



IT ADVISORY SERVICES

Identity and Access Management

ADVISORY

Introduction

As the use of Internet and intranet technologies expands, businesses face the realities of managing user identities. Emerging regulatory pressures such as the Health Insurance Portability and Accountability Act (HIPAA), the Gramm-Leach-Bliley Act (GLB), FERC, Basel II and Sarbanes-Oxley call for organizations to keep tabs on those with access to corporate data. Whether employees, external users, business partners, or suppliers, these user identities, if not managed and maintained by secure and efficient systems, can put your organization at risk. KPMG's Enterprise Identity Management services help organizations collect the identities in use, develop a strategic approach to consolidating and managing them, and implement the processes and systems needed to maintain them.

How can we help?

KPMG's Identity and Access Management (IAM) services help organizations create a strategic approach to identity management by helping to develop the necessary business processes to efficiently manage identities and access to information. Additionally, IAM services design and build the systems required to support the business processes. Potential benefits of KPMG's IAM services include:

- Greater use from your current identity management processes and systems
- Increased security through ability to enforce corporate security policies across multiple platforms
- Stronger authentication and managed access to sensitive information
- Reduced application development costs and times by providing access and user management as a common service

- Lower help desk costs by providing self-service functions to users
- Faster time-to-market for new applications and services

Focused IAM Services

Any organization whose interaction with customers and business partners relies on Web-based or Internet technology, and who is concerned with business, technology, operational, financial, or regulatory risks, understands the importance of identity management. Businesses facing regulatory controls or privacy issues recognize the need for having systems that balance regulatory reporting requirements with identity privacy protections. KPMG's IAM services are designed to help clients respond to the needs and demands of today's rapidly evolving technology, compliance environment, and ever-present identity risks.

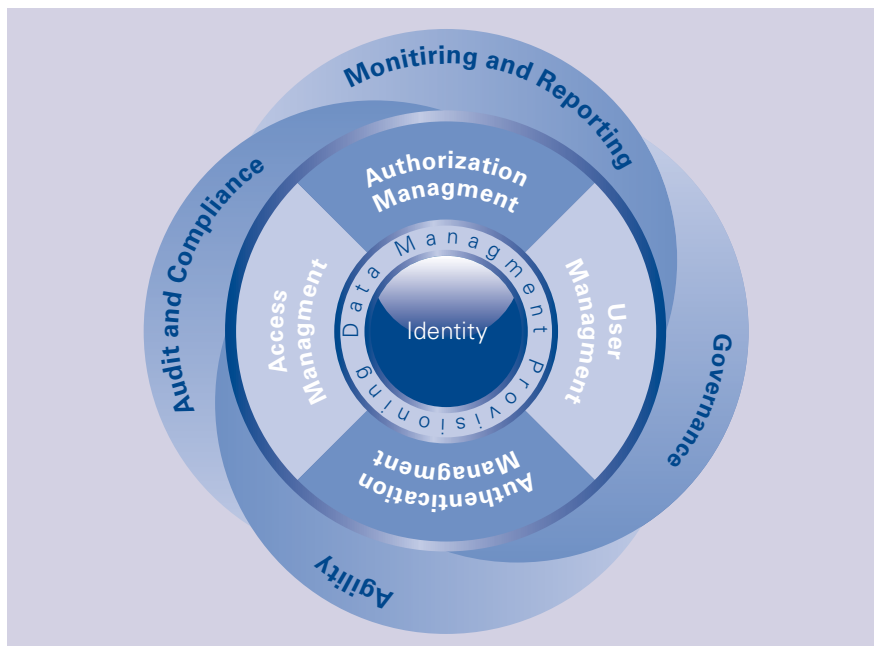
KPMG's Approach

KPMG customizes our approach to suit your needs. Critical success factors for IAM engagements include:

- The depth of industry knowledge and technical experience we bring to our advisory services
- Our ability to team with management, implementation professionals, and internal audit personnel
- Our consistent, modular, and easy-to-use methodology
- Our focus on knowledge transfer
- Vendor neutrality

Our approach helps ensure minimal disturbance of in-house resources and encourages the support and confidence of senior management.

KPMG's IAM Methodology



business strategy to help meet your specific identity management requirements.

This process follows the ACE principle: automate low-value procedures, consolidate redundant technologies, and eliminate ineffective systems and processes to help determine and realize a realistic return on investment. KPMG can help implement the IAM technology infrastructure with a focus on knowledge transfer to your team. From assessment of your current identity management position, to development of a strategy, to implementation of necessary processes and systems, our full cycle of IAM services represents a valuable investment in security and efficiency.

How We View IAM

KPMG views IAM as the combination of processes and technologies required to support Enterprise Access Management (EAM), Enterprise Directory Services (EDS), and Enterprise User Management (EUM). EAM systems govern access to enterprise resources (e.g., Web pages, applications, etc.). EDS integrates existing and future data stores to assist in more efficient use while reducing the costs associated with maintaining data in multiple locations. EUM systems help enable the provisioning of users throughout an enterprise network by populating directories and other data stores with appropriate user account information. By combining all three processes and technologies under one comprehensive strategy, organizations are better able to achieve a greater return on investment.

IAM Services

Our services consist of three areas: IAM Baseline Assessment Services, IAM Architecture Services, and IAM Implementation Services. Each of these service offerings focuses not only on the technology structure that makes up identity management but, more importantly, on the foundational processes underpinning how identity is managed in the organization. KPMG can assess your organization's current identity management initiatives and opportunities. Through interviews, documentation reviews, and evaluation of your application and network infrastructures, we can provide an analysis of your current IAM capabilities with a scorecard rating of your IAM systems and a strategic vision of where your focus should be. Our IAM Architecture and Implementation services focus on helping to develop and deliver a technology and process framework aligned with your organization's

KPMG's Vendor-Neutral Position

Our IAM services distinguish us from providers of identity management services who are tied to specific vendor loyalties. Unlike those who are focused on implementation of individual components of an overall architecture and who are limited on product independence due to their vendor alliances, KPMG takes a vendor-neutral approach to your current IAM activities.

Phase	High-level objectives	Stage overview	Potential outputs
Plan 1.0	<ul style="list-style-type: none"> Gain an understanding and agreement with the client regarding the scope and objectives of the IAM engagement 	Prepare engagement approach with team → Engagement kickoff	<ul style="list-style-type: none"> Kick off agenda and presentation Engagement letter Stakeholder matrix Risk/issue register
Insight 2.0	<ul style="list-style-type: none"> Identify the need to change in the clients' IAM 	Document current state (2.1) → Envision future state (2.2) → Conduct gap analysis (2.3)	<ul style="list-style-type: none"> Prepared by client list Document current state assessment report Document client vision Document gaps and recommendations
Design 3.0	<ul style="list-style-type: none"> Design the foundation for IAM program execution 	Develop future state strategy and road map (3.1) → Develop IAM business case (3.2) → Assist client to design PMO and IAM governance (3.3)	<ul style="list-style-type: none"> Future state strategy and road map document Client IAM business case Conceptual architecture design PMO and governance structure plan
Implement 4.0	<ul style="list-style-type: none"> Begin executing the IAM program in a controlled and staged manner 	Assist client to establish PMO (4.1) → Detail design of IAM roadmap plateau (4.2) → Assist client with solution selection (4.3)	<ul style="list-style-type: none"> System selection methodology deliverables Proof of concept toolkit Deployment toolkit
		Assist client with Data Management (4.4) → Assist client to pilot IAM solution (4.5) → Assist client with deploying IAM roadmap plateau (4.6)	
Monitor 5.0	<ul style="list-style-type: none"> Conduct post implementation assessment Track benefits realization 	Conduct post-implementation review (5.1) → Audit client IAM program (5.2) → Assist client to remediate & optimize program (5.3)	<ul style="list-style-type: none"> Audit program guide/report Benefits realization report Remediation or optimization plan Quality assurance checkpoint or definition



Contact us

This approach allows KPMG to remain objective when working with clients during the assessment and design phase to help determine which product best meets their specific business needs and technical environment. We have the experience of having worked on more than 50 IAM programs and have built a strong understanding of the evolving strengths and weaknesses of IAM vendor capabilities. We have strong relationships with key vendors of IAM solutions and hands-on experience implementing their products:

BMC, CA™, HP®, IBM®, Microsoft®, Novell®, Oracle®, Siemens, Sun®

The Next Step

KPMG's Information Risk Management (IRM) services focus on the business risks inherent in the deployment and use of technology systems used to support our clients' business objectives. These services are delivered to enterprise business technology stakeholders, including executive, operational, and technology management leadership. Our team of highly skilled IRM professionals has the knowledge and experience to help clients manage business information and technology risk and provide them with the information they need to meet their strategic and financial goals. Let us help your organization.

KPMG Tanácsadó Kft.

1139 Budapest
Váci út 99.

Tamás Gaidosch, Partner

Tel.: +(36) 1 887 7139
E-mail: tamas.gaidosch@kpmg.hu

György Sallai, Senior Manager

Tel.: +(36) 1 887 6620
E-mail: gyorgy.sallai@kpmg.hu

For more information, e-mail us at assuranceservices@kpmg.com

Or visit our Web site at www.us.kpmg.com/ras.

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 on such information without appropriate professional advice after a thorough examination of the particular situation.

KPMG and the KPMG logo are registered trademarks of KPMG International, a Swiss cooperative.

© 2008 KPMG Tanácsadó Kft., a Hungarian limited liability company and a member firm of the KPMG network of independent member firms affiliated with KPMG International, a Swiss cooperative. All rights reserved. Printed in Hungary.