Capability Framework for Privileged Access Management

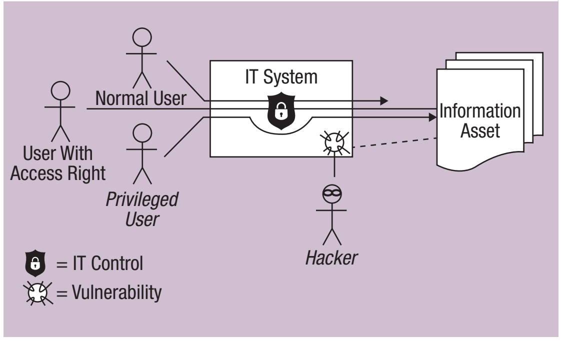
The average total cost of a data breach is about US $4 million, whereas the average cost for a stolen record increased slightly from US $154 in 2015 to US $158 in 2016.[1] Why are these data lost? About 48 percent of all breaches are caused by malicious attacks.[2] Passwords are often the entrance door for attackers: 63 percent of all passwords were either weak, got hijacked or had not been changed from their default value.[3]

Attacks from insiders are another key challenge to consider; these are the most difficult attacks to detect and are often not detected at all.[4] The reason for this lack of detection is that perimeter defense is ineffective against a potential intruder who is already behind the firewalls and defense systems. Data are exposed to such actors. Hence, sophisticated attackers will strive to get the highest privileges, as this allows them to access the most valuable information by circumventing IT controls.[5]

This article focuses on electronic access and will not discuss physical access or privileged access gained via social engineering. With this restriction in mind, the model shown in **figure 1** illustrates types of access to information assets. It consists of four elements

- **Users**—Humans who have access to IT systems
- **IT systems**—These provide access to information assets. They are typically networks, routers, servers, databases, devices, applications and other access means.
- **IT controls**—These are measures to protect information assets against noncompliant access. An example might be an enforced dual control when a bank grants credit to a customer.
- **Information asset**—This is any part of the IT environment of value for the business. It is what needs to be protected. This can be data, software, hardware and any resource considered an information asset.

Figure 1—Distinguishing Privileged Access From Regular Access to Information Assets



Source: R. Hoesl, M. Metz, J. Dold, S. Hartung. Reprinted with permission.

Richard Hoesl, CISSP, SCF
Is responsible for identity and access management (IAM) consulting services with Accenture's security practice in Germany, Austria and Switzerland. He is a seasoned expert on identity and access management and enterprise application security with a focus on financial services, helping organizations to resolve information security and compliance challenges in a digital world.

Martin Metz, CISA
Is a manager with Accenture's security practice, author and expert on IAM. During his career, Metz designed and implemented SAP GRC systems, SAP role concepts and overarching IAM frameworks. He has led large-scale privileged access management (PAM) implementations. He conducted information security audits at clients across a wide variety of markets in Europe and the United States.

Joachim Dold
Is an IT strategy principal working for Accenture with 19 years of experience in the telecommunications, banking and insurance industry. He has worked in security transformation programs, software development and infrastructure projects and has held executive responsibility as the country manager of an offshore unit during the unit's ramp-up phase.

Stefan Hartung
Is an IT security consultant with Accenture's security practice. During his career, he has designed large-scale PAM implementations, researched in the areas of botnet detection and policy enforcement for bring-your-own-device setups, and developed security-related Android applications. Hartung is an expert for IAM, focused on privileged accounts.

This model distinguishes the three types of access channels:

- **Regular access channels**—These are protected channels that are subject to IT controls.
- **Privileged access channels (PACs)**—These are channels that might circumvent controls but are deemed necessary and legitimate channels for reasons of practicality or cost.
- **Vulnerabilities**—These are unintended access channels, not demanded by any technical or business requirement.

This article focuses on PACs that are of high interest for attackers. Examples include domain administrators, root accounts and emergency users.

Due to their importance, PACs are the subject of standards, norms, frameworks and laws. For instance, the SANS Institute requires multifactor authentication (CSC 12-12) for privileged accounts, frequent reviews of the use of these accounts (CSC 16-1) and analysis of anomalous behavior (CSC 12-1).[6] Banks in the European Union are required to recertify critical privileged accounts every six months. International Organization for Standardization (ISO)/International Electrotechnical Commission (IEC)'s ISO/IEC 27001:2013 requires restriction and control of the allocation and use of privileged access.

A 2016 study conducted by Thycotic and Cybersecurity Ventures found that 80 percent of the more than 500 chief information security officers (CISOs) surveyed consider privileged access management (PAM) a significant topic, and a number of them have already implemented specific PAM solutions.[7] Typical objectives of such solutions are:

- Keeping the number of privileged access channels low
- Authorizing, activating and deactivating the usage of privileged access channels
- Detecting, evaluating, recording and terminating the usage of privileged access channels

What makes a PAM solution successful? The following framework will introduce the four building blocks of any PAM solution:

1. Governance
2. Privileged access channel inventory management
3. Privileged users management

> **“Governance is critical since measures to limit and control PACs are often regarded as a sign of mistrust by IT administrators.”**

4. Control and monitoring

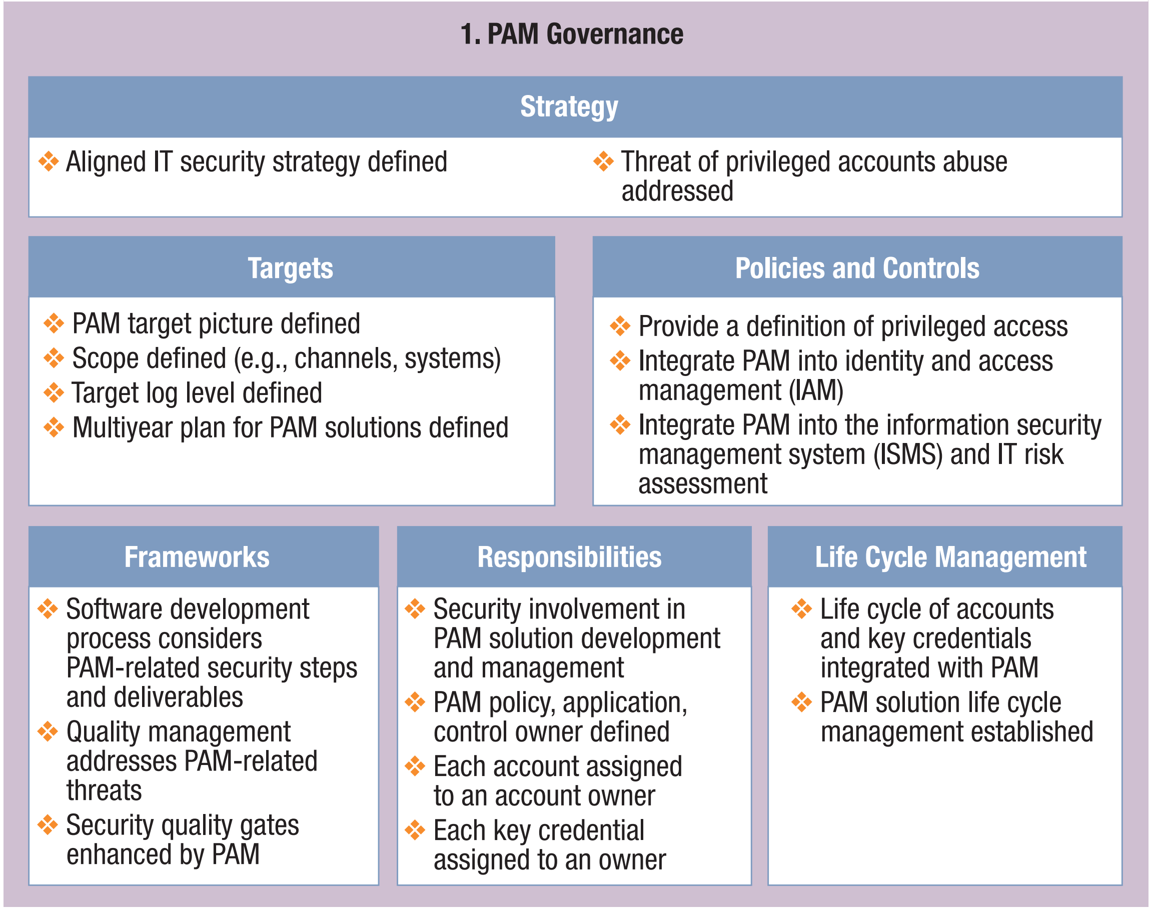
Each building block contains several components to consider in an assessment or audit. Indicators are provided per component to enable practitioners to ask the right questions and finally strengthen PAM at the organization.

Governance

Without governance, security efforts tend to be random, and the benefits from one-off investments erode quickly. Governance is critical since measures to limit and control PACs are often regarded as a sign of mistrust by IT administrators. To gain their support but also to control the implementation of PAM measures is, therefore, a crucial component of governance.

Figure 2 shows important indicators concerning the integration of PAM into IT governance. Any IT security strategy not addressing these indicators must be considered incomplete and as exposing the company to significant risk. The types of indicators include:

Figure 2—Governance Components of PAM



1. PAM Governance

Strategy

- Aligned IT security strategy defined
- Threat of privileged accounts abuse addressed

Targets

- PAM target picture defined
- Scope defined (e.g., channels, systems)
- Target log level defined
- Multiyear plan for PAM solutions defined

Policies and Controls

- Provide a definition of privileged access
- Integrate PAM into identity and access management (IAM)
- Integrate PAM into the information security management system (ISMS) and IT risk assessment

Frameworks

- Software development process considers PAM-related security steps and deliverables
- Quality management addresses PAM-related threats
- Security quality gates enhanced by PAM

Responsibilities

- Security involvement in PAM solution development and management
- PAM policy, application, control owner defined
- Each account assigned to an account owner
- Each key credential assigned to an owner

Life Cycle Management

- Life cycle of accounts and key credentials integrated with PAM
- PAM solution life cycle management established

Source: R. Hoesl, M. Metz, J. Dold, S. Hartung. Reprinted with permission.

- **Strategy indicators**—How does PAM relate to the overall IT and IT security strategy? The latter should highlight the principles underlying the company's approach to PAM. For example, a key principle could be that privileged access is not allowed except if technically unavoidable or if required to avoid privileged rights accumulations in a single PAC.

- **Target indicators**—The scope of PAM must be specified in a meaningful way, derived from risk targets of the IT organization, and addressing systems, infrastructure components, applications, accounts and other related areas. The scope is the baseline of the implementation work and the biggest driver of costs.

- **Policies and controls**—An applicable definition of privileged access must be given, which allows IT system owners, development teams and others to derive a system-specific specification of what constitutes a PAC. Furthermore, an authorization policy for PACs must be given, as must be controls on how to safeguard the company from PAC misuse.

- **Frameworks, responsibilities and life cycle management**—PAM must be integrated into the frameworks, critically contributing to its targets. A prominent example is software development, where important decisions about future PACs are made.

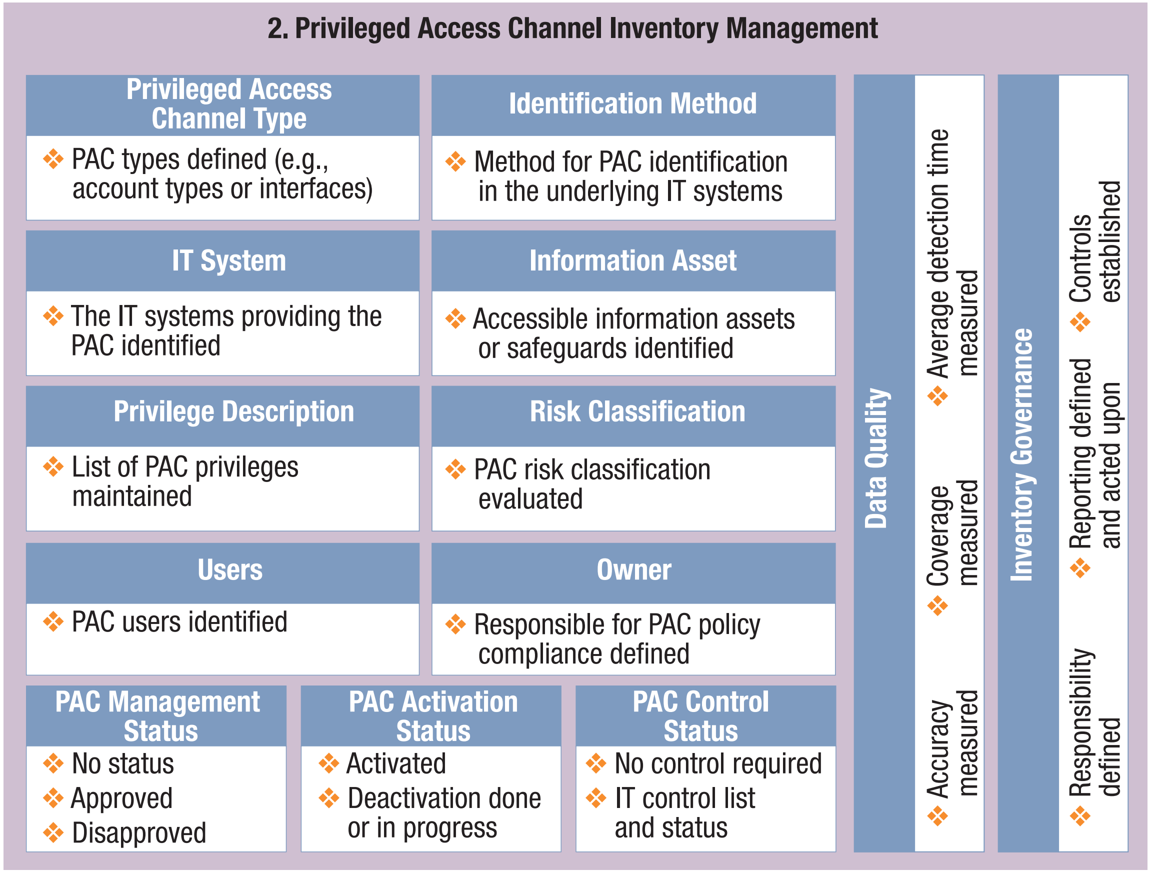
- **Life cycle management**—Governance makes sure that processes, controls, responsibilities and other factors will meet the requirements of the entire life cycle. Considering the processes until decommission or phase-out is as crucial for security gains as setup and maintenance phases.

Inventory

The PAC inventory is the basis for the management of PACs. It identifies PACs and shows their risk, owner and users and whether actions regarding a PAC are required. **Figure 3** shows the core indicators for PAC inventory management:

- **Privileged access channel type and identification method**—A classification of PAC types is a strong sign that a company has moved from an *ad hoc* PAM to a systematic approach. However, only if PACs can be identified on an IT system level can the organization credibly protect against their misuse.
- **IT system, information asset, privilege description, users and risk classification**—To assess the risk of a PAC and to control it against misuse, knowing which IT system provides it, which information assets are accessed and who (the users) can do what (the privileges) with them is necessary.
- **Owner, PAC management, activation and control status**—These are the management parameters of a PAC, allowing for the extraction of key performance indicators (KPIs), e.g., the number of active, but disapproved PACs.
- **Quality of the inventory**—The availability of the previously mentioned data is a strong indicator that a company has adopted a systematic PAC management approach. Accuracy, IT system

Figure 3—Attributes of Privileged Access Channels in a PAC Inventory



2. Privileged Access Channel Inventory Management

Privileged Access Channel Type
- PAC types defined (e.g., account types or interfaces)

Identification Method
- Method for PAC identification in the underlying IT systems

IT System
- The IT systems providing the PAC identified

Information Asset
- Accessible information assets or safeguards identified

Privilege Description
- List of PAC privileges maintained

Risk Classification
- PAC risk classification evaluated

Users
- PAC users identified

Owner
- Responsible for PAC policy compliance defined

PAC Management Status
- No status
- Approved
- Disapproved

PAC Activation Status
- Activated
- Deactivation done or in progress

PAC Control Status
- No control required
- IT control list and status

Data Quality
- Accuracy measured
- Coverage measured
- Average detection time measured

Inventory Governance
- Responsibility defined
- Reporting defined and acted upon
- Controls established

Source: R. Hoesl, M. Metz, J. Dold, S. Hartung. Reprinted with permission.

coverage and average PAC detection time are important quality measures.

- **Governance of the inventory**—Inventory quality tends to deteriorate over time if it is not managed by governance processes. Therefore, organizations should ensure that the quality of the inventory improves. This includes KPIs, reporting lines and quality controls.

Privileged Users

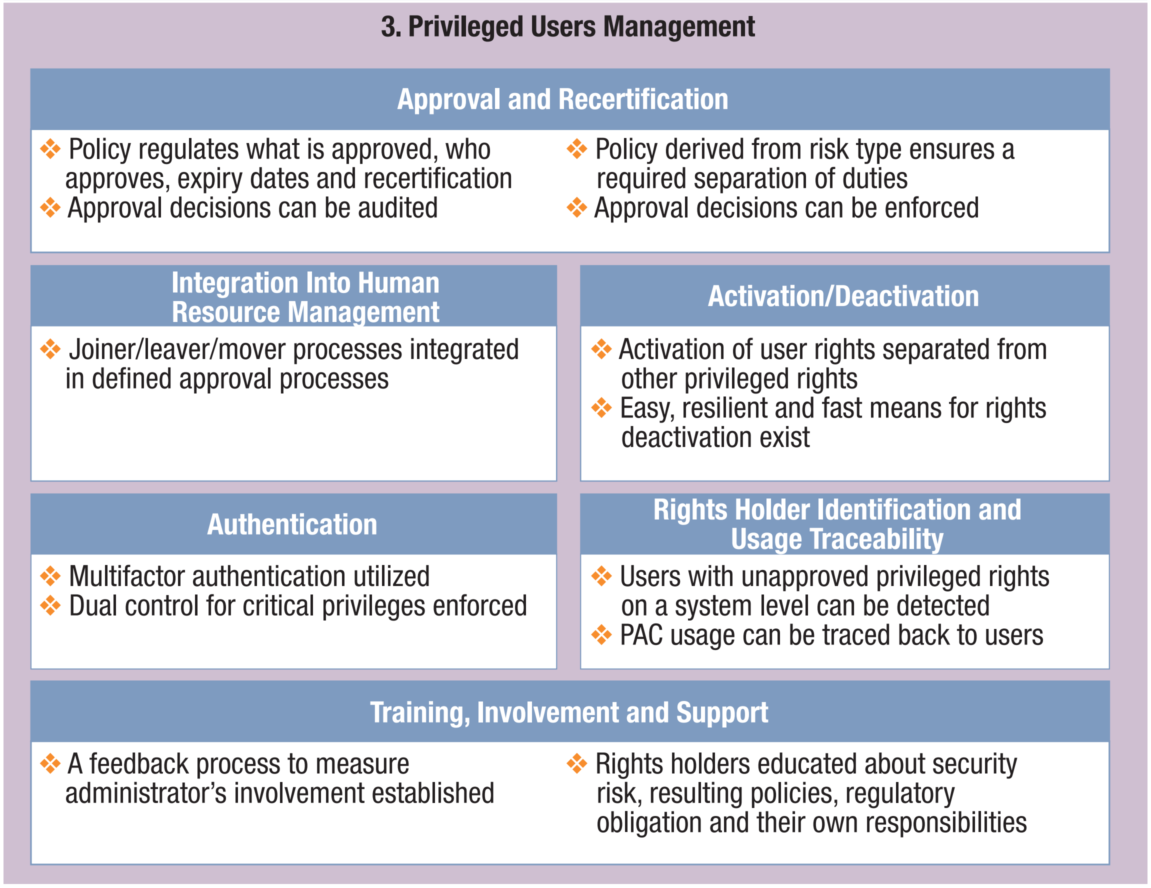
Having identified the existing privileged rights on a system level, it is now necessary to control who has the right to use PACs. **Figure 4** provides an overview of the indicators:

- **Approval and recertification**—Basic implementations comprise organizational guidelines and a clearly defined process specifying how roles and rights have to be requested, providing rules for expiry dates, and enabling recertification and on-demand auditing. Compliance with least privilege and segregation of duties (SoD) is enforced technically in mature implementations. This discipline culminates in automated processes deriving parts of the policy based on risk ratings.

> **“Inventory quality tends to deteriorate over time if it is not managed by governance processes.”**

- **Integration into human resource management and activation/deactivation**—Because IT landscapes experience constant change,

Figure 4—Identity and Access Management for Privileged Users



3. Privileged Users Management

Approval and Recertification

- Policy regulates what is approved, who approves, expiry dates and recertification
- Approval decisions can be audited
- Policy derived from risk type ensures a required separation of duties
- Approval decisions can be enforced

Integration Into Human Resource Management

- Joiner/leaver/mover processes integrated in defined approval processes

Activation/Deactivation

- Activation of user rights separated from other privileged rights
- Easy, resilient and fast means for rights deactivation exist

Authentication

- Multifactor authentication utilized
- Dual control for critical privileges enforced

Rights Holder Identification and Usage Traceability

- Users with unapproved privileged rights on a system level can be detected
- PAC usage can be traced back to users

Training, Involvement and Support

- A feedback process to measure administrator’s involvement established
- Rights holders educated about security risk, resulting policies, regulatory obligation and their own responsibilities

Source: R. Hoesl, M. Metz, J. Dold, S. Hartung. Reprinted with permission.

integration of the PAM solution with joiner/mover/leaver processes is a key factor of a successful PAM implementation. Manual provisioning of users and target systems is not an option in times of turnover rates of several hundred users/systems per week. Because of the SoD principle, it must be ensured that user access rights assignment is separated from other privileged rights wherever possible.

- **Authentication and rights holder identification and usage traceability**—The dual control is key when it comes to highly critical privileges, which in mature processes can also be enforced in the authentication phase. Multifactor authentication or succeeding zero-factor authentication methods are state of the art and likely to become obligatory in the next few years.
  The ability to trace back privileged activities to personal identities and to detect illicitly assigned privileges signals a more mature PAM implementation, even more mature when fully automated.
- **Training, involvement and support**—An asset of mature PAM implementations is the active support and training of responsible persons and users. Furthermore, open discussions with administrators who are likely to be most affected by changes will improve end-user satisfaction and thereby also the level of security by means of users living the processes.

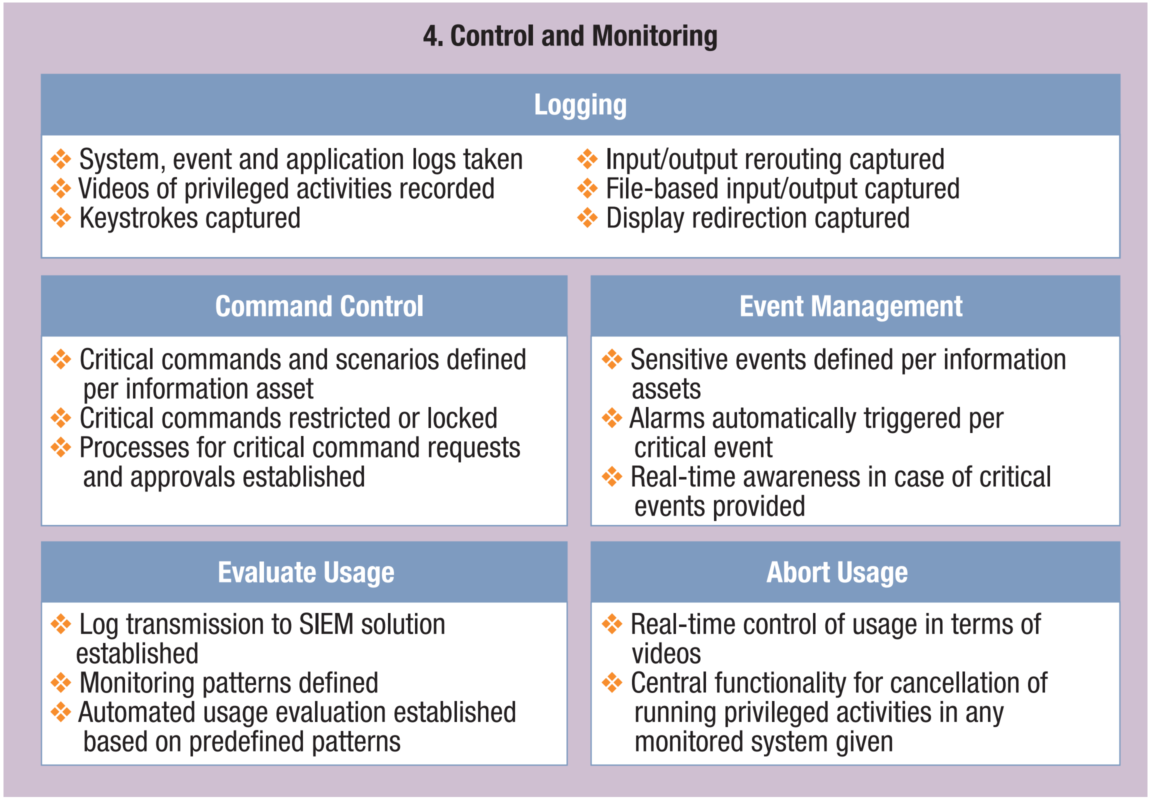
Control and Monitoring

Having defined the governance structure and implemented the means to identify PACs and assign them to users, it is now necessary to take care of the usage of such channels. PAM solutions strive to accomplish several objectives: trace back privileged abilities to users, audit privileged actions, evaluate privileged rights usage in real time, terminate suspicious actions, and block specific rights or make them subject to additional approvals. **Figure 5** shows indicators concerning the ability of a company to attain these targets:

- **Logging**—This category reflects a technical core feature of any PAM implementation: session monitoring. Log data can be divided into system events (captured via agents), keystroke logs and video logs. Keystroke logs and video logs might be captured directly on the system (PAM agent) or within the network (proxy implementation).
  Care should be taken to complement a proxy implementation by additional safeguards on the target system, since critical activities on the target system cannot be detected by the network-based proxy implementation.
- **Command control and event management**—Command control might also be a sign of more mature PAM implementations since command control requires that critical activities have been defined and are suppressed. One good practice example is enforcing case-by-case approvals of critical commands. Another example is a modern security information and event management (SIEM) solution that detects critical system events and initiates real-time countermeasures.

- **Evaluate usage and abort usage**—Log data can be archived and held for forensic analyses. More mature implementations come with SIEM integration (forwarding of critical PAM-related events), definitions of monitoring patterns and automated controls of session data. Near-time evaluation is a prerequisite for decisions to cancel running sessions from a central point of control.

Figure 5—Control and Monitoring Building Block



4. Control and Monitoring

Logging

- System, event and application logs taken
- Videos of privileged activities recorded
- Keystrokes captured
- Input/output rerouting captured
- File-based input/output captured
- Display redirection captured

Command Control

- Critical commands and scenarios defined per information asset
- Critical commands restricted or locked
- Processes for critical command requests and approvals established

Event Management

- Sensitive events defined per information assets
- Alarms automatically triggered per critical event
- Real-time awareness in case of critical events provided

Evaluate Usage

- Log transmission to SIEM solution established
- Monitoring patterns defined
- Automated usage evaluation established based on predefined patterns

Abort Usage

- Real-time control of usage in terms of videos
- Central functionality for cancellation of running privileged activities in any monitored system given

Source: R. Hoesl, M. Metz, J. Dold, S. Hartung. Reprinted with permission.

Conclusion

New PACs are constantly created in today's fast-changing IT organizations. These channels are the most desirable target for attackers, and any diligent IT organization must strive to protect these channels. An important enabler in this effort is technology, which allows these channels to be detected. Another important enabler is appropriate processes to manage and protect channels. Governance, in turn, focuses and sustains this technological and organizational effort. But only if governance succeeds in creating a strong security culture can privileged access management truly succeed. Thus, PAM must not be regarded as a tool but as an integral part of an ongoing organizational effort to increase the security of the organization.

Endnotes

1 Ponemon Institute, *2016 Cost of Data Breach Study*, Ponemon Institute, 2016, *www-03.ibm.com/security/data-breach/*

2 *Ibid*.

3 *Ibid*.

4 *Ibid*.

5 Wenzler, N.; "Managing Privileged Access is Crucial to Preventing Data Breaches," *Security Magazine*, 28 June 2016, *www.securitymagazine.com/articles/87241-managing-privileged-access-is-crucial-to-preventing-data-breaches*

6 SANS Institute, *CIS Critical Security Controls—Version 6.0*, Center for Internet Security, *https://www.cisecurity.org/critical-controls/*

7 Thycotic and Cybersecurity Ventures, *The State of PAM Security*, 2016, p. 3, *https://thycotic.com/wp-content/uploads/2013/03/State-of-PAM-Executive-Summary.pdf*