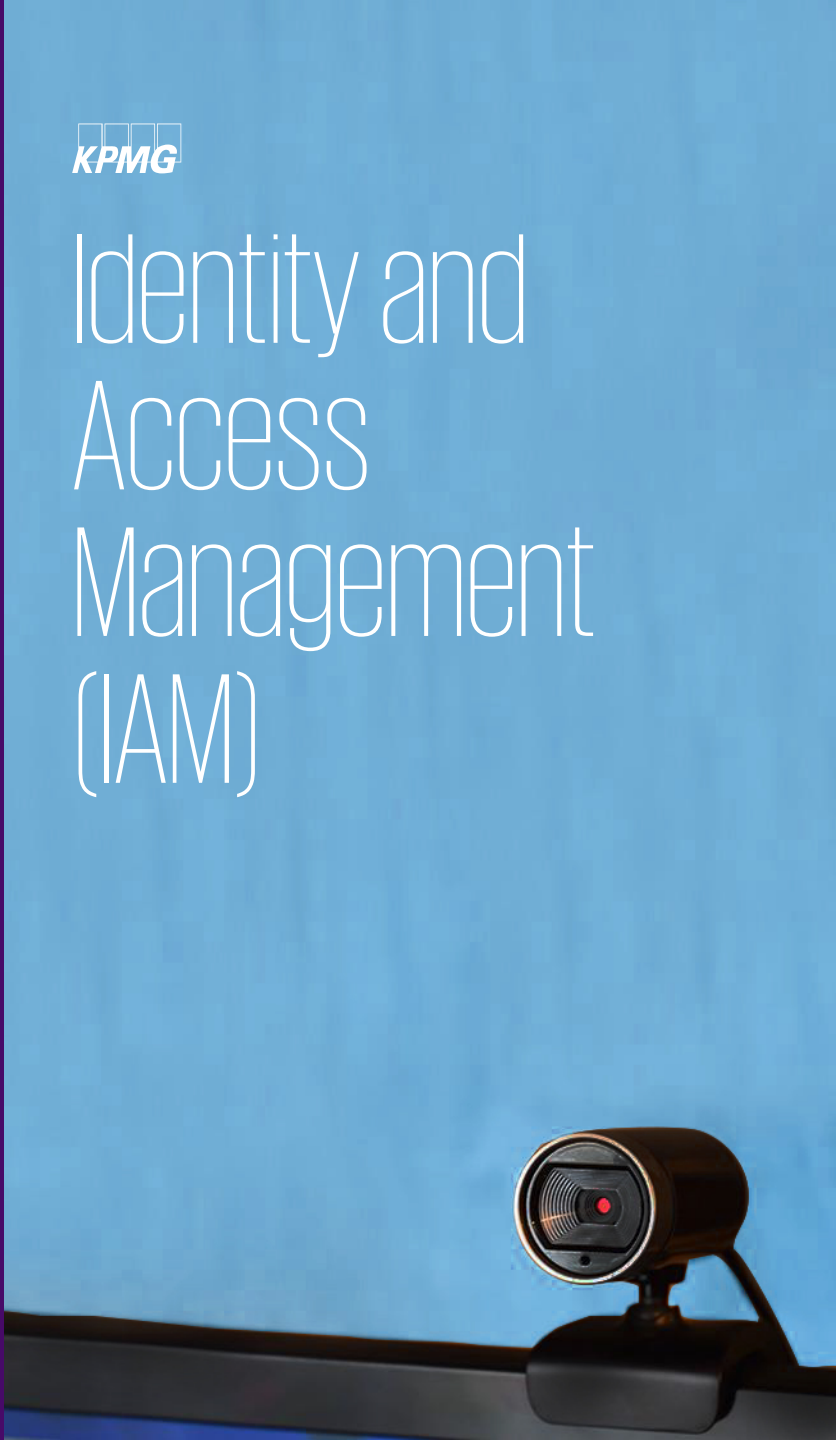
KPMG

Identity and Access Management (IAM)



Helping the public sector manage and secure the digital identities of users (humans and devices) that use enterprise, consumer and partner enabled digital services

© 2019 KPMG LLP, a Delaware limited liability partnership and the U.S. member firm of the KPMG network of independent member firms affiliated with KPMG International Cooperative ("KPMG International"), a Swiss entity. All rights reserved. NDPPS 878399

Overview

In its simplest form, an identity provides a digital representation of an individual, entity or device and their associated access privileges. The primary function of Identity & Access Management (IAM) is to reduce the risk of a data breach by controlling who or what can access information assets based on defined access policies, ensuring that users do not have more access than is needed to perform a designated business function. IAM also provides an efficient mechanism for facilitating access to online products or services. The capabilities offered by IAM, when correctly implemented, can help agencies improve business efficiencies, reduce operational costs, mitigate potential cyber risks, satisfy regulatory compliance needs and enhance user experience.

As agencies have become more conscious about the role of digital identity as both a potential risk factor and business enabler, the level of investment in sophisticated IAM tools and services has grown dramatically.

Nearly every federal agency has some form of IAM programs and processes in place. The varied level of maturity across agencies using disparate, fragmented and sometimes duplicative solutions has led to development of standards, guidelines and policies like NIST 800-63, HSPD-12 and OMB policies.

Several initiatives like the Continuous Diagnostics and Mitigation (CDM) program from DHS and the Federal Identity Credential and Access Management (FICAM) program, managed by GSA, provide collaboration opportunities and guidance on IT policy, standards, implementation and architecture, to help federal agencies implement ICAM. The addition of "Credential" adds the aspect of PIV/CAC card issuance and acceptance. Depending on the agency, we see references to IAM, ICAM, and/or FICAM.

KPMG

© 2019 KPMG LLP, a Delaware limited liability partnership and the U.S. member firm of the KPMG network of independent member firms affiliated with KPMG International Cooperative ("KPMG International"), a Swiss entity. All rights reserved. NDPPS 878399

Key considerations guiding an IAM strategic plan

— Strategically approach the new build-out of IAM capabilities **guided by industry best practices**

— Future-proof the IAM capabilities with a **technology-agnostic plan with modularity of capability-areas** to allow for interoperability and flexibility in choice for best-of-breed technology & extensibility to hybrid cloud integration points

— Take this opportunity to build a **multi-faceted and structured IAM Program for Client** that –

- provides ongoing direction and avoids maturity plateaus with program governance,
- reduces operating inefficiencies with standardized IAM processes, and,
- iteratively releases evolving technical capabilities to applications akin to an agile new product development journey to match the Client's application dispositions & growing deployments

— **Evolve to a fully mature enterprise role-based access model** that goes beyond access profiles to a more sustainable & automated hybrid model that is tended to by well-governed upkeep of role lifecycle management, and keeps pace with growing application access needs & privileged access environment.

KPMG

© 2019 KPMG LLP, a Delaware limited liability partnership and the U.S. member firm of the KPMG network of independent member firms affiliated with KPMG International Cooperative ("KPMG International"), a Swiss entity. All rights reserved. NDPPS 878399

KPMG approach and services

KPMG has extensive delivery experience and success working in both EIAM and CIAM domains and has invested in governance models, technology platforms and the ability to execute across both stakeholder groups. Our professionals are delivering timely insights and perspectives aimed at optimizing these critical dimensions of identity for success in the digital age.

KPMG can help agencies achieve their mission, from identity and access strategy planning to capability implementation and integration and end-user rollout. KPMG takes a business-first approach to identity and access solutions, from enabling security posture and reducing risk to supporting regulatory issues to helping to enable our clients' digital transformations.

KPMG's cross functional professionals from Cyber Security, Customer Success, Digital Experience, and Risk and Compliance, among other practices, help you enable customer engagement by implementing a secure, one-enterprise approach to customer identity so you can improve customer experience and develop a more intimate relationship with your customer.

Service elements

- IAM assessment
- IAM vision, strategy, roadmap
- IAM architecture
- IAM product and solution evaluation and selection
- IAM governance and operating model
- IAM solution implementation
- IAM solution adoption
- IAM software selection
- Access governance (roles, data, certification)

KPMG

© 2019 KPMG LLP, a Delaware limited liability partnership and the U.S. member firm of the KPMG network of independent member firms affiliated with KPMG International Cooperative ("KPMG International"), a Swiss entity. All rights reserved. NDPPS 878399

Key capability areas for IAM

Program governance

IAM Program Governance establishes, endorses, and oversees the strategic direction and execution of IAM efforts (projects, technologies, processes, and people) to operate collaboratively and measurably, to implement various IAM capabilities that improve various IAM capabilities such as how identities are to be represented, what systems/applications they are entitled to access, how do identities access various systems/applications, when and how should access authorizations be used, and when and by whom they should be audited.

Identity & access modeling

This encompasses a set of capabilities that enable organizations to aggregate and model user access data. This involves creation of an *Identity Warehouse* that is seeded by "person" data from authoritative source repositories, resulting in the creation of digital identities for identified persons. Each identity is then enriched with user account and entitlement data from connected information systems to create a 360 degree view of all user access, capabilities and roles within the enterprise. Rogue or orphan accounts that cannot be correlated to a valid user identity can then be flagged for investigation and remediation.

User management & provisioning

These capabilities help address any change to user access, including the creation, modification and revocation of privileges. These processes can be triggered by changes to authoritative source data, such as in the case of a new hire, transfer or termination. These are known as *identity lifecycle processes*. These processes can also be invoked via a user interface, such as an access request form, helpdesk administration tool or password reset function. The fulfillment of a these process can be performed either by a automated, provisioning-enabled connectors, or manually if no such connector is available for the target system.

Access control

These capabilities are a collection of runtime mechanisms and processes that validate a user's identity, enforce access to systems and ensure that users can only access the information assets for which they have the appropriate permissions. Access Control also encompasses various technologies and methods by which a privileged user can access a privileged system to perform administrative changes.

Monitoring and analytics

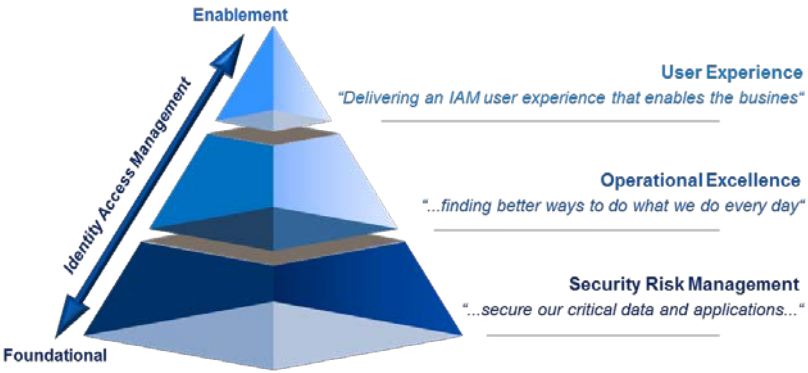
These capabilities comprise of user access reviews, certifications and attestation campaigns, inappropriate access violations, SOD violations, analysis of user permissions and behavior and user/access reports.

KPMG

© 2019 KPMG LLP, a Delaware limited liability partnership and the U.S. member firm of the KPMG network of independent member firms affiliated with KPMG International Cooperative ("KPMG International"), a Swiss entity. All rights reserved. NDPPS 878399

Digital identity as a business enabler

Risk reduction is the primary driver for IAM programs, providing a foundation upon which operational efficiencies and improved user experience can be achieved.



Risk Reduction
- Detective and preventative policy enforcement
- Risk measurement and analytics
- Discovery and cleansing of privileged, orphan, rogue and zombie accounts

Operational Efficiencies
- Automated password management and access fulfillment
- Closed-loop attestation and remediation of access
- Streamlined business processes (e.g. Joiners, Movers and Leavers)

Platform Consolidation
- Migration from legacy and homegrown IAM technology
- Consolidation of IAM infrastructure, platforms and tools
- Directory consolidation, virtualization and cleansing

Regulatory Compliance
- 360o view of user privileges, activity and risk
- Compliance-driven reporting and user access reviews
- Risk mitigation for sensitive information assets

User Experience
- Single Interface for requesting and approving access
- Single or Consistent Sign-On to secure systems
- Faster onboarding and provisioning of users

KPMG
© 2019 KPMG LLP, a Delaware limited liability partnership and the U.S. member firm of the KPMG network of independent member firms affiliated with KPMG International Cooperative ("KPMG International"), a Swiss entity. All rights reserved. NDPPS 878399

Benefits and outcomes

Potential client benefits by adopting a standardized/ structured CDM data architecture framework:

01	Strategic alignment with business goals
02	Value-added spend on Cyber security
03	Better integration with enterprise architecture
04	More effective protection from cyber attacks
05	Continuous monitoring of security risk
06	Risk-focused security strategy
07	Auditable compliance
08	Ongoing Authorization support
09	Consistent CDM data flow to Agency and Federal Dashboards

KPMG

© 2019 KPMG LLP, a Delaware limited liability partnership and the U.S. member firm of the KPMG network of independent member firms affiliated with KPMG International Cooperative ("KPMG International"), a Swiss entity. All rights reserved. NDPPS 878399

Evolution of identity and access management

As the demand for intuitive, user-friendly, secure and omni-channel digital government services has gathered pace, the notion of perimeter security became obsolete. Secure management of digital identities significantly impacts the security of the digital services, and mitigates negative impacts to delivery of digital services and maintenance of online trust. IAM is the new security "perimeter" of the digital ecosystem.

As digital transformation of business models has gathered pace, identity and access management (IAM) has evolved into two broader fields:

- **Consumer identity and access management (CIAM):** CIAM is focused on business opportunity, growth, and identifying customer preferences to respond with relevant, timely, highly personalized experiences.
- **Enterprise identity and access management (EIAM):** EIAM is focused on compliance, risk, governance, security, privacy, employee lifecycle management, and operational efficiency.

Modern technology trends like Cloud Migration efforts, Internet of Things (IoT), Robotic Process Automation (RPA), DevOps and SecOps along with APIs for digital services have led to the emergence of a new type of digital Identity called "Device Identity." Both CIAM and EIAM frameworks and solutions should be able to secure access to these privileged services.

KPMG

© 2019 KPMG LLP, a Delaware limited liability partnership and the U.S. member firm of the KPMG network of independent member firms affiliated with KPMG International Cooperative ("KPMG International"), a Swiss entity. All rights reserved. NDPPS 878399

Evolution of identity and access management (continued)

Factors fueling investment in IAM

Security

- Consistent security across the enterprise
- Prevention of unauthorized access
- Stronger authentication credentials
- Management of privileged access
- Remediation of rogue and orphan accounts

Compliance

- Record of who has access to what
- Revocation of access upon termination
- Certification of access for sensitive information assets
- Regulatory compliance, such as OMB M-18XX and NIST 800-63
- Policy enforcement (e.g., SOD violations and toxic combinations)

Disruptive Technologies

- Mobile Technologies are Bring-Your-Own-Device (BYOD)
- Cloud adoption and Software-as-a-Service
- E-Government Services
- Social Media (Facebook, LinkedIn, etc.)
- Internet of Things and device-specific identities

Operational Excellence

- Rapid onboarding of new hires
- Automation of provisioning processes
- Centralized access request and approval processes
- Role based access controls
- Reduced helpdesk and operational costs

KPMG

© 2019 KPMG LLP, a Delaware limited liability partnership and the U.S. member firm of the KPMG network of independent member firms affiliated with KPMG International Cooperative ("KPMG International"), a Swiss entity. All rights reserved. NDPPS 878399

Key questions to jump start the IAM conversation within your Agency

What's your agencies maturity around IAM

1) Are you currently going through or planning to undertake any digital transformation initiatives?
2) Are you having identity-related challenges with your digital transformation?
3) Have you had a data breach?
4) Have you seen increased fraud or business losses due to recent identity thefts caused by industry breaches?
5) Do you have any access-related regulatory requirements or issues?
6) Does your IAM solution support personalizing the digital experience?
7) Can you securely manage devices and their associations to users?
8) Does your IAM solution align with your product or service consumption model, identify your customers accurately and represent the customer journey for all business functions?
9) Does your identity solution help you meet and stay compliant with regulations such as NIST 800-63-3, FICAM, OMB M-19-17, etc.?
10) Are your access recertification processes achieving risk reduction and regulatory compliance goals?
11) Have you been unable to demonstrate completeness and accuracy of identity data?
12) Are your access request and recertification processes business-friendly?
13) Is your current IAM solution alienating your workforce and impeding the performance of your agency?
14) Have you encountered audit issues or findings related to access control?

KPMG

© 2019 KPMG LLP, a Delaware limited liability partnership and the U.S. member firm of the KPMG network of independent member firms affiliated with KPMG International Cooperative ("KPMG International"), a Swiss entity. All rights reserved. NDPPS 878399

Contacts

If you have questions or want more details regarding KPMG's IAM services, please contact us:

Tony Hubbard
Principal, Government
Cyber Leader
T: 03-286-8320
E: hubbard@kpmg.com

Shane Cashdollar
Director, Cyber Security
T: 703-286-8236
E: scashdollar@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.

© 2019 KPMG LLP, a Delaware limited liability partnership and the U.S. member firm of the KPMG network of independent member firms affiliated with KPMG International Cooperative ("KPMG International"), a Swiss entity. All rights reserved. NDPPS 878399

The KPMG name and logo are registered trademarks or trademarks of KPMG International.