jamk.fi

Newcomer’s introduction to Privileged Access Management

Antti Kuokkanen

Bachelor’s thesis
October 2020
Technology
Bachelor of Engineering, Information and Communications Technology

Jyväskylän ammattikorkeakoulu
JAMK University of Applied Sciences

jamk.fi

Description

Author(s) Kuokkanen, Antti	Type of publication Bachelor’s thesis	Date October 2020
		Language of publication: English
	Number of pages 61	Permission for web publication: x

Title of publication
Newcomer’s introduction to Privileged Access Management

Degree programme
Bachelor of Engineering, Information and Communications Technology

Supervisor(s)
Rantonen, Mika; Jokinen, Juha

Assigned by
Nixu Corporation Oyj

Abstract

A considerable portion of today’s cybercrime involves misusage of privileged accounts. It has been estimated that on average in company environments there is double the number of privileged accounts compared to the number of employees. Often these accounts are left behind in different systems without being actively managed, sometimes leading to eventually being completely forgotten. Considering the access level of such credentials to confidential and critical company resources, they pose a severe risk to the company’s cybersecurity. In different organizations awareness has been increasing about the need to bring these privileged accounts under active management and protection.

A growing need for privileged access management in the customerfield has also been noticed in the assigner company of this work. Based on the theory part, the goal was to write an introduction guide for the assigner company, which could be used in introducing new employees to PAM (Privileged Access Management).

Privileged accounts can be managed by taking benefit from PAM tools and processes. The theory part concentrated on PAM backgrounds, necessity, features, and implementation. Locating PAM in a wider IAM (Identity and Access Management) framework was also one of the addressed topics.

The introduction guide was divided into three main categories: PAM backgrounds, components, and lifecycle process. The guide can be used to gain necessary base-level understanding about PAM, which provides the possibility to further deepen knowledge about technical implementations and PAM products from different vendors. Goal of the guide is not to give detailed description about technical configurations or features, but instead give introduction to the subject for someone who gets involved in the subject for the first time.

Keywords/tags (subjects)
PAM, IAM, privileged access, access management, introduction guide

Miscellaneous (Confidential information)

jamk.fi

Kuvailulehti

Tekijä(t) Kuokkanen, Antti	Julkaisun laji Opinnäytetyö, AMK	Päivämäärä Lokakuu 2020
		Julkaisun kieli: Englanti
	Sivumäärä 61	Verkkojulkaisulupa myönnetty: x

Työn nimi
Newcomer's introduction to Privileged Access Management

Tutkinto-ohjelma
Insinööri (AMK), tieto-ja viestintätekniikka

Työn ohjaaja(t)
Rantonen, Mika; Jokinen, Juha

Toimeksiantaja(t)
Nixu Corporation Oyj

Tiivistelmä

Suuri osa tämän päivän kyberrikollisuudesta on kytköksissä korkeiden käyttövaltuuksien käyttäjätunnusten väärinkäyttöön. Tällaisia tunnuksia on arveltu olevan yrityksissä keskimäärin kaksinkertainen määrä yrityksen henkilömäärään nähden. Usein tunnukset ovat jääneet eri järjestelmiin ilman aktiivista hallinnointia, jolloin pahimmassa tapauksessa tunnusten olemassaolosta ei ole edes tietoa. Ottaen huomioon tunnusten pääsy korkeankin suojaustason ja yritysten kannalta kriittisiin tietoihin, tilanteesta muodostuu merkittävä tietoturvariski. Eri organisaatioissa onkin alettu havahtua tarpeelle tällaisten tunnusten aktiiviseen hallintaan ja suojaamiseen.

Asiakasorganisaatioiden kasvanut tarve korkeuden käyttövaltuuksien hallintaan on havaittu myös toimeksiantajayrityksessä. Teoriapohjaan perustuen tavoitteena olikin tuottaa työn toimeksiantajalle opas, jota voidaan hyödyntää PAM:in (Privileged Access Management) parissa työskentelevien henkilöiden perehdyttämisessä.

Korkeiden käyttövaltuuksien tunnuksia voidaan hallita PAM työkaluilla ja prosesseilla. Työn teoriaosuudessa paneuduttiin PAM:in taustoihin, tarpeeseen, ominaisuuksiin ja käyttöönottoon. Työssä käsiteltiin myös PAM:in sijoittumista laajempaan IAM:in (Identity and Access Management) viitekehykseen.

Tuloksena syntynyt opas jaettiin kolmeen osa-alueeseen: PAM:in taustoihin, komponentteihin ja elinkaareen. Opasta voidaan hyödyntää tarpeellisen pohjatiedon hankkimiseen PAM:ista, jonka perusteella on mahdollista edetä syvemmälle teknisiin implementaatioihin ja toimittajakohtaisiin tuotteisiin. Oppaan tarkoitus ei ole kuvata eri PAM-tuotteiden teknisiä konfiguraatioita tai ominaisuuksia, vaan antaa aiheen pariin ensi kertaa tulevalle tarvittava perehdytys aiheeseen.

Avainsanat (asiasanat)
PAM, IAM, korkean tason tunnusten pääsy, pääsynhallinta, perehdytysopas

Muut tiedot (Salassa pidettävät liitteet)

Contents

Figures

Tables

Abbreviations

2FA	2-Factor Authentication
ABAC	Attribute-Based Access Control
ACA	Advanced Control and Audit
AD	Active Directory
API	Application Programming Interface
AtoA	Application to Application
CIA	Confidentiality, Integrity and Availability
DBA	Database Administrator
DevOps	Development and Operations
DNS	Domain Name System
FIM	Federated Identity Management
HA	High Availability
IAM	Identity Access Management
IGA	Identity Governance and Administration
IdP	Identity Provider
ISP	Internet Service Provider
IT	Information Technology
ITSM	Information Technology Service Management
KPI	Key Performance Indicator
KRI	Key Risk Indicator
LDAP	Lightweight Directory Access Protocol
MFA	Multi-Factor Authentication
OAuth	Open Authorization
OS	Operating System
PAM	Privileged Access Management
RBAC	Role-Based Access Control
RDP	Remote Desktop Protocol
SAML	Security Assertion Markup Language
SIEM	Security Information and Event Management
SSH	Secure Shell
SSO	Single sign-on

UBA	User Behavior Analysis
VPN	Virtual Private Network
XML	Extensible Markup Language

1 Introduction

1.1 Brief introduction to Nixu Corporation

Nixu was founded in 1988 by Pekka Nikander. The company's name was a result of combining Pekka’s family name, Unix operating system, and a student lab “Niksula” at Helsinki University of Technology. Soon after that, in 1989, Nixu already organized the first virus seminar. During its first years, Nixu was not concentrating in cybersecurity, however. Assignments included more general Internet operations, such as helping customers with their e-mail systems and working closely on different ISP (Internet Service Provider) platforms. For example, between 1994 and 1998 Nixu administered the DNS (Domain Name System) service of Telecom Finland, which later became Telia. (About | Nixu Cybersecurity 2020.)

Today Nixu is probably most known for its mission to *“keep the digital society running”* by providing a wide range of cybersecurity-related services. This catalogue holds over 60 titles varying from digital forensics and incident response services all the way to organizing escape rooms for the customers. (All services | Nixu Cybersecurity 2020.)

Nixu started as a one-man company but has been growing at an accelerating rate since. First paid employees started their work in 1992, and later in the ‘90s, Nixu made its first acquisition of another IT-company by acquiring NetPeople Oy in 1999. In 2010 the number of Nixuans exceeded 100 professionals, and in 2017 number had increased to over 300. In 2020 Nixu employs over 400 people in several Nordic countries. (About | Nixu Cybersecurity 2020.)

Nixu also owns an independent subsidiary company, Nixu Certification Oy, which offers official security inspections to companies. These include for instance VAHTI, Katakri 2015, and Kanta information system audits. Nixu Certification Oy is also the only Finnish company that provides CSA STAR audits. (Nixu Certification Ltd. n.d.)

1.2 Background of Thesis

The first months of employment in Nixu included an introduction to several topics and technologies that Nixu is involved with. Among others, those topics included being familiarized to titles such as IAM (Identity and Access Management) and PAM (Privileged Access Management). Those sessions revealed some impressive statistics about how big percentage of cybercrimes involved the usage of privileged accounts. One study shows that this number can be as high as 80% (Peterson 2019). Something about the current relevance of PAM indicates also that Gartner Research listed Privileged Access Management as one of the top 10 security projects for 2019 (Top 10 Security Projects for 2019). Also, at Nixu there has been a notion that in the customer-field there is a constantly growing need for Privileged Access Management.

Introduction sessions led to the idea of creating an introduction guide to PAM for Nixu. This kind of guide will serve the needs of the company as well as support personal professional growth, so the suggestion about the subject was met with approval.

1.3 Goal and research method

This thesis will try to answer the question “What is relevant general information about Privileged Access Management for someone who gets involved in PAM projects?”. To answer the question, an introduction guide to PAM is created, which will be placed in Nixu’s intra-network. This guide is also found as an appendice of this thesis.

Research can be done using either quantitative or qualitative methods or mixing them. Quantitative methods are well suited for making surveys for example by conducting measurements or rankings. This kind of methodology might aim to identify patterns or make generalizations about the causes of a phenomenon. Quantitative data is typically expressed in numbers. (McCombes 2019.)

Qualitative research methods are based on analyzing non-numerical data, as opposed to quantitative research. The aim can be to get a better in-depth understanding of concepts or experiences and typically does not include statistical analysis. Approaches to qualitative research are often flexible. (Bhandari 2020.)

As the goal of this thesis is to try to understand concepts and share knowledge about them, qualitative research was chosen as the method. The material is gathered using the secondary research method by searching for pre-existing documents about the subject. These documents include various sources such as articles, books, and videos.

2 Defining identity

2.1 What is identity?

By a quick glance, identity might seem like a simple concept but diving deeper brings up lots of various aspects. Things that can have their own identity vary from individuals to nations and just about everything between. Identity can further be divided to for example cultural, linguistic, moral, online, and social identities. No wonder why people have their own diverging views about the meaning of identity, which is also the case in different scientific contexts. (Coulmas 2019, 1-2.)

The word *Identity* comes from the Latin word “Iden”, originally meaning “the same”. Even though the word is used in different ways in different contexts, two main ideas are persistent. One way to approach identity is to describe it as characteristics to differentiate from one another. This means describing identity from an external perspective, finding a way to identify an individual from a group. The second definition is linked to a person’s essential character, giving a more internal perspective for identity. (Cynthia & Brian 2012, 139-140.)

Identity can be described to be the result of combining three sets of data: identifier, credentials, and attributes. Identifiers may be a series of characters, digits, and symbols, or any other data to identify a subject. Identifiers can be globally unique over time or temporal and exist only within a particular service. Some examples of identifiers are usernames and phone numbers. Credentials are a way to justify claims regarding identities. These can be for example passwords or fingerprints. Attributes are used to describe elements of a subject to make identifying possible. Name, age, gender, and roles are for instance attributes. (Bertino & Takahashi 2010, 21-22.)

Today the word “identity” is present everywhere. Some idea of the increased commonness gives the number of English-language books in the Library of Congress having “Identity” in the title: By 2010 the total amount was around 10 000. Since 2010 the number has increased by more than 10 000 items. “Identity” has even been chosen as the Word of the Year in 2015 by Australian National Dictionary Centre. (Coulmas 2019, 1-2.)

2.2 Identity and digitalization

In today’s world, people are constantly interacting in rich and engaging virtual reality. To be able to participate in these activities, they must first have a virtual identity. It is important to note that this virtual identity does not necessarily represent one’s regular or “true” identity. For instance, it is common that on a social networking site person has a virtual identity that matches his regular identity. However, in other cases, the same person may use a very different digital identity to keep his regular identity hidden. (Cynthia & Brian 2012, 141.)

Even if virtual identity would seem distinct from the person’s regular identity, identities cannot be completely separated. This is the case since the person who is controlling the virtual identity remains the same. So even though virtual and regular identity would act very differently, an inevitable link exists between them. This can be called “projective identity”. (Cynthia & Brian 2012, 141-142.)

An individual person can be associated with several digital identities, in the same way as an individual may be known by several nicknames. Even when an individual is associated with several identities, it is necessary to be able to unambiguously point these different identities to the same individual. Individuals can be identified through a set of attributes, sometimes referred to as a *profile*. It is good to note that besides representing humans, identity in the digital era extends to including various other entities as well. For instance, such are host systems, network devices, and programming agents. In modern networked computing systems, these different identity entities often cross the boundaries of a single system. (Benantar 2006.)

2.3 Identity vs User vs Account

In information technology, user and end-user terms are often used side by side. They refer to a person or an individual who is using an IT-device, for example, a PC. Users may be further divided for example based on their expertise level, such as an advanced user or a basic user. (User 2020.)

The user account combines a username, password, and any other additional information related to the user. One common account type is an email account. Most systems which are accessed by users take advantage of accounts. Account determines which resources a user can access. (User Account n.d.)

In computing, term *identity* has wider coverage than the *user*. Identity can a representation of an entity that can be either physical or a programming agent. Physical entities can refer for example to a human, a host system, or a network device. (Benantar 2006.)

3 Basics of Identity and Access Management

3.1 Brief history

Identity and access management is the discipline that enables the right individuals to access the right resources at the right times for the right reasons. (Identity and Access Management (IAM) n.d.)

Limiting access to information is thousands of years old. Having such restrictions is not exclusive to humans, as also many animals wish to withhold some information. For an animal, this vital secret could be the location of their den or food storage. Over time several techniques have been invented to properly identify and control access. (Kael 2019.)

Managing access to information requires a confirmation that persons involved in exchanging the information are who they claim to be. Passwords are an old invention for such purposes. In military purposes passwords have also been used in a challenge-response form: one password would be the challenge, and the other side would need to know the matching password as the response. Another old way for verifying identity is called “shibboleth”, which is based on pronouncing a word or a phrase. It has been used to identify outsiders to a tribe or a region. (ibid.)

Most traditional ways of identifying the sender of a message were based on different seals. These date back to ancient Mesopotamia before pen and paper when messages were passed on clay tablets. Later when messages were delivered on paper, seals evolved to signet rings, which were used to stamp a seal on sealing wax. This would ensure the identity of the sender as well as the integrity and confidentiality of the message. (ibid.)

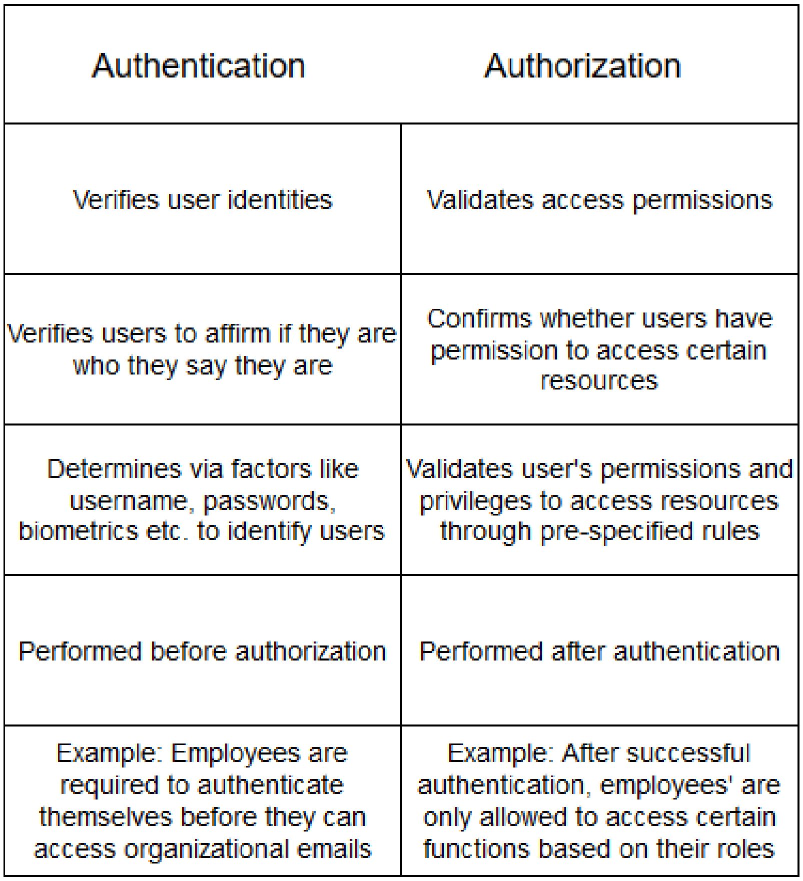
Passports have come into play as an identity document first time in 1414 in England. At that time, those documents served the purpose of securing a person even when travelling in other kingdoms. Later passports have evolved to include a photograph, biometrics, and other security measures. (ibid.)

In the digital realm, things started moving forward in 1960 when Fernando Corbato introduced the possibility to use passwords for protecting computer files. This laid foundation for first IAM solutions, which first companies started adapting in the 1980s. Controlling access took another big turn in the late 1990s when the Internet started becoming more accessible to anyone. Companies then realized that their web applications could be accessed by anyone, so securing company data began to require more control. This led to some organizations starting to develop their own IAM solutions. However, those initial solutions had issues with handling the offboarding process and lateral movement of an employee within the company. (The Evolution of IAM 2019.)

The year 2002 was significant for identity and access management when the *sarbanes-oxley* act was passed in the congress of the USA. This act was made to protect shareholders from dishonest enterprise practices, and it made public companies to be held accountable for their employee access control. Soon after that, the first generation of true IAM solutions was built by companies such as IBM and Oracle. First managed identity services were published in 2006 and first identity as a service cloud came out in 2010. The need for these services is expected to be constantly growing. (The Evolution of IAM 2019.)

3.2 Authentication

Authentication may sometimes be confused with authorization. These two terms however cover entirely distinct processes. Different steps of authentication and authorization are compared in figure 1. Authentication in short means proving ownership of an account and the process itself does not give direct access to any resources. The process is typically completed by providing a login/username and a secret. Often secret is a password or some other form of a key. Going through the authentication process simply answers the question “Are you who you say you are?”. (Haber & Rolls 2020.)



Authentication	Authorization
Verifies user identities	Validates access permissions
Verifies users to affirm if they are who they say they are	Confirms whether users have permission to access certain resources
Determines via factors like username, passwords, biometrics etc. to identify users	Validates user's permissions and privileges to access resources through pre-specified rules
Performed before authorization	Performed after authentication
Example: Employees are required to authenticate themselves before they can access organizational emails	Example: After successful authentication, employees' are only allowed to access certain functions based on their roles

Figure 1: Authentication and authorization (adapted from Authentication vs. Authorization Defined, 2020.)

Authentication can be based on three different things: something you have, something you know, or something you are. These three things could be represented respectively for example by a physical key, a password, and a fingerprint. Different types of authentication processes can also be combined. (Santuka, Banga & Carroll 2011.)

Single Sign-On (SSO) allows users to authenticate to several applications by completing just one authentication process. This can increase the user’s productivity and efficiency when credentials are not asked at every turn during accessing different resources. Single Sign-On can be commissioned in several environments, including for instance web applications, client-server applications, and SSO across multiple domains. (Scheidel 2010.)

3.3 Authorization

Authorization happens after the user has been authenticated. The authorization step is obligatory since it determines which resources the user is allowed to access. Even if the user is authenticated as a Guest, some resources - although probably very limited - can still be available. After authentication and authorization steps are completed, the target system knows the user’s identity and assigned privileges within the system. (Haber & Rolls 2020.)

Authorization can have multiple levels. When one user might be authorized to view and edit certain information, another user is allowed to only view the same resource or only part of the same resource. This can be done for example by dividing users into groups and assigning certain entitlements to certain groups. Then by being a member of a group, the user will inherit the entitlement from the group and be authorized to the resource based on the entitlement’s access level. (Scheidel 2010.)

3.4 Access controls

The traditional way in IAM to authorize users takes advantage of RBAC, role-based access control. In RBAC, permissions are inherited from the user’s job function, also known as a role. There are different roles for different job functions. These roles are then attached to identities, which might be users or groups. The best practice is to grant minimum permissions to be able to complete the defined job function. This is known as the principle of least privilege. A user might have more than one role, and if the user’s job changes in the company, the attached roles may be changed as well. Challenge in RBAC is that when new resources are added, roles must be updated accordingly to enable access to those resources. (What is ABAC for AWS? n.d.)

ABAC, attribute-based access control, is another authorization concept. Its capability to control access is based on three attribute types: user attributes, attributes related to the application or system which is accessed, and current environmental conditions. ABAC is a more flexible model than RBAC and can be used to give fine-grained access to resources. For example, defined users may be given access to certain resources only during office-hours within the same timezone as the company. (Carter 2017.)

3.5 Identity management

Proper identity management includes controlling the life-cycle of identities. Lifecycle has four phases: creation, usage, update, and revocation. Governance should be involved in every phase. Figure 2 demonstrates the lifecycle steps and relation of governance. (Bertino & Takahashi 2010, 29-30.)

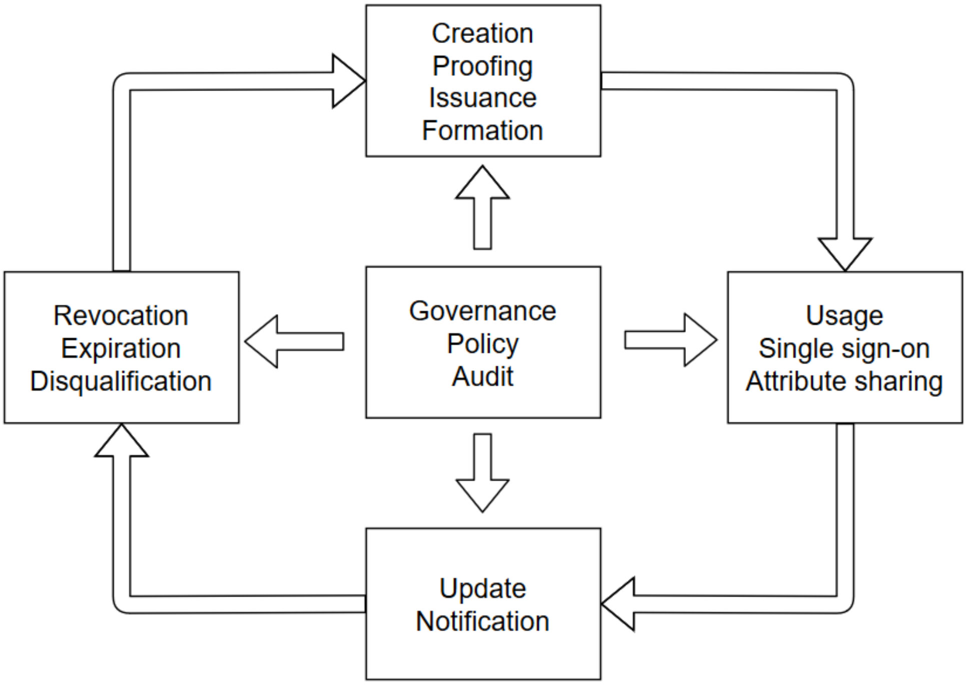


Figure 2: Identity life cycle (adapted from Bertino & Takahashi 2010, 30.)

Creation of an identity has three steps: attribute proofing, issuing credentials, and forming the identity. In attribute proofing attributes are attested by authorities which are trusted by the recipient of attributes. This process should tell in which context the proofing is done. Date of birth is one example of an attribute that can be proofed. Next step after proofing is credential issuing. This may be done by authorities which did proofing, or by the subjects themselves. Passwords and fingerprints are a few examples of such credentials. Finally, identity is created based on three items appointed by third parties or subjects themselves: attributes, credentials, and identifiers. Created identities may then be used in different identity-enabled services. To form trusted communications, it should be possible for both sender and receiver of messages to identify the other end. (ibid, 30-32.)

Information about identities should be kept up to date to sustain data integrity. Attributes might change over time and all such changes should be communicated to the parties hosting the identity data. Some key identity attributes should be designed to be permanent in nature for enabling sustainable auditability trace of the identity. (ibid, 34-35.)

At some point, identity might become obsolete or invalid. In such case, the identity and related credentials should be revoked. A typical example of a revocation event is when an employee’s contract is terminated or when a user loses his password. In the first case, the whole identity and credentials should be revoked, in the latter case just resetting password would be sufficient. Ideally, such acts are recorded so that they are part of audit trails. (ibid, 35.)

Throughout the lifecycle of identity, governance elements should be in place, which includes extensive policies and audit recordings. Governance is also compulsory in order to meet the requirements of certain regulations. Policies verify that information exchanging between identity-related parties is controlled. Audits ensure detailed records about all identity-related transactions. Audits should therefore be secured in a similar manner to other identity data. (ibid, 37.)

3.6 IdP, FIM and SSO

IdP (Identity Provider) offers a possibility for an end-user to use a single set of credentials to authenticate across multiple systems and applications. A typical example of such set-up is when a webpage offers a possibility to login using their Google Account. In this case, Google Sign-In would be the identity provider. When one same identity is used in multiple platforms as in this example, it is called a federated identity. Identity provider aims to secure credentials and make them accessible to other directory services. Identity provider offers the same fundamental functionalities for managing different identities as directory services, such as Microsoft AD. (Lutkevich 2019.)

Communication between different identity providers and web service providers is handled using languages like SAML or formats such as OAuth. Messages consist of three basic types: authentication assertion, attribution assertion and authorization assertion. The first message tells whether the requester is authenticated. The second message transmits relevant data about the connection request. The third message has information about giving access to the requested resource. The assertions make up XML-documents which hold needed data to verify users to a service provider. Service providers are entities which maintain the resources that users try to access. (ibid.)

Main two varieties of identity providers are social-based and enterprise-based. Enterprise-based are typically used in corporations for IAM purposes. Popular social-based IdPs are for instance Google, Facebook, and Instagram. Lightweight Directory Access Protocol, SharePoint, and Active Directory are some examples of enterprise-based IdPs. (ibid.)

Single sign-on is a part of the federated identity management concept. It enables users to access multiple applications with one set of credentials. SSO can help to reduce the number of credentials that the user needs to remember, therefore easing so-called password fatigue. In a typical web SSO service flow is following: application server hosts an agent module, which collects specific authentication credentials for the user from the SSO policy server. At the same time, the user is authenticated against a user directory, like LDAP. Finally, the SSO service authenticates the user for those applications which user has been given rights. Flow is demonstrated in figure 3 from the user’s point of view. (Teravainen, 2020.)

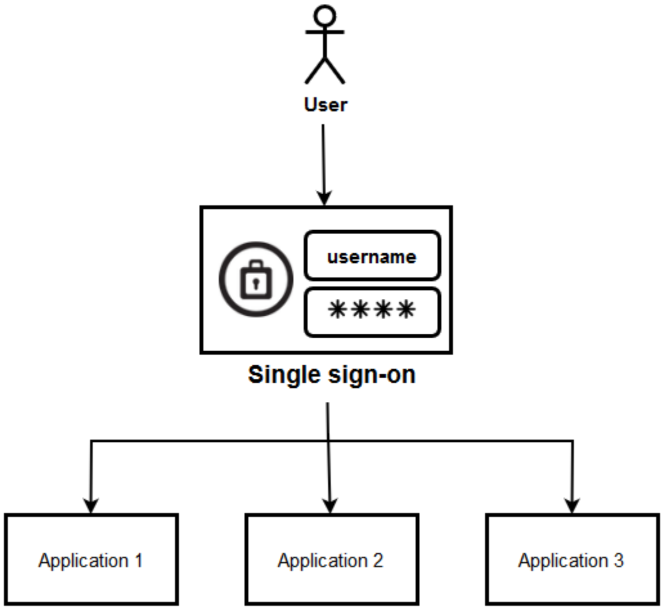


Figure 3: SSO from the user's point of view (adapted from Teravainen, 2020.)

Federated Identity Management can be formed between several organizations to let members of the FIM use the same identification data. This arrangement is called identity federation. User’s identity is linked between several security domains, which makes possible for a user to authenticate to one domain and then have access to another domain without additional login process. (Rosencrance 2018.)

Even though SSO and FIM share similarities, they are not the same. One typical difference is that normally SSO is used to access multiple applications within a single organization, whereas FIM offers access across several organizations. SSO does not necessarily take advantage of FIM, but FIM cannot exist without SSO technologies. As is the case with SSO, the main advantage of FIM is also its ability to increase convenience for users. One challenge about FIM besides its cost is that all federation members must be able to agree about necessary policies which all parties find satisfying. (ibid.)

3.7 Data security

Security can be approached from points of confidentiality, integrity, and availability, known also as CIA. Together those three factors form the base for security infrastructure. It is justified to claim that each time there has been a security breach, at least one of these factors has been violated. CIA is often modelled as a triangle, so-called "CIA Triad", which is illustrated in figure 4. (Walkowski, 2019.)

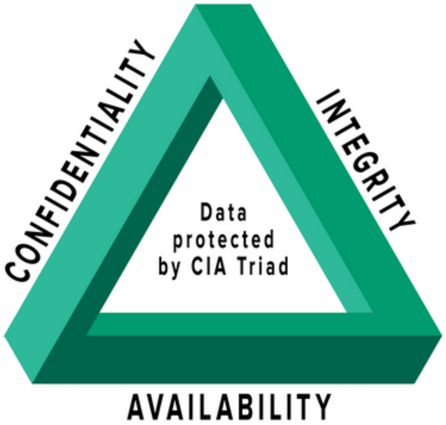


Figure 4: CIA Triad (Walkowski, 2019.)

Confidentiality concentrates on assuring that only the authorized users are allowed to access the defined resources. At the same time, non-authorized users are actively prevented from accessing the resource. The goal is to keep the data private and protected. Violation may be a consequence for failing to protect passwords or sharing account credentials for example. Measures to secure confidentiality include among others having access control features, data encryption, and giving adequate education to those who are handling the protected data. (ibid.)

Integrity aims to keep the data complete. This means that the data has not been altered without authorization, and therefore can be relied on. To assure that, data must be protected both when it is being sent and stored. Steps to protect integrity include for instance encryption, hashing, certificates, and auditing. Integrity may become compromised in case of several attack vectors or through human error. Non-repudiation is an essential counterpart of integrity, which means not being able to deny something. One example is the email: if the sender is using a digital signature, the sender cannot later deny sending the message. At the same time, the recipient cannot question the identity of the sender. (ibid.)

Availability means that the protected data can be accessed by authorized users when necessary. This requires that all required systems and components to provide the access are online. Failure to provide availability may result due to software or hardware errors, power outage, natural disasters, or human error. Also, some attacks could cause availability issues, for example, denial-of-service attack. Typical ways of assuring availability include implementing infrastructure redundancy, keeping systems updated, backups, disaster recovery plans, and protective solutions from attacks. (ibid.)

4 Diving into Privileged Access Management

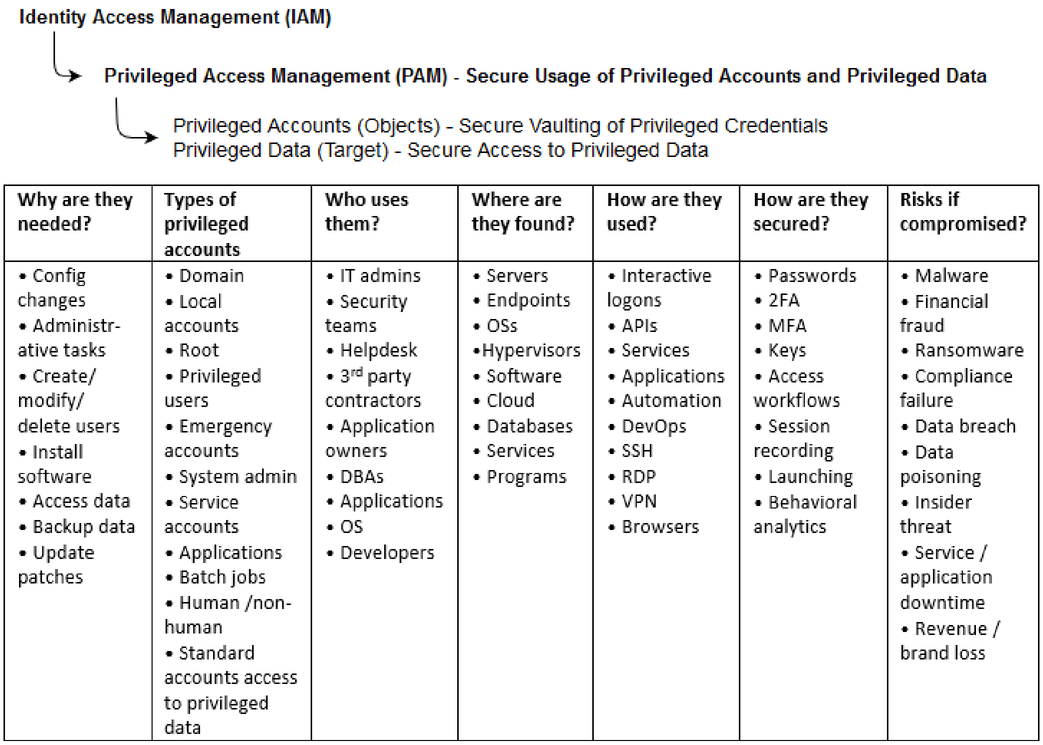
4.1 Brief history of PAM

Recent years have shown a growth in demand for enhanced Identity and Access Management. Companies are facing tightening compliance and regulation requirements, forcing them to pay more attention to authentication and authorization processes and managing users. Stolen credentials are often used in data thefts, which makes securing privileged accounts a crucial task. (Carson 2019.)

Privileged Access Management has its origins in password management. Different password managers have existed for decades, aiming to harbour credentials in a concentrated safe. Often these safes store information about various accounts, such as email, bank, and other target systems. When a company has a password manager in use, it tends to happen that users are left to manage the credentials on their own. Traditional password managers are well sufficed for creating complex passwords, but they however struggle with controlling privileged access, which often means more security controls, auditing, integrations, and compliance. (ibid.)

Privileged Account Management followed the first initial password managers. It brought possibilities for integration, sharing and delegation of passwords to employees, password rotation, auditing, and check-in/check-out capabilities. Organizations could store accounts with high-level access in this tool, and limit accessing those credentials. Passwords could be shared for a limited time and they could be changed after use to prevent knowing the current password afterwards. Privileged Account Management was above all about controlling passwords. (ibid.)

The successor to Privileged Account Management is the current generation, Privileged Access Management. New PAM has become a more holistic solution, extending coverage to how the privileged accounts are used, instead of just managing access to credentials. Access to both privileged accounts and privileged data can be secured with modern PAM technologies. Figure 5 defines some key elements of how and why PAM is used. (ibid.)



Identity Access Management (IAM)

Privileged Access Management (PAM) - Secure Usage of Privileged Accounts and Privileged Data

Privileged Accounts (Objects) - Secure Vaulting of Privileged Credentials
Privileged Data (Target) - Secure Access to Privileged Data

Why are they needed?	**Types of privileged accounts**	**Who uses them?**	**Where are they found?**	**How are they used?**	**How are they secured?**	**Risks if compromised?**
• Config changes • Administrative tasks • Create/ modify/ delete users • Install software • Access data • Backup data • Update patches	• Domain • Local accounts • Root • Privileged users • Emergency accounts • System admin • Service accounts • Applications • Batch jobs • Human /non-human • Standard accounts access to privileged data	• IT admins • Security teams • Helpdesk • 3rd party contractors • Application owners • DBAs • Applications • OS • Developers	• Servers • Endpoints • OSs •Hypervisors • Software • Cloud • Databases • Services • Programs	• Interactive logons • APIs • Services • Applications • Automation • DevOps • SSH • RDP • VPN • Browsers	• Passwords • 2FA • MFA • Keys • Access workflows • Session recording • Launching • Behavioral analytics	• Malware • Financial fraud • Ransomware • Compliance failure • Data breach • Data poisoning • Insider threat • Service / application downtime • Revenue / brand loss

Figure 5: PAM matrix (adapted from Carson 2019.)

4.2 Sharing privileges

Privilege as a term is traditionally described as a special right or an advantage. Therefore, privilege can be defined as a right which is not automatically assigned to everyone, something above the normal or default level. In information technology, for example, a normal user could be granted access to a web browser and office applications, whereas a privileged user could in addition install applications and edit settings which are forbidden to the normal user. (Haber & Hibbert 2018.)

Misuse of credentials which are tied to certain privileges is a very common attack scenario. Typical threats can be divided into three categories:

- Insiders who have unnecessary or excessive rights and can access accounts without being monitored
- Insiders whose accounts have been compromised due to for example phishing or social engineering.
- Accounts which have been compromised due to weak passwords, devices, or applications.

According to 2017 Verizon Data Breech report, 81% of successful attacks originating from external sources took advantage of stolen or poor passwords. (ibid.)

Privilege granularity may be divided to as many levels as an organization finds suitable. A very basic approach includes two levels: Standard user and administrator. In this interpretation standard user privileges are assigned to all users for completing trusted tasks. Administrator users are given a very wide range of privileges to have complete control over target systems. Another example of granulate privileges has four levels (ibid.):

- No access. Means that user has no account at all, or it has been deleted or disabled. No access privilege means that also anonymous access is denied.
- Guest. No access Guest is often described as an anonymous user and has very limited access.
- Standard user. Standard user privileges are the default rights assigned to all users who need to run trusted tasks.
- Administrator. Administrators are given the highest level of access. Administrator privileges may also be further divided into local administrator and domain administrator rights.

It is crucial to keep in mind that privileges must be built into all layers of resources to be actually efficient. The role of privileges is extended much wider than just to the executed application. When user authentication is completed by any form of username and password combination, at least following components need to be considered privilege-wise: operating system, file system, application, database, hypervisor, cloud management platform, and network segmentation. (ibid.)

4.3 Privileged accounts

It is estimated that organizations often have two to three times more privileged accounts than employees. These are needed for different administrative and management tasks. Privileged accounts exist in nearly every connected device, server, database, and application. They also extend beyond traditional IT infrastructure covering for instance corporate social media accounts which are managed by employees. Typically, a normal user account represents a human identity in a directory such as AD. Normally there is one such account for each person in an organization. A privileged account on the other hand may represent a human or non-human user. It is common that these accounts are shared between IT staff. (Carson 2017, 4-6.)

Different types of privileged accounts which are normally in use in organizations include local administrative accounts, domain administrative accounts, break glass accounts, service accounts, active directory or domain service accounts, and application accounts. One type of privileged is called superuser accounts. In Unix/Linux systems these are known as “Root” and in Windows environments as “Administrator”. Local administrative accounts give privileged access only to a localhost, whereas domain administrative accounts give permissions within the whole domain. Break glass accounts are used in case of an emergency, for instance for disaster recovery purposes. Service accounts may be local or domain accounts which an application or a service uses for communicating with the underlying OS. Application accounts are used by applications, and they may be used for running batch jobs, connecting to databases, or giving access to other applications. (Privileged Access Management (PAM) n.d.)

4.4 PAM vs. IAM

The principle behind both PAM and IAM are the same; both aim to guarantee that the right people have access to the right resources. PAM however has a smaller scope, and it can be described as an extension or a part of IAM. PAM, as the Privileged Access Management suggests, concentrates on controlling and securing the most powerful accounts which form the biggest risk to organizations. Different scopes of IAM and PAM are demonstrated in figure 6. (Haber & Hibbert 2018.)

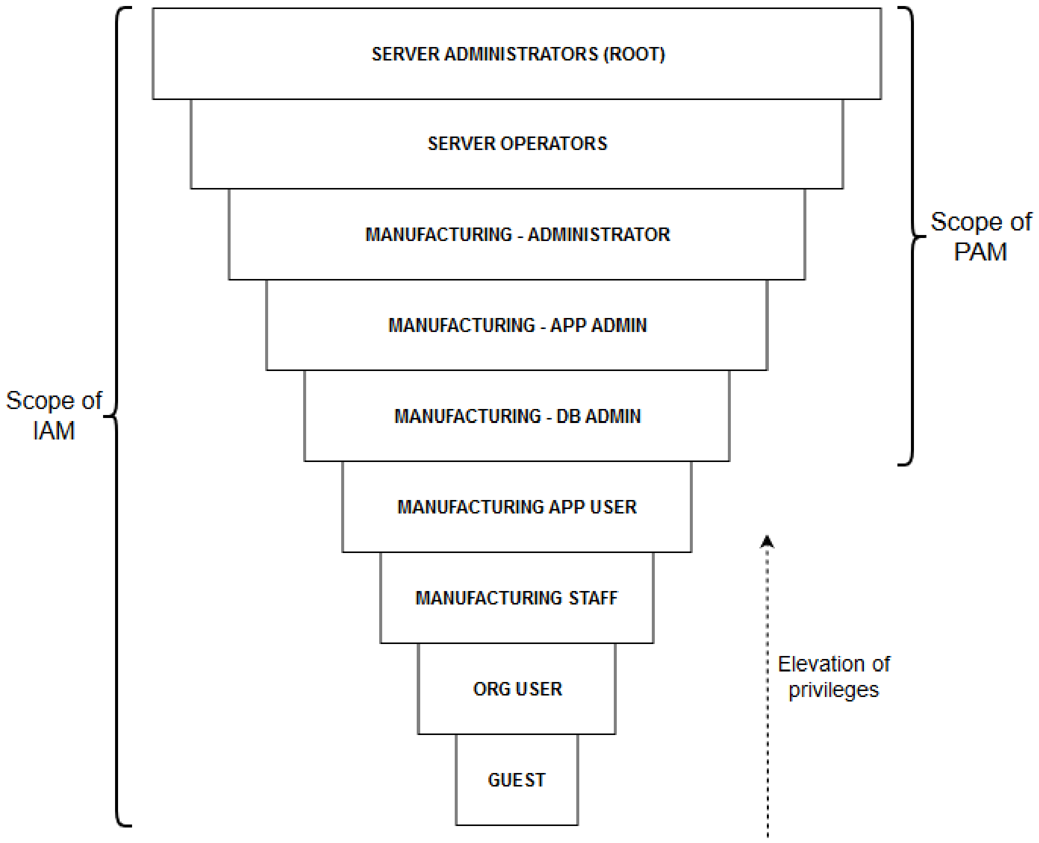


Figure 6: Scopes of IAM and PAM (adapted from Haber & Hibbert 2018.)

IAM covers all users in an organization, and it can help to manage privileged *users*. By adding PAM tool to the equation, more layers of protection can be added to guard privileged *accounts*. Some IAM solutions come with built-in monitoring and reporting capabilities, which might be enough to fulfil compliance requirements. However, if only IAM is used, there is a high risk that not all details are considered and for example some privileged accounts might be left unmanaged, posing a great risk of being compromised at some point. (Wang 2018.)

4.5 Why is PAM needed?

It is a widespread scenario that organizations have plenty of accounts, which are not properly managed, or in the worst case might be totally forgotten. Each such account poses a risk to companies, as in time they might be compromised by malicious users, potentially including former employees. (Privileged Access Management (PAM) n.d.)

Even though limiting privileges is encouraged, too tight restrictions can cause hindered performance and efficiency. In many cases, this leads to end-users being given too wide permissions in the first place. Users might also end up having too many privileges due to being assigned to new tasks which require additional permissions. In time permissions might accumulate if assigned permissions are not reviewed regularly. It is also a common scenario that user logs into workstation unnecessarily with administrative privileges. Excessive privileges concern often also application and service accounts. (ibid.)

Sharing administrative account credentials is a frequent case within IT teams. This may be convenient for the users, but at the same time removes the possibility to effectively tie performed actions to a certain user. This kind of highly privileged accounts are also often managed in different ways across various organizational silos, leading to inconsistency in the implementation of best practices. (ibid.)

Hardcoded and embedded credentials pose a severe risk. Many devices and applications are shipped with embedded insecure default credentials, and sometimes these are taken directly into use without changing credentials. Additionally, credentials are often hardcoded by employees in scripts or files for convenience. (ibid.)

Cloud and virtualization environments bring new challenges to privileged account management. In those environments administrative consoles allow users to easily create and manage a vast number of virtual machines, at the same time producing new privileges and privileged accounts. Taking control of these new resources requires careful planning from any organization. (ibid.)

4.6 PAM components

Enterprise-class PAM solutions typically have an extensive list of components, which are also listed in figure 7. PAM works as a secure vault for passwords, and it should be able to discover accounts in a network and import them under PAM's control. Password can be shared in the vault using the one-to-many approach when several users need access to the same privileged account. Stored passwords should be strongly encrypted, and commonly PAM solution enables automatic injection of passwords for better user experience. (Haber & Rolls 2020.)

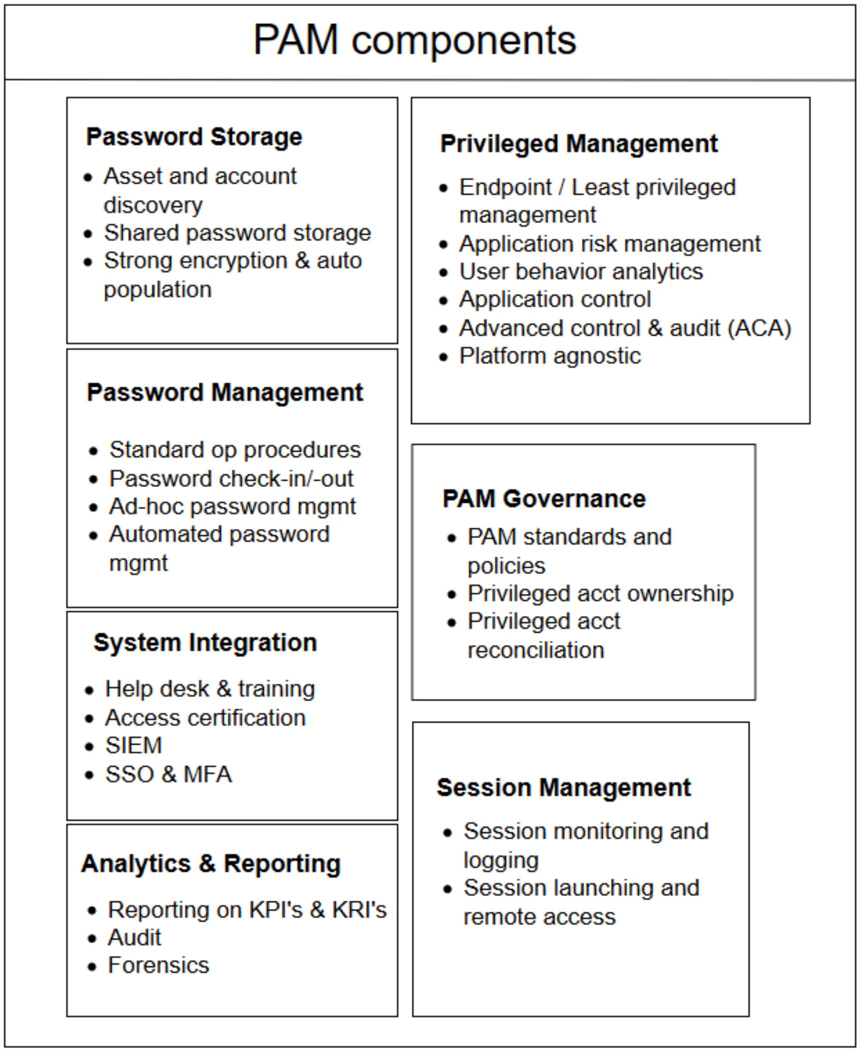
Besides just storing passwords, PAM solutions can also manage passwords. This includes various automated tasks, such as password changing for both human and non-human accounts. PAM can also assure that used passwords are compliant with organizations password policy by fulfilling for instance rotation or complexity needs. Password retrieval may further be placed behind a check-in/check-out feature which prevents overlapping account usage. Besides automated tasks, also manual controlling of passwords is supported. Ad-hoc password management may be necessary for example in disaster recovery situations. (ibid.)

PAM may be used to manage privileged sessions. This includes documenting and controlling users' access, and the ability to automatically launch and inject credentials to target system from the PAM tool. Capability to having a holistic control over privileges is essential. Monitoring, controlling, and terminating privileged access are such features and should be supported regardless of platform. Management should be extended to cover for example Windows, macOS, cloud, virtual and network devices. User behaviour analysis, UBA, is a way to recognize known threat patterns in a user's activity and makes it possible to trigger alarms or events based on UBA observations. Advanced Control and Audit, ACA, may be deployed to control commands which are hidden from plain sight, providing tighter control over executed applications. (ibid.)

To become a part of organizations ordinary workflows, PAM will need several system integrations. Integrating to helpdesk and ticketing system can assure that a ticket must be opened or will be opened when privileged access occurs. Authentication to PAM solution should not be based only on username and password, so PAM should be integrated into existing SSO and/or MFA (Multi-Factor Authentication) solutions for securing access. In case SIEM (Security Information and Event Management) is implemented in the organization, all auditing data produced by PAM should be delivered there for enhanced anomaly detection. (ibid.)

Any PAM solution should include extensive auditing and reporting capabilities. This will help the organization to meet different compliance needs as well as internal auditing and monitoring risks related to privileged access. Audits and reports should include for instance information about who has access to a resource, when has a resource been accessed and by whom, and what has been done during the access. (ibid.)

PAM governance focuses on instructing how PAM should be implemented into organizations day-to-day operations. Standards and policies should dictate who is entitled to access and which resources. Not every PAM-solution user should have access to every company resource. Governance aspects will detail assignment and revocation of privileges. (ibid.)



PAM components

Password Storage

- Asset and account discovery
- Shared password storage
- Strong encryption & auto population

Password Management

- Standard op procedures
- Password check-in/-out
- Ad-hoc password mgmt
- Automated password mgmt

System Integration

- Help desk & training
- Access certification
- SIEM
- SSO & MFA

Analytics & Reporting

- Reporting on KPI's & KRI's
- Audit
- Forensics

Privileged Management

- Endpoint / Least privileged management
- Application risk management
- User behavior analytics
- Application control
- Advanced control & audit (ACA)
- Platform agnostic

PAM Governance

- PAM standards and policies
- Privileged acct ownership
- Privileged acct reconciliation

Session Management

- Session monitoring and logging
- Session launching and remote access

Figure 7: PAM components (adapted from Haber & Rolls 2020.)

Careful PAM strategy and implementation of PAM components will result in having strong management and control over privileged accounts. Probability of accidental or deliberate misuse of privileges is significantly reduced and capability to monitor privilege usage and access is at the same time improved. This is achieved by narrowing down attack surface and implementing wide auditing. Deployment of PAM components will typically lead into a strictly controlled workflow which is demonstrated in figure 8. (Haber & Hibbert 2018.)

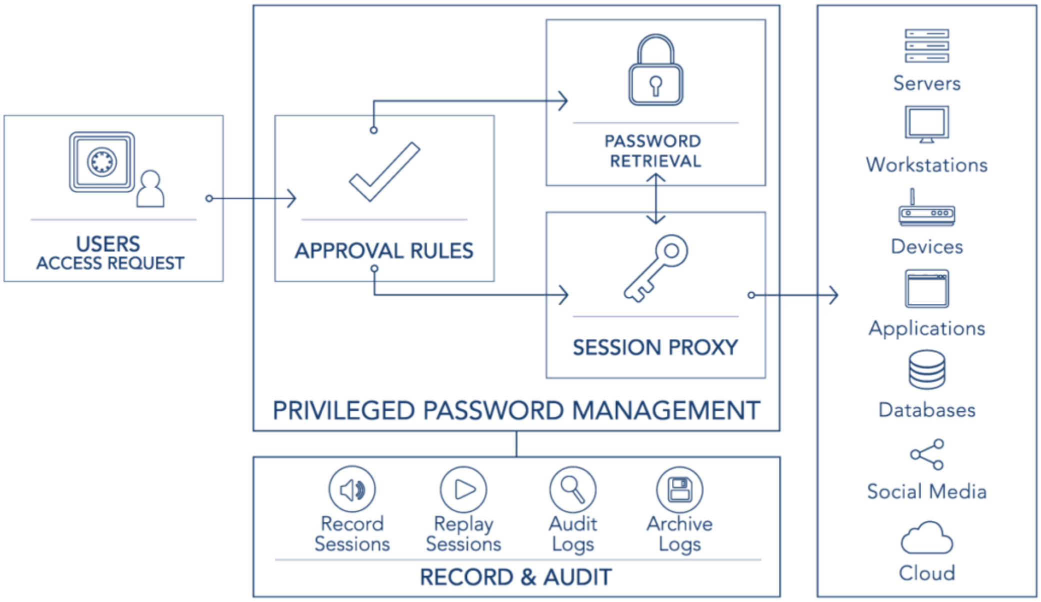


Figure 8: PAM workflow (Haber & Hibbert 2018.)

4.7 PAM lifecycle

Planning and preparation are the keys to successful PAM implementation. By paying attention to those points from the very beginning can save from a lot of unnecessary work at a later stage. First, the necessary data and user groups should be identified accurately. Several PAM vendors have their own scanning and discovery tools, which can be used to help investigate the current situation, and at this point, some dormant privileged accounts might already be found. To make sure that proper PAM technology is chosen for the organization, the data model should be designed and reviewed together with end-users. Technology may also be impacted by actual use-cases and business requirements. Responsibility and ownership about PAM solution should also be defined at an early stage. (Hintsanen 2020.)

It is good to note that migration to using a PAM solution can be a significant task. Necessary policies and security controls for all target systems need to be defined and set in place. Applications used in an organization need to be mapped and investigate the possible need and requirements for PAM integration. Different processes must be modelled, not forgetting 3rd party access and disaster recovery scenarios. (ibid.)

Even though the company-wide implementation of PAM will bring the most benefits, the implementation should be started from identified urgent cases. To later cover all necessary areas, it is crucial to have planned a PAM roadmap. Coverage should be extended to not just passwords but for instance SSH keys, DevOps, scripts, and RPA. For different needs, PAM solutions typically support usage also through other interfaces than the graphical interface. During PAM implementation MFA and SIEM integrations should be in place from the start. Hardening PAM and related platforms must be included, and different exceptional scenarios should be gone through in practice, such as backup, high-availability, and disaster recovery. (ibid.)

After the initial implementation phase, it is important to keep maintaining the PAM solution. PAM implementation should go through internal auditing at regular intervals to make sure that users have correct privileges based on segregation of duties and least privilege. PAM usage should be monitored, and alerts should be set to trigger alarms based on suspicious events. Both internal PAM monitoring tools and external SIEM solutions are suitable for this. Like most software, PAM technologies also receive software updates, and keeping technology up to date is essential. As the company evolves, PAM usage and needs should be considered accordingly. (ibid.)

Ongoing PAM management can be described as PAM lifecycle, as demonstrated in figure 9. This covers steps from defining to reviewing and auditing and indicates that PAM management is a process which should not have an end. Only when all steps are gone through comprehensively, PAM solution can properly protect the privileged accounts and resources. (Carson 2018.)

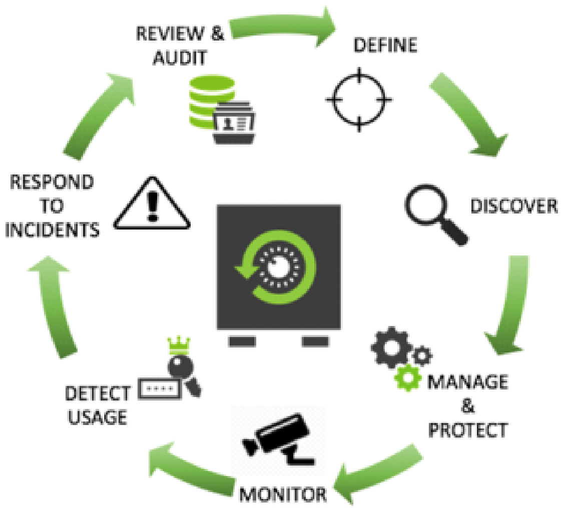


Figure 9: PAM lifecycle (Carson 2018.)

Different use-cases will have a big impact on how PAM should be implemented. Also, the location of resources affects the best implementation, whether the resources are placed in cloud, on-premises, or in some hybrid model. Regardless, table 1 can be used to determine the maturity level of PAM implementation in an organization. The model can also help to improve the current PAM setup. (Haber & Hibbert 2018.)

Table 1: PAM maturity model (adapted from Haber & Hibbert 2018.)

The Privilege Maturity Model	Level 1: Absent	Level 2: Adhoc	Level 3: Standardized	Level 4: Managed	Level 5: Advanced
Shared accounts	• Limited controls • No shared account password mgmt. • Lack of accountability	• Manual Controls & processes • Paper trail is not reliable	• Automated discovery, inventory & onboarding • Centralized Password Mgmt. with workflow approval and automated rotation • Privileged account usage reporting	• Password-less session access & management • Context-aware privileged access using RBAC and MFA	• Identity integrated (IAM, SSO, AD-Bridge, AD Audit & Recovery) • Advanced coverage (Cloud, SaaS, Apps) • HSM • User behaviour analysis
Application & Service Accounts	• Unknown & Unmanaged	•Documented •Hard coded •Rarely changed, if ever	•Targeted AtoA management •Eliminated targeted hard-coded passwords •API driven retrieval	•Centralized AtoA management •No hard-coded passwords; ever	•DevOps Integrated •High Volume •HA and Caching for redundancy

Active Monitoring & Threat Detection	• No monitoring	•Distributed logs •Lack of tracking individuals use of shared accounts	•Centralized audit controls •Individual accountability over use of shared accounts •Deep Visibility with session and keystroke	•Advanced threat detection & UBA •SIEM integration •Automated keyword and activity indexing.	•Automated Privilege Active Response (Deny, Disable, Quarantine, Alert) •IGA integration •Platform independent
Fine-grained Desktop Management	• Unmanaged users have Admin access	•Remove some administrator rights •Desktop tools for ad-hoc elevation	•Centralized Password Management •Limited whitelist \ blacklist proxy access •Reputation services	•Fine grained access •Controlled remote server sessions •FIM •Control lateral movement	•Context-aware access policy (user risk, asset risk, ITSM validation, MFA) •IGA integration with separation of duties •Desktop Asset and user policy independence
Fine-grained Server Management	• Unmanaged users have Root access	•Siloed •Open Source (SUDO)	•Centralized Password Management •Limited whitelist \ blacklist proxy access •Platform dependant	•Fine grained access •Privileged Shell •Controlled remote server sessions •FIM •Control lateral movement	•Context-aware access policy (user risk, asset risk, ITSM validation, MFA) •IGA integration with separation of duties •Server Asset and user policy independence
Fine-grained Infrastructure Management	• Unmanaged Users have Root access	•Siloed •Vendor dependant	•Centralized Password Management •Limited whitelist \ blacklist proxy access	•Fine grained access •Controlled remote server sessions •Control lateral movement	•Context-aware access policy (user risk, asset risk, ITSM validation, MFA) •IGA integration with separation of duties

5 About introduction guides and trainings

5.1 What is workplace training for?

Training is needed for example when a new job starts, the job changes or after the employee comes back after a long absence. Training needs to consider different requirements, which may vary a lot between employers. It is good to note that there is also variation regarding training needs between employees. (Perehdytä hyvin! 2017.)

Workplace training helps employees to increase their knowledge and become more efficient at their job. This is an important part of any employee's lifecycle in a company. Training comes with many benefits. In addition to skill increase, this may lead for example to better motivation, promotion, or gaining certifications. Training can be organized in many forms:

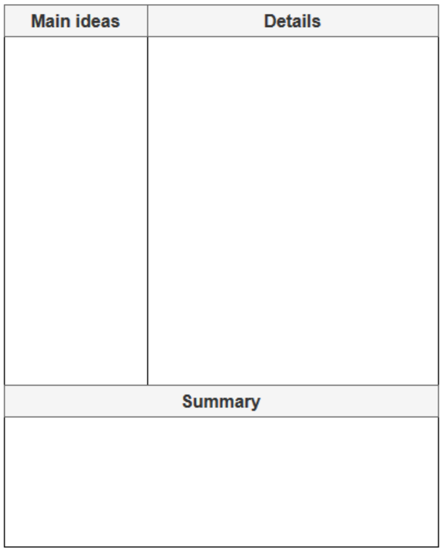
- Orientation. Typically, a one-time process which is conducted when a new employee starts. Normally organized by the company's human resources team, and includes topics such as company culture, company mission and company policies.
- Onboarding. Planned to familiarize the employee with his role at the company. Orientation is normally one part of the onboarding process. Onboarding often addresses topics such as the needs of the new employee, jobs' technical aspects and department goals.
- Technical skill development. This kind of training aims to strengthen employee's technical skills, such as writing content, coding, or programming.
- Soft skill development. Soft skills help at behaving professionally and they refer to communication and cooperation skills.
- Products and services training. These trainings aim to familiarize the employee with offerings of the company. Topics may include available options, benefits, features and maintenance.
- Quality training. Give employees the capability to ensure that produced goods meet certain quality criteria. Criteria may be dictated by the company itself, industry or third parties.
- Safety training. Aims to protect from work-related accidents. Top priority especially in companies which are involved with toxic chemicals or other dangerous substances.
- Team training. Used to build stronger relationships and work more efficiently as a team. Typical topics include for example communication skills, team collaboration, team productivity and team motivation. (What Are the Different Types of Workplace Training? 2019.)

5.2 How to create an introduction guide

When creating a new guide, it is important to remember who the guide is aimed for. This will define the high-level approach of the guide: how complex the guide is, what kind of language is used and other characteristics. It is also helpful to get familiarized to the writing process in general. (Parker 2019.)

Writing workflow can be divided into four steps:

- Step one: Research. During this part, it is a good idea to take notes about the main points. One way for making notes is the *Cornell note-taking system* demonstrated in figure 10, in which paper is divided into three columns: main ideas, details and summary. Another technique is called the *Feynman technique*. The main idea behind that technique is to imagine telling other people about what has been learnt. This helps to keep writing as understandable as possible.
- Step two: Draft. This can be further divided into 5 steps:
  - Describing ideas
  - Creating the structure of the project
  - Reviewing the draft and ensuring that it makes sense
  - Asking someone else to read the draft and give feedback
  - The final version of the draft
- Step three: Editing and reviews. At this point following steps can be taken:
  - Checking grammar
  - Using text-to-speech to go through the document
  - Styling the guide to represent the company
  - Asking feedback from company staff
- Step four: Publish. Publishing the ready document. (Parker 2018.)



Main ideas	Details
Summary	

Figure 10: Cornell note-taking system (adapted from Parker 2018.)

Before writing is started, it is good to gather useful material for the guide and make a plan. Gathered material may be any additional information about the topic of the guide. If the guide is visualized beforehand, writing will be easier. Some advice for creating the guide:

- Language should be concise and plain
- Lists are helpful when steps are described
- Visual content should be used, including photos, screenshots, and diagrams
- Content should be divided into different sections
- Grammar and spelling must be revised (Parker 2019.)

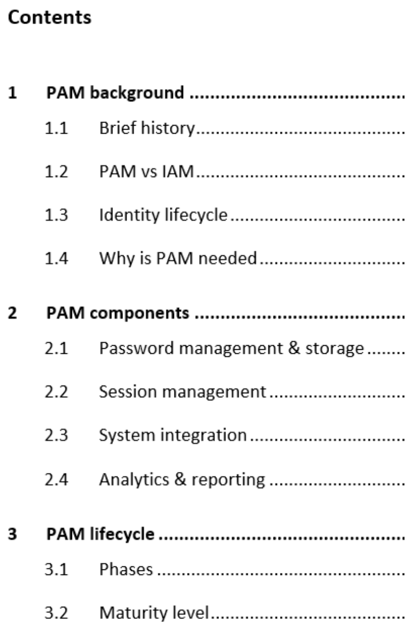
6 Creating PAM introduction guide

6.1 Goal

PAM introduction guide aims to provide base-level generic information about Privileged Access Management. The guide is designed to be a starting point for those, who are not yet familiar with PAM solutions. The guide explains key areas around PAM, like where the need for PAM comes from, what kind of capabilities it brings and how PAM should be implemented. Detailed technical configurations or implementations are not covered in the guide.

6.2 Structure

Based on the theoretical framework the guide was divided into three main categories: PAM background, components, and implementation process. These main categories were further divided into subcategories based on recognized needs. Table of contents is shown in figure 11.



Contents

Figure 11: Table of contents of the guide

Background section starts by giving an introduction about the roots and history of PAM. It also addresses questions about what PAM is needed for, and what kind of accounts the privileged accounts consist of. As PAM is part of a larger IAM framework, the background also gives a general introduction to IAM and describes differences between IAM and PAM. This part aims to answer the question *“Why use PAM?”*.

Components part concentrates on defining different capabilities which PAM solutions typically provide. Different features are listed and given a description of their intended effects. This part aims to answer the question *“What are PAM core functionalities?”*.

Lifecycle topic covers the process of taking PAM into use and maintaining the implemented solution. Necessary phases are listed in this section and description is given for each step. This gives the base for managing the lifecycle of PAM. Implementation part also describes that how implemented PAM maturity can be determined. This part seeks to answer, *“How should PAM implementation be done and how implementation-level can be measured?”*

7 Conclusions

We, as individuals or companies, wish to limit access to our most sensitive resources. This has been the case for thousands of years, so there is nothing new in access management as a concept. However, the last few dozens of years have radically changed the way of interacting as digitalization has taken its permanent place in our everyday lives. This has brought whole new challenges and possibilities to access management field.

In IT environments access management is resolved by providing access based on user roles. These roles may allow a standard user to access only an Internet browser, whereas different types of privileged accounts are used to provide access to protected resources and functionalities. These permissions can be given on a granular level, enabling different levels of privileges within a single system. Typically, the higher sensitivity of the resource, the more elevated privileges are needed for access. Some examples of privileged accounts are different administrative accounts, break glass accounts, service accounts, and application accounts. Balancing in granting privileges can be a daunting task, as too few privileges might reduce employee's performance, whereas excessive privileges can pose a security risk.

Studies show that privileged accounts are involved in a very high portion of all cybercrimes. It is also estimated that companies have double the number of privileged accounts compared to the number of employees. Sometimes these privileged accounts are left unmanaged, and in time their existence might be totally forgotten. Such dormant accounts may later be compromised by malicious users, potentially including former employees. Considering the potentially critical resources that these accounts can access, it is no wonder why Privileged Access Management has been identified as an increasingly important part in developing companies' processes.

Compared to traditional IAM, PAM provides a more targeted scope for account management. PAM does not aim to control all user access in a target environment but concentrates on the accounts which need the most protection, the privileged accounts. In any environment, privileged accounts often give *keys to the kingdom*, and this justifies the usage of additional security functionalities that PAM provides. Even though some IAM solutions have the capability to provide partly same features as PAM usually does, they do not enable the same kind of tight control over privileged access.

PAM tools have come a long way from their password management origins, and typically offer several components which help to keep privileged access actively and securely managed. PAM still can store passwords, but besides that also manage them. This means that password rotation can be configured to meet company policy needs, such as password complexity and password maximum age. Beyond password management, PAM can usually manage privileged sessions as well. During session launching, credentials can often be automatically injected to the target system. Having control over the session also makes it possible for PAM to enforce monitoring over the whole launched session, including keystrokes and other process metadata.

To get the best performance out of PAM, it should be integrated with the company's workflows and tools. These include ticketing system and SIEM-integrations for instance. For increased security integration to existing SSO and/or MFA should also be implemented.

When thinking about PAM lifecycle, it is crucial to note that work is not done after the initial implementation. PAM will need constant maintenance and reviewing to effectively fulfil its purpose. These steps include discovering new accounts, managing them, monitoring, and detecting privileged access, responding to incidents, and doing regular auditing. This process will also help the organization to meet different compliance needs.

This work has tried to address familiarizing newcomers to PAM ideology, components, functionalities, and lifecycle process. The aim has been to provide such information, that an individual could start investigating individual technologies further and have a base-level understanding about objectives of PAM.

Main findings of this work have been provided in the form of a PAM introduction guide. Based on the theory framework need for three different main categories in the guide was recognized: background, components, and lifecycle. Together these topics will help a newcomer to get a grasp about Privileged Access Management as a whole. The guide may also later be a part of a bigger PAM-guidance, which could include topics such as vendor-related features and configurations.

As time passes, the requirements for efficient Privileged Access Management will also evolve accordingly. Therefore, getting to know PAM is a never-ending process, as is often the case with different technologies. To truly become familiarized with PAM solutions, one will need to dive further into different PAM technologies and actual hands-on implementations.

References

About | Nixu Cybersecurity. 2020. Nixu Corporation web page. Accessed on 25 August 2020. Retrieved from https://www.nixu.com/about

All services | Nixu Cybersecurity. 2020. Nixu Corporation web page. Accessed on 2 September 2020. Retrieved from https://www.nixu.com/all-services

Authentication vs. Authorization Defined: What's the Difference [Infographic]? 2020. Security boulevard blog page. Accessed on 20 September 2020. Retrieved from https://securityboulevard.com/2020/06/authentication-vs-authorization-defined-whats-the-difference-infographic/

Benantar, M. 2006. *Access Control Systems: Security, Identity Management and Trust Models*. Accessed on 12 September 2020. Retrieved from https://library.books24x7.com

Bertino, E. & Takahashi, K. 2011. *Identity Management: Concepts, Technologies, and Systems*. Accessed on 19 September 2020. Retrieved from https:// ebookcentral.proquest.com/

Bhandari, P. 2020. *An introduction to qualitative research*. Scribbr web page. Accessed on 15 September 2020. Retrieved from https://www.scribbr.com/methodology/qualitative-research/

Carson, J. 2019. *The Evolution from Password Managers to Privileged Access Management. Which is right for you?* Thycotic Cyber Security Blog. Accessed on 20 September 2020. Retrieved from https://thycotic.com/company/blog/2019/04/02/privileged-access-vs-account-management/

Carson. J. 2018. *The Privileged Access Management Lifecycle and Path to Maturity.* Thycotic Cyber Security Blog. Accessed on 27 September 2020. Retrieved from https://thycotic.com/company/blog/2018/08/07/privileged-access-management-lifecycle-path-to-maturity/

Carson, J. 2017. *Privileged Account Management for dummies*. E-book. Retrieved from https://thycotic.com/resources/wiley-dummies-privileged-account-management/

Carter, S. 2017. *RBAC vs ABAC Access Control Models - IAM Explained*. Identity Automation blog. Accessed on 26 September 2020. Retrieved from https://blog.identityautomation.com/rbac-vs-abac-access-control-models-iam-explained

Coulmas, F. 2019. *Identity: A very Short Introduction*. New York: Oxford University Press. Accessed on 6 September 2020. Retrieved from https://books.google.com/

Cynthia, C. & Brian J. 2012. *Constructing the Self in a Digital World*. New York: Cambridge University Press. Accessed on 12 September 2020. Retrieved from https://ebookcentral.proquest.com/

Haber, M. & Hibbert, B. 2018. *Privileged Attack Vectors: Building Effective Cyber-Defense Strategies to Protect Organizations*. Accessed on 23 September 2020. Retrieved from https://library.books24x7.com

Haber, M. & Rolls, D. 2020. *Identity Attack Vectors: Implementing an Effective Identity and Access Management Solution*. Accessed on 16 September 2020. Retrieved from https://library.books24x7.com

Hintsanen, K. 2020. *Privileged Access Management – lessons learned*. Nixu blog. Accessed on 27 September 2020. Retrieved from https://www.nixu.com/blog/privileged-access-management-lessons-learned

Identity and Access Management (IAM). N.d. Glossary on Gartner webpage. Accessed on 12 September 2020. Retrieved from https://www.gartner.com/en/information-technology/glossary/identity-and-access-msanagement-iam

Kael, N. 2019. *Who Are You and What Do You Need? Introduction to Identity and Access Management (IAM) Systems*. Ericom company blog. Accessed 12 September 2020. Retrieved from https://blog.ericom.com/identity-and-access-management-intro/

Lutkevich, B. 2019. *Identity provider*. TechTarget webpage. Accessed 26 September 2019. Retrieved from https://searchsecurity.techtarget.com/definition/identity-provider

McCombes, S. 2019. *How to write a research methodology*. Scribbr web page. Accessed on 15 September 2020. Retrieved from https://www.scribbr.com/dissertation/methodology/

Nixu Certification Ltd. n.d. Nixu Corporation web page. Accessed on 21 September 2020. Retrieved from https://www.nixu.com/services/nixu-certification-ltd

Parker, K. 2019. *Creating a 'How to' Guide*. Article on Medium webpage. Accessed on 3 October 2020. Retrieved from https://medium.com/technical-writing-is-easy/creating-a-how-to-guide-186070b37c42

Parker, K. 2018. *Great Technical Writing Process*. Article on Medium webpage. Accessed on 3 October 2020. Retrieved from https://medium.com/@kesiparker/great-technical-writing-process-483fafa07d9b

Peterson, T. 2019. *5 Signs of a Privileged Access Abuser*. Security Boulevard web page. Accessed on 3 September 2020. Retrieved from https://securityboulevard.com/2019/09/5-signs-of-a-privileged-access-abuser/

Perehdytä hyvin! 2017. Työturvallisuuskeskus webpage. Accessed on 3 October 2020. Retrieved from https://ttk.fi/ajankohtaista/teemat_2017/perehdyta_hyvin!.7271.news

Privileged Access Management (PAM). N.d. Glossary on BeyondTrust webpage. Accessed on 24 September 2020. Retrieved from https://www.beyondtrust.com/resources/glossary/privileged-access-management-pam

Rosencrance, L. 2018. *Federated identity management*. Accessed 26 September 2019. Retrieved from https://searchsecurity.techtarget.com/definition/federated-identity-management

Santuka, V., Banga, P. & Carroll, B. 2011. *AAA Identity Management Security*. Accessed on 17 September 2020. Retrieved from https://library.books24x7.com

Scheidel, J. 2010. *Designing an IAM Framework with Oracle Identity and Access Management Suite*. Accessed on 17 September 2020. Retrieved from https://library.books24x7.com

Teravainen, T. 2020. *Single sign-on (SSO).* TechTarget webpage. Accessed 26 September 2019. Retrieved from https://searchsecurity.techtarget.com/definition/single-sign-on

The Evolution of IAM. 2019. Video on Solutions Review webpage. Accessed on 12 September 2020. Retrieved from https://solutionsreview.com/identity-management/video-the-evolution-of-iam-identity-and-access-management

Top 10 Security Projects for 2019. 2019. Gartner web page. Accessed on 3 September 2020. Retrieved from https://www.gartner.com/en/documents/3900996-top-10-security-projects-for-2019

User. 2020. Computer Hope dictionary. Accessed on 3 October 2020. Retrieved from https://www.computerhope.com/jargon/u/user.htm

User Account. N.d. Techopedia dictionary. Accessed on 3 October 2020. Retrieved from https://www.techopedia.com/definition/13458/user-account

Walkowski, D. 2019. *What is the CIA Triad?* F5 Labs web page. Accessed on 20 September 2020. Retrieved from https://www.f5.com/labs/articles/education/what-is-the-cia-triad

Wang, R. 2018. *Privileged Account Management and Identity Access Management: Same Family, Different Strengths*. Thycotic's Cyber Security Blog. Accessed on 24 September 2020. Retrieved from https://thycotic.com/company/blog/2018/08/14/privileged-account-management-and-identity-access-management-same-family-different-strengths/

What Are the Different Types of Workplace Training? 2019. Indeed web page. Accessed on 3 October 2020. Retrieved from https://www.indeed.com/career-advice/career-development/different-types-of-workplace-training#2

What is ABAC for AWS? N.d. Amazon webpage. Accessed on 26 September 2020. Retrieved from https://docs.aws.amazon.com/IAM/latest/UserGuide/ introduction_attribute-based-access-control.html

Appendices

PAM Introduction Guide

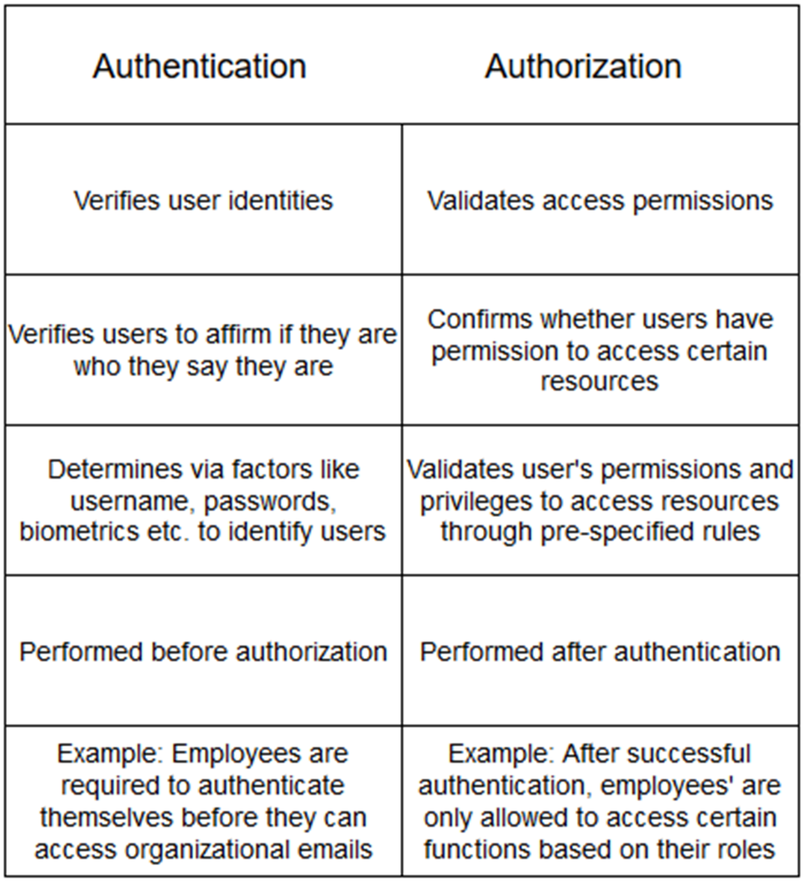
Contents

1. PAM background

1.1 Brief history

Need to limit access to information has already existed for thousands of years. Humans are also not the only species which seeks to protect certain information from unauthorized access; many animals do the same.

As time has passed, several mechanisms have been invented for fulfilling the needs of *authentication* and *authorization.* Below table explains some differences between the two:



Authentication	Authorization
Verifies user identities	Validates access permissions
Verifies users to affirm if they are who they say they are	Confirms whether users have permission to access certain resources
Determines via factors like username, passwords, biometrics etc. to identify users	Validates user's permissions and privileges to access resources through pre-specified rules
Performed before authorization	Performed after authentication
Example: Employees are required to authenticate themselves before they can access organizational emails	Example: After successful authentication, employees' are only allowed to access certain functions based on their roles

In order to manage access in the first place, there needs to be a confirmation that the persons who are exchanging the information truly are who they say they are. Passwords are one of the oldest ways to assure this. Passwords can be used for example as a challenge-response form, in which one password would be the challenge, and the other party would need to give the corresponding password as the response. During history, seals have been used for verifying the identity of the message's sender. At the same time, the unbroken seal would ensure the message's integrity and confidentiality.

First computer files got password protection in 1960, which laid the foundation to the first IAM solutions. Providers of IAM solutions have had to later adjust to evolving IAM needs due to the widespread usage of the Internet and increased need for cloud-based solutions.

Privileged Access Management has its' roots in password management. Traditional password managers have existed for decades, aiming to offer a secure vault for credentials. Traditional password managers are well sufficed for vaulting and creating complex passwords, but they however lack in capabilities of having good control over privileged access.

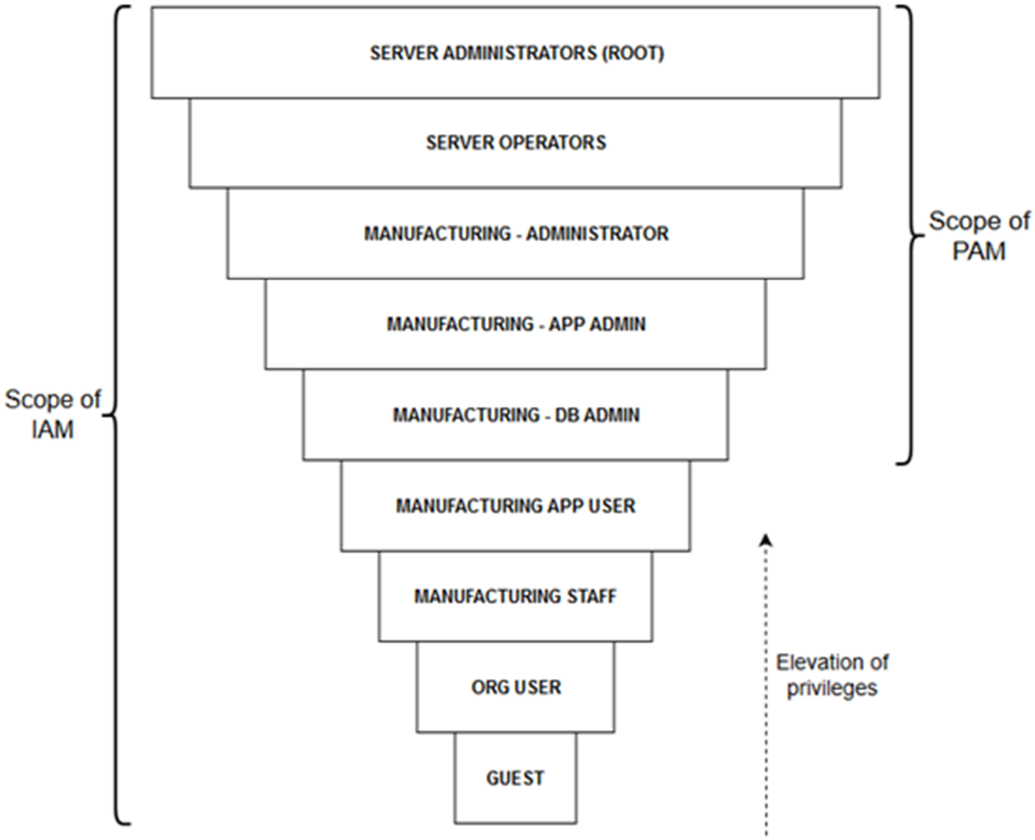
The first type of PAM was Privileged Account Management. It brought possibilities for integration, sharing and delegation of passwords to employees, password rotation, auditing, and check-in/check-out capabilities. Organizations could store privileged account credentials in this tool, and limit accessing those credentials. Passwords could be shared for a limited time and they could be changed after use to prevent knowing the current password afterwards. Privileged Account Management was above all about controlling passwords.

The successor to Privileged Account Management is the current generation of PAM, Privileged Access Management. New PAM has become a more holistic solution, extending coverage to how the privileged accounts are used, instead of just managing access to credentials. Access to both privileged accounts and privileged data can be secured with modern PAM technologies.

1.2 PAM vs IAM

Identity and access management is the discipline that enables the right individuals to access the right resources at the right times for the right reasons.

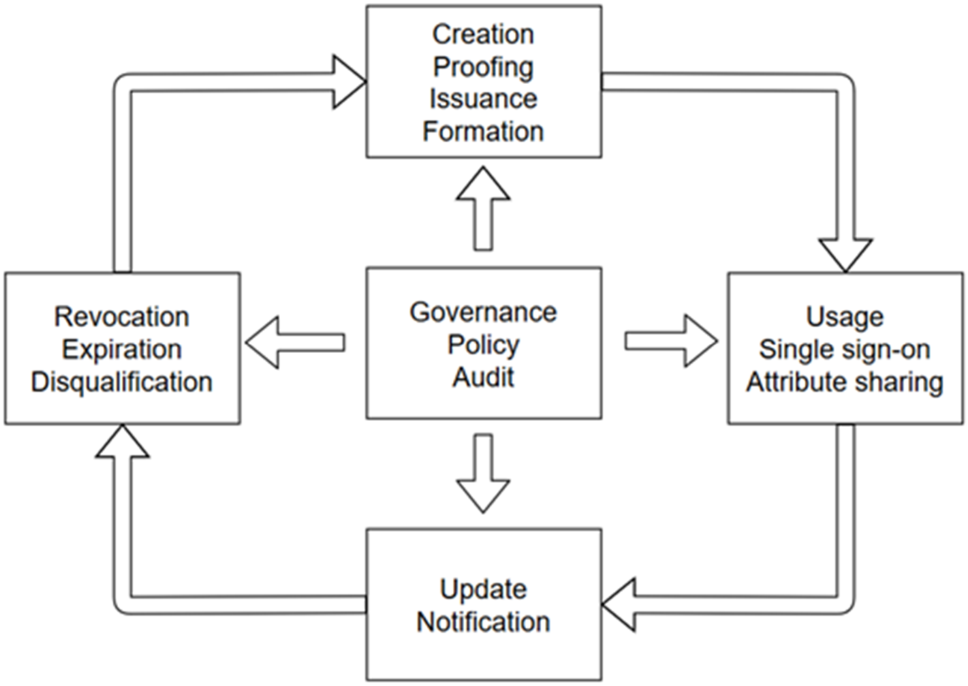
The principle behind both PAM and IAM are the same; both aim to guarantee that the right people have access to the right resources. PAM however has a smaller scope, and it can be described as an extension or a part of IAM. PAM, as the Privileged Access Management suggests, concentrates on controlling and securing the most powerful accounts which form the biggest risk to organizations. Different scopes of IAM and PAM are demonstrated below:



IAM covers all users in an organization, and it can help to manage privileged *users*. By adding PAM tool to the equation, more layers of protection can be added to guard privileged *accounts*. *User* refers to a person who is interacting with the target system. User *account* combines a username, password and any other additional information related to the user. *Account* determines which resources a user can access. Some IAM solutions come with built-in monitoring and reporting capabilities, which might be enough to fulfil compliance requirements. However, if only IAM is used, there is a high risk that not all details are considered and for example some privileged accounts might be left unmanaged, posing a great risk of being compromised at some point.

1.3 Identity lifecycle

Proper identity management includes controlling the lifecycle of identities. Lifecycle has four phases: creation, usage, update, and revocation. Governance should be involved in every phase. Below is an illustration:



Creation of identity has three steps: attribute proofing, issuing credentials and forming an identity. In attribute proofing attributes are attested by authorities which are trusted by the recipient of attributes. This process should tell in which context the proofing is done. Date of birth is one example of an attribute that can be proofed. Next step after proofing is credential issuing. This may be done by authorities which did proofing, or by the subjects themselves. Passwords and fingerprints are a few examples of such credentials. Finally, identity is created based on three items appointed by third parties or subjects themselves: attributes, credentials, and identifiers. Created identities may then be used in different identity-enabled services. To form trusted communications, it should be possible for both sender and receiver of messages to identify the other end.

Information about identities should be kept up to date to sustain data integrity. Attributes might change over time and all such changes should be communicated to the parties hosting the identity data. Some key identity attributes should be designed to be permanent for enabling sustainable auditability trace of the identity.

At some point, identity might become obsolete or invalid. In such case, the identity and related credentials should be revoked. A typical example of a revocation event is when an employee's contract is terminated or when a user loses his password. In the first case, the whole identity and credentials should be revoked, in the latter case just resetting password would be sufficient. Ideally, such acts are recorded so that they are part of audit trails.

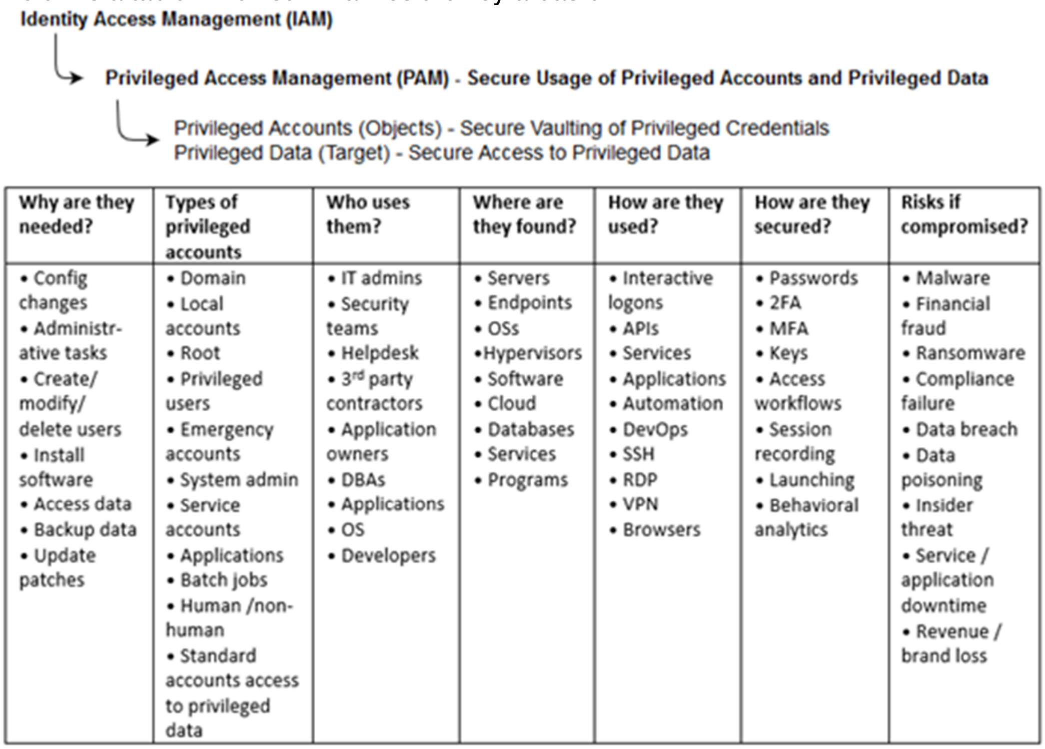
Throughout the lifecycle of identity, governance elements should be in place, which includes extensive policies and audit recordings. Governance is also compulsory in order to meet the requirements of certain regulations. Policies verify that information exchanging between identity-related parties is controlled. Audits ensure detailed records about all identity-related transactions. Audits should therefore be secured in a similar manner to other identity data.

1.4 Why is PAM needed

It is estimated that organizations often have two to three times more privileged accounts than employees. These are needed for different administrative and management tasks. Privileged accounts exist in nearly every connected device, server, database, and application. They also extend beyond traditional IT infrastructure covering for instance corporate social media accounts which are managed by employees. Typically, a normal user account represents a human identity in a directory such as AD. Normally there is one such account for each person in an organization. A privileged account on the other hand may represent a human or non-human user. It is common that these accounts are shared between IT staff.

Different types of privileged accounts that are normally in use in organizations include local administrative accounts, domain administrative accounts, break glass accounts, service accounts, active directory or domain service accounts, and application accounts. One type of privileged is called superuser accounts. In Unix/Linux systems these are known as “Root” and in Windows environments as “Administrator”. Local administrative accounts give privileged access only to a localhost, whereas domain administrative accounts give permissions within the whole domain. Break glass accounts are used in case of an emergency, for instance for disaster recovery purposes. Service accounts may be local or domain accounts which an application or a service uses for communicating with the underlying OS. Application accounts are used by applications, and they may be used for running batch jobs, connecting to databases, or giving access to other applications.

Below is a table which summarizes the key areas of PAM:



Identity Access Management (IAM)

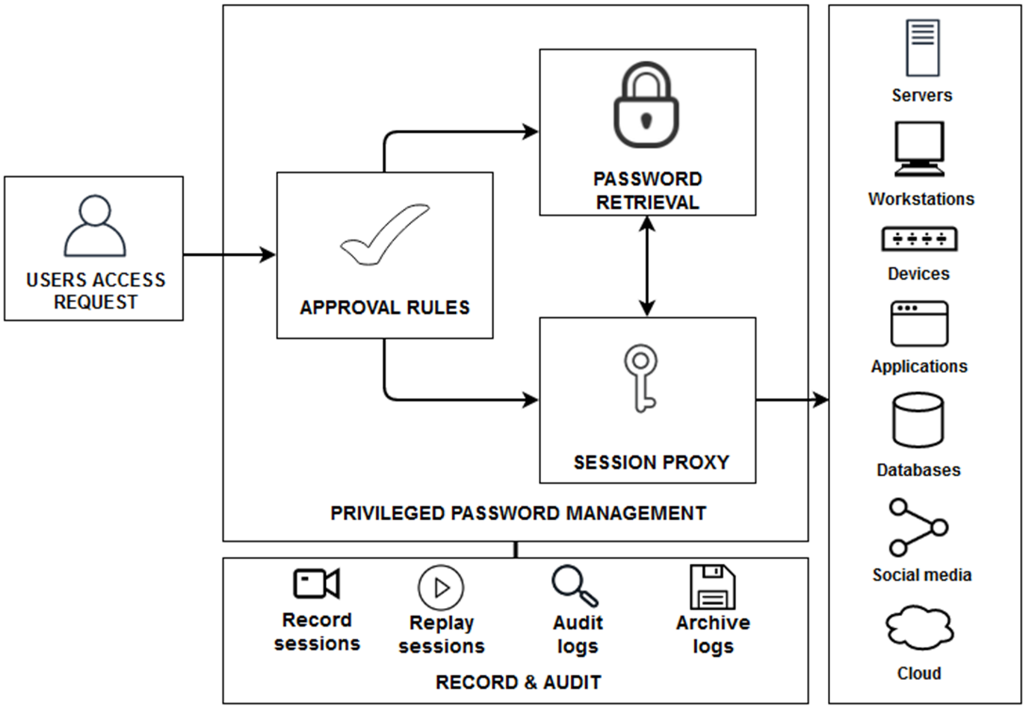
Privileged Access Management (PAM) - Secure Usage of Privileged Accounts and Privileged Data

Privileged Accounts (Objects) - Secure Vaulting of Privileged Credentials
Privileged Data (Target) - Secure Access to Privileged Data

Why are they needed?	**Types of privileged accounts**	**Who uses them?**	**Where are they found?**	**How are they used?**	**How are they secured?**	**Risks if compromised?**
• Config changes • Administrative tasks • Create/ modify/ delete users • Install software • Access data • Backup data • Update patches	• Domain • Local accounts • Root • Privileged users • Emergency accounts • System admin • Service accounts • Applications • Batch jobs • Human /non-human • Standard accounts access to privileged data	• IT admins • Security teams • Helpdesk • 3rd party contractors • Application owners • DBAs • Applications • OS • Developers	• Servers • Endpoints • OSs •Hypervisors • Software • Cloud • Databases • Services • Programs	• Interactive logons • APIs • Services • Applications • Automation • DevOps • SSH • RDP • VPN • Browsers	• Passwords • 2FA • MFA • Keys • Access workflows • Session recording • Launching • Behavioral analytics	• Malware • Financial fraud • Ransomware • Compliance failure • Data breach • Data poisoning • Insider threat • Service / application downtime • Revenue / brand loss

2. PAM components

Careful PAM strategy and implementation of PAM components will result in having strong management and control over privileged accounts. Probability of accidental or deliberate misuse of privileges is significantly reduced and capability to monitor privilege usage and access is at the same time improved. This is achieved by narrowing down attack surface and implementing wide auditing. Deployment of PAM components will typically lead to a workflow which is shown below



2.1 Password management & storage

Enterprise-class PAM solutions typically have an extensive list of components, which are also listed in figure 7. PAM works as a secure vault for passwords, and it should be able to discover accounts in a network and import them under PAM's control. Password can be shared in the vault using the one-to-many approach when several users need access to the same privileged account. Stored passwords should be strongly encrypted, and commonly PAM solution enables automatic injection of passwords for better user experience.

Besides just storing passwords, PAM solutions can also manage passwords. This includes various automated tasks, such as password changing for both human and non-human accounts. PAM can also assure that used passwords are compliant with organizations password policy by fulfilling for instance rotation or complexity needs. Password retrieval may further be placed behind a check-in/check-out feature which prevents overlapping account usage. Besides automated tasks, also manual controlling of passwords is supported. Ad-hoc password management may be necessary for example in disaster recovery situations.

2.2 Session management

PAM may be used to manage privileged sessions. This includes documenting and controlling users' access, and the ability to automatically launch and inject credentials to target system from the PAM tool. Capability to having a holistic control over privileges is essential. Monitoring, controlling, and terminating privileged access are such features and should be supported regardless of platform. Management should be extended to cover for example Windows, macOS, cloud, virtual and network devices. User behaviour analysis, UBA, is a way to recognize known threat patterns in the user's activity and makes it possible to trigger alarms or events based on UBA observations. Advanced Control and Audit, ACA, may be deployed to control commands which are hidden from plain sight, providing tighter control over executed applications.

2.3 System integration

To become a part of organizations ordinary workflows, PAM will need several system integrations. Integrating to helpdesk and ticketing system can assure that a ticket must be opened or will be opened when privileged access occurs. Authentication to PAM solution should not be based only on username and password, so PAM should be integrated into existing SSO and/or MFA solutions for securing access. In case SIEM is implemented in the organization, all auditing data produced by PAM should be delivered there for enhanced anomaly detection.

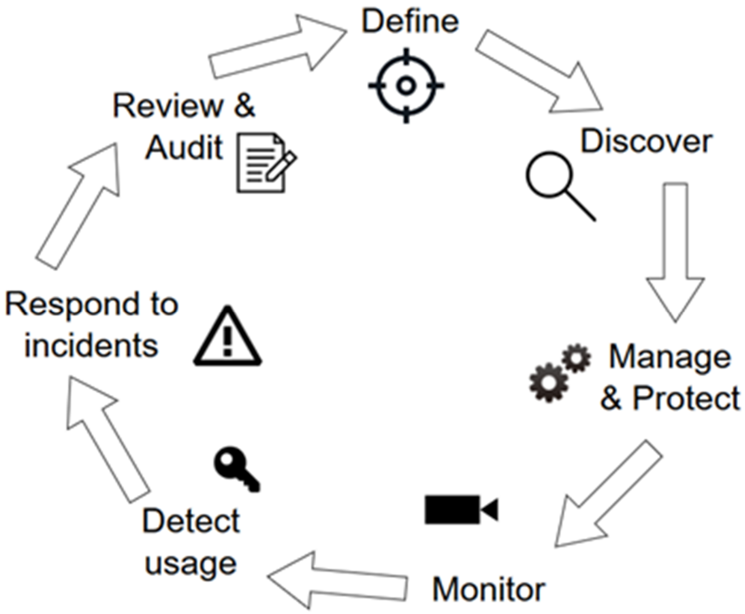
2.4 Analytics & reporting

Any PAM solution should include extensive auditing and reporting capabilities. This will help the organization to meet different compliance needs as well as internal auditing and monitoring risks related to privileged access. Audits and reports should include for instance information about who has access to a resource, when has a resource been accessed and by whom, and what has been done during the access.

3. PAM lifecycle

3.1 Phases

Ongoing PAM management can be described as PAM lifecycle. This covers steps from defining the scope to reviewing and auditing and indicates that PAM management is an ongoing process which should not have an end. Only when all steps are gone through comprehensively, PAM solution can properly protect the privileged accounts and resources.



Planning and preparation are the keys to successful PAM implementation. By paying attention to those points from the very beginning can save from a lot of unnecessary work at a later stage. First, the necessary data and user groups should be identified accurately. Several PAM vendors have their own scanning and discovery tools, which can be used to help investigate the current situation, and at this point, some dormant privileged accounts might already be found. To make sure that proper PAM technology is chosen for the organization, the data model should be designed and reviewed together with end-users. Technology may also be impacted by actual use-cases and business requirements. Responsibility and ownership about PAM solution should also be defined at an early stage.

It is good to note that migration to using a PAM solution can be a significant task. Necessary policies and security controls for all target systems need to be defined and set in place. Applications used in an organization need to be mapped and investigate the possible need and requirements for PAM integration. Different processes must be modelled, not forgetting 3rd party access and disaster recovery scenarios.

Even though the company-wide implementation of PAM will bring the most benefits, the implementation should be started from identified urgent cases. To later cover all necessary areas, it is crucial to have planned a PAM roadmap. Coverage should be extended to not just passwords but for instance SSH keys, DevOps, scripts, and RPA. For different needs, PAM solutions typically support usage also through other interfaces than the graphical interface. During PAM implementation MFA and SIEM integrations should be in place from the start. Hardening PAM and related platforms must be included, and different exceptional scenarios should be gone through in practice, such as backup, high-availability, and disaster recovery.

After the initial implementation phase, it is important to keep maintaining the PAM solution. PAM implementation should go through internal auditing at regular intervals to make sure that users have correct privileges based on segregation of duties and least privilege. PAM usage should be monitored, and alerts should be set to trigger alarms based on suspicious events. Both internal PAM monitoring tools and external SIEM solutions are suitable for this. Like most software, PAM technologies also receive software updates, and keeping technology up to date is essential. As the company evolves, PAM usage and needs should be considered accordingly.

3.2 Maturity level

PAM implementation's maturity level can be determined by cross-referencing the current setup against a maturity level matrix. This can help the organization in both determining the current level and in planning for PAM improvements. Below is one example of such matrix:

The Privilege Maturity Model	Level 1: Absent	Level 2: Adhoc	Level 3: Standardized	Level 4: Managed	Level 5: Advanced
Shared accounts	• Limited controls • No shared account password mgmt. • Lack of accountability	• Manual Controls & processes • Paper trail is not reliable	• Automated discovery, inventory & onboarding • Centralized Password Mgmt. with workflow approval and automated rotation • Privileged account usage reporting	• Password-less session access & management • Context-aware privileged access using RBAC and MFA	• Identity integrated (IAM, SSO, AD-Bridge, AD Audit & Recovery) • Advanced coverage (Cloud, SaaS, Apps) • HSM • User behavior analysis
Application & Service Accounts	• Unknown & Unmanaged	•Documented •Hard coded •Rarely changed, if ever	•Targeted AtoA management •Eliminated targeted hard coded passwords •API driven retrieval	•Centralized AtoA management •No hard-coded passwords; ever	•DevOps Integrated •High Volume •HA and Caching for redundancy
Active Monitoring & Threat Detection	• No monitoring	•Distributed logs •Lack of tracking individuals use of shared accounts	•Centralized audit controls •Individual accountability over use of shared accounts •Deep Visibility with session and keystroke	•Advanced threat detection & UBA •SIEM integration •Automated keyword and activity indexing.	•Automated Privilege Active Response (Deny, Disable, Quarantine, Alert) •IGA integration •Platform independent
Fine-grained Desktop Management	• Unmanaged users have Admin access	•Remove some administrator rights	•Centralized Password Management	•Fine grained access	•Context-aware access policy (user risk, asset risk, ITSM validation, MFA)

		•Desktop tools for ad-hoc elevation	•Limited whitelist \ blacklist proxy access •Reputation services	•Controlled remote server sessions •FIM •Control lateral movement	•IGA integration with separation of duties •Desktop Asset and user policy independence
Fine-grained Server Management	• Unmanaged users have Root access	•Siloed •Open Source (SUDO)	•Centralized Password Management •Limited whitelist \ blacklist proxy access •Platform dependant	•Fine grained access •Privileged Shell •Controlled remote server sessions •FIM •Control latteral movement	•Context-aware access policy (user risk, asset risk, ITSM validation, MFA) •IGA integration with separation of duties •Server Asset and user policy independence
Fine-grained Infrastructure Management	• Unmanaged Users have Root access	•Siloed •Vendor dependant	•Centralized Password Management •Limited whitelist \ blacklist proxy access	•Fine grained access •Controlled remote server sessions •Control lateral movement	•Context-aware access policy (user risk, asset risk, ITSM validation, MFA) •IGA integration with separation of duties