KPMG and SailPoint Alliance

Transform your information security with wide-ranging identity and access management

Cyber attacks threaten organizations every day. A single breach can result in intellectual property loss, reputational damage, financial penalties, wasted time, and administrative cost. From the C-suite through the Information Technology (IT) department, managers are expected to protect data and systems from accidental leakage and deliberate cyber attacks.

KPMG LLP (KPMG) and SailPoint can work with your company to build a customized cyber strategy that provides informed threat intelligence and alignment with your threat exposure comfort level, creating a balance of data protection and data accessibility needed for business growth.

Challenges of identity and access management

Identity and access management (IAM) is critical to an effective security strategy, but a constantly changing environment of users and applications challenges IT departments.

On the human side, different types of users need different levels of access—ranging from full information to a small subset of the data. In all cases, there must be appropriate segregation of duties (SoD) to protect your company and ensure compliance. Additionally, changes in the employee life cycle cause people to leave, join, or move. Often, there are no effective processes in place to update or remove access when these events occur. Finally, you must manage access for an expanding portfolio of digital identities, such as customers, contractors, partners, and suppliers.

On the technology side, you face a growing number of systems, applications, services, and data. The expanding use of mobile, cloud, and Web-based technologies increases the complexities of managing user identities.

KPMG

KPMG's Identity Access Management teams work across industries to help clients conceptualize, design, implement, measure, and improve their information security programs. KPMG's 2014 acquisition of certain assets of Qubera Solutions—a leading provider of IAM strategy and deployment services and SailPoint's 2014 Global Partner of the Year and 2013 Americas Partner of the Year—strengthened KPMG's ability to help companies safeguard their organizations' most valuable information assets and maintain sustainable business operations. The transaction extends several of KPMG's current large-scale market offerings in IT security and transformation, and makes KPMG a top deployment partner for SailPoint solutions.

KPMG can help clients safeguard valuable information and effectively address:

- IAM strategy
- Identity controls and governance
- Cloud identity
- Identity assurance
- Privileged access management
- IAM implementation transformation.

SailPoint

Positioned as a leader in the 2014 and 2013 Gartner Identity Governance and Administration Magic Quadrant reports, SailPoint delivers a solution that integrates access provisioning and compliance management under a single identity governance framework. Its flagship product, IdentityQ, delivers access to applications and information that business users need, when they need it, from wherever they need it—while at the same time helping to ensure enterprise security policies are consistently enforced. It helps satisfy audit and compliance requirements by providing transparency and proof of strong controls.

Why KPMG and SailPoint

Together, KPMG's Identity Access Management services and SailPoint technology provide a broad business-centric transformation program that leverages leading IAM technologies and tested information security practices to help minimize risk, address compliance requirements, enhance user experiences, streamline business processes controls, and help optimize user administration operations. Led by KPMG's highly skilled and experienced professionals, the companies have worked on many joint engagements and achieved multiple successes in the marketplace. With the combined knowledge and technology, you can increase efficiencies and drive down costs, while simultaneously enhancing your customers' experiences to expand revenue opportunities.

By 2018, 30 percent of organizations will have replaced more than 50 percent of manual access certification and request approvals by automated intelligent policies driven by analytics.

Source: Gartner, Magic Quadrant for Identity Governance and Administration, January 12, 2015.

Service delivery

KPMG professionals can help you transform your information security policy to streamline compliance reporting, access provisioning, and password management.

Compliance reporting

In highly regulated industries such as financial services, oil and energy, and healthcare and life sciences, your company must be compliant with current regulatory requirements and industry practices. To do this, you should be able to:

- Scan for inappropriate access and entitlements with real-time risk scoring
- Identify when and to whom system access is granted
- Define and enforce comprehensive access policy across the enterprise.

KPMG can help you align the security organization's capabilities with corporate objectives and governance structures, and automate compliance reporting with business-friendly processes. KPMG's effective access certification processes also match a user's access privileges to the requirements of the job function and help ensure enforcement of business policies and SoD. IdentityQ's certification technology tracks and reports on the status of certifications by individual, application, and organizational group. With a single view into identity access, you will know who has access to what information.

Access provisioning

You need to improve operational efficiency by automating access provisioning and allowing for self-service access requests. KPMG and SailPoint can help implement processes that manage changes to user access—including self-service access requests, password changes, and resets. Employing automatic, event-driven changes can help you manage workforce churn and the resulting impact to identities and access privileges. By integrating IdentityQ with human resource systems and corporate directories, KPMG can help you:

- Securely manage identity for life cycle events such as hires, transfers, or terminations
- Implement role-based access controls, including defining business and IT roles
- Execute role mining
- Consolidate access and application entitlements.

Password management

Your help desk is inundated with calls to reset passwords so you need to empower users to request access and reset passwords independently. KPMG can leverage the capabilities of IdentityQ to:

- Implement self-service password reset
- Enable delegated password management by managers and administrators
- Automatically detect and synchronize passwords
- Enforce strong password policies.

In addition, business users will be able to reset passwords and unlock accounts with their mobile devices, enhancing their productivity and reducing downtime.

The potential benefits of KPMG's security transformation service offerings include:

- Gain a single view of users, accounts, and entitlements across all applications
- Improve identity controls by quickly locating access risk areas
- Simplify user access administration with role-based access
- Provide proof of compliance to audit teams
- Mitigate risk through detection and prevention of inappropriate access
- Unify and centralize access certifications across data center, cloud, and mobile systems.

Strategy	Road map	Design	Implement	Monitor
— Assess and analyze the current state. — Identify quick wins.	— Outline a target identity transformation model. — Inventory user accounts and applications.	— Design an identity operating model and architecture. — Rationalize user accounts, access, and permissions.	— Build the identity operating model and put it into production. — Install the identity management software and processes.	— Monitor identity operations and solution performance. — Continuously improve the identity and access solution. — Maintain systems.

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

Contacts

For more information on KPMG's Information Protection services and strategic alliance with SailPoint, please contact:

Jim Wilhelm
Managing Director, Advisory
T: 267-256-7271
E: jameswilhelm@kpmg.com

Debbie Patterson
Alliance Director
T: 512-423-6150
E: deborahpatterson@kpmg.com

kpmg.com/socialmedia

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.