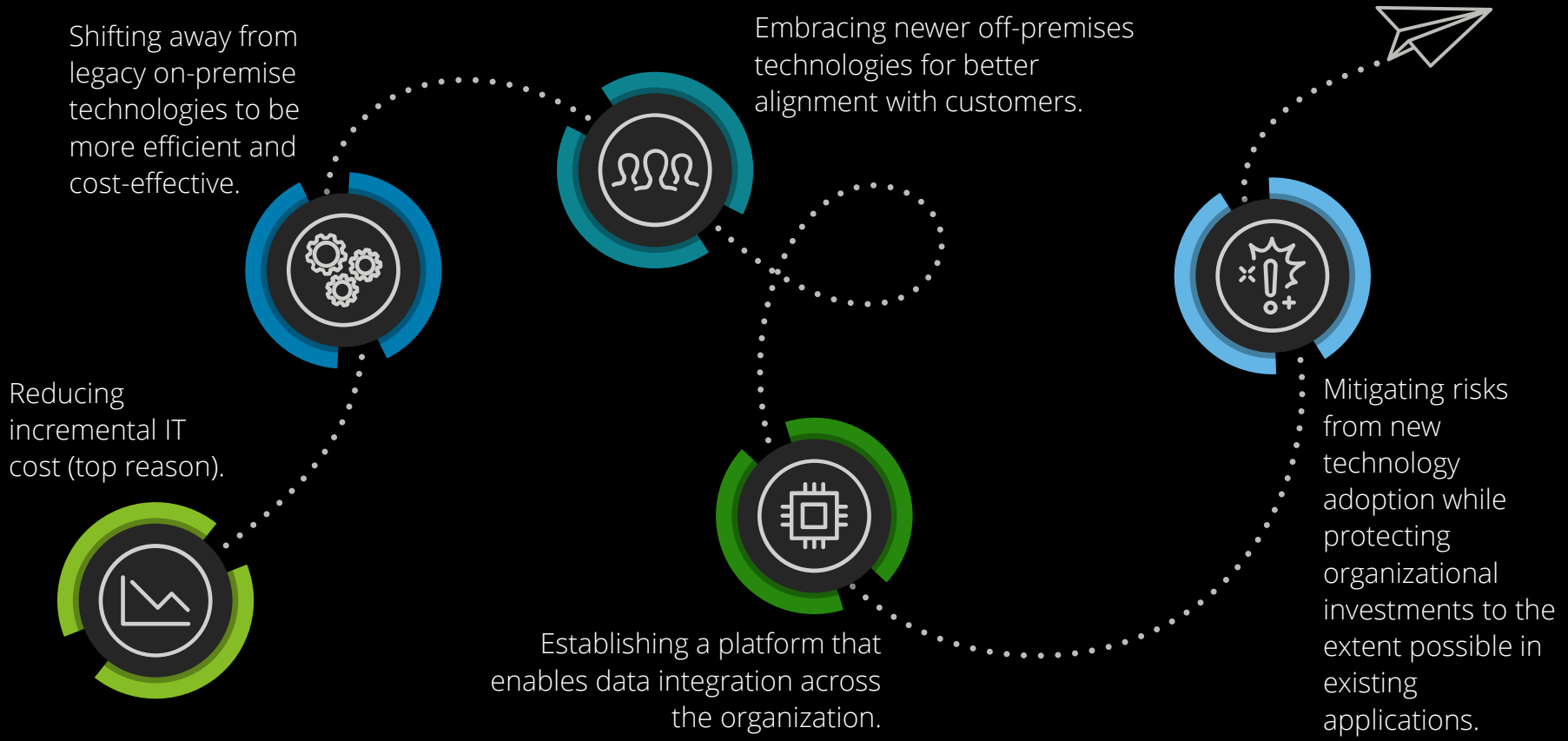
Figure 5: Modes of IT deployment – current and planned



Key findings

Multiple facets of the cloud

The survey captured the top five reasons for a high rate of cloud adoption across the respondents of this survey (figure – 6).



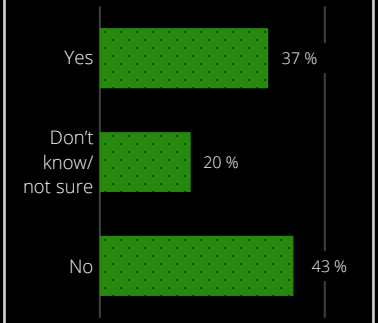
Key findings

Multiple facets of the cloud

It should be noted that these primarily reflect the technology perspective (mainly from IT teams) that drive operational discussions. However, we are starting to see a much bigger influence on cloud adoption as a result of business-driven decisions from executive leadership which IT has to execute without the capability to keep up with the expected speed or quality of transformation.

01 Reducing IT cost

FinOps setup will become key in reducing cloud cost, optimizing cloud consumption and forecasting cloud cost.



02 Shifting away from legacy on-premise technologies to be more efficient and cost-effective

03 Embracing newer off-premises technologies for better alignment with our customers

04 Establish a platform that enables data integration across the organization

05 Mitigating the risks arising from adopting new technologies too fast

Key findings
Multiple facets of the cloud

The need to strengthen ITAM teams and related processes can no longer be ignored

As discussed above, it is important to note that cloud costs are also rapidly increasing with greater adoption of cloud-technology adoption as a significant game-changer for organizations. It is therefore easy to forecast that cloud costs will only go up further with business growth. The more astute organizations are therefore already starting to implement business processes that enable them to understand the constituents of this increasing cloud cost, optimize cloud consumption and even forecast this increasing cloud cost.

This, in turn, will require ITAM teams to be strengthened further to be able to work more collaboratively with growing stakeholder teams described in the earlier chapter of this report, not just to help manage the rising cloud costs, but to also facilitate the achievement of other objectives such as gaining efficiencies from off-premises technologies, facilitating data integration by helping these stakeholders (including FinOps teams and providers of external assistance – see chapter 5) understand what is where in the extended IT estate and mitigating emerging risks (including but also going broader than IT and cyber security) as new technologies are adopted. Similarly, the growing dominance of SaaS solutions is expected to widen the capability gap in ITAM for those organizations that are ill-equipped to discover, manage, report, or optimize the expanding SaaS component in their IT applications and infrastructure.

Growing adoption of multiple facets of the cloud increases hidden compliance risks

Since the start of the pandemic, organizational strategies have largely been driven by business teams. Some of these decisions have been taken very quickly in a rapidly evolving working landscape. Other stakeholders from teams such as risk management and compliance (e.g., Data Protection Officer) have been left to follow behind, playing catch-up on a post-facto basis.

In a similar vein, our client experience indicates that the responsibility for cloud adoption has typically been managed by internal business teams and IT, with the help of specialist cloud project managers who also report to the business. This implies that significant digital transformation is taking place without the specialist support of specialist risk or compliance teams including ITAM input, albeit for limited considerations such as ensuring end-to-end technical visibility, particularly in hybrid or multi-cloud environments).

Key findings
Multiple facets of the cloud

Our survey data mirrors this concern. For instance:

Data security (for instance due to the inability to ensure shared responsibility between the cloud service provider and the user organization) presents itself as the highest area of concern in 36% of respondents.

This is followed by the risk of non-compliance related to data privacy and other similar legislation/regulation (31% of respondents).

In response to the above threats, organizations are taking a number of measures (figure – 7) which include:

01 Educating and collaborating with employees more regularly around software used by them (59%)

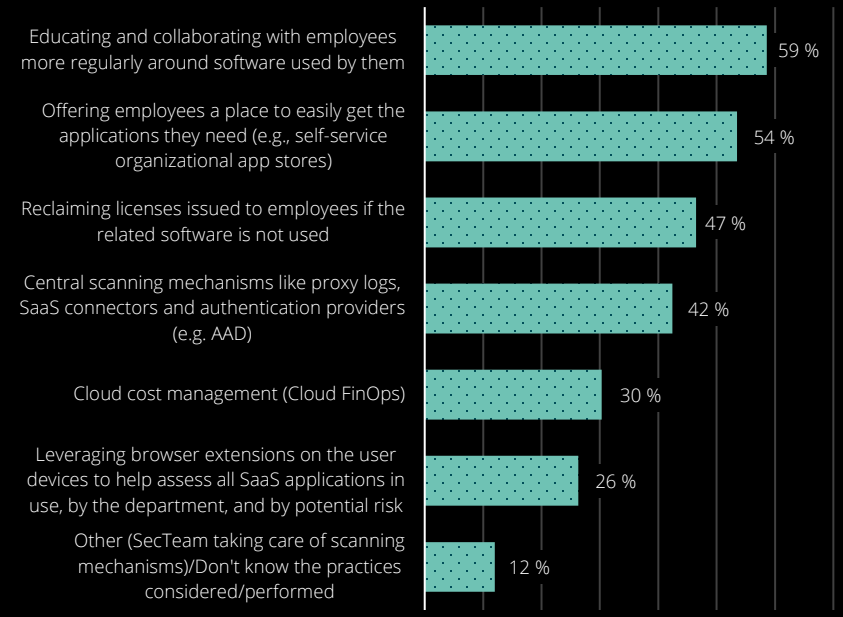
02 Offering employees a place to easily get the applications they need (e.g., self-service organizational app stores) (54%)

03 Reclaiming licenses issued to employees if the related software is not used (47%)

04 Using central scanning mechanisms like proxy logs, SaaS connectors and authentication providers (e.g., AAD) (42%).

Figure 7: Practices considered/ performed to mitigate cloud-related risks

Practices to mitigate cloud-related risks



Deloitte point of view and predictions

Deloitte ITAM specialists anticipate that hybrid IT will increasingly become the de facto standard for deploying enterprise IT resources, on-premise as well as off-premises by effectively combining in-house and externally-sourced technology resources in a holistic and integrated manner. This will enable organizations to transform and evolve with greater agility arising from the ability it provides in the following areas.

Seamless execution of applications and workload migration across platforms (including multi-cloud infrastructure arising from PaaS, IaaS etc.)

Consistent application development lifecycles that stretch across diverse environments.

Presents the potential for OPEX-based IT capacity expansion.

Creates the opportunity for multi-location backup facilities and recovery efforts.

It also enables seamless across disparate environments.

However, to reap these benefits, the primary challenge is being able to manage the complexity that these heterogeneous IT environments, often across multiple providers create for these organizations in what has been described as the "messy real world" of the future.

But this is also precisely where next-generation IT Asset Management can make a significant difference by catalyzing the implementation of that much-desired integrated and holistic approach across the entire IT estate (see also discussion on FinOps in section 5). It can do so by providing visibility over the technology landscape with dashboards and reporting to optimize costs at different organizational levels, reduce spending, manage performance, risk and compliance, and help accelerate digital transformation initiatives through governance and process orchestration – as a **true strategic business advisor at least in the more progressive organizations.**

03

Cyber security alignment

Key findings
Cyber security alignment

The lack of cyber security alignment is now considered the greatest concern for ITAM. Respondents believe that lack of visibility of IT assets and weaknesses within existing ITAM tools possibly represents the greatest limitation that organizations face in achieving better alignment with their IT security teams.

ITAM teams need to enable full visibility of IT elements and be more closely aligned or integrated with those responsible for IT governance and security.

Evolving IT security standards as well as broader cyber security standards have now explicitly started to highlight the need to understand the IT assets, however procured, hosted, or operated, that form their IT estate. And, with most organizations now embracing multiple facets of the cloud, the call for **full visibility** of the various technology elements has become even more critical. This is because the cyber-security chain is only as strong as the weakest link. It is only by finding the hardware, software, and firmware that this weakest link can be addressed to ensure a secure environment.

Further, this is the time when the IBM Cost of a Data Breach Report 2022 indicates that the cost of a data breach averaged US$ 4.35 million in 2022. This figure represents a 2.6% increase from last year, when the average cost of a breach was US$ 4.24 million. The average cost has climbed 12.7% from US$ 3.86 million in the 2020 report[1].

Our client experience reconfirms that proper visibility across multiple technologies and modes of deployment makes vulnerability management and incident response processes more efficient and effective by enabling quicker response, faster patching etc.

It is therefore reassuring to see the growing realization across our survey respondents that IT security and ITAM need to be closely interconnected with ITAM teams helping enable full visibility of IT assets.

As a matter of fact, more than three quarters of respondents, (77%), believe that their ITAM team is foundational to an effective cyber security strategy.

However, in contrast to this increasing realization, in practice only 54% of ITAM teams participating in this survey indicate that they are aligned to their cybersecurity teams, helping them detect and identify vulnerabilities and incidents within their organizational IT estate.

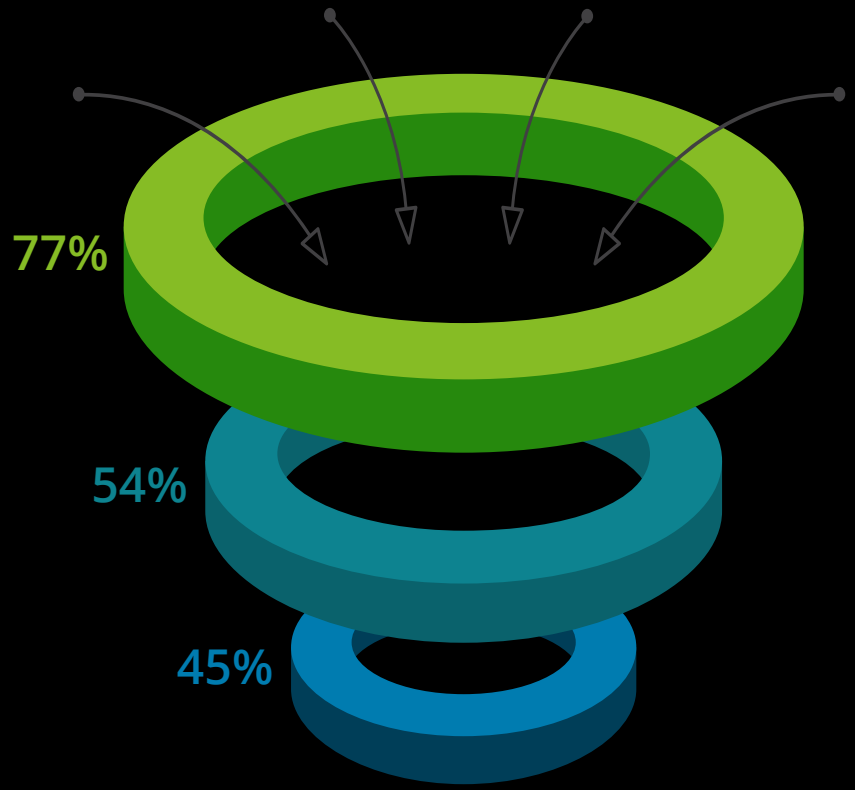
[1]See https://www.ibm.com/downloads/cas/3R8N1DZJ

Key findings

Cyber security alignment

And more shockingly, only 45% of respondents believe they are making the appropriate investments that ensure that their ITAM function enhance IT asset visibility for their security analysts (figure – 8).

Figure 8: Practices considered/ performed to mitigate cloud-related risks



01 We believe that our ITAM is foundational to an effective cybersecurity strategy

02 Our ITAM team is aligned to our cybersecurity team in helping them detect and identify IT assets in our organizational IT estate

03 We are making appropriate investments to ensure that our ITAM function would enhance IT asset visibility for security analysis

Key findings

Cyber security alignment

Limited functionality of current ITAM tools is inhibiting closer alignment on IT security.

Deloitte ITAM specialists believe that most of the inputs required to manage IT and cyber security should be a part of the standard functionality for a good ITAM tool. Given the current setting of a post-pandemic world, it should also increasingly focus on proactive rather than reactive controls, including:

Key findings

Cyber security alignment

Unfortunately, the current survey also reveals that this is not always the case.

The lack of capabilities within existing ITAM tools possibly represents the greatest limitation that organizations face in achieving better alignment with their IT security teams.

The deficiency is highest in tools and functionality that enable unauthorized asset recovery (i.e., requiring continuous monitoring, and tracking of IT assets) in as many as 72% of participating organizations in the survey.

The other limitations with regard to existing ITAM tools that should be aligned to IT security include the lack of software installation restriction controls (expressed by 56% of respondents) and permitted hardware and software controls (identified by 54% of participating organizations) (figure – 9).

This in turn increases the need for infusing the missing functionality and cross-integrating tools to develop the missing capabilities. organizations can also consider adopting a specialist IT security asset tool portfolio with its own specific focus e.g., on vulnerability scanning and asset discovery. The key to success here will be the need to have both the ITAM and the cyber tools enrich each other.

The process flow will however need to be re-architected as follows

1. Asset discovery info for visibility
2. Cyber intelligence for vulnerability detection, and
3. Link to patch management to fix the issue.

Key findings

Cyber security alignment

But while there is more to do, progress made so far in this area needs to be acknowledged. Our survey data shows that organizations seem to have gained competence with regard to IT and cybersecurity in three specific areas in the following order:

Incident response

As many as 63% of them appear to be using enriched coordinated data on IT assets from different data sources to help expedite incident, response, investigations, and remediation.

End-point protection

60% believe they are good at ensuring end point protection which involves detecting assets missing an end point agent or identifying those that do not have the right agent installed, or where the agent is not working.

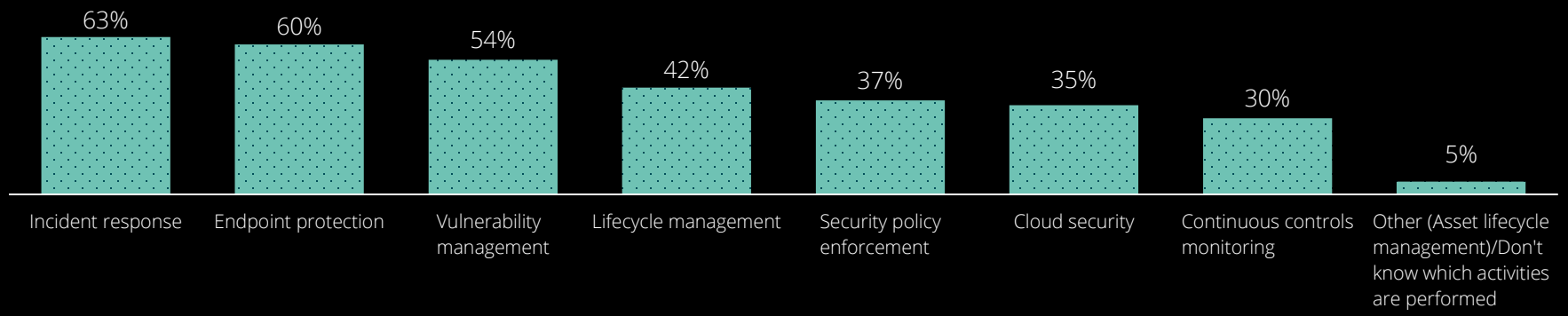
Vulnerability management

Uncovering assets not being scanned by a vulnerability assessment tool (54%).

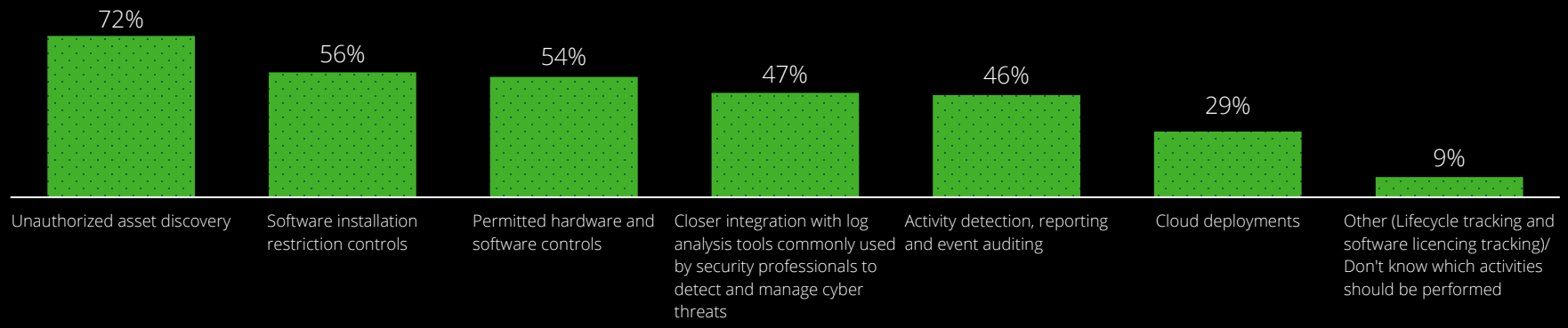
Key findings

Cyber security alignment

Figure 9: ITAM tool capabilities and aspirations



Additional capabilities required



In case of all these three areas, some progress has been made here, but there is more to be done to enhance the efficiency and effectiveness of IT security initiatives enabled by ITAM.

Deloitte point of view and predictions

The USA's National Institute of Standards and Technology (NIST) published a Cyber Security Guide for ITAM back in 2018-19, co-authored with the National Cyber Security Center of Excellence (NCCoE). This guide provides an insight into specific areas that those charged with cyber and IT governance can expect a best-in-class ITAM system to provide, using large financial institutions as an illustrative example. It therefore outlines a future for ITAM where such teams are much more closely aligned with organizational IT security teams, equipping them with a stronger mandate that can help them deliver even more value for the organization.

Other significant legislative/regulatory developments include the DORA (Digital Operational Resilience Act) that is currently relevant for financial services companies in the EU or organizations dealing with them. This act is focused on resilience (security and operational) with cyber security as a critical element underpinning the legislation which covers IT asset risk management, reporting, testing, and more. It will expand the regulatory perimeter for the relevant regulators once the final EU law is ready for implementation. For this too, a strong focus on IT Asset Management focus is needed. 'Knowing what you have' to apply the requirements to the full IT Asset Lifecycle will be key. Although it is focused on financial services organizations, it will be relevant for all other organizations across all industry segments that deal with them as well to acknowledge the need more generally for strong asset management, given its close link with cyber security.

The recent White House initiative to improve the security of open-source software and identify ways in which new collaboration could rapidly drive improvements is also expected to accelerate faster alignment between IT security, ITAM and other organizational teams.

One of the key challenges identified in this report is the lack of centralized control of IT asset deployment and the increasing variety of devices and software deployed. This mirrors our actual client experience as do the potential areas of assistance from ITAM from an IT security perspective that organizations can use as to steer their journey towards better integration and alignment:

- Discovery of device location, configuration, and ownership.
- Prioritization of critical infrastructure (by identifying the most significant assets).
- Enabling compliance with Sarbanes-Oxley (SoX) and with standards such as PCI-DSS.
- Monitoring and managing inventory as against the entitlement of hardware and software assets.
- Patching to ensure vulnerabilities have been fixed, thereby reducing the attack surface of IT assets.
- Helpdesk response improvement (by enabling helpdesk staff already know what is installed and the latest pertinent errors and alerts).

There is no doubt that mapping IT assets to services is a tedious and time-consuming process that requires input from ITAM and specialized dependency mapping tools but also needs a thorough understanding of scope and purpose that such an exercise will serve. Our client experience indicates that many such initiatives lose the synergies by focusing on some of the constituent activities rather than the overall intent, hence a top-down approach is key to ongoing success.

04

Green IT and other sustainability considerations

Key findings

Green IT and other sustainability considerations

Many ITAM teams acknowledge lack of attention to the "invisible materiality" of information technology in organizational sustainability initiatives.

Green and sustainable IT represents a growing area of focus and priority for ITAM and IT procurement teams.

"Green IT" aims to minimize the negative impact of technology operations on the environment by designing, manufacturing, operating, and disposing of computers and other technology-related equipment and components in an environment-friendly manner. Once again, the visibility and understanding that ITAM teams typically have in respect of hardware, software and other IT elements naturally puts such teams in an advantageous position to help drive such initiatives.

Yet, in our experience, many organizations still fail to see how material or significant the environmental impact of IT used by them is. In the words of three researchers from Washington State University, "it's difficult to see the ecological impact of IT when its benefits are so blindingly bright", calling this the "invisible" materiality of IT[2].

Although the role of ITAM with regard to sustainability initiatives around IT is still evolving, it is encouraging to see from our survey data that some organizations are starting to take the initial steps in this journey (figure – 10):

- The vast majority (76%) of respondents to this survey agree that the adoption of Green IT and other sustainability considerations represents a growing organizational priority for ITAM and other IT procurement teams.
- To this end, the majority of organizations that participated in our survey (57%) buy hardware, software, and other IT components from companies with sustainable practices to minimize any potential harm to the environment.
- 47% of organizations dispose of IT assets with help from a specialist – particularly independent parties who tend to score highly for reuse or avoiding landfill.

However, the survey indicates that there is room for improvement in certain other areas that can potentially have a significant impact on IT sustainability initiatives and targets:

- Only 36% of respondents buy low-power devices and support proactive power management for all IT assets.
- Similarly, only 32% buy user-repairable devices that come with long warranties and support after the last sale.
- Only 30% have established initiatives that reduce the energy footprint of their data center and set clear goals to measure progress in this area.
- Only 23% return IT assets back to the manufacturer through reverse logistics compared to the time of acquisition.

[2]BORNING, A., FRIEDMAN, B. and LOGLER, N. (2020) 'The "Invisible" Materiality of Information Technology: It's difficult to see the ecological impact of IT when its benefits are so blindingly bright', Communications of the ACM, 63(6), pp. 57–64. doi:10.1145/3360647.

Key findings

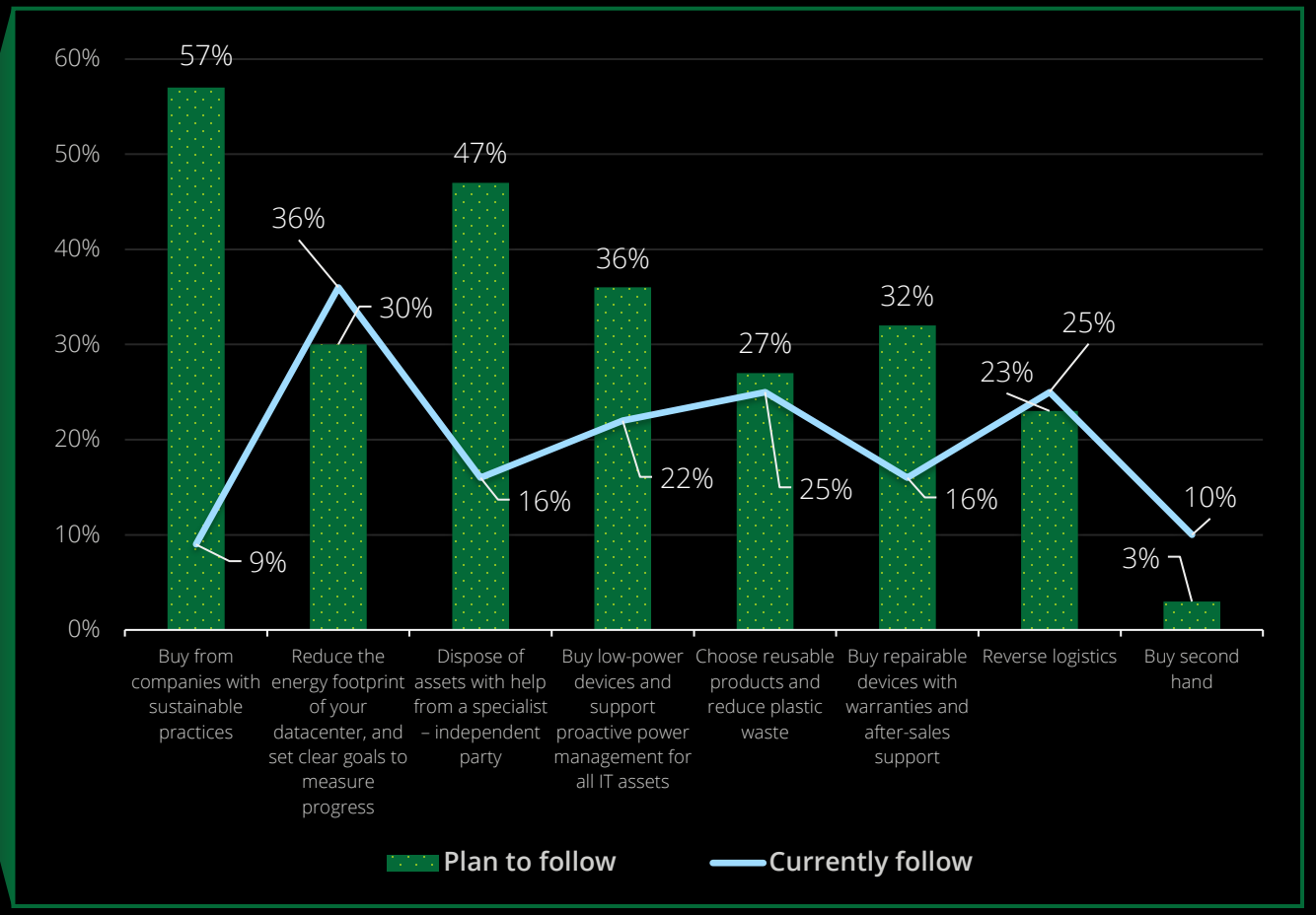
Green IT and other sustainability considerations

76
Yes

10
Don't know/not sure

14
No

Figure 10: ITAM and sustainability practices



Deloitte point of view and predictions

The appreciation and discussion of the role that ITAM teams can potentially play in addressing issues related to sustainable IT is only starting to evolve. At present, mandatory reporting of ESG is restricted to specific territories such as the UK and is likely to be implemented shortly across the EU and in the US. At this stage, there is still no specific need for the mandatory involvement of IT teams. Therefore, before we can expect further involvement of ITAM teams, organizations first need to fully recognize:

- The ways in which their use of information technology impinges on the physical world.
- The **materiality** of that impact while extracting, processing, maintaining, and ultimately disposing of the materials used to support IT, producing the energy used both by the devices in operation, as well as in their production and disposal in a more comprehensive manner.

The materiality consideration is key to this discussion. Such considerations can sometimes go beyond just the environmental or moral factors (or even a "green" contract with a technology provider focused on electricity usage) to include tangible business benefits by incorporating this materiality perspective into ongoing technical research. For example, a topic of current research centers around developing algorithms that allow for trade-offs between energy use and technical accuracy or adding support to high-level programming languages for making these trade-offs.

Technical architecting of IT solutions can, for instance, be revisited by consulting ITAM teams, leveraging their knowledge and visibility on the related IT elements. Similarly, coding can be improved so that it requires a more optimized level of IT resources. Other evolving practices that can be explored with ITAM teams could include:

- Raising awareness of the eco-design best practices among product owners, architects, and lead developers
- Anticipating the impact of user paths on resource consumption
- Establishing eco-friendly architecture standards
- Prioritizing eco-friendly solutions, technologies, frameworks, and languages when selecting software
- Retiring unnecessary features and applications
- Concretely measuring resource consumption and its evolution throughout the life cycle of all relevant technology elements.

However, as the thinking on these lines develop further, it must be kept in mind that ITAM is only a part of the puzzle and will clearly not hold all the answers.

It is widely believed that cloud computing has already been a boon for sustainability by consolidating technology operations in shared facilities. In addition, some of the major cloud providers are making the extra effort to make their own cloud platforms more environmentally friendly. As a result, organizations must select a cloud provider who is more environmentally conscious. Such an evaluation could include considering the provider's carbon-neutrality commitments, extent of renewable energy use, energy-efficiency in data centers, sustainable building design and environmentally sensitive data destruction processes.

05

External assistance and FinOps

Key findings
External assistance and FinOps

Delivery of managed services and other forms of external assistance in ITAM are rapidly evolving to ensure efficiency and collaboration, mirrored by the rise of a FinOps culture in organizations.

The proportion of organizations that are engaging specialist third party advisors to supplement internal capability has increased significantly since our last survey.

Our ongoing conversations with clients and experience from engagements indicate that the more successful ITAM operating models increasingly rely on external assistance from trusted advisors. This is not just true for ITAM transformation, but also for certain aspects of day-to-day execution of Third-Party Risk Management activities. Especially those that represent the main pain points for the organization and often the greatest opportunities for improvement (from streamlining workflow processes to governance of end-to-end software lifecycle management, optimizing vendor contract terms and conditions and KPI reporting as examples). This is increasingly making managed services solutions a critical catalyst for data-driven, agile, and cost-effective ITAM on an end-to-end basis.

This conclusion concurs with our past research which has shown that organizations are more commonly complementing their in-house ITAM capabilities by leveraging external assistance in key areas as opposed to doing everything themselves, possibly as this provides quicker access to readily trained workers and specialist technology faster and more efficiently.

Key findings

External assistance and FinOps

Our current survey data mirrors the increasing challenges that respondent organizations continue to face in their ability to readily hire skilled ITAM talent from the marketplace (Figure – 11):

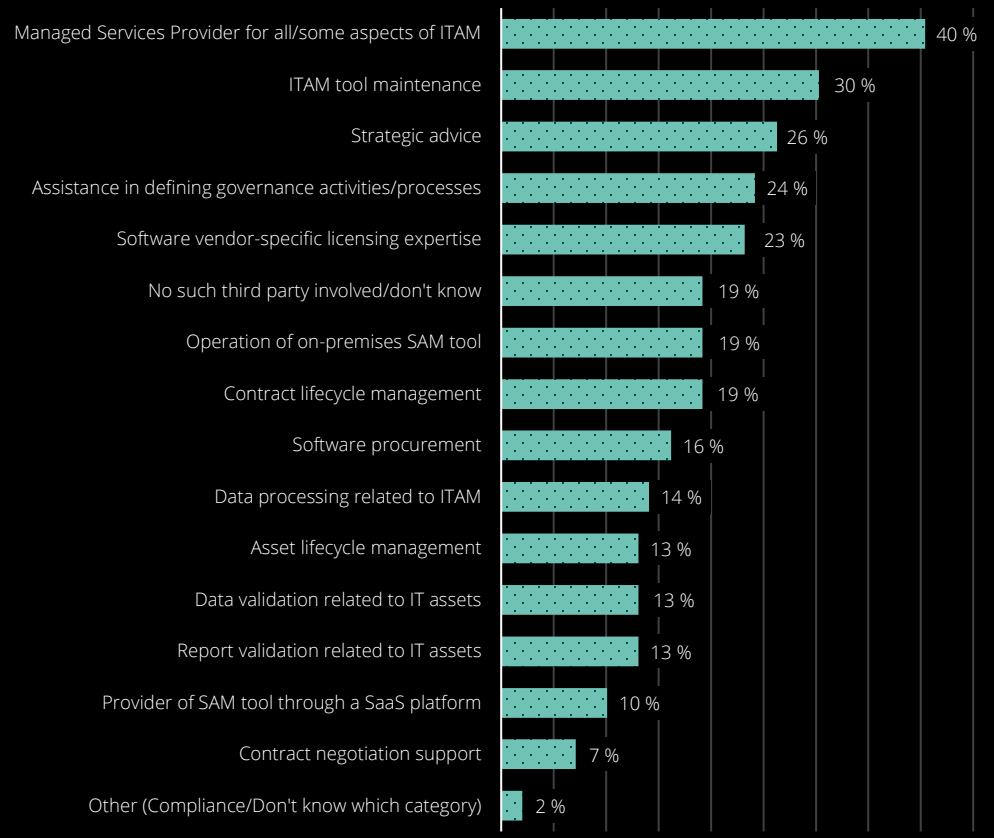
01 More than 81% of respondents (up from around two-thirds last year) are taking the assistance of third-party business advisers, consultants, or managed services providers.

02 ITAM managed services solutions, in particular, continues to be a high-growth area for respondents with as many as 40% (up from around one in five) working with a managed services provider that could cover all or specific aspects of ITAM.

03 This is followed by outsourcing of specific ITAM processes (30%), getting other forms of strategic advice (26%) and assistance in developing governance activities or processes (24%).

04 23% of respondents also leverage software vendor-specific licensing expertise to gain control over ITAM

Figure 11: Nature of external assistance for ITAM



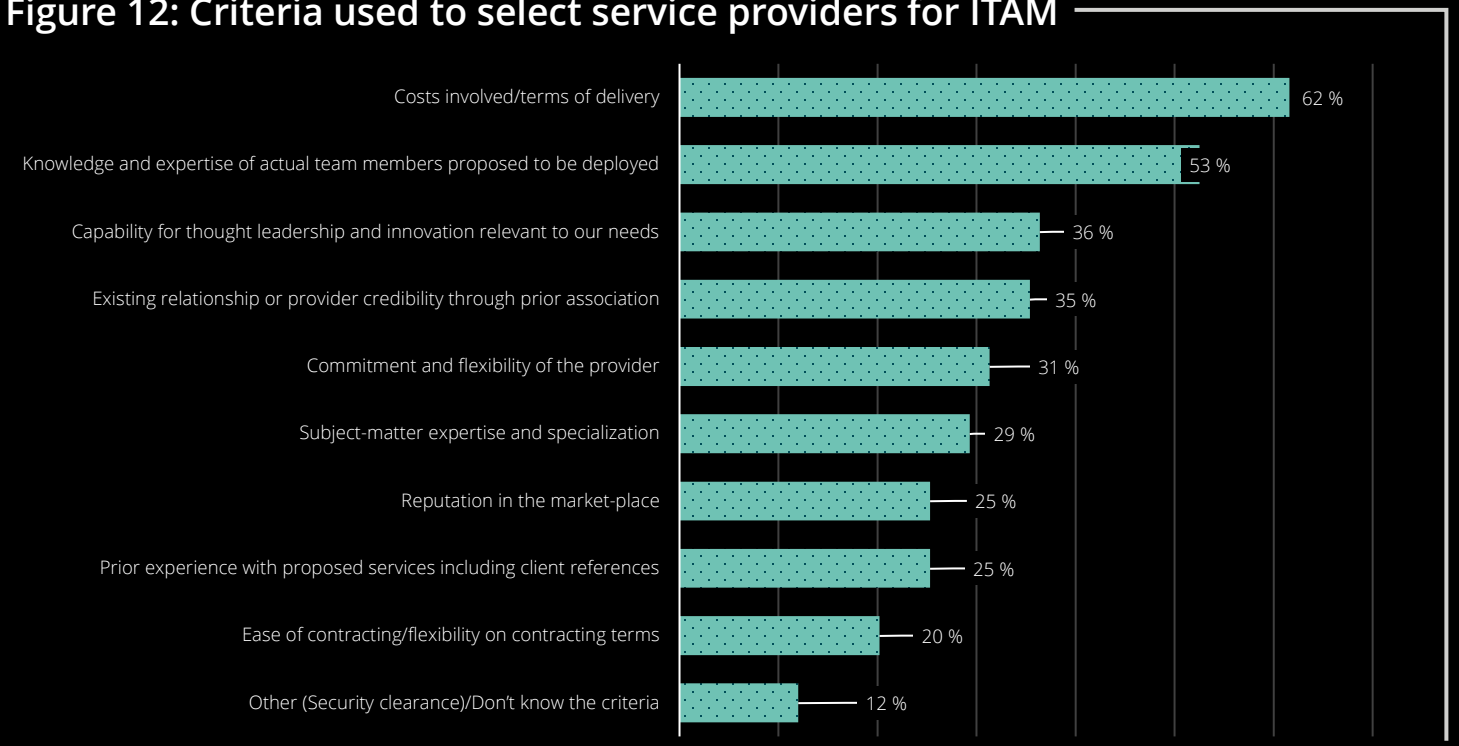
Key findings

External assistance and FinOps

The criteria for engaging specialist third party managed service providers and strategic advisors are also changing with the criticality and expectations from the evolving roles.

While the cost of involving such a management consultant is often the most important criteria used by an organization to select such a third-party business advisor, consultant or managed services provider for ITAM (62% of organizations), other criteria considered important here are the knowledge and expertise of actual team members proposed to be deployed (53%) as well as the potential provider's capability for thought leadership and innovation relevant to their needs in more than one out of three respondents (figure – 12).

Figure 12: Criteria used to select service providers for ITAM



Key findings

External assistance and FinOps

While it is true that building talent and technology capabilities inhouse can sometimes provide cost advantages, the problem is that it can also limit speed and agility—including the ability to rapidly respond to regulatory shifts and address emerging skill, resource, and/or ecosystem needs.

The common challenges of developing inhouse talent and technology capabilities include

New opportunities and/or disruptive technologies are not well understood

Slower adjustments to shifts in market trends and regulatory requirements

Staff are focused on legacy technology and their skills are often out of date

Existing approaches are not service-oriented or adaptive to business

Service delivery is slow and unresponsive

With those challenges in mind, our survey participants believe that managed service solutions from the more established external providers can enable organizations to take advantage of disruptive solutions, such as cloud technologies, robotics process automation (RPA) and artificial intelligence (AI), that are challenging traditional approaches. When executed well this can deliver competitive advantage by transforming the way an organization operates.

Key findings

External assistance and FinOps

Improved coordination between FinOps approaches in organizations and their ITAM teams

Currently, there is a global shortage of skilled ITAM resources. This phenomenon, coupled with the increasing adoption of management services, is likely to lead to better performance, improved speed to market, and increased innovation.

This comes at a time when nearly four out of ten (38%) of organizations have also adopted a FinOps approach to ITAM. They aspire to connect all relevant functional disciplines in their organization, including finance and operations in managing the cloud.

The recently established FinOps Foundation (late 2020) acknowledges this in their definition of "FinOps":

"FinOps is an evolving cloud financial management discipline and cultural practice that enables organizations to get maximum business value by helping engineering, finance, technology and business teams to collaborate on data-driven spending decisions."

Data collection, normalization, reporting, cost analysis, utilization, unit metrics, all are complicated by the sheer volume and complexity of the data coming in from cloud providers in different formats and with different taxonomies. Therefore, where cloud usage is concerned, these FinOps practitioners deal with many of the same challenges ITAM teams do, reinforcing the business case to align FinOps and ITAM as part of the same team or in a much more coordinated way than ever before.

To mirror this coordinated FinOps approach, some managed service providers now offer a centralized data and reporting repository that integrates with existing client systems. This integrated repository of IT asset and licensing data is also typically used to run various reports and populate executive dashboards on a near-real time basis.

Deloitte point of view and predictions

Our research thus clearly indicates that Third-party risk management processes are being revolutionized by disruptive shifts in the market. organizations must think, organize, and work differently to respond to highly integrated market disruptors. But with these challenges comes the opportunity to benefit from real-time decision-making and leverage diverse yet interconnected analytical insights. An attractive proposition for organizations that aim to continually enhance their competitive advantage. This is clearly where an end-to-end ITAM managed services solutions that bundle expertise with emerging automation technology can fit in as an attractive proposition for organizations that aim to continually enhance their competitive advantage.

To be able to leverage these opportunities, we predict that the more complex organizations will continue to prefer global providers of ITAM managed services solutions. These providers bring the skills, experiences with license optimization technologies, and with own proprietary tools to help organizations realize software optimization, cost savings, and improve operational efficiency even in the more traditional focus areas such as audit cost avoidance or software license optimization in addition to the evolving expectations around the rise of cloud technologies and a stronger imperative for collaboration on cyber security and green/sustainable IT.

This is particularly relevant in an environment where shifts to more dynamic business models demand more flexible organizational structures and a reduction in long term investments involving Capital Expenditure (CAPEX). As a result, organizations are rapidly replacing traditional fixed term, fixed scope partnerships (often associated with sunk costs) with more flexible consumption and unit-or volume-based constructs that managed services platforms can provide.

06

Key takeaways

Key findings

ITAM maturity and inability to develop fit-for-purpose operating models

Despite growing desire and maturity, most organizations acknowledge their failure to establish an appropriate level of capability and a fit-for-purpose ITAM framework and operating model amid a complex and rapidly changing business, regulatory and technological environment.

Multiple facets of the cloud

Rapid adoption and evolution of multiple facets of the cloud is increasingly impacting various aspects of ITAM with only some organizations starting to respond with help from their employees. Data security continues to remain a major area of concern, primarily due to challenges in ensuring shared responsibility between the cloud service provider and the user organization.

Cyber security alignment

The lack of cyber security alignment is now considered the greatest concern for ITAM. Respondents believe that lack of visibility of IT assets and weaknesses within existing ITAM tools possibly represents the greatest limitation that organizations face in achieving better alignment with their IT security teams.

Green IT and other sustainability considerations

Many ITAM teams acknowledge lack of attention to the “invisible materiality” of information technology in organizational sustainability initiatives.

External assistance and FinOps

Delivery of managed services and other forms of external assistance in ITAM are rapidly evolving to ensure efficiency and culture of collaboration, mirrored by the rise of a FinOps culture in organizations.

07

Profile of the authors

Profile of the authors

Diederik Van Der Sijpe
Partner

Diederik is a leader for IT & Software Management in Extended Enterprise at Deloitte. Based in Belgium, Diederik works with his clients to build robust ITAM programs that provide value to their business. He looks at both process and technology solutions, assists in managing clients' contractual obligations to generate efficiencies and savings and helps out in reinforcing relationships with software publishers and IT vendors. Diederik also has significant experience leading compliance programs for large national and multinational organizations, assessing license compliance against contractual obligations.

Throughout his career he assisted in the revision of several SAM standards and best practices and contributes to the ITAM community by presenting at forums and hosting roundtables on this subject. He has experience in a variety of industry sectors including financial services, energy and resources, government and public services, technology, media and consumer.

Hans Vandewijer
Partner

Hans is a seasoned expert in software license auditing and advisory services related to various industry and business contractual relationships. He has assisted clients in identifying and recovering lost revenue, such as those resulting from contract misinterpretations and misunderstanding of product use rights.

Furthermore, Hans is advising clients on implementing a sound IT Asset Management ("ITAM") strategy and governance along with the corresponding processes and procedures leading to enhanced cost and risk management. Based on his in-depth understanding of the software vendor industry, he has supported clients through the implementation of technology to track software assets, the optimization of spend and the enablement of contractual and software license requirement analyses.

Profile of the authors

Robbert Pyfferoen
Senior Consultant

Robbert is a Senior Consultant working for the Extended Enterprise Risk Management (EERM) team of Deloitte Belgium, based in Brussels. Prior to joining Deloitte, Robbert was active in Configuration Management as well as IT License Management. Currently, he is focused on leading the delivery of ITAM solutions to our clients across the EMEA region. Robbert has a varied licensing skillset which helps our customers get the best value from every service. He has an extensive experience in managing various licensing products from a wide variety of vendors and is currently leading several Managed Service engagements in EMEA. Robbert possesses Oracle and ServiceNow certifications which he leverages to further assist our customers.

Dr Sanjoy Sen
Head of Research and Eminence Extended Enterprise Risk Management

Dr Sanjoy Sen is the head of research for third party risk management at Deloitte LLP. He has a doctorate in business administration from Aston University in the UK based on his global research on strategic governance and risk management related to the third-party ecosystem. He also holds the honorary title of visiting senior fellow in strategy and governance in the school of business and economics at Loughborough University. Since 2014, Sanjoy's work has been cited in various global academic and professional journals, newspapers and conference papers.

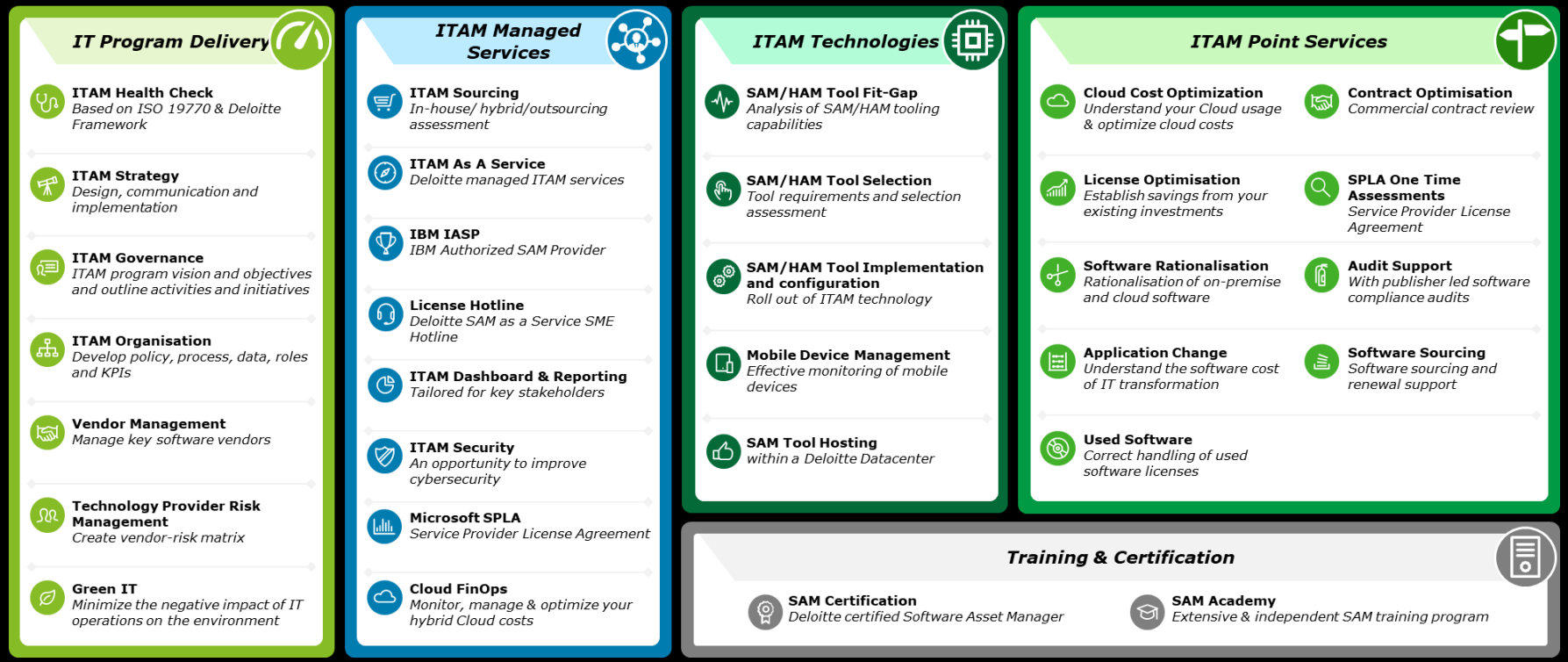
Sanjoy has extensive experience advising boards, senior leadership, heads of risk, and internal audit on strategic governance and risk management of the extended enterprise, outsourcing, and shared services. He has worked across the UK, Gibraltar, India, and various countries in the Middle East.

He is a chartered accountant (FCA), cost and management accountant, and certified information systems auditor (CISA) with over 30 years of experience, including 17 years of partner-level experience at Deloitte and another Big Four firm.

08

How we help clients

How we help clients



09

Global contacts

Global contacts

Global Leadership Team

Global leader

Kristian Park
+44 2073 034110
krpark@deloitte.co.uk

Americas leaders

Adam Thomas
+1 (773) 677-1074
adathomas@deloitte.com

Dan Kinsella
+1 (402) 997-7851
dkinsella@deloitte.com

Asia Pacific leaders

Jimmy Wu
+886 2 2725 9988
jimwu@deloitte.com.tw

Anthony Yu Kun Tai
+60 3-7610 8853
yktai@deloitte.com

EMEA leaders

Jan Corstens
+32 2 800 24 39
jcorstens@deloitte.com

Diederik Van Der Sijpe
+32 2 800 24 62
dvandersijpe@deloitte.com

Jan Minartz
+49 40 320 804915
jminartz@deloitte.de

Global contacts

Americas

Argentina
Esteban Enderle
+54 (11) 432 027
eenderle@deloitte.com

Brazil
Fabiana Mello
+55 21 3981-0927
fabianamello@deloitte.com

Canada
Roxana Greszta
+1 416-874-4335
rgreszta@deloitte.ca

Chile
Christian Duran
+56 227 298 286
chrduran@deloitte.com

LATCO
Esteban Enderle
+54 (11) 432 027
eenderle@deloitte.com

Mexico
Ricardo Bravo
+52 55 5080 6159
ribravo@deloittemx.com

United States
Dan Kinsella
+1 (402) 997-7851
dkinsella@deloitte.com

Global contacts

Asia Pacific

Australia
Rajat Saigal
+61 470 333 760
rasaigal@deloitte.com.au

China
Golden Liu
+86 10 8512-5309
goliu@deloitte.com.cn

Hong Kong
Hugh Gozzard
+852 2852 5662
huggozzard@deloitte.com.hk

India
Munjal Kamdar
+91 9820-998335
mkamdar@deloitte.com

Indonesia
Budiyanto
+62 812-8294-8888
budiyanto@deloitte.com

Japan
Niki Kazuhiko
+81 90-6020-8466
kazuhiko.niki@tohmatsu.co.jp

Japan
Bruce Kikunaga
+81 90-8347-7656
bruce.kikunaga@tohmatsu.co.jp

Korea
Min Youn Cho
+82 2-6676-1990
minycho@deloitte.com

Malaysia
Anthony Yu Kun Tai
+60 1-2378 2838
yktai@deloitte.com

New Zealand
Aloysius Teh
+64 21 544 628
ateh@deloitte.co.nz

Philippines
Anna Pabellon
+63 2-85810-9038
apabellon@deloitte.com

Taiwan
Jimmy Wu
+886 2 2725 9988
jimwu@deloitte.com.tw

Singapore
Kenneth Leong
+65 8322 5090
keleong@deloitte.com

Thailand
Weerapong Krisadawat
+66-2-0340145
wkrisadawat@deloitte.com

Vietnam
Ivan Pham
+84 287 101 4567
ivanpham@deloitte.com

Global contacts

EMEA

Austria
Alexander Ruzicka
+43 1 537 00 7950
aruzicka@deloitte.at

Belgium
Diederik Van Der Sijpe
+32 2 800 24 62
dvandersijpe@deloitte.com

Czech Republic
David Korniet
+420 7 35 70 33 52
dkorniet@deloittece.com

Denmark
Monika Silkart
+45 30 93 43 74
msilkart@deloitte.dk

Finland
Jouni Viljanen
+358 20 755 53 12
jouni.viljanen@deloitte.fi

France
Sonia Cabanis
+33 6 40 15 44 57
scabanis@deloitte.fr

Germany
Jan Minartz
+49 40 320 804915
jminartz@deloitte.de

Greece
Alithia Diakatos
+30 21 0 678 1176
adiakatos@deloitte.gr

Hungary
Zoltan Szollosi
+36 1 428 6701
zszollosi@deloitte.com

Ireland
Eileen Healy
+353 21 490 7074
ehealy@deloitte.ie

Italy
Sebastiano Brusco
+39 2 83322656
sbrusco@deloitte.it

Kuwait & Qatar
Tamer Charife
+965 9731 4314
tcharife@deloitte.com

Luxembourg
Laurent Berliner
+352 45 145 2328
lberliner@deloitte.lu

Middle East
Tariq Ajmal
+971 506 522 859
tajmal@deloitte.com

Netherlands
Birthe Van der Voort
+31 610 980186
bvandervoort@deloitte.nl

Norway
Erling Pettersen Hessvik
+47 95 90 77 90
ehessvik@deloitte.no

Poland
Bartosz Zajac
+48 694 960 069
bzajac@deloittece.com

Portugal
Joao Carlos Frade
+351 21 042 7558
jfrade@deloitte.pt

Global contacts

EMEA

Romania
Andrei Ionescu
+40 21 207 5485
aionescu@deloittece.com

Saudi Arabia
Nader Farid
+966 506 664 200
nafarid@deloitte.com

South Africa
Nombulelo Kambule
+27 11 806 5548
nkambule@deloitte.co.za

Spain
Oscar Martín Moraleda
+34 91 4432 660
omartinmoraleda@deloitte.es

Sweden
Charlotta Wikström
+46 733 971 119
cwikstroem@deloitte.se

Switzerland
Ronan Langford
+41 582 799 135
rlangford@deloitte.ch

Turkey
Cuneyt Kirlar
+90 212 366 6048
ckirlar@deloitte.com

United Arab Emirates
Ziad El Haddad
+971 552 542 548
zhaddad@deloitte.com

United Kingdom
Peter Kunorubwe
+44 2070 079530
pekunorubwe@deloitte.co.uk

Global contacts – Authors of the ITAM Survey

Diederik Van Der Sijpe
Partner, Extended Enterprise
+32 2 800 24 62
dvandersijpe@deloitte.com

Hans Vandewijer
Partner, Extended Enterprise
+32 473 95 42 52
hvandewijer@deloitte.com

Robbert Pyfferoen
Senior Consultant, Extended Enterprise
+32 473 84 51 14
rpyfferoen@deloitte.com

Dr Sanjoy Sen
Head of Research & Eminence, Extended Enterprise
+44 1216 955044
sanjsen@deloitte.co.uk

Deloitte.