KPMG

Privileged Access Management

Cyber Security

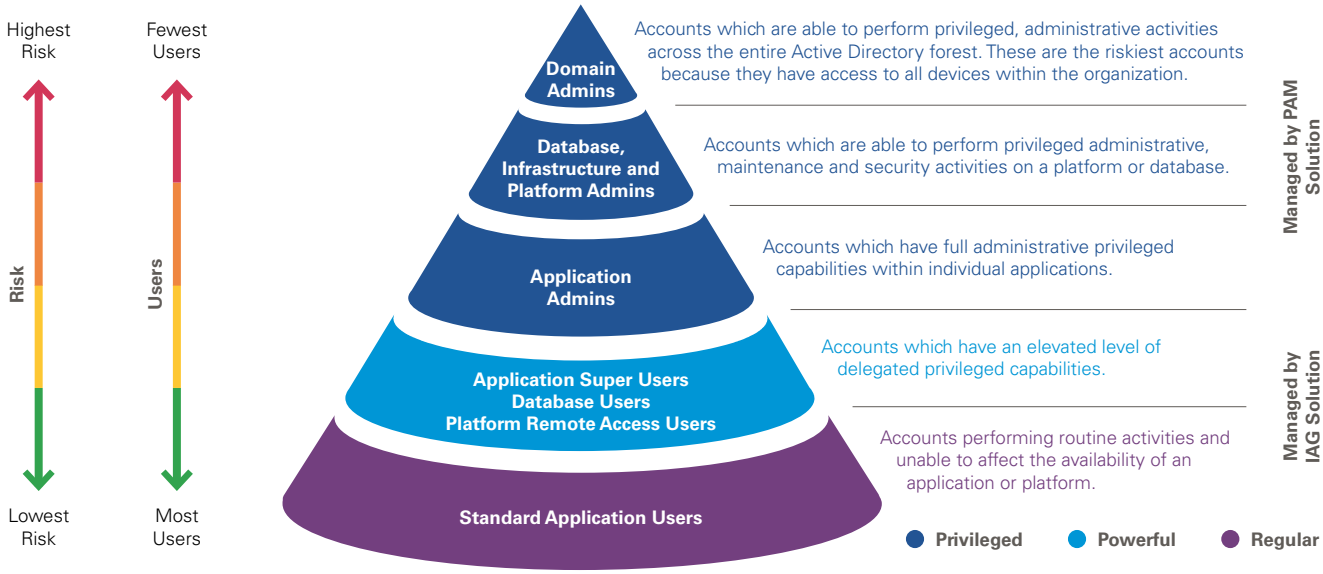
One of the biggest security threats in the cyber security landscape is the potential misuse of accounts with high, elevated ('privileged') permissions on IT systems. Privileged Access Management (PAM) helps organizations manage their privileged accounts in order to protect their critical assets, meet compliance regulations and to prevent data breaches.

"Increasingly, malicious insiders target privileged users to obtain their access rights. In 2011, only 21 percent said it would be likely that malicious insiders would use social engineering or other measures to obtain someone's access rights. This has increased significantly to 47 percent of respondents. In addition, more respondents say it is likely that social engineers outside the organization target privileged users to obtain their access rights (45 percent in 2014 and 30 percent in 2011)."

Ponemon Institute, "Privileged User Abuse & The Insider Threat", 2014

Privileged accounts are the most critical and powerful accounts within the IT infrastructure of an organization. These powerful accounts are typically targeted by cyber-attacks to gain possession of resources and to access confidential and customer data. Given the increase in highly publicized cyber security breaches and insider threats, privileged access management (PAM) has become a board-driven initiative. Information technology (IT) organizations have long struggled with protecting and controlling powerful access to the accounts that administer their most critical assets and data while still allowing their administrators the flexibility they need to perform their daily job functions.

Types of users within an organization



Why KPMG?

Led by experienced identity architects, business analysts and implementers, the KPMG Privileged Access Management team is well placed to ensure customers maximize value from their PAM solution. KPMG offers an end-to-end solution offering for PAM including:

Discovery and Analysis
Discover accounts, SSH keys and create an inventory of privileged accounts using a light-weight, easy to use tool. This tool exposes the magnitude of the privileged account problem, including scanning unmanaged parts of an organization. Vulnerability analysis of privileged credentials.

Business Policies and Process Optimization
Review of privileged access management processes, identifying opportunities for improvement in accordance with best practices. Develop effective target operating model to manage the PAM solution on an ongoing basis.

Solution Architecture and Design
Solution design and planning services. Infrastructure planning, hardware and sizing requirements and diagrams. Design and develop secure policies in compliance with least privilege and Segregation of Duties requirements.

Solution Configuration and Customization
Expert technical assistance in installation and configuration of privileged access management solution.

Quality Assurance and Health Check Assessments
Quality assurance services delivered as part of the solution implementation services. Deep dive diagnostic review of existing PAM solution deployments, with recommendations for improvements.

The KPMG Approach

KPMG's PAM offering is comprised of a three phased approach. This approach lays out what we offer against a client's transformational Privileged User Access Management (PUAM) journey and consists of best practices, templates and other tools to efficiently execute the project. We have a highly skilled global team with the right experience for implementing Privileged Access Management (PUAM) within your organization.

Strategic planning and requirements development

- Define privileged accounts in the context of the organization's technology and risk environment
- Define a target operating model that provides a holistic view of operational roles and responsibilities, as well as detailed policies, processes and procedures

Operationalization and continuous improvement

- Continuous discovery and analysis of privileged accounts throughout the environment
- Develop a scalable solution architecture that addresses the organization's needs in the current and future state

Technology implementation and process development

- Implement analytics to better understand privileged account usage and further improve access controls by integrating logging, monitoring and alerting capabilities
- Reduce reliance on manual processes by automating capabilities for system builds and other procedures

Contact

KPMG AG
Badenerstrasse 172
PO Box
CH-8036 Zurich

kpmg.ch/cyber

Matthias Bossardt
Partner
Cyber Security

+41 58 249 36 98
mbossardt@kpmg.com