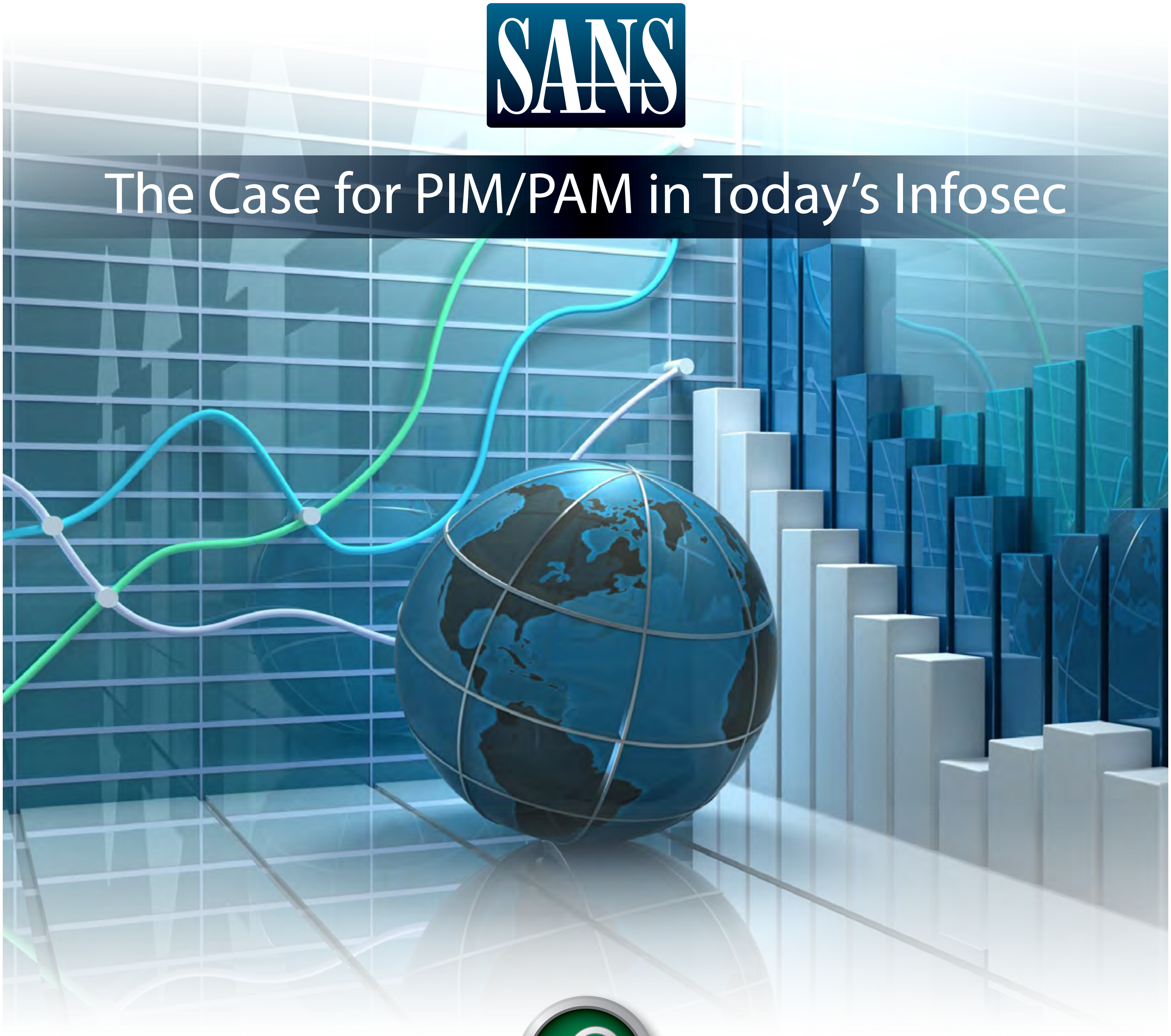
The Case for PIM/PAM in Today's Infosec



A SANS Whitepaper

Written by Barbara Filkins

July 2016

Sponsored by
CA Technologies

©2016 SANS™ Institute

Introduction

To see how serious a threat the misuse of privileged credentials represents, look no further than the astonishing scope of the breach discovered in 2015 at the United States Office of Personnel Management (OPM). To realize how often similar threats become real, look no further than the 2016 Verizon Data Breach Incident Report (DBIR), which found that privilege misuse was the second-most frequent cause of security incidents and the fourth-most common cause of breaches.

In June 2015, the OPM announced it had been the target of a massive data breach that began more than a year earlier. Initial estimates put the number of records compromised at close to 4 million. Subsequent investigation estimated that sensitive information had been compromised for a total of 22.5 million people—7 percent of the U.S. population. Compromised data included Social Security numbers, job records, names and addresses of family members and friends and, in 5.6 million instances, fingerprint records.[1]

Privilege misuse is the second-most frequent cause of security incidents and the fourth-most common cause of data breaches.

—2016 Verizon Data Breach Investigations Report[4]

What was the root cause of this breach? Former OPM Director Katherine Archuleta testified before lawmakers that attackers gained access to OPM systems with a username and password belonging to an external contractor. The attackers were able to avoid the notice of several high-profile intrusion-detection systems as they exfiltrated reams of sensitive data because they had disguised themselves as a user who had legitimate access rights.[2] U.S. investigators said they suspect a foreign-state intelligence agency was behind the attack, but they have made no firm accusations. In December, China announced it had arrested two criminal hackers it accused of being behind the OPM attack.[3]

Privilege misuse is the second-most frequent cause of security incidents and the fourth-most common cause of data breaches, according to the DBIR.[5] Almost one-third of the roles involved in incidents cited by the DBIR were end users who had access to sensitive data as a requirement to perform their jobs. Only 14 percent were in roles that had elevated privilege, such as systems administrators. That 14 percent, however, represents the gatekeepers that maintain the controls over access to sensitive information. Though it confirms the general perception that collusion between attackers and administrators is rare, when collusion between actors does happen, the population of privileged administrators is a frequent source.

[1] "Millions more Americans hit by government personnel data hack," Reuters, July 9, 2015, www.reuters.com/article/us-cybersecurity-usa-idUSKCN0PJ2M420150709

[2] "OPM hack may finally end overuse of 'privileged' user access," The Christian Science Monitor, June 26, 2015, www.csmonitor.com/World/Passcode/2015/0626/OPM-hack-may-finally-end-overuse-of-privileged-user-access

[3] "Chinese government has arrested hackers it says breached OPM database," The Washington Post, Dec. 2, 2015, www.washingtonpost.com/world/national-security/chinese-government-has-arrested-hackers-suspected-of-breaching-opm-database/2015/12/02/0295b918-990c-11e5-8917-653b65c809eb_story.html

[4] Verizon, 2016 Data Breach Investigations Report, www.verizonenterprise.com/verizon-insights-lab/dbir/

[5] Verizon, 2016 Data Breach Investigations Report

Figure 1 shows the possible universe of privileged users in a modern enterprise that depends on people, applications and services both on and off premises, hosted in the enterprise data center and in the public cloud.

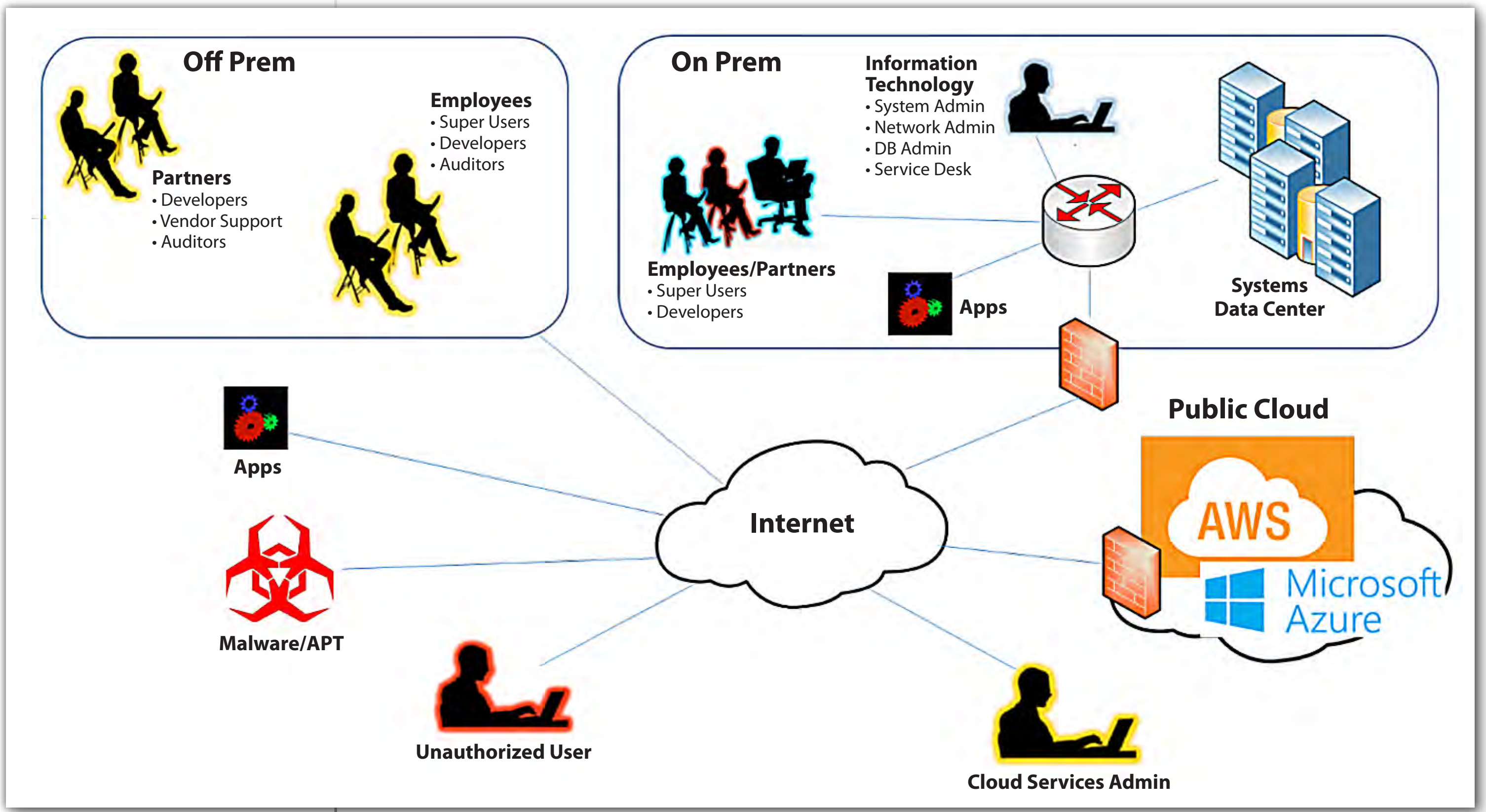


Figure 1. The Universe of Privileged Users

Accurate monitoring and control of that access requires solutions that are able to establish a shared governance framework. Effective governance is supported by policy, process and technology. It can serve as a mechanism to centralize the management and control of the privileged identities and access across the multiple endpoints, applications and systems deployed in an organization.

We can consider privileged identity management/privileged access management (PIM/PAM) as a domain within identity and access management (IAM), but the practical differences are not always well understood. In this paper, SANS will provide a concise background on privileged identity and access solutions, addressing the fundamental functional requirements, the reasons it is needed and the challenges of making it work effectively.

What Is the Need? Regulatory Compliance for a Start

Even before the OPM breach was discovered in 2015, the U.S. government had started to pay closer attention to insider threats. On Oct. 7, 2011, President Obama signed Executive Order 13587, Section 6.0 of which established an interagency task force to develop a government-wide program for "deterring, detecting, and mitigating insider threats" related to classified information.[6] On Nov. 21, 2012, the White House issued a Presidential Memorandum[7] that included the National Insider Threat Policy,[8] providing governmental departments and agencies with minimum standards for the establishment of effective insider-threat programs. The policy may have been sparked by the 2010 arrest of U.S. Army PFC Bradley Manning for releasing protected documents to WikiLeaks.[9] By fiscal year 2014, all federal government agencies, not just the Department of Defense, were ordered to take steps to comply with the full terms of the Nov. 21, 2012, memorandum. The minimum standards call for "timely, and, if possible, electronic access to the information necessary to identify, analyze and resolve insider-threat matters." From an information-assurance perspective, this includes "personnel names and aliases, levels of network access, audit data, unauthorized use of removable media, print logs and other data needed for clarification or resolution of an insider-threat concern." It also calls for monitoring user activity on networks.[10]

[6] Executive Order 13587 — Structural Reforms to Improve the Security of Classified Networks and the Responsible Sharing and Safeguarding of Classified Information, The White House, Oct. 7, 2011,
www.whitehouse.gov/the-press-office/2011/10/07/executive-order-13587-structural-reforms-improve-security-classified-net

[7] Presidential Memorandum — National Insider Threat Policy and Minimum Standards for Executive Branch Insider Threat Programs, The White House, Nov. 21, 2012,
www.whitehouse.gov/the-press-office/2012/11/21/presidential-memorandum-national-insider-threat-policy-and-minimum-stand

[8] National Insider Threat Policy, National Counterintelligence and Security Center, Nov. 21, 2012,
www.ncsc.gov/nittf/docs/National_Insider_Threat_Policy.pdf

[9] "White House Issues National Insider Threat Policy," SecurityWeek, Nov. 29, 2012,
www.securityweek.com/white-house-issues-national-insider-threat-policy

[10] Memorandum for the Heads of Executive Departments and Agencies, The White House, Nov. 21, 2012,
www.cdse.edu/documents/toolkits-insider/20121121-policy-minimum-standards.pdf

Of course, compliance with other regulations that handle personally identifiable information (PII) must be maintained. Table 1 illustrates the regulatory crosswalk that supports the detailed need for PAM against several of the major federal regulations that deal with both privacy and security.

Table 1. PIM/PAM Regulatory Compliance Crosswalk

Regulation (and entities affected by it)	**FISMA** (NIST 800-53) (defense contractors, information processors)	**HIPAA** (providers, insurance plans, employers, clearinghouses)	**NERC** (transmission and generation service providers, owners, load-serving operators)	**PCI-DSS** (entities that store, process or transmit credit card data)	**U.S. NRC** (operators, vendors, contractors)
Identify and track the location of privileged account credentials	AC-2 AC-4		B.R5.1. (Implicit)	7.2.1	Appendix A, B.1.2 Appendix A, B.1.3 Appendix A, B.1.4
Enforce rules for password strength, uniqueness, change frequency	AC-2	45§164.308(5)(D) 45§164.312(2)(i)	B.R5.3.1. B.R5.3.2. B.R5.3.3.	8.5.5 8.5.8 8.5.9	Appendix A, B.1.2
Delegate so that only appropriate personnel can access	AC-3 AC-6	45§164.308(3)(i) 45§164.308(3)(B) 45§164.308(3)(C) 45§164.312(a)(1)	B.R5.1. B.R5.2. B.R5.2.1. B.R5.2.3.	2.1 6.3.6 7.7.1 8.5.4 8.5.6	Appendix A, B.1.2 Appendix A, B.1.3 Appendix A, B.1.5 Appendix A, B.1.6
Audit and alert to show requesters, access history, purpose, duration, etc.	AU-3 AU-9	45§164.308(5)(C)	B.R5.1.2.	10.2	Appendix A, B.1.2 Appendix A, B.1.3

Source of the Threat: With Privilege Comes Risk

Definitions of privileged identities and privileged access are often imprecise and tend to be insufficiently well known or understood. You can consider a privileged user to be anyone or anything (such as a system service) that has elevated access to information assets, operations or both. People represent one set of threats that can render protected resources vulnerable, whether through deliberate actions (with motivations that range from financial gain to disgruntlement), carelessness or neglect. The resulting threats can be manifested in many ways, including the following:

- **Fraud:** unwanted use, modification, addition or deletion of an organization's data for personal gain.
- **Espionage:** sharing restricted information with the intention of harming the organization.
- **Sabotage:** purposefully inflicting harm on an organization.
- **Intellectual property theft:** stealing intangible assets (e.g., discoveries, inventions, designs) from an organization.
- **Unwanted information disclosure:** a communicated or physical transfer of information to a recipient who is not authorized to access the information.

SANS recommends organizations incorporate trust relationships and privileged access that is granted via SSH keys into a PAM system for consolidated and regular review.

Because misuse or abuse of elevated access can significantly compromise the critical assets of an organization, the enterprise must be fully aware of the potential for privileged users to exploit their organizational roles:

- What are the policies and processes by which IT administrators—systems, network, application or database—normally establish, maintain and monitor access to the infrastructure? Who should be responsible for overseeing their actions?
- What essential services or support do vendors, contracted development or incident response staff render that require elevated access? Where do these vendors reside? Ars Technica reported that contractors used by OPM included a UNIX systems administrator in Argentina and another person located in the People's Republic of China, both of whom had root access to every row of data in every database.[11]
- How often and for how long do auditors and compliance officers need access to sensitive information?

[11] "Encryption 'would not have helped' at OPM, says DHS official," Ars Technica, June 16, 2015, http://arstechnica.com/security/2015/06/encryption-would-not-have-helped-at-opm-says-dhs-official

Operators can be fooled, bribed or recruited, but system services operating with elevated privileges are also susceptible to compromise by attackers if not properly secured. The lack of defined governance for SSH key-based trust relationships can allow an attacker who compromises one system to quickly pivot from that system to another and extend a breach into other parts of an organization. Enough keys may be stolen, leaked or disused—without having had their trust relationships terminated—to pose a serious, ongoing threat to an organization.[12] For that reason, SANS recommends organizations incorporate trust relationships and privileged access that is granted via SSH keys into a PAM system for consolidated and regular review.[13]

The Center for Internet Security (CIS) Critical Security Controls, a highly focused set of prioritized actions that leverage automation-based processes to help organizations of all sizes avoid breaches, considers "Controlled Use of Administrative Privileges" among the top five controls because "the misuse of administrative privileges is a primary method for attackers to spread inside a target enterprise."

[12] "New Critical Security Controls Guidelines for SSL/TLS Management," SANS Institute InfoSec Reading Room, June 2015, www.sans.org/reading-room/whitepapers/analyst/critical-security-controls-guidelines-ssl-tls-management-35995

[13] "Securing SSH with the CIS Critical Security Controls," SANS Institute InfoSec Reading Room, December 2015, www.sans.org/reading-room/whitepapers/protocols/securing-ssh-cis-critical-security-controls-36462

Identity and access management (IAM) is the security discipline that enables the right individuals to access the right resources at the right times for the right reasons.
—Gartner[14]

IAM is a critical foundation for any industry vertical that deals with sensitive or critical information—health and human services, financial, retail and manufacturing. IAM has several distinct elements that must work together. See Figure 2.

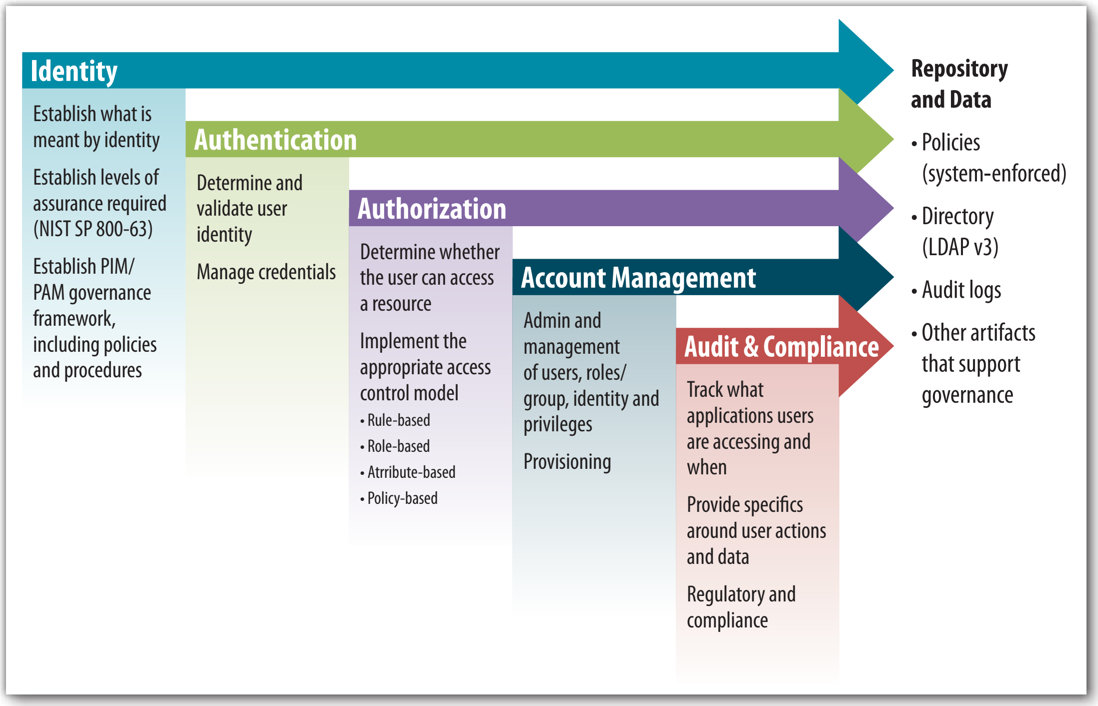

Identity
Establish what is meant by identity
Establish levels of assurance required (NIST SP 800-63)
Establish PIM/PAM governance framework, including policies and procedures
Authentication
Determine and validate user identity
Manage credentials
Authorization
Determine whether the user can access a resource
Implement the appropriate access control model
• Rule-based
• Role-based
• Atrribute-based
• Policy-based
Account Management
Admin and management of users, roles/group, identity and privileges
Provisioning
Audit & Compliance
Track what applications users are accessing and when
Provide specifics around user actions and data
Regulatory and compliance
Repository and Data
• Policies (system-enforced)
• Directory (LDAP v3)
• Audit logs
• Other artifacts that support governance

Figure 2. The Elements of IAM

Enterprises must provide access for a growing number of identities, both inside and outside the organization, without compromising or exposing sensitive information. Implementing IAM solutions is not simple. It involves people, processes and products to manage identities and access to resources of an enterprise. The information must be correct at all levels—identities, credentials, authorization and access, and audit.

[14] Gartner IT Glossary, www.gartner.com/it-glossary/identity-and-access-management-iam

PIM/PAM—the terms are used interchangeably—is considered a domain within IAM that focuses on the specific requirements needed to govern those identities that wield greater power within the IT infrastructure of an enterprise. Table 2 presents some of the differences between IAM and PIM/PAM solutions.

Table 2. Differences Between IAM and PAM Solutions

IAM	PIM/PAM
Governs the identities on each individual system, each system having potentially thousands of managed identities.	Governs privileged identities in an enterprise, mapping and managing these identities centrally across multiple systems.
Manages the creation and deletion of IDs and security entitlements related to those IDs.	Manages access to privileged IDs and associated elevated entitlements by users who already have IDs through the IAM solution.
Grants entitlements on a permanent/persistent basis until deletion (e.g., "User X shall have entitlement Y from now on").	Grants access to privileged accounts/elevated privileges for defined time windows (on the order of minutes or hours), just long enough to perform the needed task.

Attribute- and policy-based access control (ABAC/PBAC) represents a more complex model than traditional role-based access. Both of these models use policies that include user attributes, user roles/groups, actions taken, access channels, time, resources requested, external data and business rules.

PIM/PAM complicates the IAM model, as shown in Figure 2. It can be difficult to securely manage access to thousands of privileged accounts that cross multiple, disparate systems. Consequently, in many organizations, the credentials (e.g., passwords, certificates and keys) to privileged accounts are known to many people (often including former staff), are the same on many systems, are rarely—if ever—changed and are stored in multiple places. The consequences can be serious: no uniform visibility into the use of shared, privileged accounts (both a security/regulatory-compliance problem and a problem with diagnosing operational problems); possible retention of sensitive access by former workforce members; and vulnerability to attack by external attackers. If one system (an IT user's PC or an application server, for example) is compromised, the attacker can leverage credentials stored on that system to pivot and compromise additional systems.

What Does This Look Like?

Both IAM and PIM/PAM require a lifecycle management approach that touches many elements, as shown in Figure 3. PIM/PAM must comply with and automate privileged identities to follow predetermined or customized policies and requirements for an organization or industry.

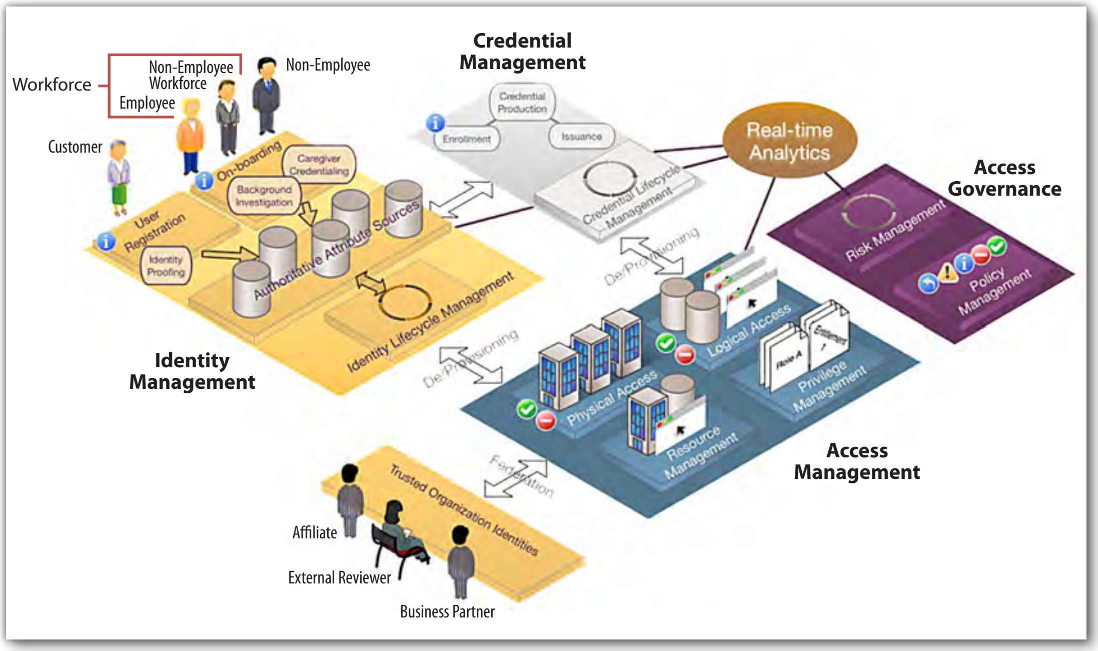


Figure 3. An Overview of the Elements of IAM and PIM/PAM [15]

A Word About Credentials

Managing and protecting privileged credentials are essential to reducing risk and achieving compliance with regulation and industry best practices. Credentials are no longer simply usernames and passwords. Depending on the environment, credential management must deal with X.509/PKI certificates, two-factor tokens, multifactor authentication (MFA) and Personal Identity Verification and Common Access Cards (PIV/CAC), which are necessary for federal-sector compliance. It must address standards and protocols such as Security Assertion Markup Language (SAML), OpenID and OAuth.

[15] Distributed Information Technologies, http://dtec.com/solutions/identity-and-access-management-solutions

Privileged user accounts are proliferating in the enterprise, far beyond those that are typically associated with privileged access. Recall that the Verizon DBIR found the majority of the roles involved in privilege misuse were not those of IT administrators; most belonged to colluding or compromised end users whose access to sensitive information was a requirement of their daily responsibilities. One example: A social media coordinator may not play a key executive role, but she is a privileged user if she has access to the primary marketing database.

Enterprises of all sizes are struggling to keep up. In her testimony to a Senate subcommittee on June 23, 2015, former OPM Director Archuleta revealed that OPM's 47 major applications were still protected by only username and password. That deficiency was a known weakness before the attack was uncovered, having been cited in the 2014 OMB Audit Report,[16] which states that "as of the end of FY 2014, … none of the Agency's 47 major applications required PIV [multifactor] authentication" as required by OMB M-11-11.

> "HSPD-12 requires agencies to follow specific technical standards and business processes for the issuance and routine use of Federal Personal Identity Verification (PIV) smartcard credentials. … Specific benefits of the standardized credentials required by HSPD-12 include secure access to federal facilities and disaster response sites, as well as multifactor authentication, digital signature and encryption capabilities."[17]

[16] Federal Information Security Management Act Audit FY2014, U.S. Office of Personnel Management, Office of the Inspector General, Office of Audits, Nov. 12, 2014, www.infrasupport.com/wp-content/uploads/2015/06/federal-information-security-management-act-audit-fy-2014-4a-ci-00-14-016.pdf

[17] Continued Implementation of Homeland Security Presidential Directive (HSPD) 12– Policy for a Common Identification Standard for Federal Employees and Contractors, Office of Management and Budget, The White House, Feb. 3, 2011, www.whitehouse.gov/sites/default/files/omb/memoranda/2011/m11-11.pdf

Systems to Control Privileged-Access Risk

The implementation of systems to control PIM and PAM access is less straightforward than agencies often assume. Many fail to realize that a PIM/PAM solution is a complex integration exercise that requires knowledge of the organizational processes, environment and business, not a simple audit of an access list. Table 3 presents an overview of the elements from the technical perspective alone that may need to be tied together to support an enterprise PIM/PAM solution.

Table 2. Differences Between IAM and PAM Solutions

Directories: Any LDAP, AD, WinNT, NDS, eDirectory, NIS/NIS+	***Servers:*** Windows NT, 2000, 2003, 2008[R2], 2012, Samba, Novell, SharePoint	***Databases:*** Oracle, Sybase, SQL Server, DB2/UDB, Informix, Progress, ODBC, Oracle Hyperion EPM Shared Services, Cache
Unix: Linux, Solaris, AIX, HP-UX, 24 more variants	***Mainframes, Midrange:*** z/OS: RACF, ACF2, TopSecret. iSeries, OpenVMS	***HDD Encryption:*** McAfee, CheckPoint, BitLocker, PGP
ERP: JDE, Oracle eBiz, PeopleSoft, PeopleSoft HR, SAP R/3 and ECC 6, Siebel, Business Objects	***Collaboration:*** Lotus Notes, iNotes, Exchange, GroupWise, BlackBerry ES	***Tokens, Smart Cards:*** RSA SecurID, SafeWord, RADIUS, ActivIdentity, Schlumberger
WebSSO: CA Siteminder, IBM TAM, Oracle AM, RSA Access Manager	***Help Desk:*** ServiceNow, BMC Remedy, SDE, HP SM, CA Unicenter, Assyst, HEAT, Altiris, Clarify, RSA Envision, Track-It!, MS System Center Service Manager	***Cloud/SaaS:*** WebEx, Google Apps, Microsoft Office 365, Success Factors, Salesforce.com, SOAP (generic)

Factors for Success and Failure

IAM and PIM/PAM both demand a lifecycle approach that involves both technical and nontechnical elements, as reflected in the nine steps suggested by the ICAM Privileged User Instruction and Implementation Guidance, Version 1.0, for an organization to improve its privileged user risk management. Table 4 reviews the potential success factors and pain points for each of these steps.[18]

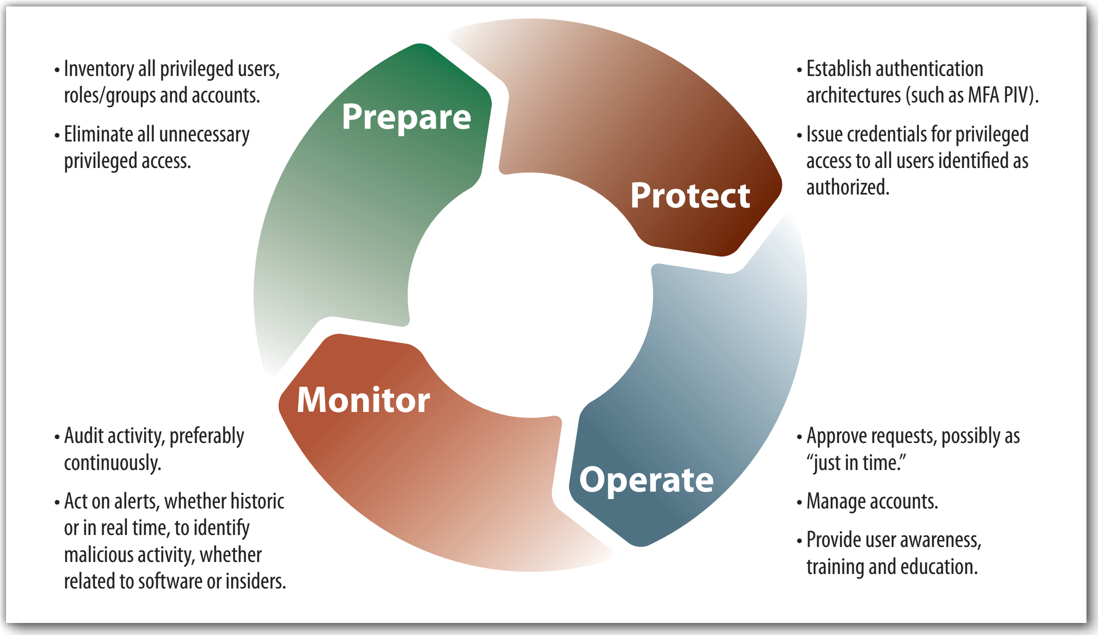
Table 4. Success and Failure Factors for PIM/PAM Implementation

	Step	Success	Failure
Goal No. 1: Identify which resources (individuals and systems) have elevated access to protected resources.	Identify and document mission-critical and sensitive resources. Identify the individuals and accounts that interact with mission-critical and sensitive resources. Identify the individuals (and services) that require elevated access to the protected resources.	Start with an honest discussion among *all* stakeholders involved in the management and strategic use of sensitive accounts; include business owners, end users and executives, not just the CSO, CIO and IT administrators. Achieve consensus as to who should be granted privileged access—the goal is to limit the number of users who can have elevated access.	Inability to achieve consensus on who should be granted elevated access. Note: PIM/PAM requires fundamental changes in how sensitive credentials are disclosed, changed and attributed. Individuals who once enjoyed unlimited, anonymous access will resist accountability or losing privilege. A PIM/PAM project is likely to succeed only with the active sponsorship of top management.
Goal No. 2: Understand the scope of privileged users' interactions with protected resources.	Conduct a risk assessment by analyzing vulnerabilities, impact and likelihood of misuse or abuse of elevated access by privileged users.	Engage those key stakeholders, such as the system owner, who understand the threats to the business scenario and/or who will suffer the most should the solution take too long to implement, unnecessarily add to IT staff workloads or provide insufficient coverage. Use a scenario-based approach to validate the results of your assessment.	The inability to define and scope the problem can lead to a wasted effort, whether at the procurement level (e.g., inadequately specified requirements) or the project level (e.g., delays, overruns, scope creep).
Goal No. 3: Establish a privileged user management framework to mitigate the risk of these users engaging in unwanted behavior.	Develop a secure operating environment for the privileged user population. Execute effective provisioning of privileged users. Implement runtime access control using privileged user management techniques. Perform ongoing monitoring of privileged users at a level commensurate to the risk posed.	Establish a governance framework that aligns with operational policies and management controls and is enabled by a secure operating environment Establish a secure operating environment (e.g., complies with the top five Critical Security Controls). Conduct the project as a series of trial deployments that build upon each other, each encompassing a test environment with a realistic sampling of target systems, applications and user roles.	Project execution without a clear roadmap on how to get there. Complex environments with unanticipated integration challenges: heterogeneous environments; inadequate bandwidth on WAN/LAN links; lack of existing change, asset, and configuration processes; and frequently changing and overlapping lines of delegation and control that will affect the deployment and management of privileged identities and accounts.
Goal No. 4: Improve this implementation by tailoring these activities based on resources, environment, mission, business needs and privileged user population.	Consult leading information security guidance on methods to further improve privileged user management throughout the enterprise.	Incorporate PIM/PAM in strategic planning for the enterprise. Establish appropriate task forces and action plans to resolve alerts and other issues raised by the PIM/PAM solution.	Lack of ongoing emphasis on privileged identity and access management. PIM/PAM solutions are not a "build and forget" solution.

[18] ICAM Privileged User Instruction and Implementation Guide, Identity, Credential, & Access Management, Oct. 15, 2014, www.idmanagement.gov/IDM/servlet/fileField?entityId=ka0t0000000TNJOAA4&field=File__Body__s

What to Look for in a Solution to Privileged Access

Procurement of a PIM/PAM solution can be a complex process, even for smaller enterprises. Successful acquisition depends on the correct level of requirements analysis and specification, especially if your organization will be turning to an outside vendor for procurement support. Operationalizing a PIM/PAM solution will require attention to four major activities, as shown in Figure 4, although the details will vary depending on the organization—its business and organization culture and its operational and technical environment.



- Inventory all privileged users, roles/groups and accounts.
- Eliminate all unnecessary privileged access.

- Establish authentication architectures (such as MFA PIV).
- Issue credentials for privileged access to all users identified as authorized.

- Approve requests, possibly as "just in time."
- Manage accounts.
- Provide user awareness, training and education.

- Audit activity, preferably continuously.
- Act on alerts, whether historic or in real time, to identify malicious activity, whether related to software or insiders.

Figure 4. Activities PIM/PAM Solutions Must Support

Many sources are available to help establish requirements for PIM/PAM solutions, but perhaps the most effective method is to base technical (and operational) requirements on key frameworks such as NIST SP 800-53, the NIST Cybersecurity Framework (CSF) and the CIS Critical Controls.

Table 5 provides a start on this process, using recommendations from the NIST April 2016 whitepaper, titled "Best Practices for Privileged User PIV Authentication."[19] This should be considered a starting point—other security (and privacy) controls will be relevant given the diversity in any given enterprise as to the business and operational needs for PIM/PAM.

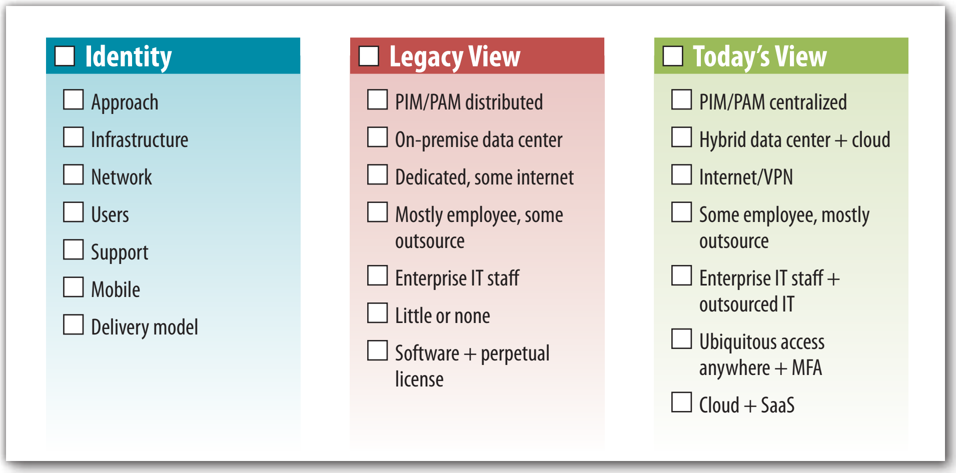
Table 5. Technical Requirements to Consider in a PIM/PAM Solution

PIM/PAM Requirement: **The solution should …**	**Requirement Source:** **NIST SP-800-53 Control Number** **NIST CSF Category**
• Support all duties associated with privileged account management, including creating, enabling, modifying, disabling and removing privileged accounts, as well as specifying each account's privileges. • Monitor all privileged account use. • Track that all requests for access to existing privileged accounts or for creation of new privileged accounts are appropriately authorized. • Limit the ability to make approved changes to systems (including the PIM/PAM solution itself) to qualified and authorized privileged users.	AC-2, Account Management AC-3, Access Enforcement CM-5, Access Restrictions for Change
• Support the assignment of privileges so that no single privileged user has excessive privileges, avoiding violation of the principles of separation of duties and least privilege.	AC-5, Separation of Duties AC-6, Least Privilege PR.AC-4 PR.PT-3
• Limit consecutive authentication failures for privileged accounts.	AC-7, Unsuccessful Logon Attempts
• Lock and/or terminate a privileged user's privileged session after a period of inactivity or upon user request. • Terminate network connections from privileged accounts after a defined period of inactivity.	AC-11, Session Lock AC-12, Session Termination SC-10, Network Disconnect
• Restrict which systems can be accessed remotely by privileged users and what actions those users can perform on each system via remote access.	AC-17, Remote Access PR.AC-3: Remote Access Is Managed
• Log the appropriate events related to privileged account use. • Generate one or more audit records for every action taken using a privileged account. • Provide alerts to identify inappropriate or unusual activity.	AU-2, Audited Events AU-3, Content of Audit Record AU-6, Audit Review, Analysis and Reporting AU-12, Audit Generation PR.PT-1
• Provide monitoring of all privileged account usage, preferably continuous, to provide rapid identification of threats.	CA-7, Continuous Monitoring SI-4, Information System Monitoring
• Uniquely identify and authenticate each privileged user. • Provide robust credential management services for user and system identifiers.	IA-2, Identification and Authentication (Organizational Users) IA-8, Identification and Authentication (Non-Organizational Users) IA-4, Identifier Management IA-5, Authenticator Management
• Protect confidentiality and integrity of all communications related to privileged user authentication and privileged sessions.	SC-8, Transmission Confidentiality and Integrity PR.AC-1

[19] Best Practices for Privileged User PIV Authentication, National Institute of Standards and Technology, April 21, 2016, http://csrc.nist.gov/publications/papers/2016/best-practices-privileged-user-piv-authentication.pdf

Legacy Versus Today and Then Toward the Future

In conclusion, the modern trends of decentralizing the enterprise structure in terms of workforce and mobility—the availability of access from anywhere using mobile/cloud computing—is giving rise to new demands for IAM. Figure 5 shows the elements that are affecting this approach as we move into the future.



□ Identity	□ Legacy View	□ Today's View
□ Approach	□ PIM/PAM distributed	□ PIM/PAM centralized
□ Infrastructure	□ On-premise data center	□ Hybrid data center + cloud
□ Network	□ Dedicated, some internet	□ Internet/VPN
□ Users	□ Mostly employee, some outsource	□ Some employee, mostly outsource
□ Support	□ Enterprise IT staff	□ Enterprise IT staff + outsourced IT
□ Mobile	□ Little or none	□ Ubiquitous access anywhere + MFA
□ Delivery model	□ Software + perpetual license	□ Cloud + SaaS

Figure 5. Elements That Affect the Approach to PIM/PAM

Today's focus on access management (PIM/PAM)—the realization that limiting the number and privileges of those who have special access to IT resources—is a good sign that organizations are concerned about data hygiene and maintenance, as well as the risk of unmonitored, elevated access to sensitive data or resources. However, better solutions are still needed. We need systems that provide for more granular, fine-tuned control and monitoring; protect against credential compromise; and provide real-time alerts for malicious activity across geographical boundaries and time zones.

About the Authoring Team

Barbara Filkins, a senior SANS analyst who holds the CISSP and SANS GSEC (Gold), GCH (Gold), GSLC (Gold), and GCPM (Silver) certifications, has done extensive work in system procurement, vendor selection and vendor negotiations as a systems engineering and infrastructure design consultant. She is deeply involved with HIPAA security issues in the health and human services industry, with clients ranging from federal agencies (Department of Defense and Department of Veterans Affairs) to municipalities and commercial businesses. Barbara focuses on issues related to automation—privacy, identity theft and exposure to fraud, as well as the legal aspects of enforcing information security in today's mobile and cloud environments.

Sponsor

SANS would like to thank its sponsor:

ca® technologies