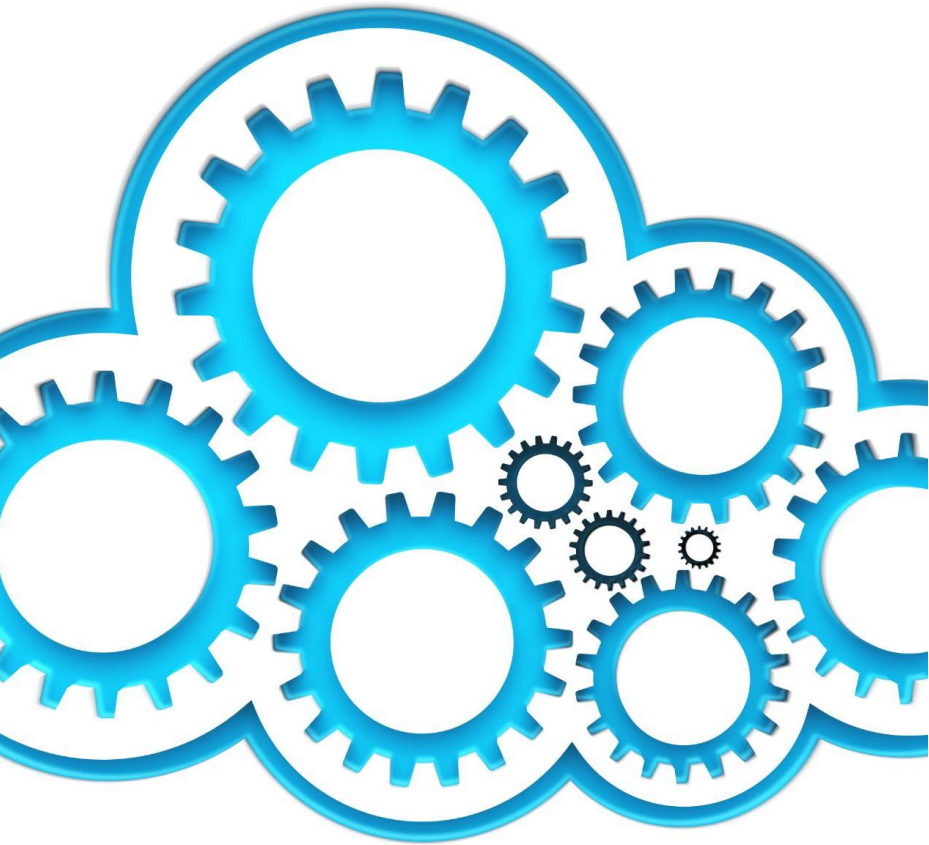


Identity Governance and Administration in Public Cloud

by Ilya Polyakov 2025



What is Identity Governance?

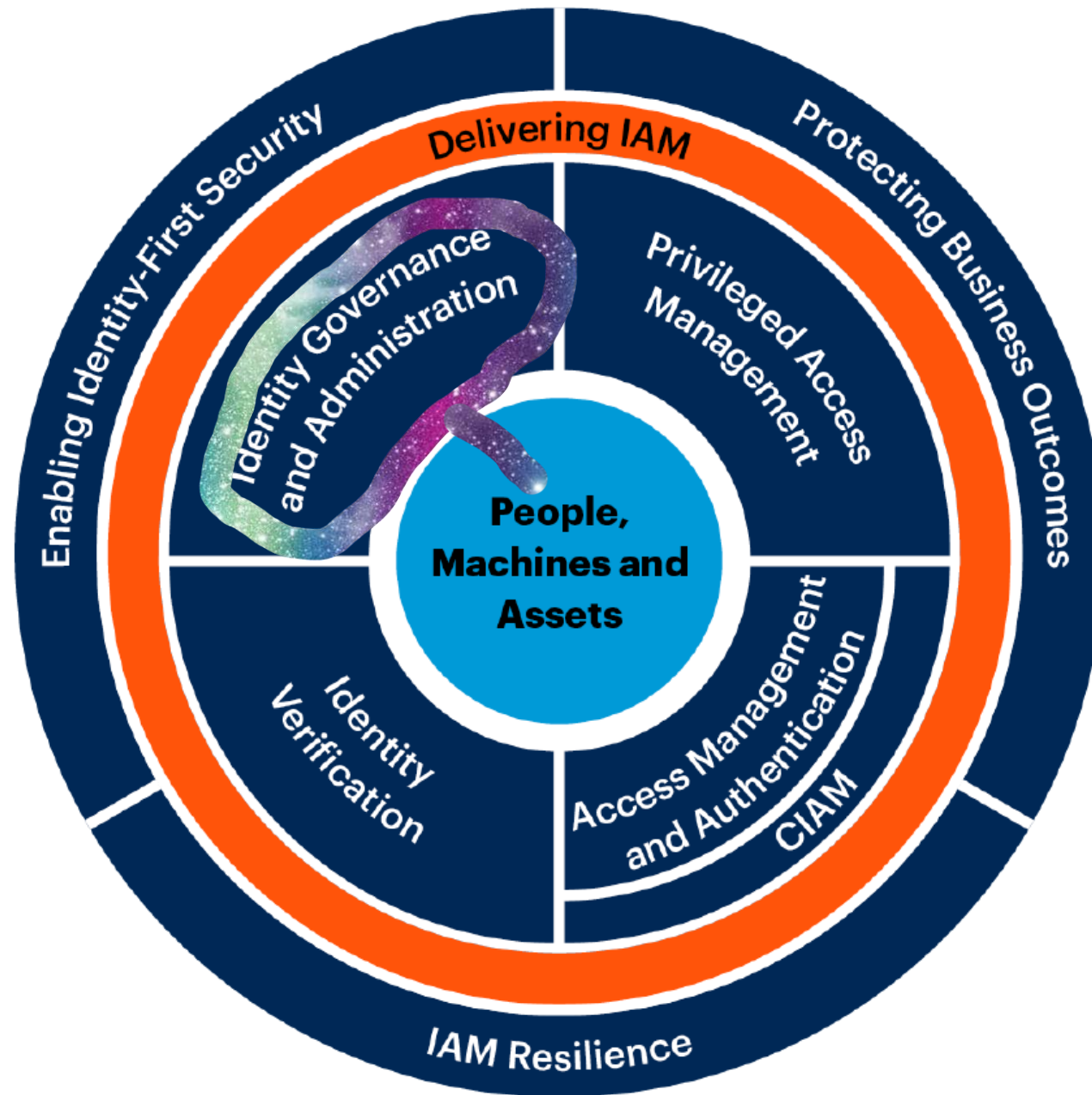


- Identity Governance refers to the framework, processes, and technologies that ensure the right individuals have the right access to the right resources at the right time. It encompasses identity lifecycle management, access controls, privilege management, and compliance monitoring to prevent unauthorized access and reduce security risks. Unlike traditional Identity and Access Management (IAM), which primarily focuses on authentication and authorization, Identity Governance extends into access reviews, policy enforcement, and auditability.

Use case discussion



- Company XYZ decided to use multicloud strategy with 2 core cloud providers used – AWS and Azure.
- Company has several offices and a network, with Active Directory that is synced to Entra ID as the main authentication service for its employees.
- Problem statement: The organisation can not decide what to do with authentication to AWS and Azure cloud environments



Why is Identity Governance Critical in Cloud Environments?

- As organizations move workloads to the cloud, the attack surface for identity-based threats increases. The cloud operates under a **shared responsibility model**, where cloud providers secure the infrastructure, but **customers must secure identities and access controls**. Without proper governance, risks such as **privilege escalation, credential theft, and misconfigured access policies can lead to security breaches**. Identity Governance also plays a crucial role in compliance with industry regulations such as **ISO 27001, NIST, GDPR, and the Australian ISM** (Information Security Manual).

Is Active Directory nearly dead as a central identity store?



Is Active Directory nearly dead as a central identity store?

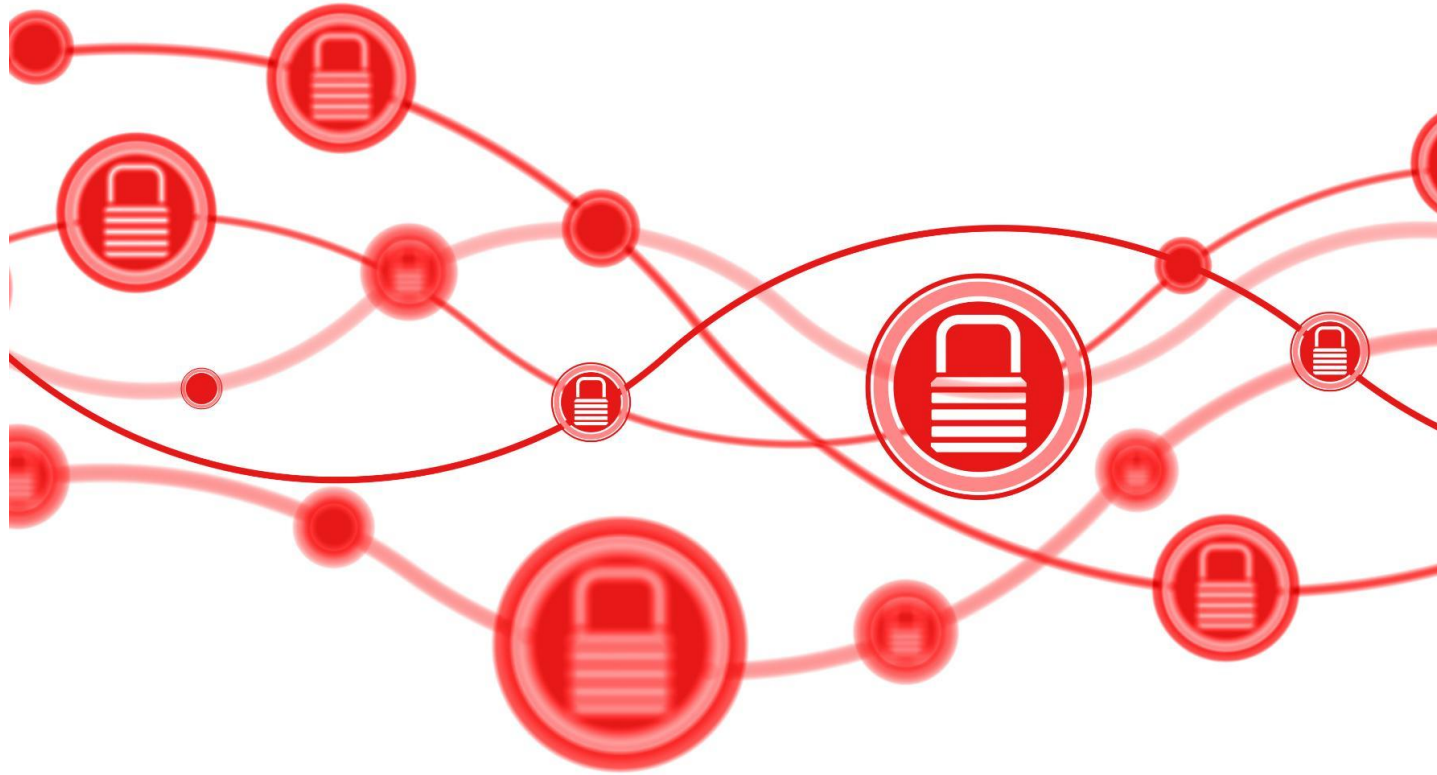
Risks	Entra ID	Active Directory
Attack surface	Entra ID is a cloud-based service, it is accessible from anywhere on the internet, making it more susceptible to attacks like password spraying, credential stuffing, and brute-force attacks.	Traditional Active Directory is usually restricted to internal corporate networks, reducing its exposure to external threats.
Credential theft risks	Entra ID relies heavily on passwords and OAuth tokens, can be targeted in phishing attacks. Compromised credentials can be used to access all federated cloud applications	While AD credentials can also be phished, the risk is mitigated by network segmentation and internal security controls.
DoS	Entra ID authentication is exposed to brute-force and DoS attacks, which can lock accounts or impact availability.	Since AD authentication traffic remains inside the corporate network, DoS attacks are less likely unless an attacker gains internal access.
Cloud service dependency	If Microsoft experiences an outage (which has happened before), all cloud-based authentication and applications relying on Entra ID could become inaccessible.	Organisations retain full control over AD availability, meaning they can implement high-availability configurations with failover mechanisms.
Performance	Entra ID authentication requires internet connectivity, introducing latency for authentication requests, especially in environments with high traffic.	AD authentication is usually faster and more reliable because it operates within the local network
Audit & Logging Limitations	Entra ID provides limited logging and event history in the default license tier. Advanced auditing features require Microsoft Defender for Identity or an Entra ID P1/P2 license	Organizations can implement detailed event logging and SIEM integration with full control over log retention and access policies.
Regulatory Compliance	Some regulations (e.g., Australian Government ISM, PCI-DSS) require stronger access controls and on-premise data control, which might be harder to enforce in Entra ID.	Active Directory allows organizations to customize security policies, enforce air-gapped access, and ensure compliance with strict security standards.

Best of both options:



- Using Microsoft Entra ID as a central identity store is beneficial for cloud-native environments, offering scalability, simplified management, and SaaS integration. However, it introduces security, availability, and compliance risks, especially for organizations with strict regulatory requirements or hybrid infrastructure.
- A Hybrid Identity Model, where Entra ID is used for cloud applications while on-prem AD remains the source of truth, can be an effective compromise. Organizations should implement strong authentication, logging, and redundancy strategies to mitigate risks and ensure resilience.


What about AWS iAM?



AWS IAM

- **AWS IAM Overview**
- AWS Identity and Access Management (IAM) is the core service for managing users, groups, roles, and policies. AWS IAM supports:
 - **IAM Users and Groups** – Managing individual user accounts and grouping them for easier access control.
 - **IAM Roles and Policies** – Assigning permissions dynamically to services and users without static credentials.
 - **IAM Permission Boundaries** – Restricting permissions even when more permissive policies are attached.
- **AWS Organizations & Service Control Policies (SCPs)**
- AWS Organizations allows multi-account management with centralized policies. **Service Control Policies (SCPs)** enforce permissions at an organizational level, ensuring compliance and governance across multiple AWS accounts.
- **AWS Identity Center & Access Analyzer**
- AWS Identity Center (formerly AWS SSO) provides centralized authentication and access management. **AWS IAM Access Analyzer** helps organizations identify and manage excessive permissions, reducing security risks.
- Wow, that sounds comprehensive, right? There is a hidden problem, in our use case all users are in Active Directory, Entra ID. But here, separate accounts are being created for users, unless....

You federate and avoid separate identity island in AWS.

Method	Best For	Pros	Cons	Comment
AWS IAM Identity Center (AWS SSO)	Multi-account AWS access using AD credentials	Simple setup, SAML & SCIM support	Requires AD connection or IdP (e.g., Entra ID, Okta)	Best for large and complex enterprise, map users or groups to the roles as a best practice
AWS Managed Microsoft AD	Extending full AD functionality into AWS	Native AD features, LDAP & Kerberos support	Requires AWS infrastructure for domain controllers	Could be used for large organisations as well, however, requires trust setup between on prem AD and AWS managed, creates additional complexity
AD Federation via SAML (AD FS)	Federated access without syncing AD users to AWS	No need to sync users, uses existing AD FS	More complex setup, requires AD FS	Mid-sized organisations
AWS iAM	Completely separate identities in AWS	No reliance on any IDP	Very manual identity management, difficult to automate governance	Good for small team or startup, btw many large organisations still use this 

Final solution

- On premise AD is synced to Entra ID
- Identities are managed in AD only with IGA and PAM capabilities
- AWS identities are federated using Identity Center direct integration with on prem AD
- AD groups are mapped to AWS roles, which allows Identity Governance of the access in AWS
- For resiliency secondary AD domain controllers are deployed in AWS and Azure (if required)

ilya@polyakov.au

<https://www.linkedin.com/in/ily-polyakov/>

