How do I know that my users only have the “appropriate level” of access? Am I comfortable that the accounts of leavers are disabled in a timely manner? Am I comfortable that system access is clearly segregated? How am I managing internal, external and customer identities? How do I demonstrate to the regulators and auditors that at all times, I am in control of who has access to systems?

Increasingly organizations are challenged to manage the risk and optimize the opportunity surrounding the digital economy. On the one hand, they need to build technology systems to protect information assets against the threats of cyber security and to control access. On the other, they are being driven by consumer expectations to open the business and encourage access in order to improve customer experience and generate new business. Identity management underpins both of these opposing forces. Managing access to your information assets can help protect your organization’s value and reputation, and avoid regulatory pitfalls.

KPMG provides services around the planning, design, delivery and support of comprehensive enterprise, consumer and citizen Identity and Access Management (IAM) programs to help you mitigate risk, improve compliance and prosper in the digital economy. Innovation and rapidly changing market conditions have caused a shift to “best of breed” software products, disrupting the older model of a single vendor IAM suite and the level of assurance promised through a one-supplier relationship. Beyond technology, our clients benefit from the wealth of management consulting and industry experience across KPMG as IAM is a confluence of technology, people and process.

Major drivers for IAM investments

**Risk Management**
- Detective and preventative policy enforcement
- Discovery and remediation of Rogue/Orphan/Privileged Accounts
- Mitigation of risks associated with BYOD, Cloud and SaaS adoption

**Mergers, Acquisitions & Divestitures**
- Improve access and reduce risk during times of high staff churn

**Digital Transformation**
- Improved customer experience
- Security, preference and privacy management

**Regulatory Compliance**
- 360° view of user access and activity
- Compliance-driven reporting and user access certifications
- Protection of sensitive information assets

**Operational Efficiency**
- Automated provisioning and password management capabilities
- Closed-loop attestation and remediation
- Streamlined identity lifecycle processes (i.e. joiners, movers, leavers)

**Cloud**
- Access governance of cloud resources

**Mobility**
- Increase productivity and accessibility
- Support BYO and CYO initiatives
- Device independent, single user view

**Major Drivers for IAM Investments**

Identity & Access Management November 2016
KPMG Identity & Access Management Consulting Services

KPMG’s well-established consulting capabilities can help avoid the pitfalls common to IAM programs, positioning clients for success from strategy through to operations. We provide comprehensive guidance as well as broad array of tools, accelerators and templates that our practitioners leverage in delivering IAM programs. Our SailPoint and CyberArk alliances combine exceptional technology platforms with KPMG’s transformation and implementation capabilities.

Why KPMG?

• KPMG combines deep solution insight with true vendor independence. We create solutions that mitigate risk and meet regulatory requirements while reducing time-to-market, effort and cost.
• KPMG’s Identity & Access Management (IAM) methodology offers a comprehensive approach to delivering value with IAM that is focused on business transformation.
• We can help establish a well-organized and high quality IAM program by aligning your requirements with the stages of our IAM methodology (Plan – Insight – Design – Implement – Monitor).

Services

IAM 5-Day Current State Health Check

• Privileged Access Assessment: Discovery & audit tool based service to determine the status of privileged account management within the organization
• Unstructured Data Risk Assessment: Tool based service to identify potential data loss risks within the organization

IAM Strategy

• Program health checks
• Roadmap development
• Vendor assessments/selection
• Operating Model
• Service management strategy
• Program governance

IAM Transformation

• Architecture & solution design
• Process design (JML, SOD, Roles)
• Identity data governance
• IAM & PAM solution deployment
• Program & change management
• Data access governance

IAM Managed Process

• Segregation of duties
• Role/Attribute based controls
• Access governance

Contact

KPMG AG
Badenerstrasse 172
PO Box
CH-8036 Zurich

Matthias Bossardt
Partner
Cyber Security

Roman Haltinner
Director
Cyber Security

Preksha Sudhakar
Manager
Cyber Security

+41 58 249 36 98
mbossardt@kpmg.com

+41 58 249 42 56
rhaltinner@kpmg.com

+41 58 249 48 76
psudhakar@kpmg.com

kpmg.ch/cyber

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. The scope of any potential collaboration with audit clients is defined by regulatory requirements governing auditor independence.

©2016 KPMG AG is a subsidiary of KPMG Holding AG, which is a member of the KPMG network of independent firms affiliated with KPMG International Cooperative (“KPMG International”), a Swiss legal entity. All rights reserved.

Identity & Access Management November 2016