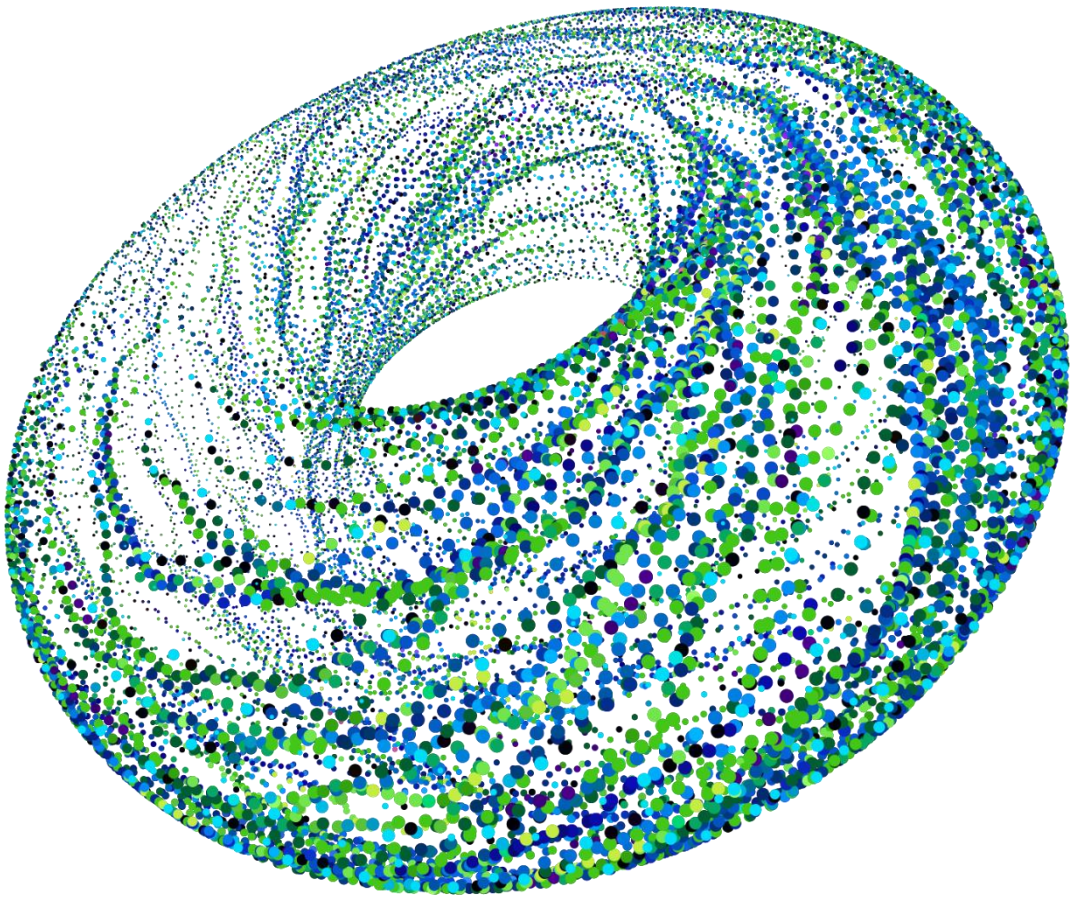
Deloitte.



The five keys to strategic ITAM in a cloud-driven, AI-powered world

Deloitte Global IT Asset Management (ITAM) Survey 2025

Introduction

Foreword

I am pleased to share with you the results of our third global survey on IT asset management (ITAM) entitled “The five keys to strategic ITAM in a cloud-driven, AI-powered world”.

Understanding the evolution and objectives of our current survey

Our two earlier surveys (launched in 2021 and 2023) had looked at the current state of ITAM in organizations at that time and 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. **Technology has never stood still, but the velocity of change now facing IT asset management (ITAM) leaders is unprecedented. With the rise of AI and Gen AI, the explosive expansion of cloud services, and digital regulations such as DORA and the EU AI Act, ITAM is no longer a quiet, back-office function. It needs to become a strategic capability which is central to how organizations manage cost, enable innovation, ensure compliance, and support resilience.**

That is precisely what inspired the title of this year’s report: “**The five keys to strategic ITAM in a cloud-driven, AI-powered world**.” The title reflects these dual forces reshaping ITAM globally. Externally, organizations are navigating greater operational complexity, rising regulatory scrutiny, and a shift to more decentralized technology ownership. Internally, many ITAM functions are being stretched or challenged to evolve from tactical trackers of hardware and software to stewards of digital assets that underpin strategic priorities.

Diederik Van Der Sijpe
Lead Partner
(IT & Software Asset Management)

Our 2025 global ITAM survey, conducted across geographies and industries, confirms that ITAM teams are now working in environments marked by volatility and disruption. Cloud, SaaS, and AI adoption have outpaced many legacy processes. Compliance expectations have risen sharply, yet the systems and structures needed to demonstrate assurance often lag behind. And at the same time, boards and executives are asking more of ITAM – from sustainability reporting to cost efficiency, cyber resilience to business agility.

To help organizations navigate this inflection point, we have organized this year’s report around five strategic “keys”. Each of these keys represent a distinct, high-impact area where ITAM can shift from reactive control to proactive value creation.

Key #1: Build the foundations for AI- and cloud-ready ITAM

The starting point is recognizing that traditional ITAM tools and taxonomies (rooted in static, on-premises models) are ill-equipped for a world of dynamic, cloud-based services and AI workloads. **Our survey reveals that fewer than 40% of organizations have fully adapted their ITAM processes to support today's hybrid environments**. In this chapter, we explore the foundational shifts required to track, classify, and govern transient assets, elastic usage patterns, and AI development stacks. This includes updating data models, redefining ownership roles, and integrating ITAM with cloud-native and DevOps tooling. In a world where assets are no longer physical or persistent, building these foundations is the critical first step.

Key #2: Revisit outdated SaaS practices to regain control

Software-as-a-Service (SaaS) is a defining feature of modern IT, but remains a blind spot for many ITAM teams. **Our survey highlights the governance challenges posed by partially decentralized SaaS management: shadow IT, weak compliance controls, fragmented vendor relationships, and poor visibility into consumption**. While some organizations are experimenting with quick fixes (like end-user training or bulk licensing) these are rarely enough. Key #2 urges organizations to modernize their SaaS governance playbooks. This includes expanding the ITAM–FinOps alliance, implementing real-time SaaS management tools, and embedding structured workflows for procurement and compliance. Without this shift, the cost and risk of SaaS sprawl will only grow.

Key #3: Position ITAM as a pillar of cyber-resilience and compliance

In the wake of growing regulatory scrutiny and escalating cyber threats, ITAM is emerging as an enabler of operational resilience and compliance**. Yet only 29% of organizations formally include ITAM in their cybersecurity strategy**. This chapter shows how deeper integration between ITAM, and security functions can improve threat response, data traceability, and regulatory assurance. We also highlight how ITAM is playing a bigger role in resilience planning, particularly under frameworks like DORA, NIS2, and the Canadian OSFI B-13. Perhaps most notably, our findings reveal a troubling lack of preparedness around open-source software risk. Forward-looking organizations are now embedding ITAM into their broader cyber and compliance fabric, not just to meet requirements but to lead with confidence.

Key #4: Use intelligent automation to enable smarter, faster decisions

Manual or partially automated ITAM processes cannot keep up with the scale, speed, and complexity of today's IT estates. This key explores how AI, Gen AI, and intelligent automation are being used to transform ITAM from a reactive function to a predictive, insight-driven capability. **Our survey identifies clear value areas for automation from license management to optimization, but also uncovers barriers around data quality, unclear ROI, and skills gaps**. The message is clear: automation is not a plug-and-play fix. To succeed, it must be grounded in clean data, embedded in strategic workflows, and supported by cross-functional alignment. Organizations that get this right are beginning to reap the benefits e.g., cutting costs, accelerating decisions, and strengthening governance.

Key #5: Align ITAM with enterprise sustainability and purpose goals

The final key takes a step back and asks a bigger question: what is the purpose of ITAM in today's world? Increasingly, the answer lies in its ability to support environmental, social, and governance (ESG) outcomes. **Nearly half of survey respondents now say their ITAM strategies directly support sustainability, while two-thirds report alignment with broader enterprise goals**. In this chapter, we examine how organizations are using ITAM to extend asset life, reduce e-waste, improve license reuse, and embed asset data into ESG reporting. Technology with purpose is not just a theme but is becoming a strategic mandate. ITAM, with its data, reach, and governance footprint, has a central role to play.

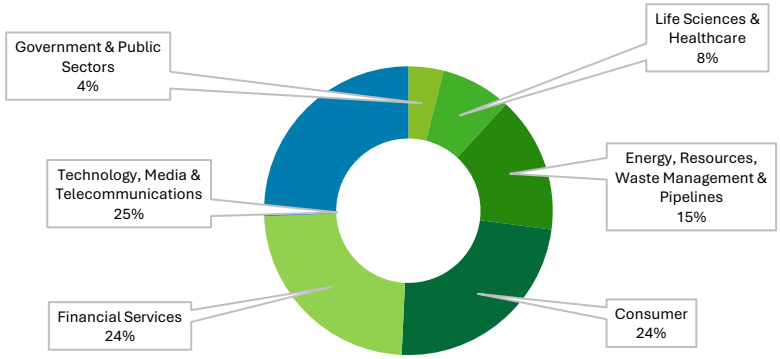
Looking Ahead

What emerges from this year's findings is the need for a **disciplined transition. ITAM is no longer just about tracking what you have, it's about understanding what it means, what it costs, and where it leads. The five keys in this report reflect a new strategic posture: one that sees ITAM as a driver of efficiency, resilience, trust, and sustainability.**

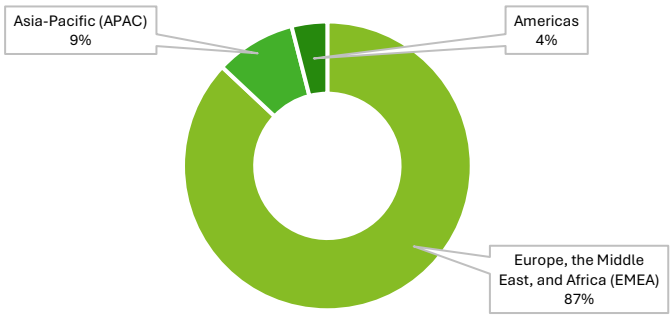
As organizations navigate an AI-powered, cloud-enabled future, ITAM has the opportunity (and the responsibility) to lead from the front. We hope this report helps spark new conversations, fresh priorities, and bold action across your enterprise.

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

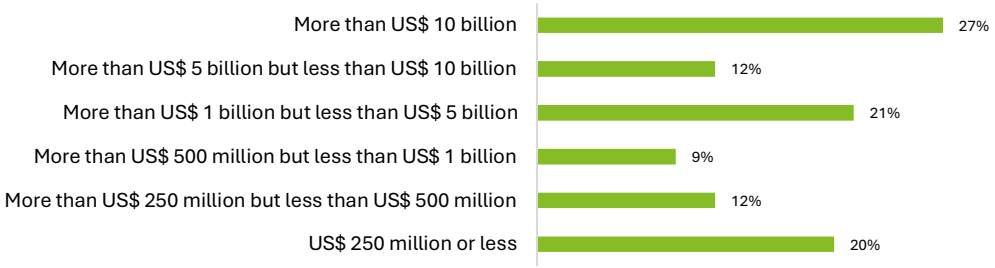
Industry



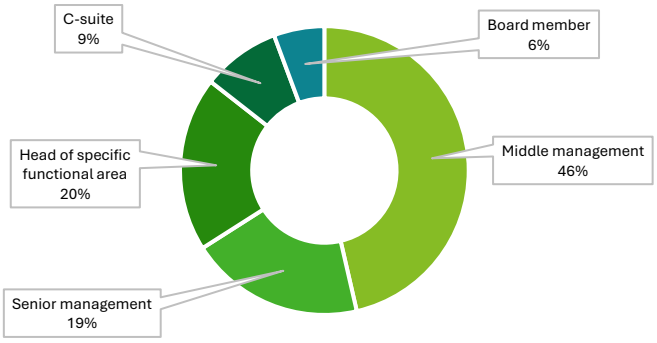
Geography



Annual Turnover of Organization



Respondent Position



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

NOTE: All percentages cited in the text have been rounded off to the nearest integer.

Chapter 1: Reimagining ITAM's command in the AI-cloud nexus

KEY #1: Exploit synergies between ITAM and FinOps to unlock financial and operational agility to navigate complexities of AI/Gen AI and cloud ecosystems.

As cloud computing and AI adoption reshape enterprise IT, ITAM teams face growing pressure to manage increasingly dynamic and transient assets. Traditional practices built for static, on-premises environments are proving inadequate in a landscape defined by consumption-based pricing, rapid scaling, and transient resources. In a world increasingly shaped by AI adoption, infrastructure demands can spike unpredictably, licensing terms are often opaque, and governance struggles to keep pace. As a result, ITAM functions must now deliver strategic control, cost optimization, and risk assurance, often without full visibility or integration with finance or technical teams.

Our current survey reveals that:

- Growing lack of **visibility** into cloud-based assets and consumption is the top challenge, reported by 47% of respondents.
- Following close behind is the lack of **coordination** between IT/cloud operations, AI project leads, ITAM, and finance teams (46%).

These top two concerns, that are also **ranked highest in terms of the severity of impact**, reflect the speed and complexity of AI and cloud environments, where real-time provisioning, decentralized innovation, and hybrid ownership models create blind spots and disconnects. Temporary assets and flexible usage patterns make it challenging to maintain governance and cost control without strong collaboration across teams. The complexities of managing temporary assets and flexible usage patterns are amplified in hybrid and multi-cloud environments. Inconsistent licensing models and metrics across different providers create significant data integration challenges, hindering effective governance and cost control.

The growing need to ensure compliance, with increasingly complex licensing terms, for AI and cloud services was cited by 42% as the third challenge. Respondents indicated that this stems from constantly evolving vendor terms, usage-based billing, and bundled AI/cloud offerings that are difficult to track and interpret without specialized expertise.

36% of respondents are also concerned about balancing cost control with continued innovation in AI. Notably, a majority of these see it as a high-severity issue. This suggests that while organizations want to move fast with AI, many lack the financial guardrails or operational maturity to do so sustainably.

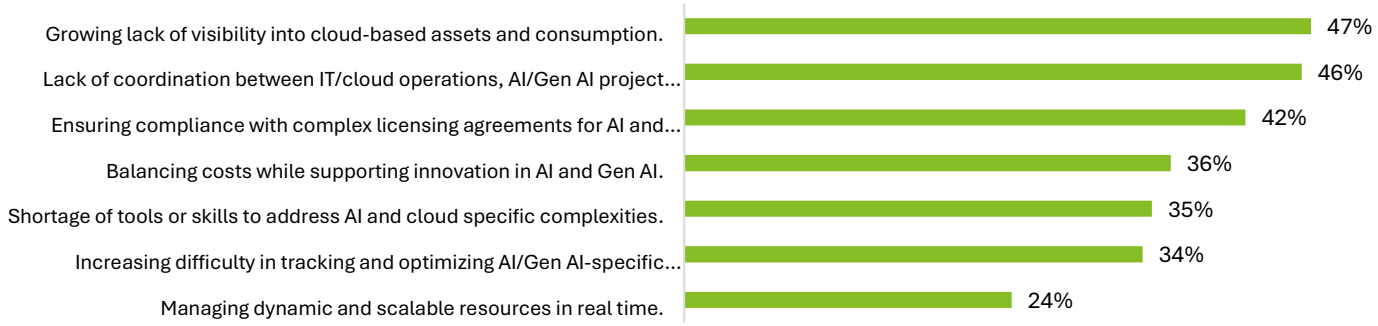


Figure 2: Top challenges faced by ITAM teams in managing assets within AI/Gen AI and cloud ecosystems

Surprisingly, only 29% of respondents report having a dedicated FinOps team or framework in place to manage cloud and AI-related spend. A further 24% are still relying on existing ITAM or operations teams, while another 24% are in transition – either establishing a FinOps capability (16%) or merging it with ITAM (8%). Alarmingly, 23% have neither a FinOps team in place nor any near-term plans to create one.

Organizations are already seeing measurable benefits where dedicated FinOps capabilities do exist:

- 46% say the combination of ITAM's asset tracking and FinOps' cost transparency helps them stay within budget while still leveraging AI and cloud innovation. **This pairing reduces waste, avoids shadow IT, and provides the financial discipline needed to scale responsibly**.
- 39% believe that financial insights from FinOps teams help ITAM make faster, data-driven decisions around asset provisioning and resource allocation. **This enables better responsiveness to business demand, while keeping spend aligned with strategy**.
- 33% report that their FinOps function ensures cross-functional collaboration among IT, finance, ITAM, and operations. **This reduces silos and enables joined-up decision-making, complementing ITAM's governance role**.
- 31% say their FinOps–ITAM integration allows them to use asset and consumption data to anticipate future needs and optimize ahead of demand. **This shift from reactive to predictive enables more strategic planning and proactive budget alignment**.

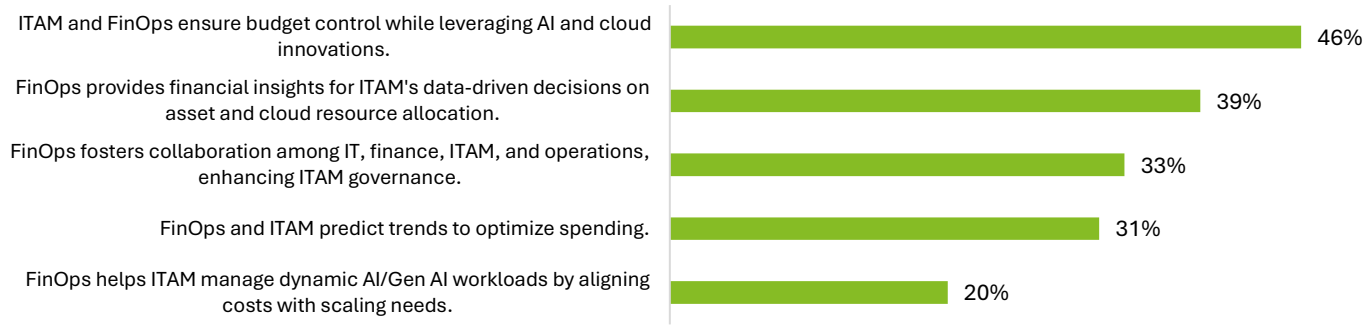


Figure 3: Synergies between ITAM and FinOps teams that respondents currently exploit for operational and financial agility

Yet, despite these benefits, **82% of respondents admit their organization has low or underdeveloped synergy between ITAM and FinOps**. Nearly half (41%) rate their maturity as very poor, while the rest consider it mediocre at best. This points to structural and cultural barriers: fragmented ownership, lack of shared KPIs, and legacy mindsets that still view ITAM as tactical rather than strategic. Addressing this requires leadership commitment, cross-functional metrics, and better integration of financial governance with asset intelligence.

In summary, AI and cloud adoption are no longer emerging trends, they are foundational shifts. Yet ITAM, in many organizations, is still catching up. The minority who have embraced a dedicated FinOps model are already seeing dividends through better governance, cost control, and strategic agility. Others risk falling behind.

Put simply, the first and most foundational key to effective ITAM in today's AI-cloud environment is to reimagine its role. This should not be a siloed control function, but as a command centre for strategic orchestration. This means embedding ITAM into the financial heartbeat of the organization via FinOps. Strategic ITAM can no longer just track assets; it must guide decisions. In a world of transient resources and exponential AI experimentation, only a deeply integrated ITAM–FinOps approach can deliver the operational agility and financial clarity needed to manage uncertainty, harness innovation, and drive responsible growth.

Chapter 2: From Chaos to Control in SaaS licensing

KEY #2: Revisit out-of-date practices to address the growing complexities of increasingly decentralized SaaS usage focused on improving governance and efficiency.

Chapter 1 emphasized the crucial role of FinOps in achieving financial agility within complex cloud and AI environments, highlighting the need for integrated financial governance and asset intelligence. This chapter focuses on applying those principles, along with the automation strategies outlined in Chapter 4 (particularly regarding license tracking and cost optimization), to the specific challenges of managing increasingly decentralized SaaS licensing. We will explore how a combined approach can lead to greater control, cost optimization, and compliance within the dynamic SaaS landscape.

As SaaS adoption accelerates across business functions, ITAM leaders are increasingly being pulled into a fragmented and fast-moving environment. Unlike traditional software, SaaS tools are often procured directly by departments, bypassing IT and central procurement. This decentralization, while enabling agility, creates major challenges around visibility, compliance, cost optimization, and vendor control. Many existing ITAM practices and governance models (designed for perpetual licenses or enterprise-wide rollouts) are simply not equipped to manage the dynamic, subscription-driven nature of modern SaaS ecosystems.

The first step in addressing the governance and efficiency challenges associated with decentralized SaaS usage is to understand how organizations currently manage SaaS licensing across departments and operating units. **Our survey reveals significant variation in SaaS management approaches, with implications for ensuring better governance and control as well as more efficient cost management.**

- Only 34% of respondents manage SaaS licensing centrally through ITAM or procurement teams.
- 18% allow individual departments or application owners to manage their own SaaS tools in a fully decentralized manner.
- The remaining 48% follow a hybrid approach, where only the most critical SaaS applications are centrally managed and governed.

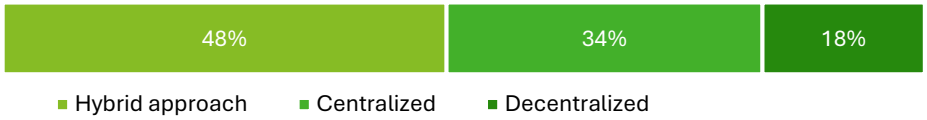


Figure 4: Approach for managing SaaS licensing across operating units or departments

Such partially decentralized models introduce subjectivity around what is considered 'critical', leading to inconsistent enforcement of policies and controls. They also often result in fragmented accountability, where no single team owns the full SaaS landscape, and inconsistent reporting, which undermines decision-making and license optimization.

Respondents cited the following as key challenges stemming from partial or full decentralization of SaaS license management:

- **Rise of shadow IT and unauthorized SaaS purchases** (69% of respondents): This raises concerns over security, data privacy, and redundancy, especially when procurement happens outside approved channels.
- **Lack of visibility into licenses, usage, and consumption (66%):** In the absence of usage intelligence, organizations risk overpaying for unused subscriptions or failing to detect redundant tools. The lack of visibility extends beyond simple license counts; it also includes a lack of integration with Identity and Access Management (IAM) systems. Without this integration, ITAM lacks the context to understand why certain SaaS applications are being used, potentially missing instances of unauthorized access or inefficient resource allocation. Close collaboration between ITAM and IAM teams, allowing ITAM to flag unusual consumption patterns to IAM for investigation, is critical for effective SaaS governance.
- **Challenges in optimizing SaaS costs (57%) and growing compliance risks (54%):**
  - Cost optimization challenges arise when there is no clear view of actual usage patterns, license overlaps, or redundant subscriptions dash leading to overprovisioning, underutilization, and wasted spend across departments.
  - Compliance risks on the other hand may include violations of subscription terms, unintended oversubscription, or breach of geographic or user-based licensing constraints.

- **Inefficient vendor management (37%):** Decentralized licensing leads to fragmented negotiations, inconsistent contract terms, and missed opportunities for enterprise-wide volume discounts.

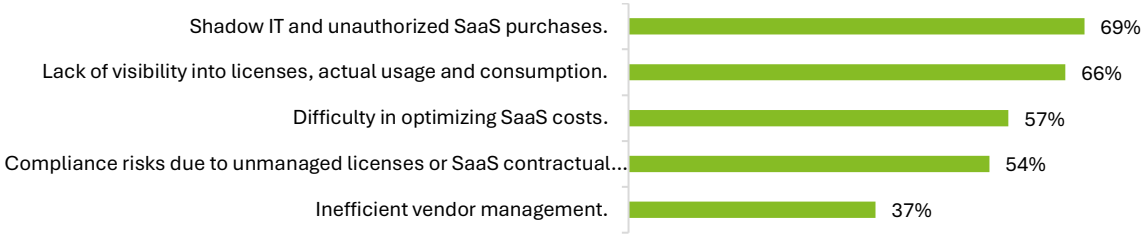


Figure 5: Key challenges arising from partial or full decentralization of SaaS license management

Against this backdrop, our survey also reveals how respondents are adopting various strategies to move from reactive firefighting to more structured SaaS governance.

- **33% believe in extending the FinOps–ITAM partnership beyond cloud cost management to include SaaS, PaaS, and IaaS**. We believe this is a sensible evolution, enabling a more holistic and integrated view of digital consumption. SaaS, like cloud, benefits from coordinated financial governance, usage visibility, and collaborative oversight.
- **31% have focused on implementing or enhancing centralized SaaS management tools, including dashboards and near real-time reporting**. This is an important foundational step. Organizations can use tools like SaaS discovery platforms, license optimization engines, or integrated Configuration Management Databases (CMDBs) to unify data across departments and drive smarter, policy-aligned decisions.
- **23% are establishing application portfolio management and clearer approval workflows for SaaS purchases**. This includes steps such as pre-approved vendor lists, role-based access provisioning, or automated approval hierarchies. All of these help rein in uncontrolled procurement and reinforce accountability.
- **A much smaller subset of respondents reported adopting quick-fix measures, such as training employees on SaaS policy compliance (7%) or negotiating enterprise-wide licensing terms with key vendors (5%).** While these are practical steps and easier to implement, they merely "nibble at the edges", raising awareness or containing costs in the short term without addressing the structural root causes of decentralized sprawl. Given the scale and persistence of these challenges, it's clear that ad hoc fixes won't suffice. The focus must shift to modernizing governance frameworks, processes, and tooling for SaaS lifecycle management.

Addressing the challenges of decentralized SaaS licensing thus requires a holistic approach. By integrating the financial governance principles of FinOps (Chapter 1), the efficiency gains of automation (Chapter 4), particularly in license tracking and cost analysis, and a robust SaaS management strategy, organizations can achieve greater control over shadow IT, reduced SaaS sprawl, improved cost visibility, and improved compliance. This integrated approach is crucial for navigating the complexities of modern SaaS ecosystems and ensuring responsible digital growth.

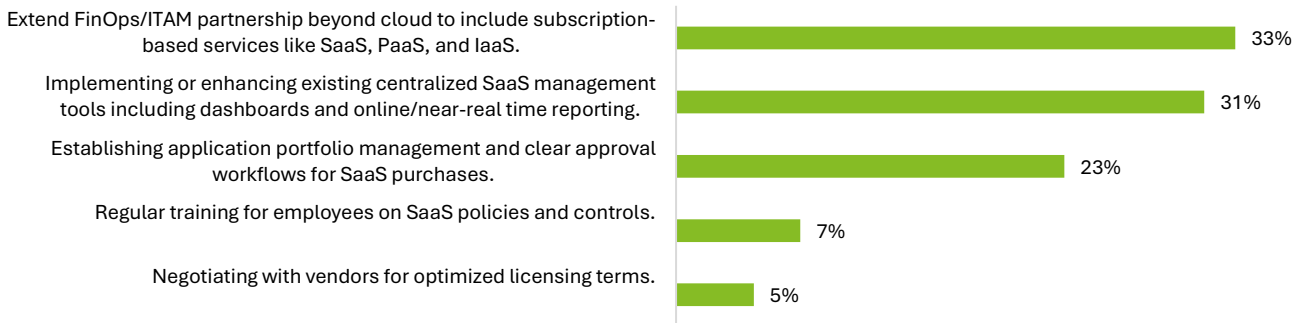
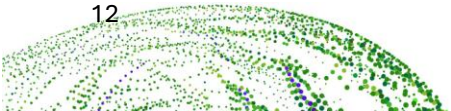


Figure 1: Most effective strategies to manage SaaS complexity

In summary, SaaS licensing has emerged as a major governance blind spot in many organizations, fueled by decentralized purchasing, lack of usage insight, and weak policy enforcement. The consequences range from cost inefficiencies to security and compliance exposures. Moving from chaos to control requires a deliberate shift: expanding the ITAM–FinOps alliance to encompass SaaS, investing in shared visibility tools, enforcing structured workflows, and phasing out legacy practices that no longer suit today's agile digital operations.

This second key to success reminds us that success in today's AI-powered, cloud-driven world demands more than cost control – it demands governance agility. By revisiting outdated SaaS management models and embedding governance into every phase of the SaaS lifecycle, organizations can restore control, reduce risk, and enable smarter digital choices.



Chapter 3: ITAM's Cybersecurity Edge for Regulatory Compliance

KEY # 3: Leverage ITAM as the key to unlock cyber-resilience in an increasingly regulated digital ecosystem

As organizations confront rising cybersecurity threats and regulatory obligations, IT Asset Management (ITAM) is likely to gain a higher level of strategic importance. In astute organizations, ITAM is no longer just about tracking hardware or software, it plays a critical role in enabling digital resilience, ensuring data and infrastructure traceability, and supporting compliance. ITAM serves as a fundamental pillar of cyber-resilience and regulatory compliance, a role underscored by its prominent presence (both explicit and implicit) in numerous regulations.

This shift is driven by mounting pressure from frameworks and regulations such as the EU's Digital Operational Resilience Act (DORA), NIS2 Directive, the EU AI Act (that is being gradually implemented), OFSI B-13 in Canada, and increasing scrutiny by U.S. regulators. With cyber risks intensifying and accountability extending beyond the CISO to the board, ITAM continues to emerge as a vital enabler of secure, compliant operations in a highly regulated digital ecosystem.

Yet, it is surprising, if not alarming, that only 29% of organizations in our survey report that ITAM is formally included within their cybersecurity strategy.

- In 48% of organizations, there is only some interaction between ITAM and cybersecurity functions, with considerable room to improve collaboration.
- In 23% of cases, ITAM operates entirely independently of cybersecurity.

This disconnect signals a missed opportunity. Cybersecurity programmes often rely on up-to-date asset inventories, configuration data, and software lineage. All these typically tend to sit with ITAM. Without alignment, security teams operate with blind spots during patching, incident response, or vulnerability scanning. Integrating ITAM and cybersecurity enables shared visibility of critical assets, speeds up threat containment, and supports continuous compliance with minimal disruption. This may also result in the failure to utilize ITAM's asset data for enhanced security posture and compliance. The increasing importance of Software Bills of Materials (SBOMs) for regulatory compliance further reiterates the need for closer collaboration.

Encouragingly, ITAM's role in resilience planning and execution is on stronger footing. 62% of surveyed organizations report that ITAM is actively involved, while 38% say it is not. This growing involvement reflects a recognition that resilience is built not just on firewalls and backups, but on knowing what you own, how it connects, and where your risks reside. By leveraging ITAM's asset intelligence, organizations can improve business continuity, reduce response times, and meet regulatory expectations for operational readiness.

Among those organizations that involve ITAM in resilience efforts:

- 47% use ITAM to provide trustworthy inventories of critical assets during disruptions such as cyberattacks or outages.
- 30% rely on ITAM to map dependencies and configurations to enable faster recovery; and
- 22% draw on ITAM to demonstrate compliance with legal and regulatory mandates around operational resilience.

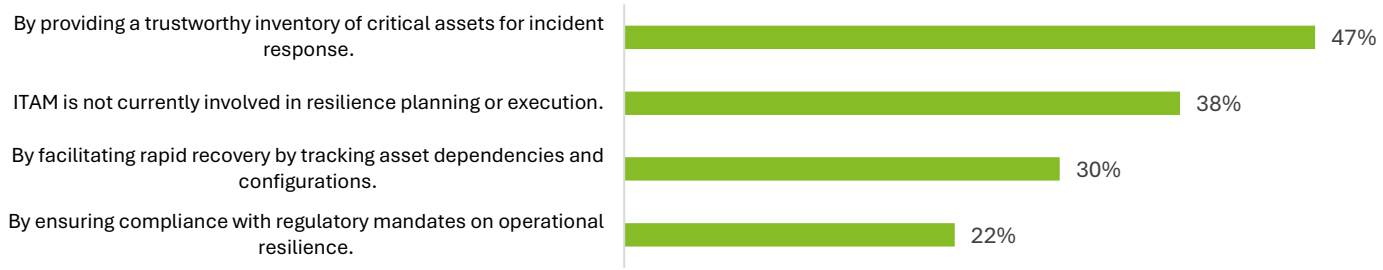


Figure 7: ITAM programme contributions to digital resilience during disruptions

81% of respondents see compliance with new digital regulations as an opportunity to improve ITAM practices. Of these, 33% consider it a significant opportunity, while 48% see some opportunity.

This indicates a growing awareness of how regulations like DORA, NIS2, and the AI Act can become catalysts for strengthening ITAM maturity. As compliance expectations rise, ITAM's ability to deliver accurate, auditable asset data will become central to an organization's ability to prove (and not just assert) its resilience posture.

However, preparedness around open-source software remains a blind spot.

- Only 17% of respondents have a dedicated Open-Source Program Office (OSPO) or equivalent framework. Just 7% align this function to recognised standards such as ISO/IEC 5230 and 18974, while the remaining 10% operate without reference to any formal framework.
- Meanwhile, 54% of organizations continue to manage FOSS within general ITAM or operations teams, and 29% report no plans to manage it explicitly.

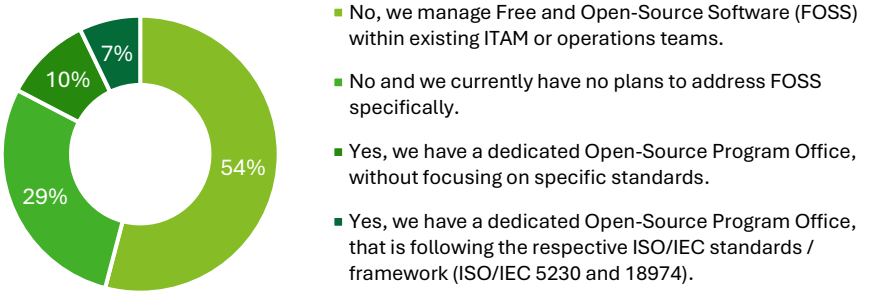


Figure 8: Dedicated Free and Open-Source teams and frameworks to manage licensing and security risks within Open-Source software components

This is concerning given the increasing relevance of open-source components in modern software stacks. As digital sovereignty becomes increasingly important in today's interconnected world, organizations must implement formal controls and mechanisms for tracking licenses in open-source software and monitor security vulnerabilities on a component level. By proactively managing licensing risks and enhancing digital sovereignty measures, organizations can better safeguard the integrity and security of their IT assets. Inappropriate management of open-source software licensing bears legal and reputational risks.

Vulnerabilities in widely used libraries, like the well-known Log4j, have shown how FOSS-related risks can escalate quickly if left unmanaged. The data suggests that while awareness of regulatory compliance is growing, FOSS risk remains underappreciated. Organizations must move beyond passive management to adopt formal controls, license tracking, and security patching mechanisms tailored to the unique nature of open-source software, including breaking down applications into their individual components and running adequate SBOM management processes to protect their estate.

As digital regulation tightens and cybersecurity becomes a board-level priority, ITAM is no longer optional, it is indispensable.

Key #3 calls for a mindset shift: ITAM must be repositioned not just as an operational function, but as a foundational pillar of cyber-resilience and regulatory readiness.

Organizations that proactively align ITAM with cybersecurity, resilience planning, and open-source risk management will be better equipped to navigate the complex and evolving digital risk landscape.

Chapter 4: Smarter insights for better outcomes (with intelligent automation for ITAM)

KEY # 4: Exploit the growing opportunities for intelligent automation of ITAM with growing complexity and ambiguity in license management

The aspiration to achieve 'smarter insights for better outcomes' reflects a strategic shift in ITAM: away from reactive reporting and toward intelligent, data-driven decisions. This chapter focuses on how intelligent automation (enabled by AI, machine learning, and Gen AI) can unlock this shift. As licensing environments grow more complex, and cloud platforms more diverse, leading organizations are embracing automation not just to scale operations, but to make smarter, faster decisions across the asset lifecycle.

Astute organizations are now looking beyond traditional inventory and compliance tasks, and towards automation as a lever for resilience, efficiency, and foresight. This includes automating license tracking across hybrid estates, generating predictive renewal alerts, triggering workflows. Ultimately, this is about getting the most out of data: automating how it's gathered, analyzed, and acted upon to achieve tighter controls and stronger performance.

With cloud adoption accelerating, this imperative is more pressing than ever. Our survey captured how organizations are (or aren't yet) using intelligent automation to monitor and optimise their cloud spend.

- Currently, 76% of respondents do not monitor at least half of their total cloud spend using intelligent automation. This leaves only 24% who do so for 51–100% of their spend.
- However, this is set to change sharply: 78% aspire to monitor at least half of their cloud spend using intelligent automation in the next 1–2 years, with only 22% expecting to remain below this threshold.

We believe this shift will be pivotal. With AI-driven monitoring and cost optimisation, organizations can avoid cloud waste, rebalance licenses dynamically, detect underutilised entitlements, and model future scenarios. It also increases FinOps collaboration by providing real-time spend signals across business units.

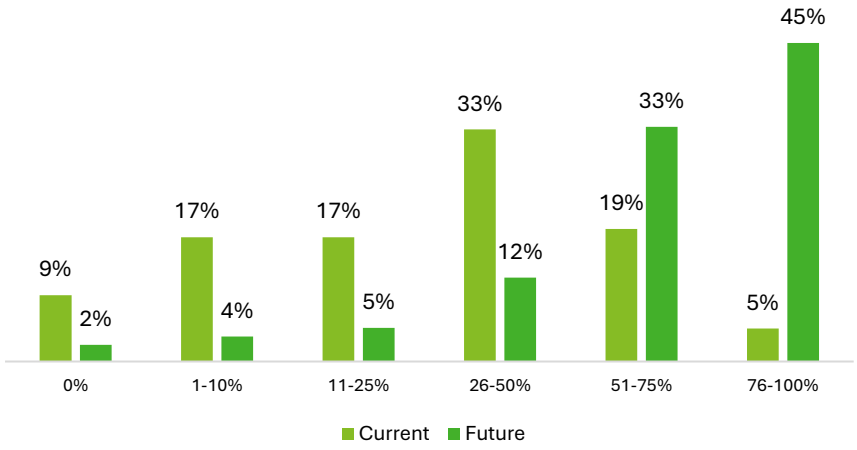


Figure 9: Proportion of total cloud spend monitored intelligently: current state and future aspiration

Against this backdrop, our survey respondents highlighted specific areas where intelligent automation could deliver the most value:

- **License optimisation** – 79% believe automation would improve compliance tracking, usage analysis, and cost control across SaaS, PaaS, IaaS, on-premises, and hybrid environments.
- **Contract and vendor management** – 60% see value in using AI to assess vendor performance, automate renewals, and scan contracts for risks. These tasks can be significantly streamlined by modern Contract Lifecycle Management (CLM) systems that provide a centralized repository for contract information and automated workflows.
- **Improved cloud management** – 48% pointed to AI-driven tools that support real-time monitoring, forecasting, and FinOps alignment.
- **Other key use cases included**:
  - Better insights across ITSM, ITAM, VM, and CM platforms (37%).
  - Incident response and predictive maintenance (36%).
  - Hardware Asset Management (HAM) with intelligent lifecycle optimisation (34%).

Together, these use cases demonstrate a growing appetite to embed AI and automation deeper into ITAM processes – from software to infrastructure. While license optimisation remains the top priority, areas like integrated platform visibility and predictive operations are emerging as the next frontier.

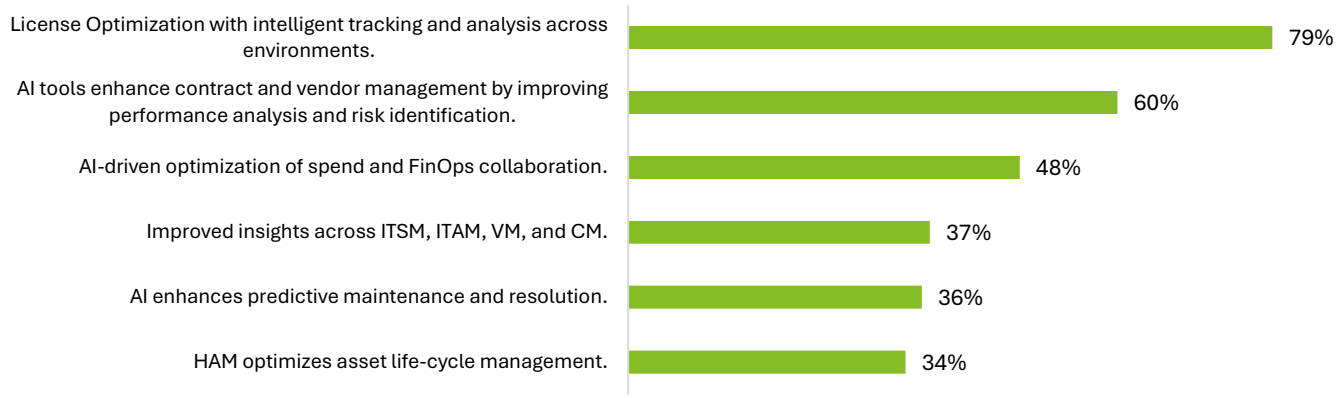


Figure 10: Specific areas where intelligent automation could deliver the most value

Interestingly, although cloud management and HAM received lower mentions overall, those who prioritised them saw them as making a much stronger strategic impact than contract/vendor automation. This could be because cloud and hardware represent high-cost, high-risk categories where automation can yield measurable business outcomes, whether through smarter provisioning, reduced lifecycle costs, or more accurate forecasting.

Despite this momentum, real-world adoption of intelligent automation in ITAM remains limited due to several key challenges:

- Poor data quality and fragmented systems were the top roadblocks (54%).
- Unclear ROI, with 51% lacking clarity on tangible cost, compliance, or risk benefits.
- 40% felt they must first address fundamental issues, such as multi-cloud complexity and decentralised SaaS use, before automating.
- Lack of internal expertise in emerging tech was a constraint for 37%.
- 34% highlighted regulatory uncertainty, especially around data privacy and cybersecurity.
- Other inhibitors included:
  - Organizational resistance to change.
  - Vendor lock-in limiting tool flexibility.
  - Insufficient collaboration with FinOps and related teams.

These findings reflect a common pattern in tech adoption: aspiration at the top, friction in the middle. Many ITAM teams are caught between the mounting complexity and limited bandwidth.

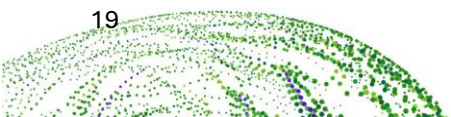
To move forward, organizations must invest in data quality, clarify automation's ROI, and prioritise foundational integration across systems. Education is key, equipping teams with skills to engage with AI tools confidently. Equally important is cross-functional alignment, particularly with FinOps, procurement, and cloud teams.

Intelligent automation must be seen not as a plug-in tool but as part of a broader operating model transformation.

The growing complexity and ambiguity in license management is now too significant to be tackled manually.

Key #4 signals a call to action: smarter insights, powered by intelligent automation, are the only way to deliver better outcomes at scale.

Organizations that embrace this shift (optimizing both their tools and their talent) will position ITAM not just as a compliance function, but as a strategic engine for efficiency, agility, and innovation in the cloud and AI era.



Chapter 5: ITAM's vision: Technology with Purpose and Actions

KEY #5: Use technology strategically to reduce waste, enhance compliance and support sustainability efforts in an evolving technology landscape

"Technology with Purpose" signals a shift in how leading organizations approach IT Asset Management. This is not simply as a cost control or compliance activity, but as a strategic lever for sustainability, efficiency, and responsible technology stewardship.

Aligned to this thinking, **this chapter explores how organizations can use ITAM to align technology use with broader goals: reducing waste, meeting regulatory demands, and supporting enterprise-wide sustainability commitments**. We will then conclude this report by discussing actions prioritised by respondents in their longer-term transformation journey described in this report with a holistic perspective.

The more forward-looking organizations are already pursuing this vision by adopting intelligent tools and data-driven processes to optimise asset utilisation, extend equipment lifecycles, and ensure assets are retired or redeployed responsibly. But this isn't just about tools: it's about integrating ITAM into decision-making frameworks that prioritise responsible growth, ethical technology use, and environmental performance.

At the heart of this approach lies the ability to harness data, intelligently, accurately, and at scale. With increasing regulatory and stakeholder scrutiny on environmental impact and governance, the ability to track and report on IT asset usage, retirement, and associated emissions is becoming a board-level concern. This is where intelligent automation, AI/Gen AI, and end-to-end ITAM–FinOps integration come into play. For instance, by using AI to model the future IT estate or syncing asset records with CMDBs, organizations can optimize outcomes while cutting waste and improving governance.

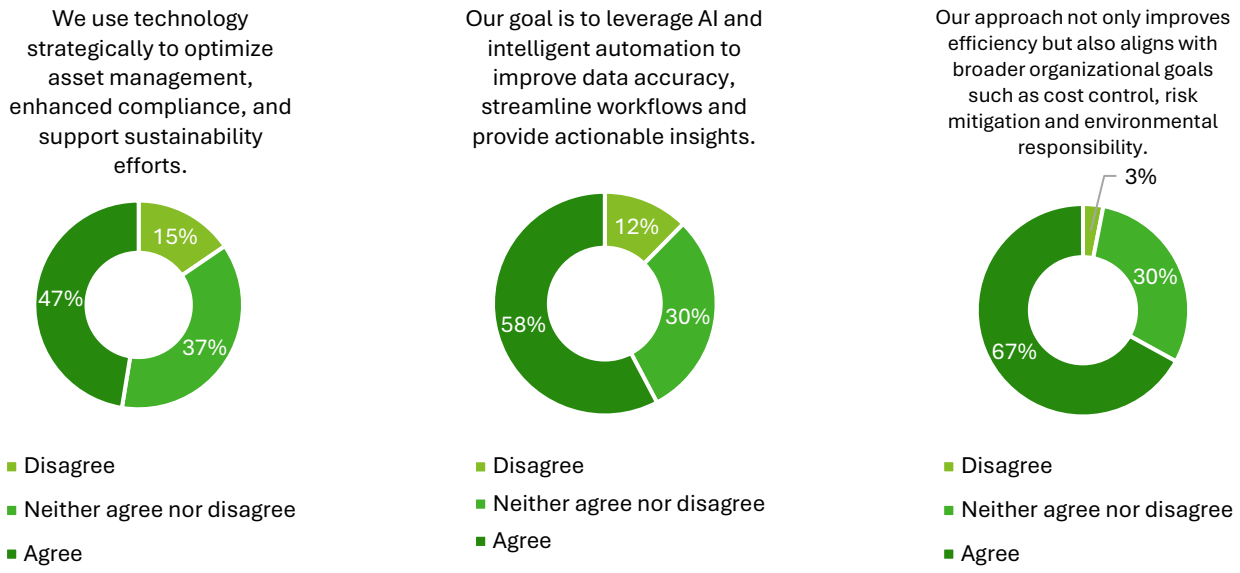


Figure 2: Leveraging ITAM programs to align technology use with broader organizational goals

- **47% of respondents already say they use technology strategically to optimize asset management, strengthen compliance, and support sustainability. 15% disagreed, while 37% were neutral.**

  This indicates that nearly half of organizations are on the right track. They are using ITAM to drive a triple impact: reducing technological waste, increasing regulatory alignment, and enabling sustainability. In practice, this can include extending device refresh intervals, ensuring accurate license reuse, and embedding asset data into ESG reporting. Going forward, the focus must shift from intent to institutionalization by codifying these practices within operating models.

- **A higher proportion of respondents (58%) said their goal is to use AI and intelligent automation to improve data accuracy, streamline workflows, and provide actionable insights.**

  This level of aspiration is encouraging. It reflects growing confidence that AI and automation can support the triple goal above. For example, intelligent license tracking, anomaly detection in SaaS usage, or auto-suggestions for energy-efficient procurement decisions are now real possibilities. To make this real, organizations must invest in the tooling, processes, and people required to operationalize AI-driven ITAM.

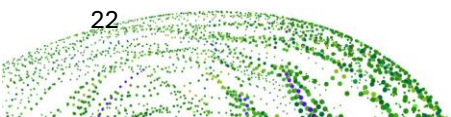
- **Even more promising, 67% believe their ITAM approach now supports broader organizational goals such as cost control, risk mitigation, and environmental responsibility.**

  This signals a shift from siloed asset management toward strategic alignment. ITAM is becoming a contributor to the enterprise's ESG, risk, and digital transformation agenda, not just a back-office compliance function. Organizations that embed ITAM into financial planning, supply chain strategy, and governance frameworks will be best positioned to lead.

In a world where sustainability, compliance, and cost-efficiency are non-negotiable, ITAM must become a strategic force. "Technology with Purpose" is not just a slogan – it's a call to action.

Key #5 highlights the role of ITAM in helping organizations reduce waste, stay compliant, and support long-term sustainability. The path forward not only requires intelligent technology, but also stronger data foundations, cross-functional collaboration, and alignment with enterprise strategy.

Organizations that embed ITAM into their sustainability and compliance agenda will not only improve their asset efficiency, but they will also future-proof their technology decisions in a rapidly evolving world.



What organizations are prioritizing as immediate next steps

Seven themes emerging from the data

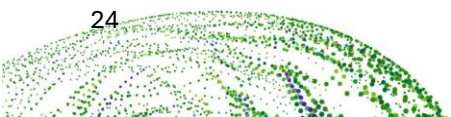
Survey responses revealed clear clusters of action areas being prioritised by organizations as immediate next steps in their journey to transformation. Here's what these themes reveal:

1. **Accelerating AI and Automation**
   Organizations are planning to continue embedding AI across license compliance, administrative automation, and data validation. This is about moving from manual reconciliations to smart triggers, from static spreadsheets to dynamic, AI-driven insights.
2. **Data Management and Quality**
   The foundation of intelligent ITAM is clean, timely data. Respondents indicated an immediate focus on addressing quality at source, improving clarity on device usage, normalising data, and enabling real-time inventory views. Quality data not only improves compliance and cost control but is also a prerequisite for automation and ESG reporting.
3. **Centralisation and Governance**
   Respondents indicated that visibility and accountability require immediate structural changes. Respondents are establishing centralised ITAM ownership, implementing governance programs, and creating unified views across clouds, particularly the hyper scalers and FOSS platforms. Dynamic CMDBs and centralised licensing budgets are critical enablers in this effort.
4. **Integration and Collaboration**
   Stronger collaboration between ITAM, Procurement, and FinOps is emerging as critical enablers of strategic asset management. Organizations are also recognising the importance of breaking down internal silos to improve data sharing, process alignment, and governance.
5. **Cloud and Licensing**
   Respondents from the more astute organizations reported that they are attempting to tackle the challenges of multi-cloud licensing head-on. This includes streamlining contracts, integrating cloud and SaaS usage data into a central repository, and responding to vendor-driven pressures like license metric changes or freeware monetisation.
6. **Cost Management and Control**
   Ensuring cost effectiveness remains a core priority in the current environment. Beyond savings, respondents would like their organizations

build business cases for ITAM investments, focusing on longer and medium-term value, risk mitigation, and sustainability-linked outcomes.

7. **Process Improvement, Skills & Strategic Integration**
   Standardizing ITAM processes, training teams, securing board-level sponsorship, and aligning ITAM with strategic finance and business planning are high on the immediate agenda. These are foundational steps in elevating ITAM to a strategic discipline.

Our IT & Software Asset Management leader's foreword to this report has already highlighted the critical need for a strategic shift in IT Asset Management (ITAM). Moving beyond simple asset tracking, organizations must now focus on understanding the value, cost, and strategic implications of their IT assets. The five key areas explored in this report demonstrate the critical success factors for this new strategic approach, positioning ITAM as a vital driver of efficiency, resilience, trust, and sustainability. In the rapidly evolving landscape of AI and cloud computing, ITAM can no longer remain just an operational function, but evolve as a strategic imperative, poised to lead organizations towards a more efficient and sustainable future.



Appendix

About the Authors

Diederik Van Der Sijpe
Lead Partner - IT & Software Asset Management | Deloitte Belgium
dvandersijpe@deloitte.com

Hans Vandewijer
Partner - IT & Software Asset Management | Deloitte Belgium
hvandewijer@deloitte.com

Dr. Sanjoy Sen
Lead Researcher | Deloitte UK
sanjsen@deloitte.co.uk

Andre Kuntze
Partner | Deloitte Germany
akuntze@deloitte.de

Eric Sullivan
Partner | Deloitte Canada
ericsullivan@deloitte.ca

Daniel Botha
Consultant | Deloitte Belgium
dbotha@deloitte.com

Deloitte.

About Deloitte

Deloitte refers to one or more of Deloitte Touche Tohmatsu Limited, a UK private company limited by guarantee ("DTTL"), its network of member firms, and their related entities. DTTL and each of its member firms are legally separate and independent entities. DTTL (also referred to as "Deloitte Global") does not provide services to clients. Please see www.deloitte.com/about for a more detailed description of DTTL and its member firms.

Deloitte provides audit, tax and legal, consulting, and financial advisory services to public and private clients spanning multiple industries. With a globally connected network of member firms in more than 150 countries, Deloitte brings world-class capabilities and high-quality service to clients, delivering the insights they need to address their most complex business challenges. Deloitte has in the region of 312,000 professionals, all committed to becoming the standard of excellence.

This publication contains general information only, and none of Deloitte Touche Tohmatsu Limited, its member firms, or their related entities (collectively, the "Deloitte Network") is, by means of this publication, rendering professional advice or services. Before making any decision or taking any action that may affect your finances or your business, you should consult a qualified professional adviser. No entity in the Deloitte Network shall be responsible for any loss whatsoever sustained by any person who relies on this publication.

CoRe Creative Services.

MAKING AN IMPACT THAT MATTERS since 1845