

五个关键策略：在云驱动、人工智能赋能的世界中实现ITAM
德勤2025年全球IT资产管理 (ITAM) 调查

引言

前言 2

第一章：在人工智能云中心重新构想ITAM的指挥

第二章：SaaS 许可中的从混乱到控制 9

第三章：ITAM在合规性网络安全方面的优势 13

第四章：智能化洞察以实现更优结果（运用智能化进行ITAM） 16

第五章：ITAM的愿景：有目的的技术与行动 20

哪些组织将优先考虑作为下一步的紧急措施

序言

我很高兴与您分享我们关于IT资产管理 (ITAM) 的第三次全球调查结果，题为“在云驱动、AI赋能的世界中实现战略ITAM的五大关键”。

理解我们当前调查的演变和目标

我们之前进行的两次调查（分别于2021年和2023年启动）研究了当时组织中的IT资产管理现状，并展示了他们如何需要调整关注点和投资优先级，以反映不断变化的技术格局，以及更具体地，硬件和软件的新许可方式。技术从未停滞不前，但现在面对IT资产管理 (ITAM) 领导者所面临的变革速度是史无前例的。随着人工智能和通用人工智能的兴起，云服务的爆炸性扩张，以及DORA和欧盟人工智能法案等数字法规的出现，ITAM已不再是安静的、后台的职能。它需要变成一种战略能力，这对于组织如何管理成本、促进创新、确保合规和支持弹性至关重要。

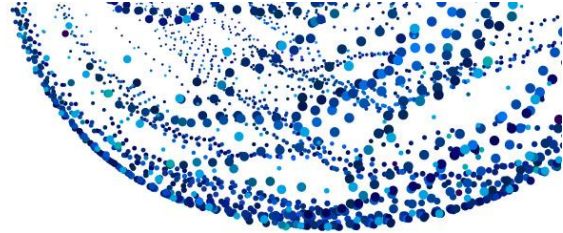
这正是今年报告标题的灵感来源：**五个云驱动、人工智能赋能世界的战略ITAM关键点**。标题反映了重塑全球ITAM的这两股力量。在外部，组织正应对更大的运营复杂性、日益严格的监管审查以及向更多去中心化的技术所有权转变。在内部，许多ITAM职能正面临拉伸或挑战，从硬件和软件的战略追踪者转变为支撑战略优先事项的数字资产的管理者。

我们于2025年进行的全球ITAM调查，覆盖地理和行业，证实了ITAM团队现在正在充满波动和破坏的环境中工作。云计算、SaaS和AI的采用已超过许多传统流程。合规预期大幅上升，但证明保证所需系统和结构往往落后。与此同时，董事会和高管对ITAM的要求也越来越高——从可持续性报告到成本效率，从网络韧性到业务敏捷性。

为了帮助组织应对这一转折点，我们今年将报告围绕五个战略“关键点”组织。这些关键点各自代表一个独特的、影响巨大的领域，在ITAM中可以从被动控制转变为主动价值创造。



迪德里克·范德锡普
领航合作伙伴 (IT与软件资产管理)



关键#1：构建AI和云准备的ITAM基础

起点在于认识到传统的ITAM工具和分类法（基于静态的本地化模型）无法适应动态的云服务世界和人工智能工作负载。**我们的调查显示，不到40%的组织已经完全调整了其ITAM流程以支持当今的混合环境。**在本章中，我们探讨了追踪、分类和治理临时资产、弹性使用模式和AI开发堆栈所需的根本性转变。这包括更新数据模型、重新定义所有权角色以及将ITAM与云原生和DevOps工具集成。在一个资产不再物理或持久的世界里，建立这些基础是关键的第一步。

关键#2：重新审视过时的SaaS实践以重新获得控制权

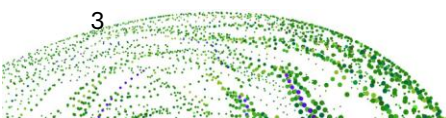
软件即服务（SaaS）是现代IT的一个标志性特征，但仍然是许多IT资产管理团队的一个盲点。**我们的调查突出了部分去中心化SaaS管理带来的治理挑战：影子IT、薄弱的合规控制、碎片化的供应商关系以及对消费的可见性不足。**尽管一些组织正在尝试快速解决方案（如终端用户培训或批量许可），但这些通常远远不够。关键#2敦促组织现代化其SaaS治理剧本。这包括扩大ITAM-FinOps联盟，实施实时SaaS管理工具，以及嵌入结构化的采购和合规工作流程。没有这种转变，SaaS扩散的成本和风险只会增加。

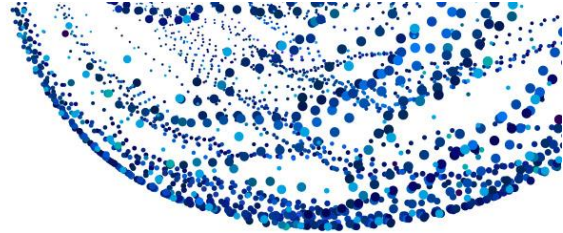
关键#3：将ITAM定位为网络安全和合规的支柱

在日益严格的监管审查和不断升级的网络安全威胁的背景下，ITAM正成为提升运营韧性和合规性的推动者。**然而，只有29%的组织将ITAM正式纳入其网络安全策略中。**本章展示了ITAM与安全功能之间更深层次的整合如何提升威胁响应、数据可追溯性和合规性保障。我们还强调了ITAM在弹性规划中扮演的更为重要的角色，尤其是在DORA、NIS2和加拿大OSFI B-13等框架下。也许最为引人注目的是，我们的发现揭示了在开源软件风险方面的准备不足问题。具有前瞻性的组织现在将ITAM融入其更广泛的网络安全和合规性架构中，不仅为了满足要求，更是为了自信地引领。

关键#4：利用智能自动化实现更智能、更快的决策

手动或部分自动化的ITAM流程无法跟上当今IT环境的规模、速度和复杂性。本篇关键文章探讨了如何利用人工智能（AGI）、通用人工智能（Gen AI）和智能自动化将ITAM从被动响应功能转变为预测性和洞察力驱动的能力。**我们的调查明确了自动化带来的价值领域，从许可证管理到优化，但也揭示了数据质量、不明确的投资回报率和技术差距等方面的障碍。**信息明确：自动化不是即插即用的解决方案。要成功，它必须基于干净的数据，嵌入到战略流程中，并得到跨职能的协调一致。那些在这方面做得正确的组织正在开始获得收益，例如，降低成本、加快决策和加强治理。





关键#5：将ITAM与企业的可持续性和目标相结合

最终关键的一步退而提出一个更大的问题：在当今世界，ITAM（信息技术资产管理）的目的究竟是什么？越来越多的人认为，答案在于其支持环境、社会和治理（ESG）结果的才能。近一半的受访者在调查中表示，他们的ITAM策略直接支持可持续性，而三分之二的人报告称与更广泛的企业目标保持一致。在本章中，我们探讨组织如何利用ITAM延长资产寿命、减少电子垃圾、提高许可重用率，并将资产数据融入ESG报告。有目的的技术不仅仅是一个主题，它正在成为一项战略命令。ITAM凭借其数据、触角和治理足迹，在其中发挥着核心作用。

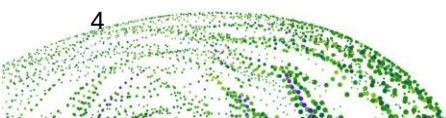
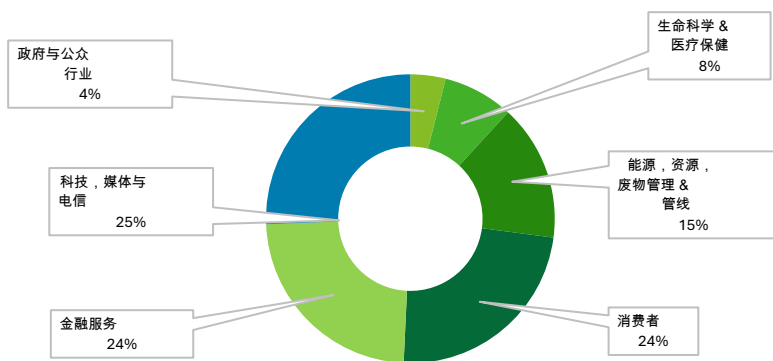
瞻望未来

What emerges from this year's findings is the need for a **有纪律的转型**。ITAM不再仅仅是跟踪你所拥有的，而是关于理解它的意义、成本以及它将引领的方向。本报告中的五个关键点反映了一种新的战略姿态：将ITAM视为效率、弹性、信任和可持续性的推动者。

随着组织迈向由人工智能驱动、云技术赋能的未来，ITAM有机会（也有责任）站在前沿引领。我们希望这份报告能激发您企业内新的对话、新的优先事项和大胆的行动。

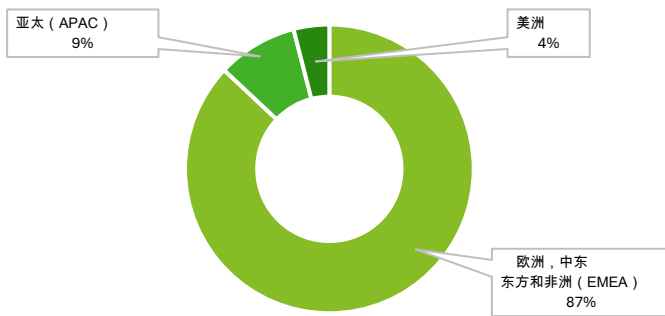
我们邀请了来自约二十个国家的超过一千名参与者参与这项调查，涵盖了所有主要行业领域。这些个人要么在较小或较大的组织中领导，要么在ITAM（信息技术资产管理）倡议中扮演关键角色（图1）。

产业

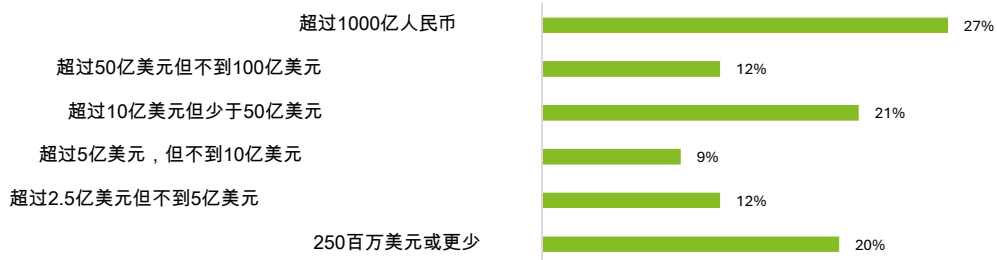




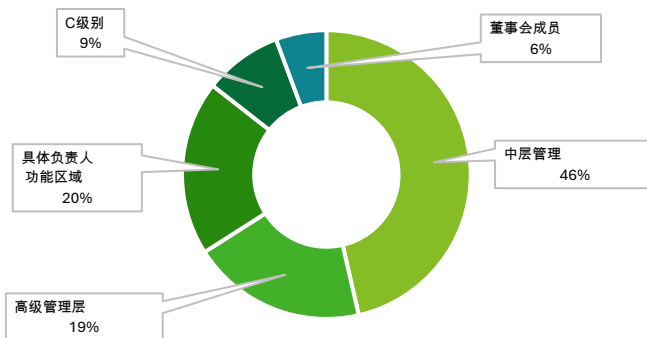
地理学



年度机构营业额

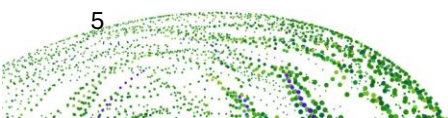


应诉方立场



我们的全球ITAM和SAM专业人士可以帮助您了解这项调查的发现如何揭示您组织独特的机遇。欲了解更多信息, 请联系您的联系人。 **本地专家**。

注意: 文中引用的所有百分比均已四舍五入至最接近的整数。





第一章：重新构想AI-云枢纽中ITAM的指挥

关键#1：利用ITAM和FinOps之间的协同效应，解锁财务和运营灵活性，以应对AI/通用AI和云生态系统的复杂性。

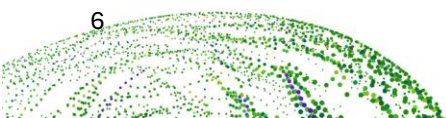
随着云计算和人工智能的采纳重塑企业IT，ITAM团队面临着越来越大的压力，以管理日益动态和短暂性的资产。为静态、本地环境构建的传统实践在以消费为基础的定价、快速扩展和短暂资源定义的格局中正显得力不从心。在人工智能应用日益影响世界的背景下，基础设施需求可能难以预测地激增，许可条款往往不透明，治理难以跟上步伐。因此，ITAM职能现在必须提供战略控制、成本优化和风险保障，通常在没有全面可见性或财务或技术团队整合的情况下。

我们的当前调查揭示：

- 日益增长的缺乏 **可见度** 进入云基础设施和消费是最大的挑战，47%的受访者表示。
- 紧随其后的是缺乏 **协调** 在IT/云运营、AI项目领导、ITAM和财务团队之间（46%）。

这些两大关注点，也是 **在影响严重程度方面排名最高** 反映人工智能和云环境的速度和复杂性，实时配置、去中心化创新和混合所有权模式产生了盲点和脱节。临时资产和灵活的使用模式使得在没有团队间紧密协作的情况下，维持治理和成本控制变得具有挑战性。在混合和多云环境中，管理临时资产和灵活使用模式的复杂性被放大。不同提供商之间不一致的许可模式和指标创造了重大的数据集成挑战，阻碍了有效的治理和成本控制。

不断增长的对确保合规性的需求，以及对AI和云服务的越来越复杂的许可条款 被42%的人认为是第三大挑战。受访者表示，这源于不断变化的供应商条款、基于使用的计费 and 难以追踪和解读的捆绑式AI/云服务，没有专业知识难以应对。





36%的受访者还担心在人工智能的持续创新中平衡成本控制。值得注意的是，其中多数人认为这是一项高度

严重问题 这表明，尽管组织希望快速推进人工智能，但许多人缺乏可持续发展的财务约束或运营成熟度。

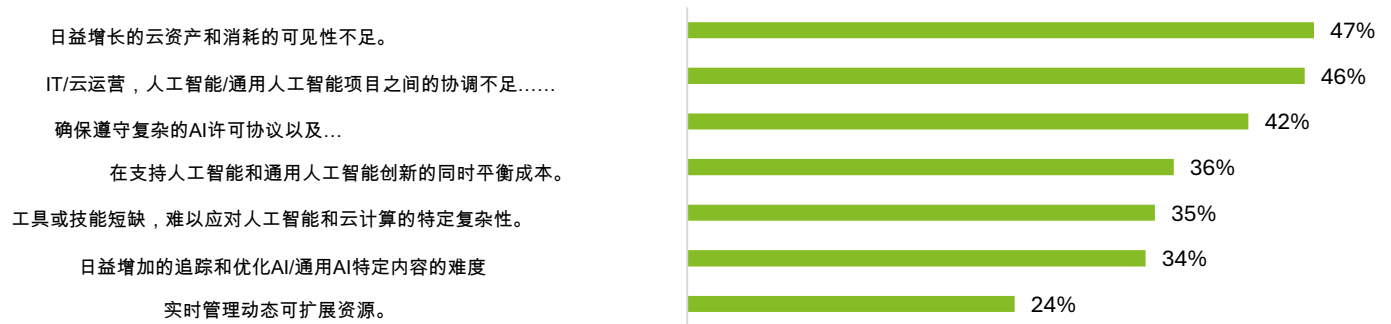
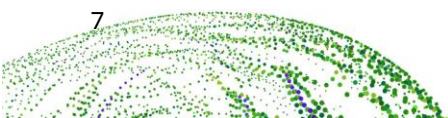


图2：ITAM团队在管理AI/通用AI和云生态系统中的主要挑战

令人惊讶的是，只有29%的受访者表示他们拥有专门的FinOps团队或框架来管理云和AI相关的支出。另外24%的人仍在依赖现有的ITAM或运营团队，还有24%正处于转型期——要么建立FinOps能力（16%），要么将其与ITAM合并（8%）。令人震惊的是，23%的人既没有设立FinOps团队，也没有制定近期内组建一个团队的计划。

组织已经在存在专门的FinOps能力的地方看到了可衡量的好处：

46%的人表示，ITAM的资产管理与FinOps的成本透明度相结合，帮助他们保持预算内，同时利用AI和云创新。这种配对减少了浪费，避免了影子IT，并且提供了扩展所需的财务纪律。39%的人认为，来自FinOps团队的财务洞察有助于ITAM在资产配置和资源分配方面做出更快、数据驱动的决策。这有助于更好地响应商业需求，同时保持支出与战略保持一致。33%的人表示，他们的FinOps功能确保了IT、财务、ITAM和运营部门之间的跨部门协作。这有助于消除信息孤岛，实现协同决策，补充了ITAM的管理职能。31%表示，他们的FinOps-ITAM整合使他们能够利用资产和消费数据预测未来需求并在需求之前进行优化。从反应性转变为预测性，有利于制定更多策略规划及前瞻性预算调配。



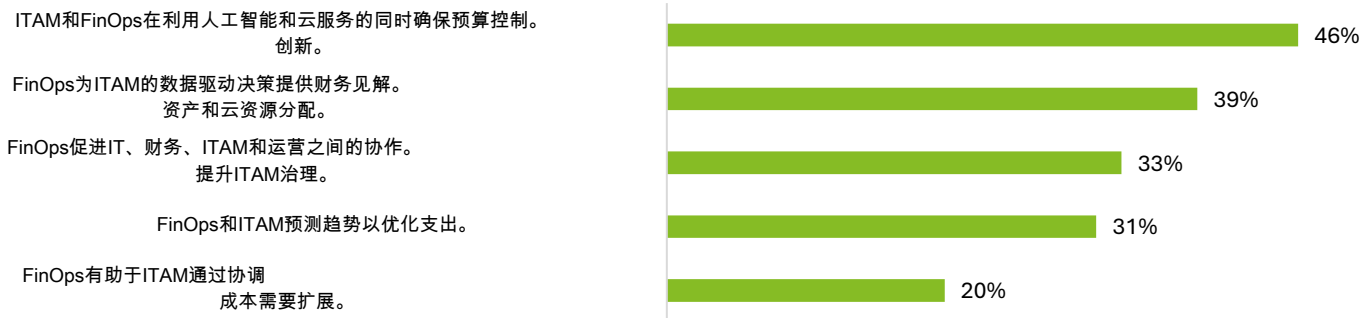
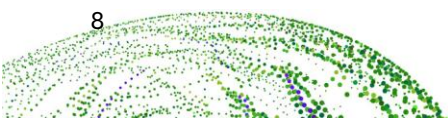


图 3：受访者利用的 ITAM 和 FinOps 团队协同效应，以实现运营和财务敏捷性

然而，尽管有这些好处，**82%的受访者承认他们的组织在ITAM和FinOps之间协同作用低或未得到充分发展。**几乎一半（41%）的人认为他们的成熟度非常差，而其他人则认为至多只是平庸。这表明存在结构和文化的障碍：所有权碎片化、缺乏共享的关键绩效指标，以及仍然将ITAM视为战术而非战略的陈旧思维模式。解决这个问题需要领导层的承诺、跨职能指标以及将财务治理与资产情报更好地整合。

总的来说，人工智能和云技术的采用不再是新兴趋势，而是基础性的转变。然而，在许多组织中，ITAM仍然在追赶。少数已经采用专注的FinOps模型的群体，已经开始通过更好的治理、成本控制和战略敏捷性获得回报。其他人则面临落后风险。

简单地来说，在今天的AI云计算环境中，有效ITAM（信息资产管理）的第一个也是最基础的关键是重新构想其角色。这不应该是一个孤立的控制功能，而是一个战略调度中心。这意味着要通过FinOps将ITAM植入到组织金融脉搏的深处。战略ITAM不能再仅仅跟踪资产；它必须引导决策。在瞬息万变的资源和指数级AI实验的世界里，只有深度集成的ITAM-FinOps方法才能提供应对不确定性的运营灵活性和财务清晰度，以充分利用创新，推动负责任的增长。





第二章：SaaS许可证从混乱到控制

关键#2：回顾过时的做法，以应对日益增长的、以改进治理和效率为核心，日益分散化的SaaS使用的复杂性。

第一章强调了FinOps在复杂云和AI环境中实现财务敏捷性的关键作用，突出了整合财务管理与资产情报的必要性。本章将重点关注将第一章提出的原则以及第四章中概述的自动化策略（尤其是关于许可证跟踪和成本优化）应用于管理日益分散的SaaS许可证的具体挑战。我们将探讨如何通过综合方法在动态的SaaS领域中实现更大的控制、成本优化和合规性。

随着SaaS在各个业务功能中的应用加速，ITAM领导者正越来越多地被拖入一个碎片化和快速变化的环境。与传统软件不同，SaaS工具通常由部门直接采购，绕过了IT和中央采购。这种去中心化，虽然提高了灵活性，但在可见性、合规性、成本优化和供应商控制方面带来了巨大的挑战。许多现有的ITAM实践和治理模式（设计用于永久许可证或企业级部署）根本无法管理现代SaaS生态系统的动态、订阅驱动的特性。

解决与去中心化SaaS使用相关的治理和效率挑战的第一步是了解组织目前如何管理和跨部门、运营单位分配SaaS许可。**我们的调查揭示了SaaS管理方法的显著差异，这对确保更好的治理和控制，以及更有效的成本管理具有重要意义。**

- 只有34%的受访者通过ITAM或采购团队集中管理SaaS许可。
- 18%允许各部门或应用所有者以完全分散的方式管理自己的SaaS工具。
- 剩下的48%采取了混合方法，只有最关键的SaaS应用程序才由集中管理和监管。

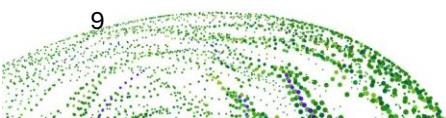




图4：跨业务单元或部门管理SaaS许可的方法

这种部分去中心化的模型在“关键”的定义上引入了主观性，导致政策和管理措施执行的不一致。它们还常常导致责任分散，没有单一团队拥有完整的SaaS领域，以及不统一的报告，这破坏了决策和许可优化。

受访者指出，以下是一些源于SaaS许可证管理部分或全面去中心化的关键挑战：

- **崛起的影子IT和未经授权的SaaS购买 (69%的受访者)**：这引发了人们对安全的担忧，特别是关于数据隐私和冗余，尤其是当采购发生在未经批准的渠道之外时。
- **缺乏对许可证、使用情况和消费情况的可见性 (66%)**：在没有使用智能的情况下，组织可能会为未使用的订阅支付过高的费用，或者未能检测到冗余的工具。缺乏可见性不仅限于简单的许可证数量；还包括与身份和访问管理 (IAM) 系统的缺乏整合。没有这种整合，ITAM 缺乏理解为什么某些SaaS应用程序被使用的上下文，可能错过未经授权访问或资源配置低效的情况。ITAM和IAM团队之间的紧密合作，允许ITAM向IAM标记异常消费模式进行调查，对于有效的SaaS治理至关重要。
- **挑战在于优化SaaS成本 (57%) 和增长中的合规风险 (54%)**：

当没有清晰的实际使用模式、许可重叠或冗余订阅导致过度配置、利用率不足和浪费时，成本优化挑战就会产生。另一方面，合规风险可能包括违反订阅条款、意外过度订阅或违反地理或用户基于的许可限制。
- **低效的供应商管理 (37%)**：分散式许可导致谈判碎片化、合同条款不一致，并错失企业全范围批量折扣的机会。

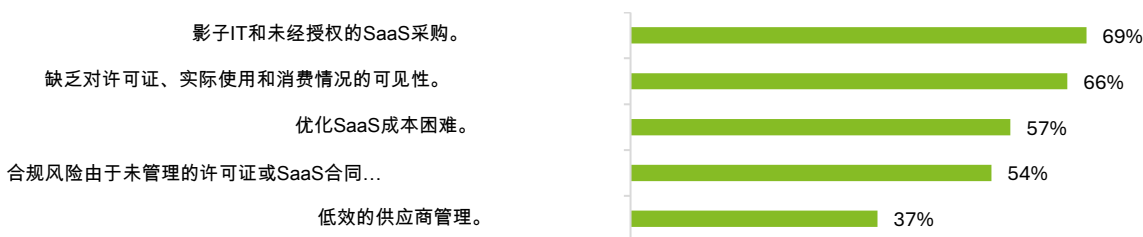
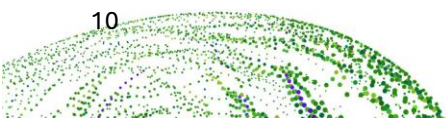


图5：SaaS许可管理部分或完全去中心化所引发的关键挑战





在这个背景下，我们的调查还揭示了受访者如何采用各种策略从被动应对式灭火转变为更加结构化的SaaS治理。

- **33%的人认为应该将FinOps-ITAM合作扩展到云成本管理之外，包括SaaS、PaaS和IaaS。** 我们认为这是合理的演变，有助于更全面、更整合地看待数字消费。像云一样，SaaS从协调的财务管理、使用可见性和协作监督中受益。

- **31% 专注于实施或增强集中式SaaS管理工具，包括仪表板和近乎实时报告。** 这是一个重要的基础步骤。组织可以利用诸如SaaS发现平台、许可证优化引擎或集成配置管理数据库（CMDB）等工具，统一跨部门数据，推动更智能、符合政策的决策。

- **23%的企业正在建立SaaS购买的应用程序组合管理和更清晰的审批流程。** 这包括预批准的供应商名单、基于角色的访问授权或自动审批层级。所有这些都助于控制无序采购并加强问责制。

- **一个更小的受访者子集报告了采取快速修复措施，例如对员工进行SaaS政策合规培训（7%）或与关键供应商协商企业级许可条款（5%）。** 虽然这些措施实用且易于实施，但它们只是“啃边角”，短期内提高意识或控制成本，而没有解决去中心化扩张的结构性根源。鉴于这些挑战的规模和持久性，显然临时修复是不够的。我们必须将重点转向现代化治理框架、流程和工具，以管理SaaS的生命周期。

解决去中心化SaaS许可的挑战因此需要一种全面的方法。通过整合FinOps（第一章）的财务治理原则、自动化（第四章）的效率提升，特别是在许可跟踪和成本分析方面，以及强大的SaaS管理策略，组织可以实现对影子IT的更大控制、减少SaaS蔓延、提高成本可见性以及改善合规性。这种综合方法对于应对现代SaaS生态系统的复杂性以及确保负责任的数字增长至关重要。

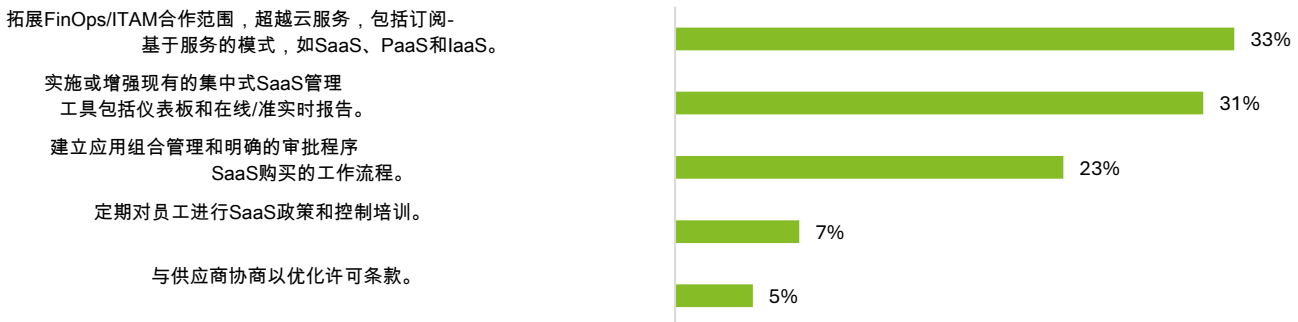
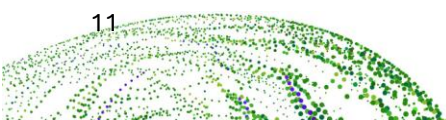


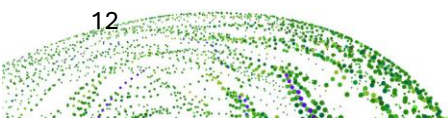
图1：管理SaaS复杂性的最有效策略





总的来说，SaaS 许可证已成为许多组织中的一个主要治理盲点，由分散的采购、缺乏使用洞察力和薄弱的政策执行所推动。后果从成本效率低下到安全和合规风险不等。从混乱走向控制需要明确的转变：将IT资产管理与金融运营联盟扩展至SaaS领域，投资共享可见性工具，执行结构化工作流程，逐步淘汰不再适应当今敏捷数字化运营的旧有做法。

这次成功的关键提醒我们，在今天以人工智能和云技术为驱动力的世界中，成功不仅仅是成本控制——它还需要治理灵活性。通过重新审视过时的SaaS管理模式，并将治理融入SaaS生命周期的每个阶段，组织可以恢复控制权，降低风险，并实现更智能的数字化选择。





第三章：ITAM在合规监管方面的网络安全优势

关键#3：利用ITAM作为解锁日益监管的数字生态系统中网络安全弹性之钥

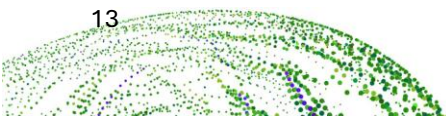
随着组织面临日益增长的网络安全威胁和监管义务，信息技术资产管理（ITAM）很可能获得更高的战略地位。在精明的组织中，ITAM不再仅仅是追踪硬件或软件，它在实现数字韧性、确保数据和基础设施的可追溯性以及支持合规方面发挥着至关重要的作用。ITAM是网络韧性和监管合规的根本支柱，这一作用在众多法规的显性和隐性存在中得到了强调。

这一转变是由来自欧盟数字运营韧性法案（DORA）、NIS2指令、欧盟人工智能法案（正在逐步实施）、加拿大OFSI B-13以及美国监管机构日益严格的审查等框架和规定的不断压力所推动的。随着网络风险的加剧和问责制从CISO扩展到董事会，ITAM继续成为在高度监管的数字生态系统中实现安全、合规运营的关键推动者。

然而，令人惊讶的是，在我们的调查中，仅有29%的组织报告称ITAM被正式纳入其网络安全策略中。如果不是令人担忧的话。

在48%的组织中，ITAM与网络安全职能之间存在一定程度的互动，有相当大的提升协作的空间。在23%的情况下，ITAM完全独立于网络安全运作。

这割裂信号着错失的机会 网络安全计划通常依赖于最新的资产清单、配置数据和软件谱系。所有这些通常都由ITAM负责。如果没有协调一致，安全团队在打补丁、事件响应或漏洞扫描时将存在盲点。整合ITAM和网络安全可以共享关键资产的可视性，加快威胁遏制，并支持最小干扰下的持续合规。这还可能致未能利用ITAM的资产数据来提升安全状态和合规性。软件物料清单（SBOMs）在监管合规性中日益重要的地位进一步强调了更紧密协作的需要。





鼓舞人心的是，ITAM在恢复力规划和执行中的作用正

更稳固的立足点 62%的受访组织表示ITAM积极参与其中，而38%则表示没有。这种日益增长的关注反映了一种认识，即韧性不仅仅建立在防火墙和备份上，还在于了解你所拥有的资产、它们如何连接以及你的风险所在。通过利用ITAM的资产情报，组织可以提高业务连续性，缩短响应时间，并满足运营准备性的监管期望。

在那些涉及ITAM在恢复力工作中的应用组织中：

- 47%的人使用ITAM在如网络攻击或停电等中断期间提供可信的关键资产清单。
- 30%的人依赖ITAM来映射依赖关系和配置，以实现更快的恢复；
- 22%的人利用ITAM来证明符合关于运营弹性的法律和监管要求。



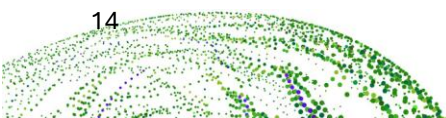
图7：ITAM项目在危机期间对数字韧性的贡献

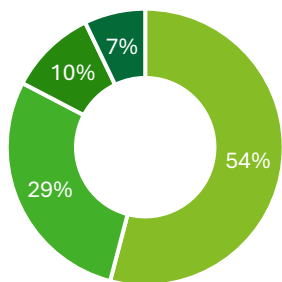
81%的受访者认为遵守新的数字法规是改善ITAM实践的机会。 在这些中，33%的人认为这是一个重大机遇，而48%的人看到了一些机遇。

这表明人们对DORA、NIS2和AIAct等法规如何成为加强ITAM（信息技术资产管理）成熟的催化剂有了日益增进的认识。随着符合性要求提高，ITAM提供准确、可审计的资产信息的能力将成为一个机构证明其弹性状况（而不仅仅是宣扬）的关键。

然而，关于开源软件的准备情况仍然是一个盲点。

- 只有17%的受访者拥有专门的开放源代码计划办公室（OSPO）或等效框架。仅有7%将该功能与公认的标准化组织如ISO/IEC 5230和18974保持一致，而剩余的10%则在没有任何正式框架的情况下运营。
- 同时，54%的组织继续在ITAM或运营团队内管理开源软件（FOSS），29%表示没有明确管理它的计划。





- 不，我们在现有的ITAM或运营团队中管理免费和开源软件 (FOSS)。
- 不，我们目前没有计划专门解决自由开源软件 (FOSS) 的问题。
- 是的，我们有一个专门的开放源代码项目办公室，而不专注于特定标准。
- 是的，我们有一个专门的开放式源码项目办公室。这是遵循各自的ISO/IEC标准框架 (ISO/IEC 5230和18974)。

图8：为开源软件组件管理许可证和安全性风险而设的专用自由和开源团队与框架

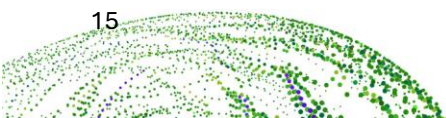
考虑到开源组件在现代软件堆栈中日益重要的地位，这令人担忧。随着数字主权在当今互联世界中变得日益重要，组织必须实施正式的控制和机制来跟踪开源软件的许可，并在组件级别监控安全漏洞。通过积极管理许可风险并加强数字主权措施，组织可以更好地保障其IT资产的安全和完整。不当管理开源软件许可存在法律和声誉风险。

广泛应用于库中的漏洞，比如广为人知的Log4j，展示了如果未得到恰当管理，开源软件相关的风险如何迅速升级。数据显示，尽管对合规的意识在增强，开源软件的风险仍被低估。组织必须超越被动管理，采取正式控制、许可跟踪和针对开源软件独特性质的定制化安全补丁机制，包括将应用程序分解为其个别组件，并运行适当的安全物料清单 (SBOM) 管理流程，以保护其资产。

随着数字监管的加强和网络安全成为董事会层面的重点，ITAM不再是可选项，而是不可或缺的。

关键词3呼吁转变思维模式：ITAM必须不只是作为一个运营职能进行重新定位，而且还应作为网络韧性基础和合规准备的基础支柱。

积极将ITAM与网络安全、弹性规划和开源风险管理相结合的组织，将更好地应对复杂且不断演变的数字风险领域。





第四章：智能化洞察以实现更优结果（运用智能自动化进行ITAM）

关键#4：利用ITAM智能自动化日益增长的机会，同时应对许可管理中的复杂性和不确定性。

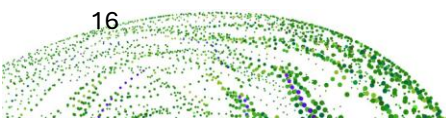
对“更智能的见解以获得更好的成果”的渴望反映了ITAM的战略转变：从被动报告转向智能、数据驱动的决策。本章重点探讨智能自动化（由人工智能、机器学习和通用人工智能推动）如何实现这一转变。随着许可环境变得更加复杂，云平台更加多样化，领先的组织正在采用自动化，不仅是为了扩大运营规模，而且是为了在整个资产生命周期中做出更智能、更快的决策。

精明的组织现在正超越传统的库存和合规任务，将自动化视为增强韧性、效率和前瞻性的杠杆。这包括在混合资产中自动跟踪许可证，生成预测性续签警报，触发工作流程。最终，这是关于最大限度地发挥数据的作用：自动化数据的收集、分析和采取行动，以实现更严格的控制和更强劲的表现。

随着云计算的加速采用，这一紧迫性比以往任何时候都更加紧迫。我们的调查捕捉到了组织是如何（或尚未）利用智能自动化来监控和优化他们的云支出的。

- 目前，76%的受访者未使用智能自动化至少监控其总云支出的半数。这仅剩24%的人对其51-100%的支出进行监控。
- 然而，这种情况将急剧改变：78%的人希望在接下来1-2年内使用智能自动化至少监控其云支出的半数，只有22%的人预计将低于这一门槛。

我们相信这一转变将是关键性的。借助由人工智能驱动的监控和成本优化，组织可以避免云资源浪费，动态调整许可证，检测未充分利用的权益，并模拟未来情景。同时，它还通过向各业务单元提供实时支出信号，增加了金融运营（FinOps）的协作。



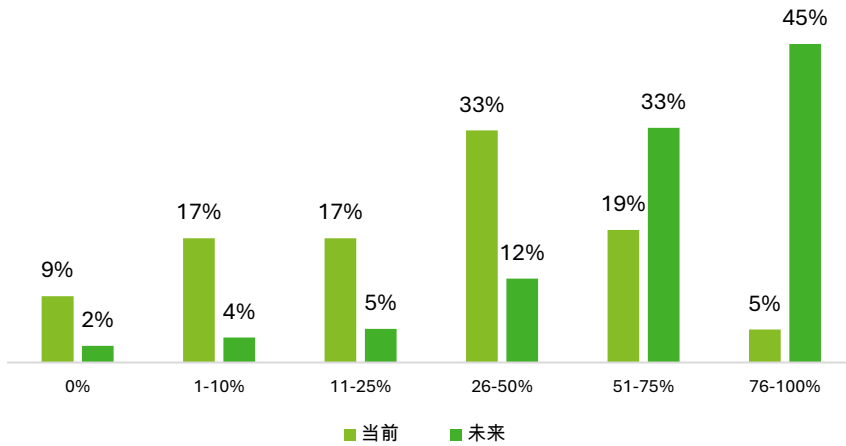
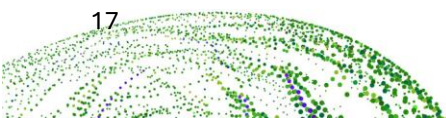


图9：智能监控总云支出的比例：当前状态和未来期望

在这个背景下，我们的调查受访者强调了智能自动化能够带来最大价值的特定领域：

- **许可证优化** 79%的人认为自动化将改善SaaS、PaaS、IaaS、本地和混合环境中的合规性跟踪、使用分析和成本控制。
- **合同与供应商管理** 60%的人认为利用人工智能评估供应商表现、自动续签和扫描合同风险具有价值。这些任务可以通过提供合同信息集中存储和自动化工作流程的现代合同生命周期管理（CLM）系统得到显著简化。
- **改进的云管理** 48%的人指出了支持实时监控、预测和FinOps对齐的AI驱动工具。
其他关键用例包括：
 - ITSM、ITAM、虚拟化（VM）和配置管理（CM）平台更好的洞察力（37%）。
 - 事件响应和预测性维护（36%）。
 - 智能生命周期优化的硬件资产管理（HAM）（34%）。

这些用例共同表明，人们越来越倾向于将人工智能和自动化更深入地嵌入到ITAM流程中。从软件到基础设施。虽然许可证优化仍然是首要任务，但像集成平台可见性和预测性运营这样的领域正在成为下一个前沿。



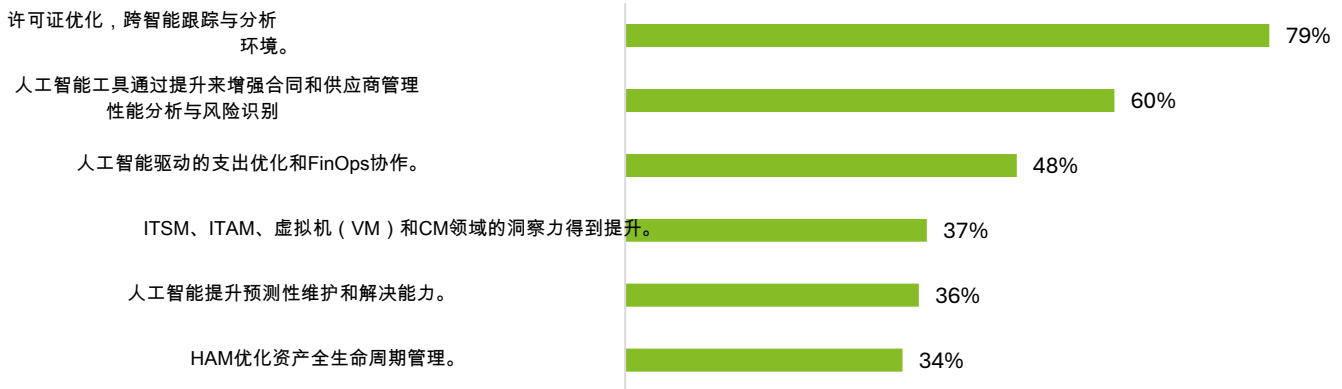


图10：智能自动化能够带来最大价值的特定区域

有趣的是，尽管云管理和HAM（人力资源管理）在整体提及中较少，但那些将其优先考虑的人认为它们对战略的影响要大得多。这可能是由于云计算和硬件属于高成本、高风险类别，而自动化可以实现可衡量的业务成果，无论是通过更智能的配置、降低生命周期成本还是更准确的预测。

尽管如此，由于几个关键挑战，智能自动化在ITAM中的实际应用仍然有限：

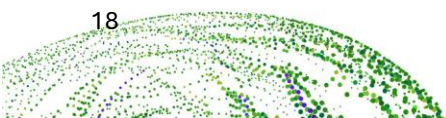
- 数据质量差和系统碎片化是最大的障碍（54%）。
- 返投资回报率不明确，其中51%的人对实际成本、合规性或风险收益缺乏清晰认识。
- 40%的人认为在自动化之前，必须首先解决基本问题，例如多云复杂性和去中心化SaaS使用。
- 对新兴技术的内部专业知识不足是37%的制约因素。
- 34%的人强调了监管的不确定性，特别是在数据隐私和网络安全方面。
- 其他阻碍因素包括：

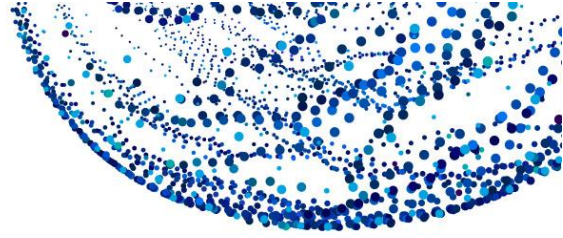
- 组织对变革的抵制。
- 供应商锁定限制了工具的灵活性。
- 与FinOps及相关团队的合作不足。

这些发现反映了科技采用中的一种常见模式：顶层有抱负，中间有摩擦。许多ITAM团队陷入日益增长的复杂性和有限的带宽之间。

为了前进，组织必须投资于数据质量，明确自动化的投资回报率，并优先考虑系统间的基础集成。教育是关键，为团队配备与人工智能工具自信互动的技能。同样重要的是跨职能协调，尤其是与财务运营、采购和云团队的合作。

智能自动化不应被视为一个插件工具，而应被视为更广泛运营模式转型的一部分。

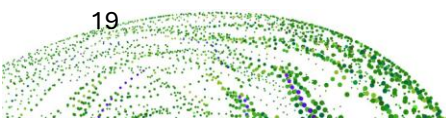




随着许可证管理的复杂性和不确定性日益增加，现在手动处理已经显得过于重要。

关键#4发出行动号召：由智能自动化驱动的更深入的洞察是实现大规模更好结果的唯一途径。

那些拥抱这一转变（优化其工具和人才）的组织，将把ITAM不仅仅定位为合规功能，更将其视为云计算和AI时代效率、灵活性和创新的战略引擎。





第五章：ITAM的愿景：有目标的技术与行动

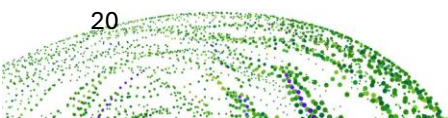
关键#5：战略性地利用技术以减少浪费，增强合规性，并支持在不断发展的技术环境中可持续发展的努力

“以目的为导向的技术”标志着领先组织在IT资产管理方法上的转变。这不仅仅是一种成本控制或合规活动，更是一种可持续性、效率和负责任技术管理的战略杠杆。

对此观点保持一致；本章探讨了组织如何利用ITAM来使技术使用与更广泛的目标相一致：**减少浪费、满足监管需求，以及支持企业级可持续性承诺。** 我们将从整体的角度，通过讨论受访者在其报告中描述的更长远的转型旅程中优先考虑的行动来结束这份报告。

那些更加具有前瞻性的组织已经开始通过采用智能工具和以数据驱动的流程来优化资产利用率，延长设备使用寿命，并确保资产得以负责任地淘汰或重新部署。但这并不仅仅是关于工具：它关乎将ITAM融入决策框架中，该框架将负责任的增长、道德的技术使用和环境影响作为优先考虑。

在这一方法的核心里，在于能够**高效、准确、规模化地利用数据的能力。** 随着对环境影响和治理的监管和利益相关者审查日益严格，跟踪和报告IT资产使用、退役及其相关排放的能力正成为董事会层面的关注点。这正是智能自动化、AI/通用AI以及端到端ITAM-金融运营（FinOps）集成发挥作用的地方。例如，通过使用AI来模拟未来的IT资产状况或同步资产记录与配置管理数据库（CMDB），组织可以在减少浪费和改善治理的同时优化成果。

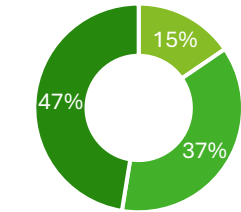




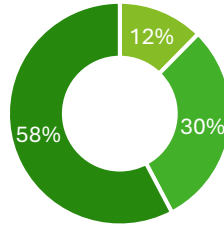
我们战略性地运用技术以优化资产管理、增强合规性并支持可持续性努力。

我们的目标是通过利用人工智能和智能自动化，提高数据准确性、优化工作流程并提供可执行洞察。

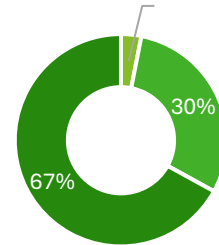
我们的方法不仅提高了效率，还与更广泛的组织目标相一致，如成本控制、风险缓解和环境保护责任。
3%



- 不同意
- 既不同意，也不同意
- 同意



- 不同意
- 既不同意，也不同意
- 同意



- 不同意
- 既不同意，也不同意
- 同意

图2：利用ITAM项目使技术应用与更广泛的组织目标相一致

- 47%的受访者表示他们已经战略性地使用技术来优化资产管理、加强合规性和支持可持续性。15%的人表示不同意，而37%的人保持中立。

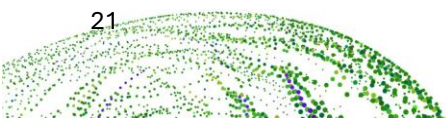
这表明近一半组织正走上正确的道路。他们正在利用ITAM产生三重影响：减少技术浪费、提高法规一致性以及实现可持续性。在实际操作中，这可以包括延长设备更新周期、确保准确的重用许可证以及将资产数据嵌入ESG报告中。展望未来，重点必须从意图转向制度化，将这些实践融入运营模式中。

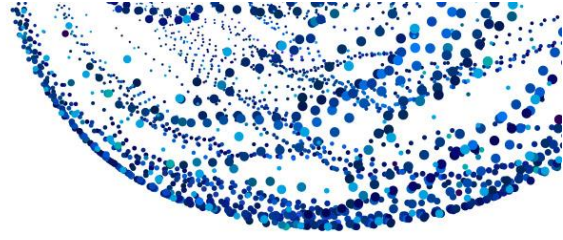
- 较高比例的受访者（58%）表示，他们的目标是利用人工智能和智能自动化来提高数据准确性、简化工作流程并提供可执行的洞见。

这种抱负令人鼓舞。它反映了对人工智能和自动化能够支持上述三项目标的信心不断增长。例如，智能许可证跟踪、在SaaS使用中的异常检测或针对节能采购决策的自动建议现在都成为了现实可能。为了使这一切成为现实，组织必须投资于推动人工智能驱动的ITAM所需的工具、流程和人员。

- 甚至更令人鼓舞的是，67%的人相信他们目前的ITAM方法现在支持更广泛的组织目标，如成本控制、风险降低和环保责任。

这标志着从孤岛式资产管理向战略一致性的转变。ITAM正成为企业ESG、风险和数字化转型议程的推动者，而不仅仅是一个后台合规职能。将ITAM融入财务规划、供应链战略和治理框架的组织将处于领先地位。

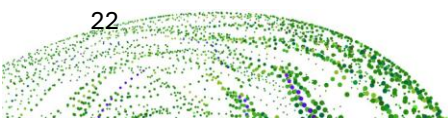




在一个可持续性、合规性和成本效益不可协商的世界里，ITAM必须成为战略力量。“有目的的技术”不仅仅是一个口号——它是一份行动号召。

关键#5突出了ITAM在帮助组织减少浪费、保持合规和支持长期可持续性方面的作用。前进的道路不仅需要智能技术，还需要更坚实的数据基础、跨职能协作以及与企业战略的一致性。

将ITAM融入其可持续性和合规议程的组织不仅能提高其资产效率，还能在未来快速变化的世界中为他们的技术决策提供保障。





哪些组织将优先考虑作为下一步的紧急行动

七个从数据中浮现出的主题

调查回应显示，组织在其转型之旅中优先考虑的行动领域形成了清晰的集群。以下就是这些主题揭示的内容：

加速人工智能和自动化 1.

机构计划继续将人工智能嵌入到许可证合规性、行政自动化和数据验证中。这是从手动核对转向智能触发，从静态表格转向动态、由人工智能驱动的洞察的过程。

数据管理和质量 2. 智能ITAM的基础是干净、及时的数据。受访者

指明了立即关注源头质量管理，明确设备使用说明，标准化数据，并实现实时库存查看。高质量的数据不仅能提高合规性和成本控制，也是自动化和ESG报告的先决条件。

集中与治理 3.

受访者表示，可见性和问责制需要立即进行结构性变革。受访者正在建立集中的ITAM所有权，实施治理计划，并在云中创建统一的视图，尤其是超大规模和开源软件平台。动态CMDB和集中的许可预算是这项工作的关键推动力。

整合与协作 4

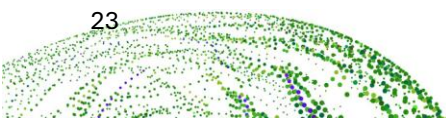
ITAM、采购和FinOps之间的合作日益变得至关重要，成为战略性资产管理的关键推动力量。组织也日益认识到打破内部隔阂、优化数据共享、过程对齐和监管的重要性。

云和授权 5

来自更为精明的组织的受访者表示，他们正直接应对多云许可证的挑战。这包括简化合同、将云和SaaS使用数据整合到一个中央存储库中，并应对由供应商推动的压力，如许可证度量标准的变化或免费软件的货币化。

成本管理与控制 6

确保成本效益在当前环境中仍然是核心优先事项。除了节约成本，受访者还希望他们的组织



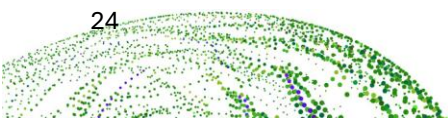


构建ITAM投资商业案例，着重关注长期和中长期价值、风险降低以及与可持续发展关联的成果。

进程优化，技能与战略整合7。

将ITAM流程标准化、培训团队、获得董事会层面的支持，以及将ITAM与战略财务和商业规划相协调，是目前议程中的首要任务。这些是提升ITAM为战略学科的基础性步骤。

我们的IT和软件资产管理领导者在报告前言中已经强调了在IT资产管理（ITAM）方面进行战略转变的迫切需要。超越简单的资产跟踪，组织现在必须关注理解其IT资产的价值、成本和战略影响。本报告探讨的五个关键领域展示了这种新战略方法的成功关键因素，将ITAM定位为效率、韧性、信任和可持续性的重要驱动因素。在人工智能和云计算快速发展的环境中，ITAM不能再仅仅是一个运营职能，而应作为一个战略性的迫切需求，引领组织走向更高效和可持续的未来。



附件

关于作者



迪德里克·范德锡普
主导合伙人 - IT & 软件资产管理 | 比利时德勤
dvandersijpe@deloitte.com

dvandersijpe@deloitte.com



汉斯·范德维耶尔
合作伙伴 - IT & 软件资产管理 | 德勤比利时
hvandewijer@deloitte.com

Dr. Sanjoy Sen
首席研究员 | 德勤英国
sanjsen@deloitte.co.uk



安德烈·库恩茨
合作伙伴 | 德勤德国
akuntze@deloitte.de



埃里克·沙利文
合作伙伴 | 德勤加拿大
ericsullivan@deloitte.ca



埃里克斯ullivan@德勤.c
丹尼尔·博塔
顾问 | 德勤比利时
dbotha@deloitte.com

Deloitte.

关于德勤

德勤指代以下一个或多个实体：德勤安永大和会计师事务所有限公司（“DTTL”），一家在英国注册的保证有限责任公司；其成员事务所网络；及其相关实体。DTTL及其每个成员事务所都是法律上独立且分开的实体。DTTL（亦称“德勤全球”）不向客户提供服务。请访问www.deloitte.com/about获取关于DTTL及其成员事务所的更详细信息。

德勤为客户提供涵盖多个行业的审计、税务和法律、咨询以及财务咨询服务。凭借在150多个国家拥有成员公司的全球网络，德勤将世界级的能力和高质量的服务带给客户，为他们提供解决最复杂商业挑战所需洞见。德勤拥有约31.2万名专业人士，他们均致力于成为卓越的标杆。

本出版物仅包含一般性信息，德勤安达信会计师事务所有限公司及其成员公司或其相关实体（统称为“德勤网络”）通过本出版物提供专业建议或服务。在做出任何可能影响您财务状况或业务的决定或采取任何行动之前，您应咨询合格的专业顾问。德勤网络中的任何实体不对任何依赖本出版物的人士遭受的任何损失负责。