

hello

I'AM

Identity Governance and Privileged Access Management

101 Booklet

CONVERGENCE

of

IDENTITY PILLARS

IAM, CIAM, IGA, PAM, IAP, SSO, MFA, AAA, BYOID, Identity Broker, ZTA, Adaptive Authentication, Policies, Workflow, Automation, Session Management, Role Delegation, Cloud Unified Directory and Zero/Low Code Security

FIRST EDITION

By: **ALi LAzim**, MSc. Computer Sciences
Entrepreneur and Technology Evangelist

About this booklet: Booklet #1

Bring a different way to simply explain some of the most important technology topics related to the Enterprises Security, Trust and Privacy

Disclaimer

The information in this book was correct at the time of publication, but the Author does not assume any liability for loss or damage caused by errors or omissions.

Copyright © 2022 ALi LAzim

All rights reserved. No part of this book may be reproduced or used in any manner without the prior written permission of the copyright owner, except for the use of brief quotations in a book review.

To request permissions, contact the publisher at ali@cr34.com.

Hardcover: ISBN here

Paperback: ISBN here

Audiobook: ISBN here

Ebook: ISBN here

Library of Congress Number: number here

First paperback edition October 2022

Edited by ALi LAzim

Cover art by ALi LAzim

Layout by ALi LAzim

Photographs by ALi LAzim

Printed by Printer Name in the USA.

Your Publisher Name

123 Main St

Anytown, IL 12345

PublisherWebsite.com

INTRODUCTION	4
I'AM Convergence	6
Privileged password management[edit]	15
Examples of privileged passwords[edit]	15
Local administrator accounts[edit]	15
Service accounts[edit]	15
Connections by one application to another[edit]	15
Securing privileged passwords[edit]	16
Required infrastructure[edit]	16
ManageEngine Password Manager Pro, comprehensive enterprise password management software that provides extensive capabilities for password security.	16
Privileged account discovery	17
Enterprise password vault	17
Strict policy enforcement	17
Advanced approval workflows	17
Periodic password rotation	18
Wide platform support	18
Credential management for business automation	18
Comprehensive activity auditing	18
Detailed compliance reporting	19
Two-factor authentication	19
IAM	24
CIAM	25
Cloud Unified Directory	25
Identity And Access Intelligence	25
Enterprise Password Manager	25
ENTERPRISE SECURITY DICTIONARY	26

INTRODUCTION

IAM is an essential part of cybersecurity that manages digital identities and user access to an organization's data, systems, and resources.

According to Gartner, **IAM** is;

“...the discipline that enables the right individuals to access the right resources at the right times for the right reasons.”

According to Gartner, **CIAM** is;

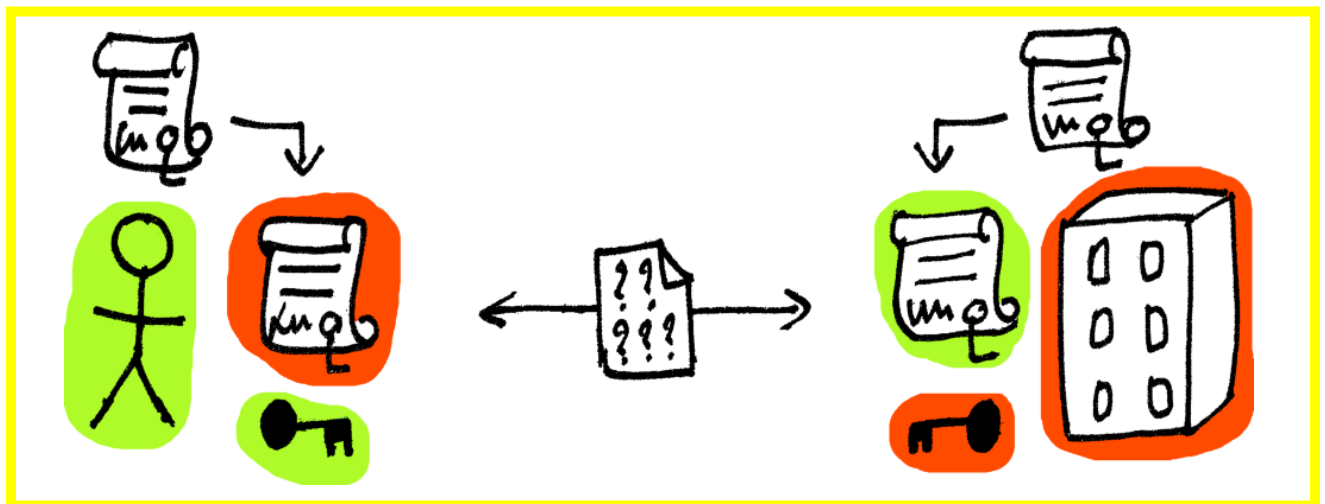
“...the discipline that enables the right individuals to access the right resources at the right times for the right reasons.”

According to Gartner, **IGA** is;

“...the discipline that enables the right individuals to access the right resources at the right times for the right reasons.”

According to Gartner, **PAM** is;

“...the discipline that enables the right individuals to access the right resources at the right times for the right reasons.”



The good solution in this space should be a balance of;

- Security
- Turst
- Privacy
- Usability: end-user experience
- Performance/effectiveness

A comprehensive approach and a turn-key IAM solution/framework enables enterprises to mitigate risks, apply compliances, and increase efficiencies across the enterprise.

There are three components of Identity and Access Management (IAM):

- Access management/Single sign-on to verify users' identities before they can access the network and applications
- Identity governance to ensure that user access is being granted according to appropriate access policies for onboarding and role/responsibility changes
- Privileged access management to control and monitor access to highly privileged accounts, applications and system assets

These technologies can be combined using identity governance, which provides the foundation for automated workflows and processes.

I believe that today's expansive digital age requires a unified IAM platform, one with a holistic, integrated approach that allows governance to play a crucial and connected role with identity and access management in all its aspects.

I'AM Convergence

I'AM is an essential part of cybersecurity that manages everything about digital identities and user access to an organization's data, systems, and resources covering all IAM, CIAM, IGA, PAM and more.

DO NOT
DO IT

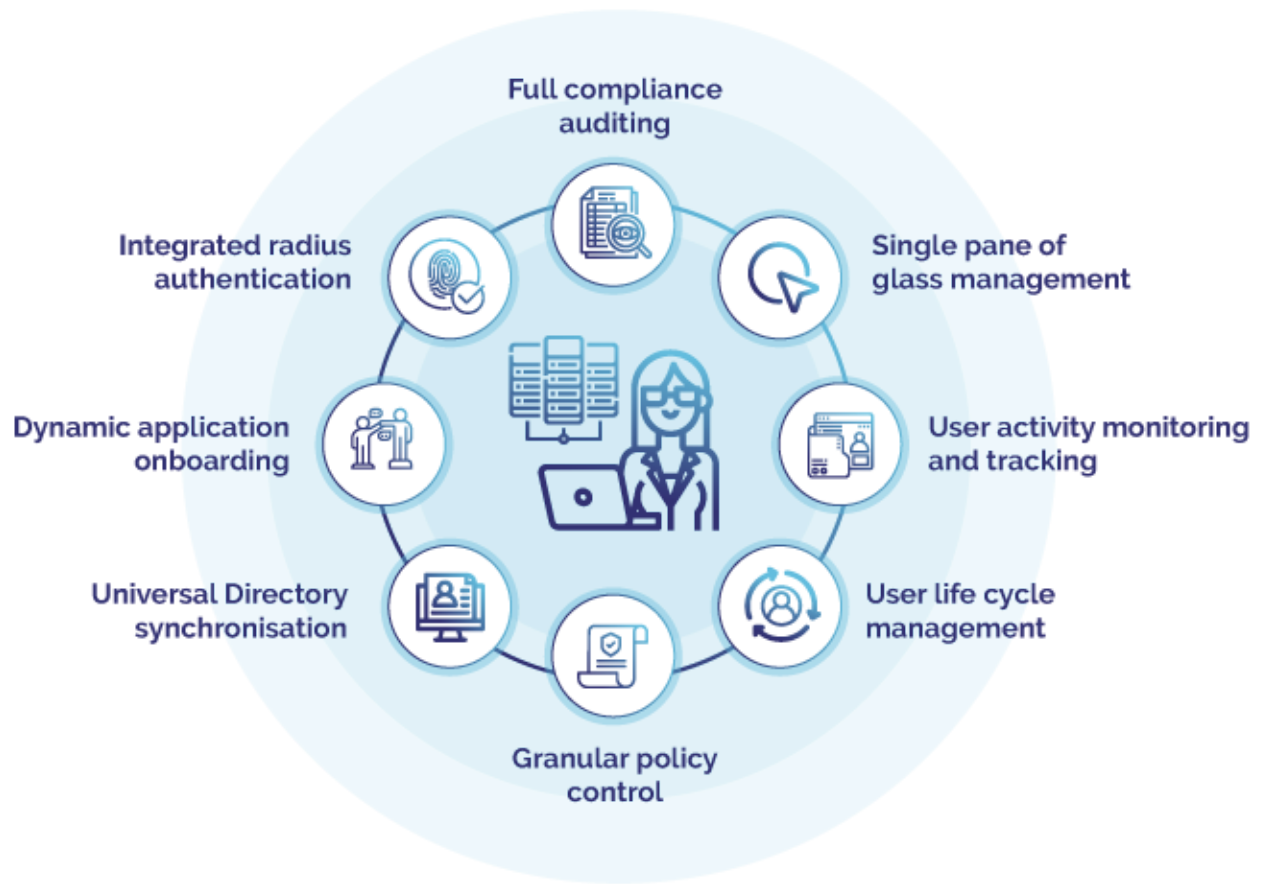
converge IAM

PRODUCT NAME: **I'AM ???**

IAM+CIAM+IGA+PAM+MFA+BYOID+++++









Why One Identity

Challenges

- Security
- Complexity
- Compliance



The path to governance

- Policy-based access control
- Governance for identities, user access, data and elevated access
- Privileged account lockdown



Business driven

- User and line-of-business self-service
- Unified policy, identity and workflow
- Complete visibility and control



Future-ready

- Configure don't code
- Configure to meet changing organizational needs
- Minimize the shock of constantly changing employee roles



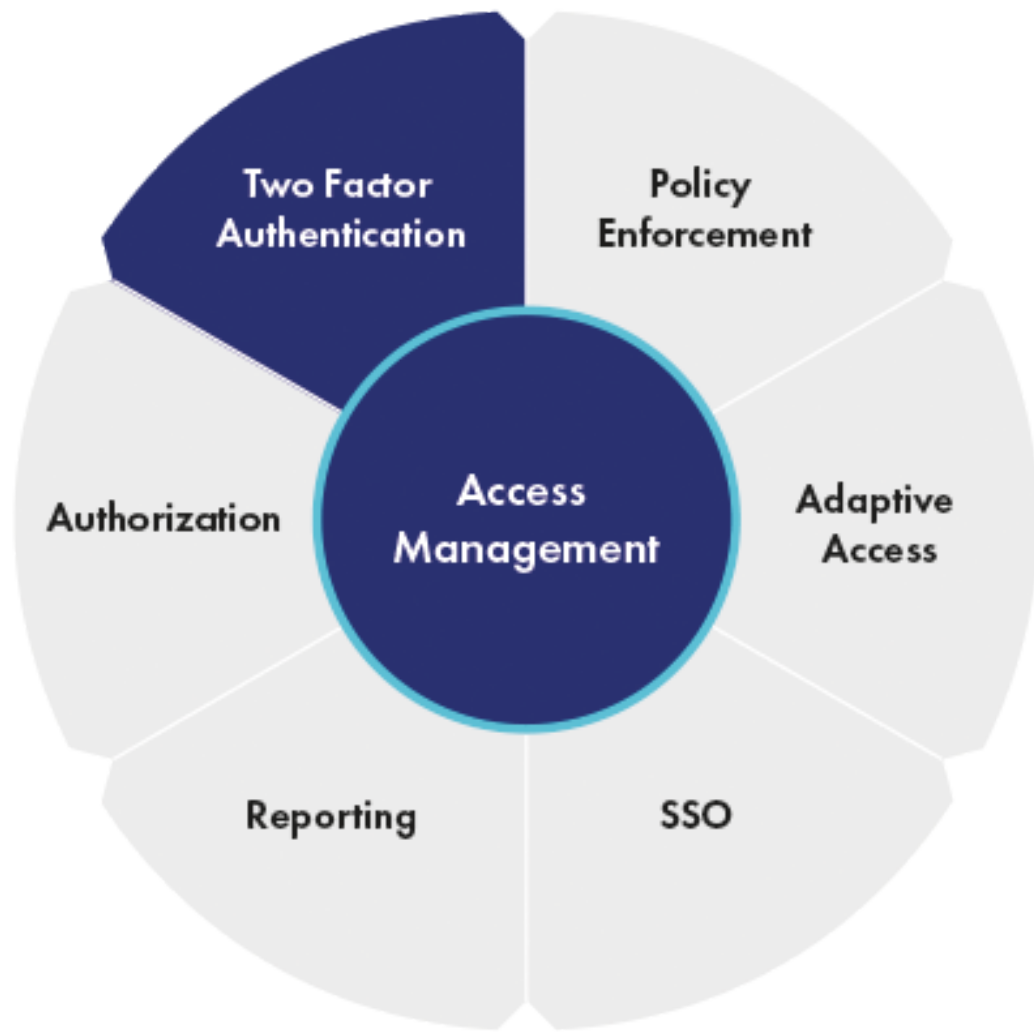
Modular & integrated

- Doesn't demand a rigid framework
- Start anywhere and build from there
- Easily plugs into existing tools and solutions



Rapid time to value

- Deploy in weeks, not years
- Streamline and automate tasks
- Extremely affordable
- Relieve the burden on IT





2022 Key Trends in Identity and Access Management

Connect Anywhere Computing Will Further Drive Need for Smarter Access Control

Improving User Experience for All Users Will Be Essential for Secure Digital Business

IGA Functions Will Evolve to Enable Decentralized Architecture

Keys, Secrets, Certificates and Machines Will Require More Attention

Hybrid Cloud and Multicloud Will Drive Ongoing IAM Architecture Maintenance/Evolution

New Applications and APIs Will Need to Leverage the Latest IAM Development Guidelines



gartner.com

Source: Gartner
© 2022 Gartner, Inc. All rights reserved. PR_1655517

Gartner[®]

- Identity lifecycle management
- Entitlement management
- Support for access requests
- Workflow orchestration
- Access certification (also called “attestation”)
- Provisioning via automated connectors and service tickets
- Analytics and reporting

Privileged password management^[edit]

Privileged password management is a type of password management used to secure the passwords for login IDs that have elevated security privileges. This is most often done by periodically changing every such password to a new, random value. Since users and automated software processes need these passwords to function, privileged password management systems must also store these passwords and provide various mechanisms to disclose these passwords in a secure and appropriate manner. Privileged password management is related to [privileged identity management](#).

Examples of privileged passwords^[edit]

There are three main types of privileged passwords. They are used to authenticate:

Local administrator accounts^[edit]

On Unix and Linux systems, the [root user](#) is a privileged login account. On Windows, the equivalent is Administrator. On SQL databases, the equivalent is sa. In general, most operating systems, databases, applications and network devices include an administrative login, used to install software, configure the system, manage users, apply patches, etc. On some systems, different privileged functions are assigned to different users, which means that there are more privileged login accounts, but each of them is less powerful.

Service accounts^[edit]

On the Windows operating system, service programs execute in the context of either system (very privileged but has no password) or of a user account. When services run as a non-system user, the service control manager must provide a login ID and password to run the service program so service accounts have passwords. On Unix and Linux systems, init and inetd can launch service programs as non-privileged users without knowing their passwords so services do not normally have passwords.

Connections by one application to another^[edit]

Often, one application needs to be able to connect to another, to access a service. A common example of this pattern is when a web application must log into a database to retrieve some

information. These inter-application connections normally require a login ID and password and this password.

Securing privileged passwords^[edit]

A privileged password management system secures privileged passwords by:

- Periodically changing each password to a new random value.
- Storing these values.
- Protecting the stored values (e.g., using encryption and replicated storage).
- Providing mechanisms to disclose these passwords to various types of participants in the system:
 - IT administrators.
 - Programs that launch services (e.g., service control manager on Windows).
 - Applications that must connect to other applications.

Required infrastructure^[edit]

A privileged password management system requires extensive infrastructure:

- A mechanism to schedule password changes.
- Connectors to various kinds of systems.
- Mechanism to update various participants with new password values.
- Extensive auditing.
- Encrypted storage.
- Authentication for parties that wish to retrieve password values.
- Access controls and authorization to decide whether password disclosure is appropriate.
- Replicated storage to ensure that hardware failure or a site disaster does not lead to loss of data.

=====

**ManageEngine Password Manager Pro,
comprehensive enterprise password management
software that provides extensive capabilities for
password security.**



Privileged account discovery

Run automated discovery scans to detect all IT assets on the corporate network and subsequently discover the associated privileged account credentials. Maintain an auto-updating database of privileged accounts with periodic synchronization schedules.



Enterprise password vault

Create an inventory of all critical, shared user accounts that hold elevated privileges, and store them in a secure vault. Isolate access to the vault with granular role-based access controls. Ensure the privileged accounts are encrypted with strong algorithms such as AES-256.



Strict policy enforcement

Standardize password management best practices across the enterprise by implementing a strict policy that covers various password security aspects. Eliminate weak passwords and satisfy compliance requirements.



Advanced approval workflows

Avoid unauthorized access attempts. Mandate an IT head's approval for every password access request. Make the workflow stronger with a dual control mechanism by requiring supervision and approval from at least two higher IT officials.



Periodic password rotation

Assign strong, unique passwords for remote resources using a robust built-in password generator. Reset credentials any time on demand or randomize them periodically through scheduled tasks.



Wide platform support

Implement robust password management for multiple platforms across physical, virtual, and cloud infrastructures. Secure the passwords of endpoints even in remote locations without direct connectivity such as the ones protected by firewalls or residing in demilitarized zones (DMZs).



Credential management for business automation

Use automations to take bold steps forward without worrying about credentials being compromised. Integrate password security best practices in your application communications, DevOps routine, and RPA workflows. Abolish hard-coded passwords.



Comprehensive activity auditing

Capture every single user operation, establishing accountability and transparency for all password-related actions. Submit exhaustive access logs during regular internal audits and ad hoc forensic investigations. Always know who did what with a password, where, and when.



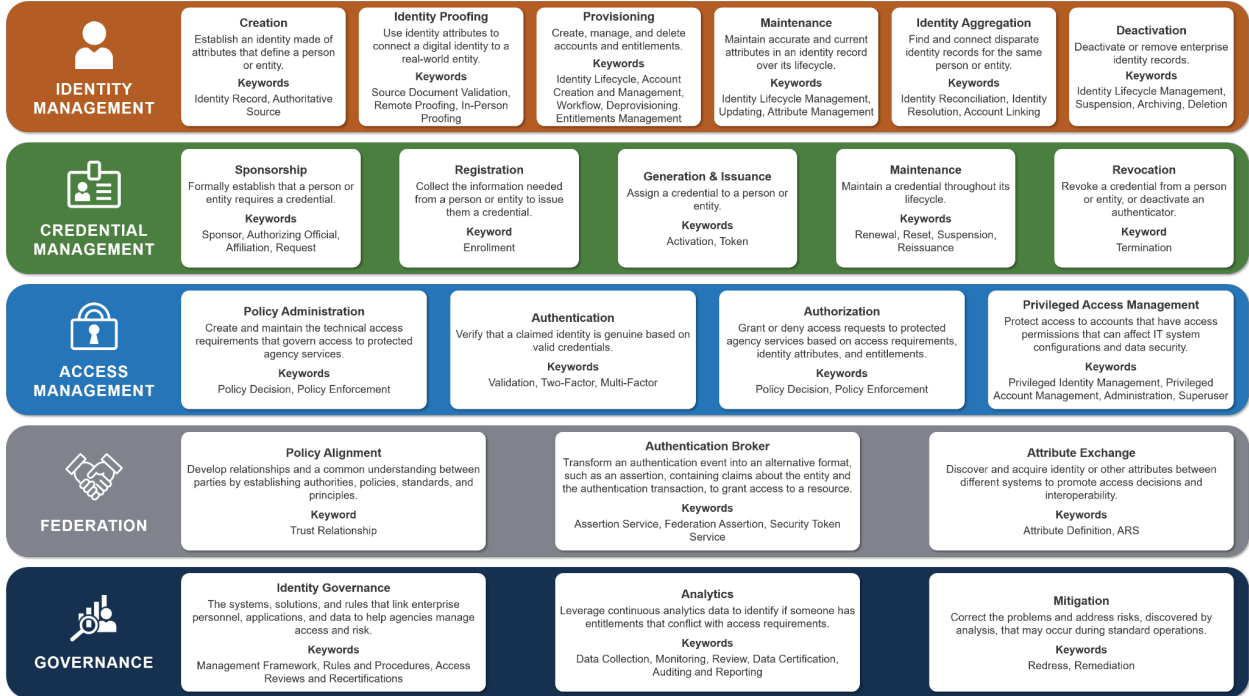
Detailed compliance reporting


Get a wider, in-depth view of password security and privileged user activity in your organization with timed reports. Generate audit-ready reports for PCI DSS, NERC-CIP, ISO/IEC 27001, and the GDPR. Exercise complete flexibility and produce custom-fit reports to meet exclusive business needs.




Two-factor authentication

Administer multiple stages of authentication and associate every password-related activity with a valid user profile. According to [Microsoft](#), multi-factor authentication (MFA) blocks 99.9 percent of unauthorized login attempts, even if hackers have a copy of a user's current password.



 **IDENTITY MANAGEMENT**


- Creation
- Identity Proofing
- Provisioning
- Maintenance
- Identity Aggregation
- Deactivation

 **CREDENTIAL MANAGEMENT**

- Sponsorship
- Registration
- Generation & Issuance
- Maintenance
- Revocation

 **ACCESS MANAGEMENT**

- Policy Administration
- Authentication
- Authorization
- Privileged Access Management

 **FEDERATION**

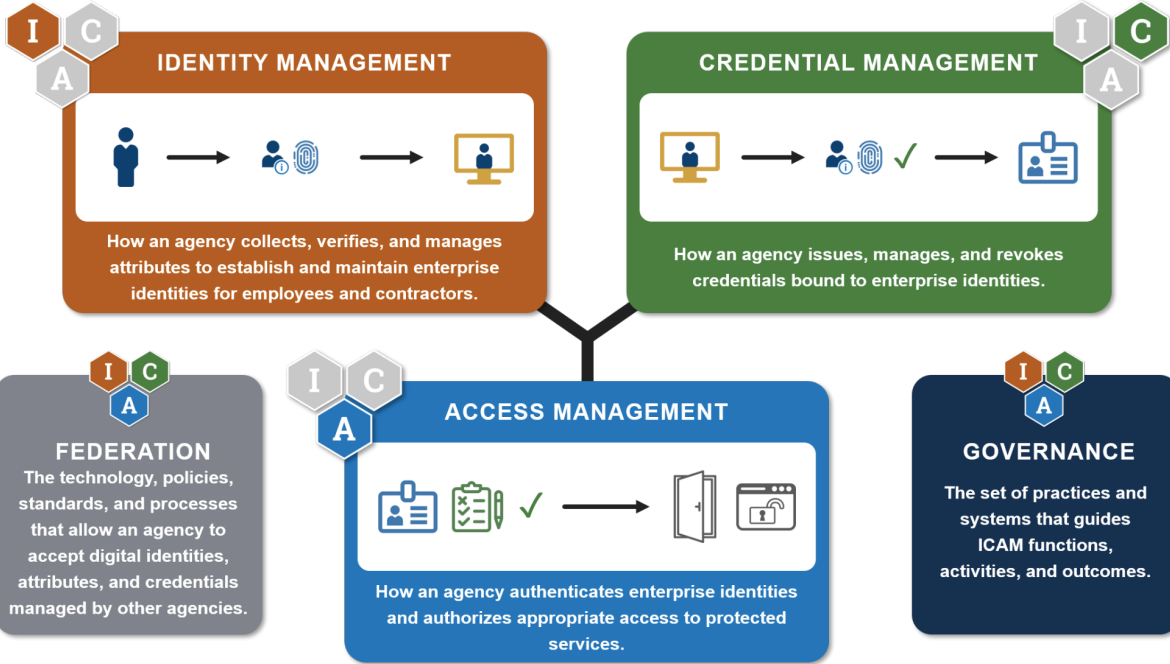
- Policy Alignment
- Authentication Broker
- Attribute Exchange

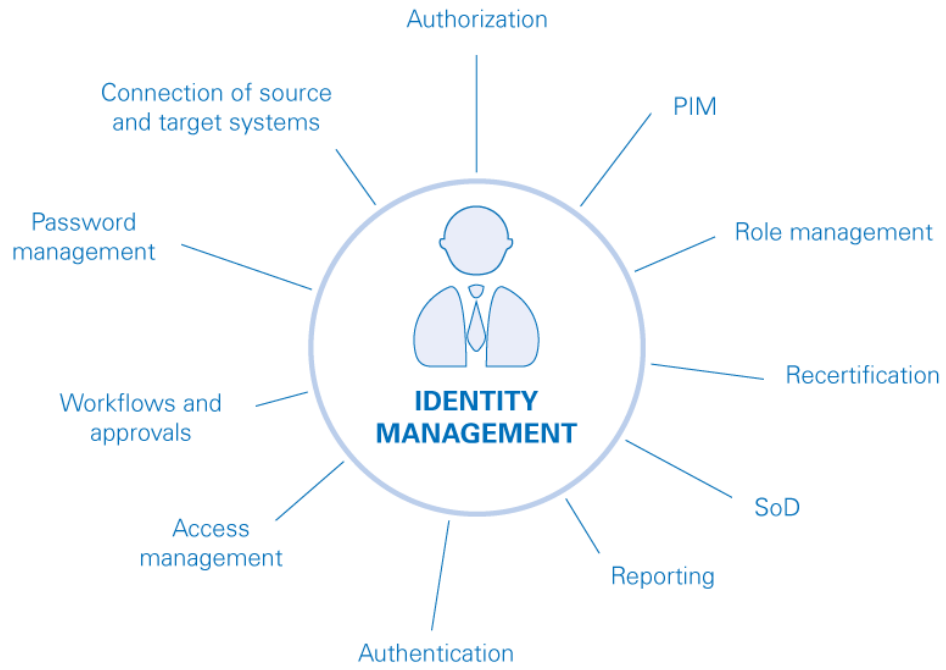
 **GOVERNANCE**

- Identity Governance
- Analytics
- Mitigation

IDENTITY, CREDENTIAL, AND ACCESS MANAGEMENT (ICAM)

The set of tools, policies, and systems that an agency uses to enable the *right individual* to access the *right resource*, at the *right time*, for the *right reason* in support of *federal business objectives*.







IAM is all about how to structure, manage and administer the identities and their accesses within your organization.

It is to control who is authenticated (signed in) and authorized (has permissions) to access the enterprise resources (computer, app, doc, etc.). Using an identity platform to manage accounts across organization applications is mandatory for any enterprise cares about their cybersecurity.







Okta Identity Governance supports that by introducing three new governance capabilities to the Okta Identity Cloud:

- Okta Access Requests: *Simplify and automate the process of requesting and approving access to applications and resources.* Self-service capabilities, tightly integrated with popular collaboration tools, meet users where they are, delivering a streamlined, frictionless experience to auto-provision their access.
- Okta Access Certifications: *Create and manage access review campaigns.* Periodically reviewing user access to critical resources, and approving or revoking access automatically, is essential for ensuring that all users have the right level of access across all resources.
- Enhanced Governance Reports: *Out-of-the-box reporting capabilities to help meet audit and compliance requirements.* Administrators can provide an audit report of who has access to what resources, who approved the access, and how they got it.

Together with lifecycle automation capabilities powered by Okta Lifecycle Management and customization and extensibility offered by Okta Workflows, customers can leverage Okta to automate the process of granting their workforce the correct levels of access to the resources they need.

Our philosophy with Okta Identity Governance was to rethink the way governance is done today by building a modern product that's easy to use and based on Okta principles of cloud-native technology. This means delivering a product that:

- Drives better security and compliance outcomes
- Is easy to deploy and maintain for IT teams
- Is modern and simple for employees to use

Let's get into the details of how Okta Identity Governance enables customers to achieve these goals.

<https://www.okta.com/blog/2022/08/introducing-okta-identity-governance/>

<https://www.okta.com/products/lifecycle-management/>

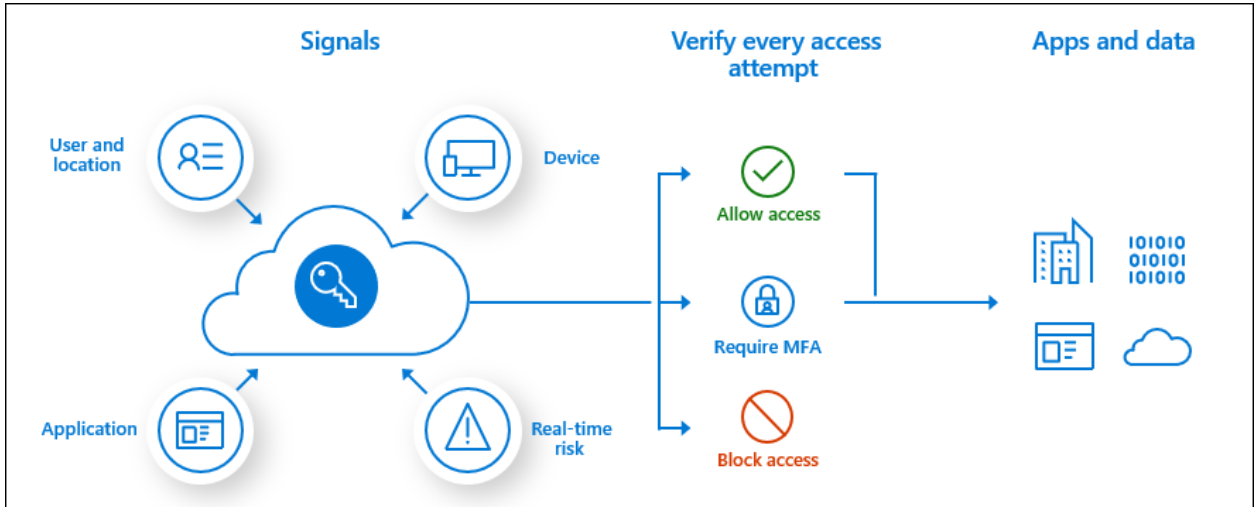
<https://www.okta.com/platform/workflows/>

Cloud Unified Directory

Intity And Access Intelligence

Enterprise Password Manager

Adaptive Authentication:



ENTERPRISE SECURITY DICTIONARY

Cybersecurity	
ID	ID entity
Identity Management	
IAM	
CIAM	
IGA	
PAM	
IAP	Identity And Access Proxy (IAP)
SSO	
AAA	
MFA	Multi-Factor Authentication
OTP	One-Time Password
Passwordless	
Adaptive Authentication	
Identity Broker	
Policies	
Role-based Access Control	
ZTA / ZTS	Zero Trust Architecture (aka Zero Trust Security)

BeyondCorp	
Token	
Soft Token	
Hard Token	
USB Token	
FIDO	
FIDO OATH	
FIDO U2F	
FIDO UAF	
OAuth2	
OIDC	OpenID Connect
SCIM	
SAML	
RADIUS	
Web Monetization	
Anomaly Detection	
Session Management	
User Monitoring	
Role Delegation	
Zero Code Security	

Low Code Security	
Workflow	
Automation	