



# Identity and access management managed support services

Protect your business and information assets

KPMG Managed Services



In today's digital landscape, identity and access management (IAM) is a crucial function for all organizations; get it wrong, and business-critical operations can grind to a halt. Yet, many information security teams face difficulties in adapting to the ever-evolving IAM landscape.

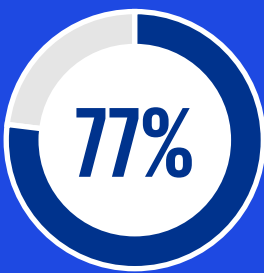
As digital transformations drive increased utilization of cloud-based services, various risks arise—such as managing sensitive data accessed from different geographic locations and multiple devices.

Additionally, the need to consistently apply security patches and upgrades to tackle potential vulnerabilities poses a significant challenge.

Simultaneously, cyber leaders must contend with priorities such as heightened user experience expectations, process excellence demands, cost reduction pressures, data breach risks, stricter regulatory compliance, skilled talent scarcity, and mounting IAM complexity.

Forward-looking companies are making managed services part of their playbook.

They're working with providers who bring a broad-ranging approach—from consulting on strategy to implementation, ongoing enforcement, continuous monitoring and ongoing evolution of their capabilities.



77% of tech executives report that their cybersecurity teams are **behind schedule** in responding to these challenges<sup>1</sup>

As finding and retaining cost-effective, skilled talent becomes more challenging, IAM resources are increasingly burdened by day-to-day risk management and operational issues—inhibiting their capacity to engage in innovative, strategic improvements for mission-critical business processes.

<sup>1</sup>Source: KPMG Global Tech Report, KPMG International, 2023

## Potential benefits



Skilled, global resources



Reduced risk



Lower, predictable costs



Compliance enablement



Ongoing support



Agile capabilities

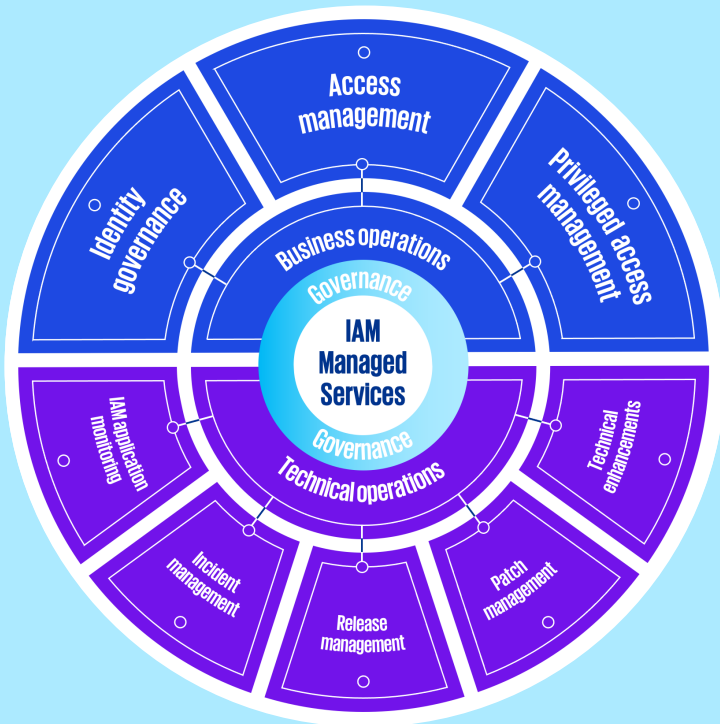
## Why KPMG?

KPMG identity and access management managed support services are designed to enable you to continuously evolve and drive business value from your IAM solution by providing day-to-day business and technical operations.

These KPMG subscription-based services combine advanced technologies with the deep knowledge of experienced resources to standardize your IAM processes through a proprietary methodology—which is designed to reduce risks and help ensure your IAM issues are addressed consistently, efficiently, and cost-effectively.

With a global network of 16 delivery centers and 6,000+ global cyber specialists, KPMG firms have the scale, experience, and resource to help you deliver on your IAM goals.

**KPMG managed services for IAM focus on delivering outcome-based results for business and technical operations that help build resilience and trust.**



**We provide a single point of contact for all aspects of your IAM program:**

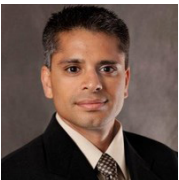
### IAM business operations

Continuous management and tracking of business processes, such as executing access review campaigns for SOX or access management for adding/removing access to applications.

### IAM technical operations

Day-to-day management of the health of the IAM solution such as application monitoring, data feed integrations, application administration and patching, and incident management.

## Contact us.



**Raj Ahuja,**  
Managing Director,  
Cyber Managed Services  
T: 602-321-8026  
E: [rajeshahuja@kpmg.com](mailto:rajeshahuja@kpmg.com)

Learn more about us:  [kpmg.com](https://www.kpmg.com)

Some or all of the services described herein may not be permissible for KPMG audit clients and their affiliates or related entities.

The information contained herein is of a general nature and is not intended to address the circumstances of any particular individual or entity. Although we endeavor to provide accurate and timely information, there can be no guarantee that such information is accurate as of the date it is received or that it will continue to be accurate in the future. No one should act upon such information without appropriate professional advice after a thorough examination of the particular situation.

© 2024 KPMG LLP, a Delaware limited liability partnership and a member firm of the KPMG global organization of independent member firms affiliated with KPMG International Limited, a private English company limited by guarantee. All rights reserved.

The KPMG name and logo are trademarks used under license by the independent member firms of the KPMG global organization.