OLERIA™

DSCI
PROMOTING DATA PROTECTION

Identity Security Maturity

in the AI Era

Executive Summary

Identity Access Management (IAM) at the Center of the Digital Enterprise

IAM has become the **primary control layer of the modern digital enterprise**. As organizations operate across cloud environments, APIs, partner ecosystems, and AI-driven systems, every interaction whether human or machine is governed through identity. This shift places identity at the core of **security, resilience, and digital transformation**.

The Expanding Identity Surface

The identity landscape has evolved beyond workforce users to include a rapidly growing ecosystem of **non-human identities (APIs, workloads, service accounts)** and **AI-driven agents**. These identities now outnumber human users and often operate with elevated privileges and limited oversight. As a result, the identity surface has become **dynamic, distributed, and increasingly autonomous**, significantly expanding the attack surface and complexity of governance.

Why IAM Maturity is Critical

In this environment, IAM maturity is a key determinant of an organization's ability to manage risk and scale securely. Fragmented identity systems, manual processes, and static controls leave organizations exposed to identity-based attacks and operational inefficiencies. In contrast, mature environments enable:

- **Unified visibility across all identity types**
- **Policy-driven, least privilege access controls**
- **Continuous monitoring and adaptive response**

IAM maturity is therefore essential not only for security, but for **ensuring business continuity, regulatory readiness, and secure adoption of AI and digital platforms**.

Key Observations

- Identity is now the **dominant attack vector**, with compromised credentials and access misuse driving a majority of breaches
- **NHIs are the fastest-growing and least-governed risk area**

- **AI systems are redefining identity interactions**, introducing autonomy, delegation, and new governance challenges
- Traditional IAM approaches remain **fragmented and tool-centric**, limiting effectiveness at scale
- Organizations lack a **structured maturity-driven approach**, resulting in inconsistent identity controls

Strategic Implications for Organizations

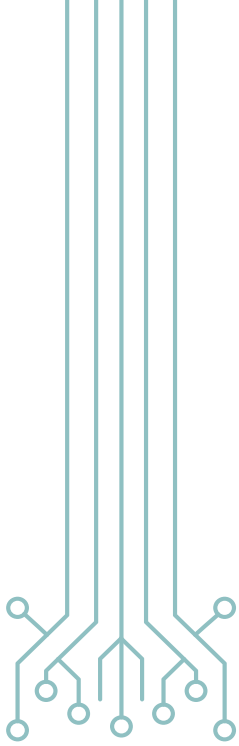
To address these challenges, organizations must:

- Treat IAM as a **core architectural layer and control plane**
- Move from **tool-centric deployments to capability-driven identity programs**
- Extend governance to **machine identities and AI agents**
- Adopt **continuous, context-aware, and intelligence-driven identity controls**
- Use **maturity models to benchmark, prioritize, and scale identity capabilities**

Identity is no longer just an access function; it is the **foundation of trust in digital enterprises**. As identity ecosystems continue to expand across humans, machines, and AI, organizations must adopt a **maturity-driven, integrated approach** to identity security. Those that do so will be better positioned to reduce risk, enable innovation, and build **resilient, future-ready digital operations**.

Table of **Contents**

The Transformation of Identity and the Digital Enterprise



The rapid digital transformation has fundamentally altered the role of identity within cyber security architecture. Traditionally, identity systems were designed primarily to manage employee access to internal applications. Today, however, Identity and Access Management (IAM) sits at the center of security frameworks, governing access across distributed infrastructure, cloud environments, digital ecosystems, and increasingly autonomous systems.

Understanding the evolving identity landscape requires examining the expanding scope of identity, the growing complexity of access across infrastructure layers, the role of identity in cyber security strategies, and the emergence of machine-driven identities.

IAM and The Role It Plays in Cyber Security

IAM governs the authentication of users and systems, authorization of access privileges, and ongoing monitoring of identity-related activities across digital environments.

In an enterprise's cyber security architecture, identity is the primary mechanism through which organizations control access to data, systems, and applications. As traditional network boundaries have eroded, IAM has replaced the network perimeter as the most reliable security control.

In June 2025, over 16 billion login credentials, including usernames and passwords, as well as session tokens and cookies were exposed and harvested from various online platforms.[1] 80% of breaches involve compromised identities.[2]

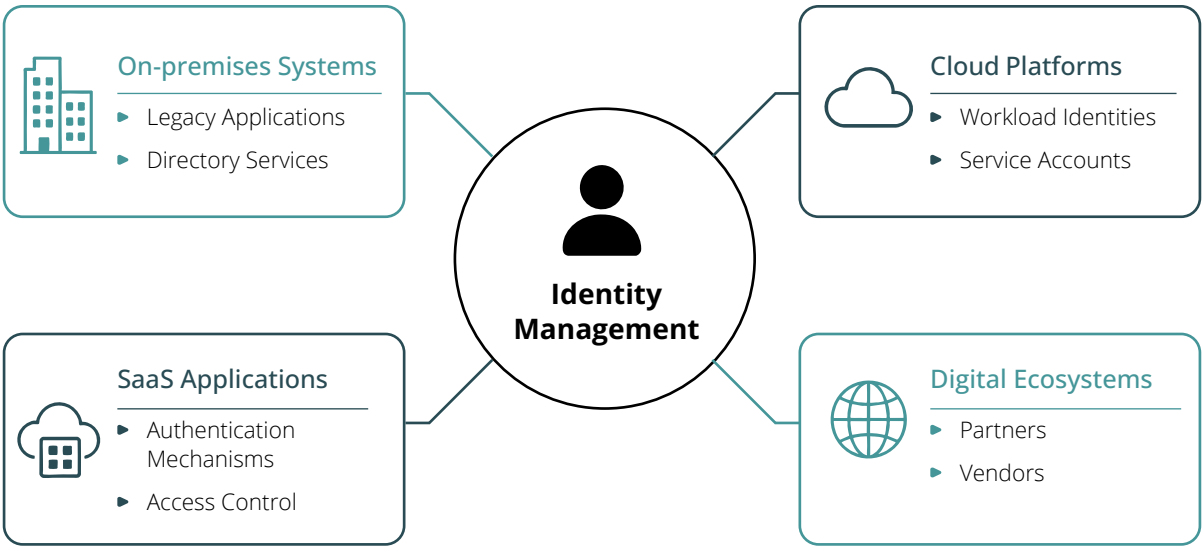
IAM serves not only as authentication gateways but as enforcement mechanisms for key security principles such as **least privilege access, continuous verification, and risk-based authentication**. Security frameworks such as **Zero Trust Architecture (ZTA)** place identity at the center of access control decisions, requiring continuous validation of users, devices, and services regardless of network location.

As organizations increasingly rely on distributed digital infrastructure, the ability to effectively manage identity and access has become essential to maintaining operational resilience and digital trust.

Identity Sprawl Across Digital Infrastructure

While identity has become central to cyber security, the environments in which identities operate have grown increasingly complex. Enterprises today operate in an interconnected infrastructure spanning on-premises systems, cloud platforms, SaaS applications, and external partner ecosystems. This has led to **identity sprawl**, where identities proliferate across multiple platforms without centralized oversight.

Identity Management within Enterprises



Organizations manage identities across dozens of identity repositories and hundreds of applications, making centralized visibility a major challenge. This distributed architecture significantly increases the complexity of identity governance. Without unified oversight, identities may be created, modified, and retained across multiple systems without consistent policy enforcement.

The fragmentation of identity across infrastructure layers also increases the risk of misconfiguration, excessive privileges, and dormant accounts. These factors collectively contribute to the growing attack surface associated with identity-based threats.

Identity Access – A Strategic Priority

Given the expansion of digital infrastructure and the increasing sophistication of identity-based attacks, organizations are placing greater strategic emphasis on identity security.

Several factors explain why IAM has become a critical priority for enterprises:

Expansion of the digital attack surface

The widespread adoption of cloud services, SaaS platforms, remote work environments, and mobile devices has expanded the number of entry points through which attackers can attempt to gain unauthorized access.

Credential-based attack techniques

Attack methods such as phishing, credential stuffing, and password spraying continue to exploit weak identity controls.

Privileged access risks

Privileged accounts provide broad access to critical systems and data, making them prime targets for attackers seeking to escalate privileges or move laterally within networks.

Compliance and regulatory requirements

Organizations must increasingly demonstrate control over who can access sensitive data and how access rights are granted, modified, and revoked.

Operational dependency on digital services

Identity systems now underpin business-critical workflows, making their reliability and security essential for organizational continuity.

These factors collectively reinforce the need for organizations to adopt mature identity governance frameworks that extend beyond basic authentication to include lifecycle management, continuous monitoring, and contextual access control.

Evolution of Identity and Access Management

IAM has evolved significantly over the past two decades in response to changing technological environments and security requirements.

The Directory Era: Centralized and Perimeter-Based

X.500 & LDAP Foundations: Early IAM relied on the X.500 standard. The **Lightweight Directory Access Protocol (LDAP)** became the industry standard for querying and modifying items in directory service providers.

Active Directory (AD) & Kerberos: Microsoft introduced AD, using **Kerberos** for authentication. This relied on "tickets" and a trusted third party (the Domain Controller).

The Technical Limit: Trust was binary. If you had the line of sight to the Domain Controller and a valid password, you were granted a "Global Catalog" of permissions that rarely expired.

The Federation Era: Cross-Domain Trust

SAML 2.0 (Security Assertion Markup Language): The introduction of XML-based assertions. This allowed an **Identity Provider (IdP)** to tell a **Service Provider** that a user was authenticated without sharing the actual password.

The Shift to Web-Scale (OAuth 2.0 & OIDC): SAML was "heavy" for mobile and modern web.

- **OAuth 2.0** introduced **Access Tokens** and **Refresh Tokens**, shifting the focus to authorization (what an app can do on your behalf).
- **OpenID Connect (OIDC)** was built on top of OAuth to add an identity layer, providing the **ID Token**.

SCIM (System for Cross-domain Identity Management): Technically automated the provisioning/deprovisioning of users across different cloud platforms using a standardized JSON API.

The Governance and Lifecycle Era

Role-Based Access Control (RBAC): Technical implementation of "Entitlements." Permissions were bundled into roles, creating a many-to-many mapping of users to permissions.

Attribute-Based Access Control (ABAC): A major technical leap. Instead of just "Roles," access was determined by **Attributes**.

Identity Cubes: Aggregating data from HR systems, ERPs, and Directories into a single "Cube" to find "Orphan Accounts" or "Toxic Combinations" of access.

The Contextual and Zero Trust Era

Adaptive MFA: Introduction of Risk Engines. These engines evaluate telemetry (IP address, device health via EDR, Geo-location) before issuing a TOTP or Push notification.

The Signal Mesh: IAM systems began consuming signals from other security tools (SIEM/SOAR). If a device is flagged as "Infected" by an antivirus, the IAM system technically revokes the OIDC session instantly.

Just-In-Time (JIT) & Ephemeral Access: Moving away from "Standing Privileges." Technically, a user has zero rights until they request them; the system then creates a temporary credential that self-destructs after a set window.

The Modern Stack: Identity Threat Detection & Passwordless

FIDO2 / WebAuthn: The most significant technical shift in 20 years. It replaces shared secrets (passwords) with Asymmetric Cryptography. The private key never leaves the user's hardware (TPM/Titan chip), making it phishing resistent.

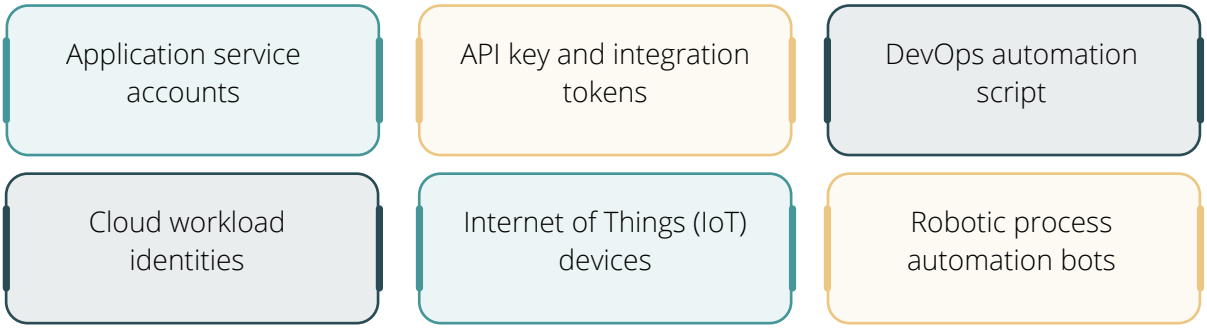
ITDR: Real-time monitoring of the identity infrastructure itself (e.g., detecting "DCShadow" attacks or "Golden Ticket" creation in AD).

Service & Machine Identity (SPIFFE/Spire): As microservices exploded, IAM had to solve for "Workload Identity." Using short-lived X.509 certificates to allow containers to talk to each other securely without hardcoded API keys.

This evolution reflects a broader shift toward identity-centric security models in which access decisions are continuously evaluated based on user context, device posture, and behavioral signals.

Rise of NHIs, Machine Identities, and Autonomous Agents

One of the most significant developments in the identity landscape is the rapid growth of **NHIs** including:



These identities enable automated systems to communicate and execute tasks without direct human involvement. As organizations adopt cloud-native architectures and automated workflows, the number of machine-driven identities has grown dramatically.

Machine identities significantly outnumber human identities with a ratio of 80:1. Only 15% of the organizations feel highly confident preventing NHI attacks.[3]

AI systems increasingly interact with enterprise data, initiate workflows, and perform decision-making tasks that require access to digital resources. These capabilities introduce new identity governance challenges related to accountability, privilege management, and monitoring of machine behavior.

The Expanding Identity Attack Surface and Enterprise Risk

Enterprises today are not struggling because they lack IAM tools. They are struggling because identity environments have outgrown traditional design assumptions. The convergence of cloud, SaaS, APIs, automation, and AI has created an identity ecosystem that is **dynamic, distributed, and continuously changing**.

Identity as the Primary Attack Vector

Attackers are increasingly bypassing traditional defenses by exploiting identities rather than systems.[4]

- 88% of attacks against web applications involve stolen credentials
- **Credential abuse accounts for 22% of breach entry points**, making it one of the most common initial access vectors
- **Credential stuffing accounts for up to 19–25% of authentication traffic in enterprises**, indicating constant attack pressure on identity systems

This results in:

- Attackers using legitimate credentials to bypass defenses
- Difficulty distinguishing malicious activity from normal behavior
- Increased dwell time of attackers within systems

Identity compromise allows attackers to operate undetected within systems.

Fragmented Identity Environments and Lack of Visibility

Most organizations today operate multiple identity systems across:

Many organizations lack unified identity strategy spanning human and non-human identities. At the same time, identity silos continue to persist, driven by rapid cloud adoption and decentralized technology ownership. Which means:

- No single view of all identities (human and non-human)
- Inability to answer "who has access to what" in real time
- Difficulty correlating identity activity across systems
- Blind spots in identity monitoring and threat detection

Fragmentation directly increases risk exposure. Security teams cannot protect what they cannot see.

Weak Lifecycle Management and Manual Processes

Identity lifecycle management (joiner, mover, leaver (JML)), remains one of the most operationally challenging areas.

Despite automation capabilities, many organizations still rely on manual approvals, ticket-based provisioning and delayed deprovisioning.

In an enterprise's environment, this presents as:

- Access provisioning is inconsistent across systems
- Role changes do not trigger entitlement updates
- Access revocation is delayed or incomplete
- Third-party and vendor lifecycle is poorly managed
- Increased overhead

Lifecycle gaps create persistent access risks, especially for dormant or orphaned accounts.

Operational and Security Implications of Identity Complexity

The convergence of **hybrid infrastructure, SaaS proliferation, machine identities, third-party ecosystems and AI-driven automation** has created unprecedented identity complexity, which will lead to:

- Increased operational overhead
- Fragmented ownership of identity functions
- Difficulty enforcing consistent policies
- Gaps between IAM, cloud security, and DevOps teams

Identity is no longer a single function, it spans to: Security, IT operations, Cloud engineering, DevOps and Risk and compliance

Complexity is now one of the biggest drivers of identity risk.

Access Governance Gaps and Entitlement Sprawl

As organizations scale, access privileges tend to accumulate. Employees change roles, projects evolve, and access is rarely revoked with the same rigor as it is granted.

This leads to **entitlement sprawl**; a condition where users retain excessive and often unnecessary access. With reported **challenges in maintaining accurate visibility into user entitlements**, especially in hybrid environments leading to:

- Access reviews becoming a checkbox exercise
- Business owners lack clarity regarding what they are approving
- Excess privileges remaining undetected
- Attackers escalating privileges once inside

Entitlement sprawl significantly increases the blast radius of identity compromise.

Privileged Access Risks

Privileged identities remain one of the most critical and exploited attack surfaces expanding to system administrators, cloud platform admins, database and application owners and privileged service accounts and APIs.

Identity-related incidents involving privileged access continue to be recurring, with attackers increasingly targeting privileged pathways to gain control over systems.

Additionally, 88% of web application attacks involve the use of stolen credentials, many of which include privileged or high-value accounts, highlighting the scale of the issue[5].

In enterprise environments, privileged access is no longer limited to human administrators. It extends to:

This can lead to challenges like:

- Standing privileges instead of dynamic access
- Poor visibility in privileged sessions
- Inconsistent controls across cloud and on-prem environments
- Lack of governance over privileged machine identities

Once privileged access is compromised, attackers gain control over systems, data, and security controls.

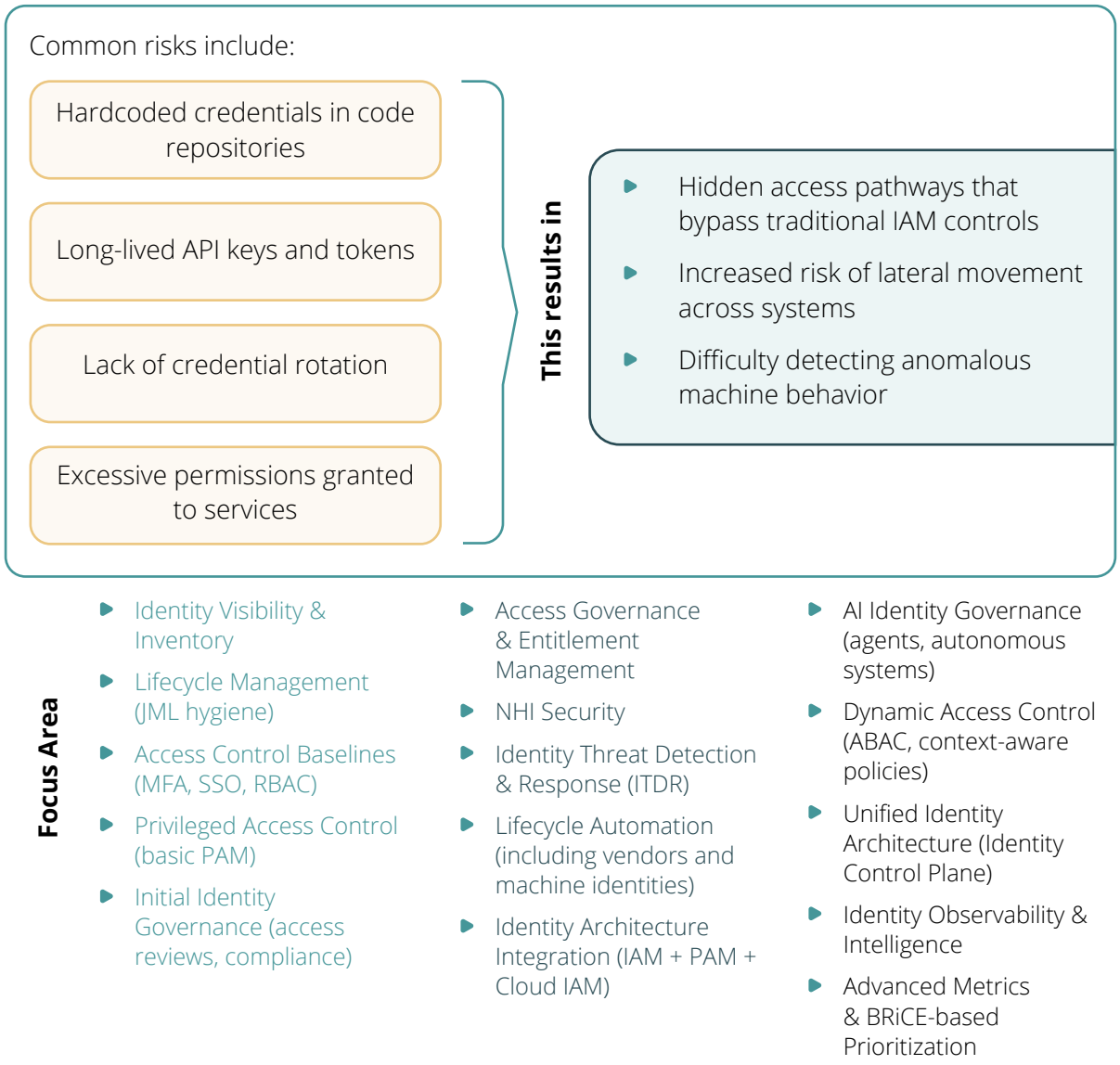
The identity challenges faced today by enterprises are systemic. Fragmentation, entitlement sprawl, privileged access risks, lifecycle inefficiencies, and identity-based attacks are all interconnected outcomes of a rapidly evolving digital ecosystem.

Reimagining Identity Security for the AI Era

Identity, today, includes **autonomous agents, decision-making systems, and dynamic workloads** that interact continuously across enterprise ecosystems. Identity is no longer just about who accesses systems, it is about what systems can do, how they act, and under what authority.

	Characteristics	Control Models
Human Identities *(Employees, contractors, partners/vendors, customers)*	▸ Human-driven actions ▸ Predictable access patterns ▸ Role-based access (RBAC) ▸ Strong lifecycle linkage (HR systems)	▸ Authentication (passwords, MFA) ▸ Role-based authorization ▸ Periodic access reviews
Machine Identities *(API keys and tokens, service accounts, cloud workloads (containers, VMs), DevOps Pipelines, RPA bots)*	▸ Machine-to-machine communication ▸ Continuous operation (24/7) ▸ Often high privilege ▸ Embedded in infrastructure and code	▸ Credential-based access (certificates, tokens) ▸ Secrets management ▸ Privileged access controls
Autonomous/ AI Identities *(AI copilots, autonomous agents, decision-making systems, multi-agent workflows, intelligent automation systems)*	▸ Context-aware decision making ▸ Dynamic and non-deterministic behavior ▸ Interacts across multiple systems ▸ Delegated authority from humans	▸ Contextual and policy based access ▸ Behavioral monitoring ▸ Real-time identity governance ▸ Auditability and traceability

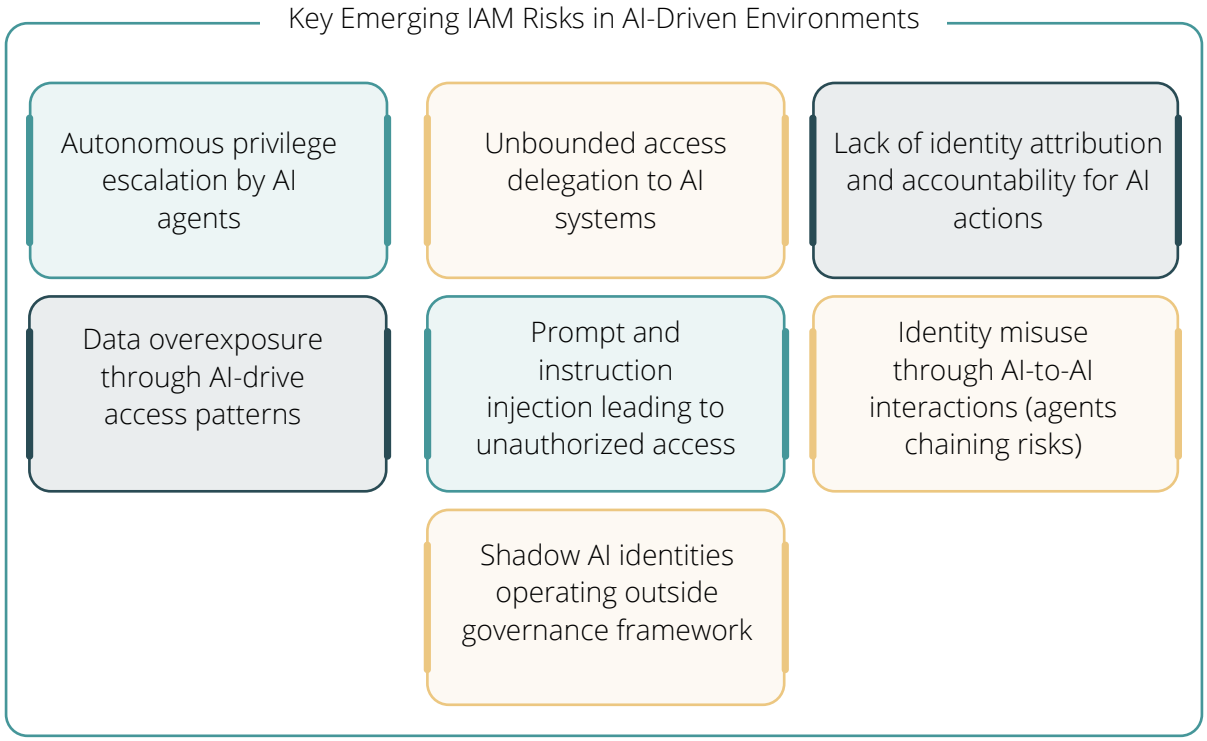
IAM focus areas for Machine and Autonomous Identities



As IAM evolves from user-centric systems to managing human, machine, and AI-driven identities, organizations must realign their focus to ensure secure, policy-driven, and least-privileged access across all identity types. This requires moving beyond static controls toward **continuous verification, adaptive access, and Zero Trust principles**. Key priorities include establishing **centralized discovery and inventory NHIs**, enforcing **short-lived credentials with automated rotation**, and applying **least privilege to machine identities**. Additionally, NHI governance must be tightly integrated into core **IAM and PAM programs** to ensure consistent control, visibility, and accountability across the entire identity ecosystem.

Identity Risks in AI-Driven Environments

The rapid adoption of AI systems and autonomous agents is fundamentally reshaping how identities are created, used, and governed within enterprises. Unlike traditional systems, AI-driven environments introduce identities that can act independently, make decisions, and interact across multiple systems without direct human intervention. This shift expands the identity attack surface in new and less predictable ways, making it critical for organizations to identify and address risks that are **unique to AI-driven identity ecosystems**, particularly where access is dynamic, delegated, and continuously evolving.



The shift from human-controlled access to autonomous and machine-driven interactions introduces new vulnerabilities that traditional IAM models are not equipped to handle. By prioritizing control over AI identities, enforcing least privilege, and ensuring visibility and accountability, organizations can build a resilient identity framework capable of supporting secure AI adoption at scale.

Governance Challenges

Delegation: Expanding Access Without Defined Boundaries

AI systems are increasingly granted access to perform tasks across applications, data systems, and workflows. AI-driven access is:

- Continuous rather than session-based
- Multi-system rather than application-specific
- Context-driven rather than rule-bound

This creates a challenge in defining **how much access is appropriate and under what conditions it should be exercised**.

Accountability: Who Owns AI-Driven Actions?

In traditional IAM, accountability is relatively straightforward where actions can be traced back to a user or system identity. In AI-driven environments, this clarity is significantly reduced.

AI systems may act autonomously based on data inputs, trigger workflows across multiple systems and operate on behalf of multiple users or business functions. This raises fundamental questions:

- Who is responsible for an AI system's actions: the developer, the business owner, or the system itself?
- How are decisions made by AI systems validated and attributed?
- How can organizations investigate incidents involving AI-driven actions?

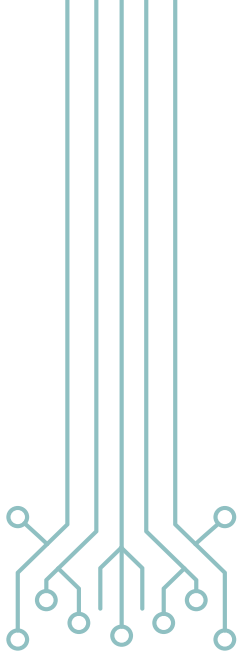
Oversight: Governing Systems That Operate Independently

AI systems can perform thousands of actions across systems in real time, making it impractical to review or validate each action manually. At the same time, the lack of continuous monitoring can allow unintended or risky behavior to go undetected.

Together, these challenges create a governance gap where AI systems can operate with **broad access, limited traceability, and insufficient supervision**.

Addressing these governance challenges in AI-driven environments requires a structured understanding of identity security maturity. As identities expand across human, machine, and autonomous systems, organizations need a consistent way to assess how effectively they manage delegation, accountability, and oversight across this spectrum, mapping identity capabilities across defined domains and stages, enabling organizations to benchmark their current state and systematically evolve toward a more integrated, policy-driven, and continuously governed identity ecosystem.

Strategic Identity Capability Areas for Modern Enterprises



To enable the organizations to move from **control-centric thinking to capability-centric execution**, where identity is managed as an integrated system rather than a collection of independent components – the twelve domains are consolidated into five thematic capability areas with an aim to:

- Aligning identity capabilities with how organizations operate across foundations, access, governance, operations, and emerging technologies
- Enable prioritized investment and decision making, rather than fragmented tool adoption
- Prepare organizations for a future where identity is not static, but dynamic, autonomous, and deeply embedded in digital infrastructure

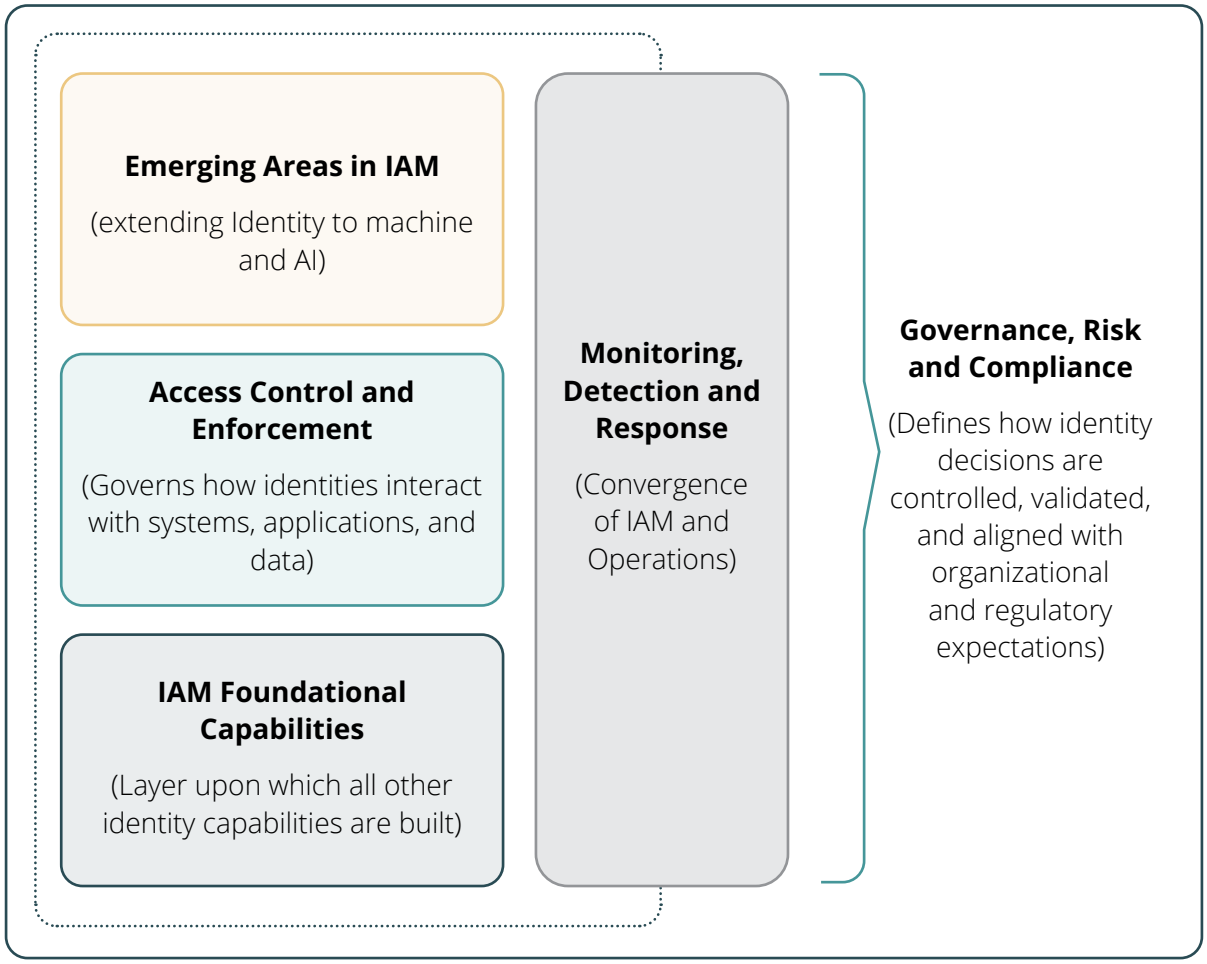
By consolidating these domains into thematic capabilities, organizations gain a **system-level view of identity**, allowing them to: understand dependencies between controls, identify gaps that exist between domains and design identity architectures that are cohesive and future-ready.

IAM Foundational Capabilities

Identity Asset Inventory and Discovery	Identity Proofing and Verification	Identity Lifecycle Management

This layer answers three fundamental questions:

- What identities exist?
- Are they trusted?
- How are they managed over time?



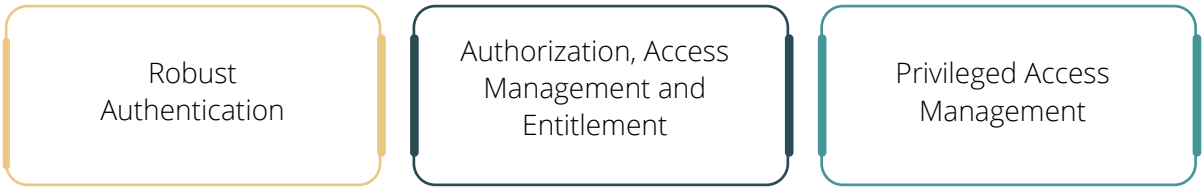
The gaps in identity foundations create systemic risks including unmanaged identities, orphaned accounts, and inconsistent access control.

From a forward-looking perspective, Identity Foundations must evolve toward:

- Continuous identity discovery across human and non-human identities
- Integrated proofing mechanisms combining identity, device, and behavioral signals
- Dynamic lifecycle management driven by events rather than static workflows

As organizations adopt AI and automation, identity foundations will increasingly need to support **ephemeral identities** (created and destroyed dynamically) making real-time lifecycle orchestration a critical capability.

Access Control and Enforcement



While traditionally focused on enforcing access policies, this layer is undergoing significant transformation. Static models such as role-based access control are giving way to **dynamic, context-aware access mechanisms**, driven by identity, device, behavior, and risk signals.

The major challenges in access and control is to ensure that access is:

- Appropriate (least privilege)
- Contextual (based on real-time conditions)
- Adaptive (responsive to risk)

Looking ahead, access control will be:

- Continuous rather than point-in-time
- Behavior-driven rather than rule-based
- Autonomous in enforcement, with human oversight

This becomes highly relevant in environments with high volumes of machine and AI-driven interactions, where access decisions must be made at scale and speed beyond human intervention.

Governance, Risk and Compliance

In traditional environments, governance has been compliance-driven focused on audits, certifications, and policy enforcement. However, as identity ecosystems become more dynamic, governance must evolve into a **continuous trust model**, where access is not assumed but verified at every interaction. The integration of Zero Trust principles into identity governance reflects this shift. Trust is no longer binary; it is **continuously evaluated based on context, behavior, and risk**.

For organizations, this means:

- Moving from periodic access reviews to continuous governance
- Embedding policy enforcement into runtime identity decisions
- Aligning identity governance with enterprise risk and fraud frameworks

Governance has already extended beyond human users to include machine identities with delegated authority and AI agents making autonomous decisions. This requires a redefinition of trust that is **measurable, adaptive, and enforceable across all identity types**.

Monitoring, Detection and Response

Identity Threat Detection and Analytics

Identity Incident Response

Until now, IAM and security operations have functioned independently. However, modern threats like credential theft, token abuse, API exploitation operate through identity pathways, making this separation ineffective.

Organizations must now treat identity as:

- A **source of telemetry**
- A **signal for threat detection**
- A **control point for response**

This requires:

- Integration of identity data into SIEM/XDR platforms
- Behavioral analytics to detect anomalies
- Automated response mechanisms to contain identity-based threats

Emerging Areas in IAM

NHI Hygiene

AI Agents

- AI driven systems have accelerated the number of emerging identities in an enterprise. These identities are: Highly dynamic and ephemeral, created and retired continuously
- Distributed across hybrid and multi-cloud environments
- Interconnected through APIs and automated workflows
- Capable of autonomous or semi-autonomous actions

Implications of Emerging Identities on IAM:

- **Shift from Human-Centric to Identity-Centric IAM**

- **Massive Increase in Identity Scale and Complexity** significantly expands the identity attack surface, making manual governance unsustainable.
- **Need for Continuous and Real-Time Identity Governance** where identities and permissions change continuously.
- **Greater Dependence on Automation** for managing machine-speed operations securely.
- **Growing Importance of Identity Intelligence** like behavioral analytics, anomaly detection, and adaptive access controls to detect evolving identity threats.
- **Emergence of AI Governance Challenges** related to autonomous actions, delegated authority, accountability, and traceability, requiring entirely new governance models.

These identity domains will become central to identity strategy. Organizations that fail to govern NHIs and AI agents effectively will face increasing risks related to unauthorized access, data exposure and autonomous misuse of privileges.

Each capability evolves across the five maturity stages, but maturity is not uniform across domains. An organization may have advanced authentication but weak lifecycle management or strong governance but limited NHI visibility. This uneven maturity creates gaps that attackers can exploit.

Understanding the **interdependencies across domains** is therefore critical:

- Identity Foundations enable effective Access Control
- Access Control feeds Governance and Trust
- Governance informs Security Operations
- Security Operations provide feedback into all layers
- Emerging Domains intersect across all capabilities

This interconnected model highlights a key principle: Identity maturity is not achieved by optimizing individual domains, but by aligning capabilities across the entire identity lifecycle.

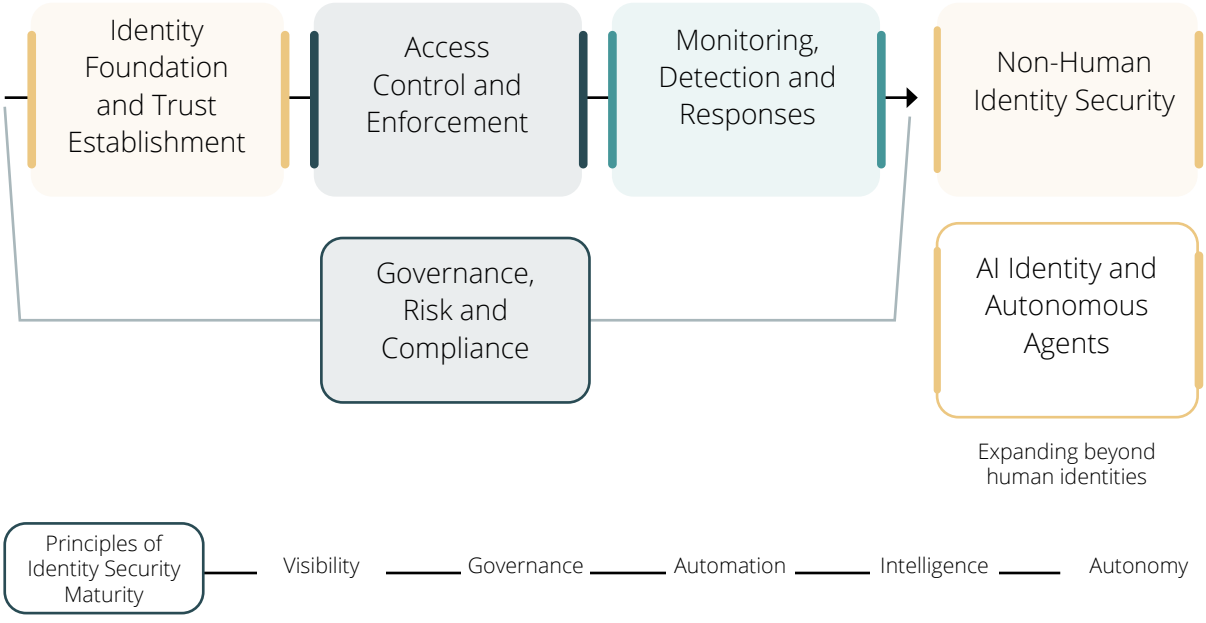
The Identity Security Maturity Model

Evaluating identity maturity becomes critical to understanding how effectively an organization can enforce least privilege, ensure accountability, and respond to evolving threats. A structured maturity assessment enables enterprises to identify gaps across identity lifecycle, access governance, and security operations, prioritize investments, and transition from reactive identity management to a **consistent, risk-aligned, and scalable identity security posture**.

An identity maturity framework enables organizations to:

- Assess their current identity capabilities across domains
- Identify gaps in visibility, governance and control
- Prioritize investments based on risk and operational impact
- Progress towards a unified, scalable, and adaptive identity architecture

Phases of Identity Access Management



Identity Maturity Model Grid

At the core of the Identity Security framework is a **12-domain maturity model**, where each domain evolves across the five maturity stages.

This grid enables organizations to:

- Evaluate maturity at a **domain level**, rather than relying on a single aggregate score
- Identify **specific capability gaps** (e.g., strong authentication but weak NHI governance)
- Prioritize improvements based on **risk exposure and business impact**
- Track progress as identity capabilities evolve over time

The model is designed to be adaptable. While the core structure remains consistent, organizations can contextualize it based on industry, regulatory environment, and operational complexity ensuring relevance across diverse enterprise environments.

IAM Phases	Categories	Objective	Criticality
IAM Foundational Capabilities	Identity Inventory & Asset Management	Establish a complete and unified view of all identities across systems (human, machine, AI)	Without visibility, identities remain unmanaged, creating blind spots and uncontrolled access across environments
	Identity Proofing	Ensure identities are verified and trustworthy at onboarding using strong validation mechanisms	Weak proofing leads to fraudulent or duplicate identities, especially critical in large-scale digital onboarding ecosystems
	Identity Lifecycle Management	Govern identity creation, modification, and deprovisioning throughout its lifecycle	Poor lifecycle controls result in orphaned accounts and unauthorized persistent access—one of the most common IAM failures
Access Control and Enforcement	Authorization, Access Management & Entitlements	Ensure identities have appropriate, least privilege access aligned to roles and business needs	Over-provisioned access is a primary enabler of lateral movement, insider threats, and data exposure
	Robust Authentication	Validate identity at access using secure and multi-factor authentication mechanisms	Authentication is the first control layer; weak methods (e.g., OTP-only) are increasingly exploited in identity-based attacks

IAM Phases	Categories	Objective	Criticality
Access Control and Enforcement	Privileged Access Management (PAM)	Control, monitor, and restrict access to critical systems and high-risk privileged accounts	Privileged identities are high-value targets; compromise can lead to full system or data control
Governance, Risk and Compliance	Identity Governance & Compliance	Enforce access policies, enable audits, and align identity practices with regulatory requirements	Ensures accountability and compliance, especially critical in multi-regulator environments (e.g., RBI, SEBI, DPDPA)
	Zero Trust Implementation	Continuously verify identity, device, and context before granting access	Traditional perimeter-based trust models fail in distributed environments; Zero Trust ensures adaptive and secure access decisions
Monitoring, Detection and Response	Identity Threat Detection & Analytics	Detect anomalous identity behavior, misuse, and potential threats in real time	Identity is the primary attack vector; without detection, breaches remain unnoticed until significant impact occurs
	Identity Incident Response	Enable timely and structured response to identity-related security incidents	Rapid containment of identity threats reduces financial loss, fraud impact, and operational disruption
Emerging Areas in IAM	NHI Hygiene	Discover, manage, and secure machine identities such as APIs, service accounts, and tokens	NHIs outnumber human identities and often lack governance, making them a major and growing attack surface
	AI Agents	Govern AI-driven identities, control delegated access, and ensure accountability of autonomous actions	AI systems introduce new risks (autonomous decisions, lack of traceability); maturity requires extending IAM to agentic systems

Identity maturity is not an abstract concept, it has a direct and measurable impact on an organization's risk posture, operational efficiency, and compliance readiness.

As identity maturity increases, exposure to identity-based attacks reduces, privileged access risks are minimized, unauthorized access and lateral movement are constrained, and detection and response capabilities improve significantly.

Maturity Levels and Progression Framework – Identity Security Maturity Matrix

The Identity Security Maturity Matrix enables organizations to understand the **evolution of identity capabilities across five distinct stages of maturity**.

It is essential to provide a progression view, helping organizations benchmark their current state, identify gaps across key identity domains, and align their efforts toward achieving a more scalable and resilient identity framework. It also incorporates India-specific considerations such as DPI, multi-regulatory requirements, and high-volume digital adoption, ensuring relevance for enterprises operating in the Indian context.

Category	Ad-hoc → Foundational visibility → Repeatable process → Automation and assurance → Autonomous identity				
	Initial	Developing	Defined	Managed	Optimized
Identity Inventory and Asset Management	Fragmented identity stores no visibility into DPI-linked identities (Aadhaar, UPI)	Partial inventory of workforce identities limited vendor visibility	Inventory includes workforce, customer, vendor, and UPI-linked identities manual mapping	Automated discovery across cloud, SaaS, on-prem, DPI Identity mapped to risk	Continuous discovery across human, NHI, AI Real-time risk classification integrated with fraud and DPI ecosystem
Identity Proofing	Basic onboarding; minimal verification	Aadhaar OTP / basic KYC; inconsistent workforce proofing	Multi-factor proofing (Aadhaar, PAN, mobile); V-CIP adoption	Integrated proofing via DigiLocker, CKYC; fraud checks embedded	AI-based validation; deepfake detection; continuous behavioral re-verification
Identity Lifecycle Management	Manual JML; delayed deprovisioning	HR-driven onboarding; limited automation	Integrated lifecycle (HR + vendor systems); partial automation	Automated lifecycle for workforce, vendors, NHIs; time-bound access	Policy-driven lifecycle for AI agents; dynamic workforce; event-based provisioning
Robust Authentication	Password / OTP-based authentication	MFA for critical users; OTP-heavy usage	Strong MFA (device, biometric, OTP); SSO	Risk-based authentication (device, location, behavior)	Passwordless; continuous authentication; fraud-aware authentication (UPI context)
Identity Governance and Compliance	Audit-driven IAM	Basic governance aligned to RBI/SEBI	Governance mapped to RBI, SEBI, IRDAI, DPDPA; periodic audits	Continuous compliance monitoring; integrated risk + fraud + IAM	Regulatory matrix view (horizontal + vertical); automated compliance enforcement
Authorization, Access Management and Entitlements	Broad access; shared accounts	Basic RBAC; manual approvals	Controlled access; periodic reviews	Context-aware access; entitlement usage monitoring	JIT, least privilege; fine-grained access; dynamic authorization for AI
Privileged Access Management (PAM)	Shared admin credentials	Basic vaulting; session tracking	PAM for critical systems; audit trails	JIT privileged access; segregation of duties	AI-driven privilege risk analysis; monitoring across cloud, DevOps, NHIs
Zero Trust Implementation	Implicit trust	Limited Zero Trust adoption	Zero Trust for critical systems	Context-aware access across environments	Full Zero Trust: micro segmentation, continuous validation, DPI-linked trust signals

Category	Ad-hoc → Foundational visibility → Repeatable process → Automation and assurance → Autonomous identity				
	Initial	Developing	Defined	Managed	Optimized
Identity Threat Detection and Analytics	Minimal logging	Basic monitoring	Correlation of identity events	Behavioral analytics; integration with fraud detection	AI-driven analytics; integration with UPI fraud systems and national threat intelligence
Identity Incident Response	Reactive response	Basic IR plans	Identity-specific IR workflows	Automated response (access revocation, lockdown)	Near real-time response; integrated with fraud systems and regulatory reporting
Non-Human Identity (NHI) Hygiene	No visibility into NHIs	Inventory of critical NHIs	Credential rotation policies	Automated rotation; monitoring API/ service access	Continuous monitoring; toxic combination detection; secure DPI API management
AI Agents	Shadow AI usage; no governance	Inventory of AI tools; basic controls	Controlled AI access; monitoring third-party AI	Governance for procured and built AI; delegation controls	AI identity governance; lifecycle management; behavioral monitoring; human-on-the-loop oversight

The framework defines five stages of identity maturity, representing the evolution of identity capabilities from basic to advanced.

Organizations at higher maturity levels are better equipped to manage modern threats, particularly those targeting credentials, tokens, APIs, and machine identities.

Operationalizing Identity Strategy and Maturity at Scale

Having assessed identity maturity across domains and stages, the critical next step for organizations is to translate these insights into **actionable transformation initiatives**. Identity maturity, in practice, is not achieved through isolated improvements but through **phased, prioritized progression across capabilities**.

The maturity model provides a structured pathway, from **ad-hoc identity environments to autonomous, intelligence-driven identity systems**. However, for Indian enterprises, this progression must be contextualized against:

- Highly **fragmented identity environments** (core banking, legacy ERPs, SaaS, APIs)
- **Scale of identities** driven by digital platforms (customers, partners, NHIs)
- Increasing reliance on **outsourced vendors and third-party ecosystems**
- Rapid adoption of **AI and automation in business workflows**

Operationalizing identity maturity, therefore, requires a **pragmatic and staged approach** while balancing immediate risk reduction with long-term architectural transformation.

Advancing Through Maturity Stages: India-Specific Execution Path

I. Initial → Developing

At early stages, Indian enterprises often operate with:

- Disparate identity stores across core systems and digital platforms
- Limited visibility into non-human identities and API access
- Manual onboarding and offboarding processes

Priority Actions:

- Establish a **centralized inventory of identities** across:
  - Workforce, vendors, partners
  - Applications, APIs, and service accounts
- Integrate identity data from:
  - HR systems

    - Vendor onboarding platforms
    - Core business systems
- Define **ownership of identity policies** (who approves, enforces, governs)
- Embed identity-centric scenarios into **incident response planning**

Quick Wins:

- Enforce MFA for:
    - Privileged users
    - High-risk service accounts
- Standardize identity proofing across onboarding channels
- Centralize identity logs for audit and monitoring

Common Pitfalls:

- Over-reliance on spreadsheets and manual tracking
- Ignoring machine identities and API access
- Continued dependence on OTP-only authentication

II. Developing → Defined

At this stage, organizations begin transitioning from visibility to **process consistency**.

Priority Actions:

- Automate identity discovery across systems
- Implement **consistent lifecycle management**:
    - Timely provisioning and deprovisioning
    - Elimination of residual access
- Conduct periodic access reviews for:
    - Privileged users
    - Critical systems
- Strengthen control over:
    - External/vendor identities
    - Third-party system access

Quick Wins:

- Track "**time to deprovision**" as a key KPI
- Monitor and eliminate orphaned accounts
- Strengthen authentication for executive and high-risk roles

Common Pitfalls:

- Deploying point solutions without integration
- Assuming initial integration solves identity fragmentation

III. Defined → Managed

As identity processes mature, the focus shifts toward **automation and continuous assurance.**

Priority Actions:

- Integrate HR and vendor systems with identity platforms for **automated lifecycle management**
- Enforce **MFA everywhere and SSO everywhere**, especially across SaaS and internal applications
- Conduct **automated access certification campaigns**
- Enable **identity behavior analytics** for anomaly detection

Quick Wins:

- Standardize identity proofing mechanisms across systems
- Identify and disable dormant accounts
- Monitor deviations from defined identity policies

Common Pitfalls:

- Conducting access reviews without business or entitlement context
- Lack of continuous monitoring, leading to regression in maturity

IV. Managed → Optimized

At advanced stages, identity systems evolve into **adaptive, intelligence-driven ecosystems.**

Priority Actions:

- Implement c**ontinuous identity discovery and classification** across all identity types
- Enable Just-In-Time (JIT) and just-enough access
- Automate enforcement of identity policies across environments
- Deploy **AI-driven systems** to recommend and enforce policy changes
- Integrate identity signals with:
  - Threat intelligence
  - Behavioral analytics

Quick Wins:

- Pilot passwordless authentication for critical users
- Use AI-driven insights to reduce excessive entitlements

Common Pitfalls:

- Treating AI agents as generic service accounts
- Ignoring risks from AI-generated identities

This stage represents the shift toward **human-on-the-loop identity governance**, where systems operate autonomously to an extent within defined guardrails.

Prioritizing Identity Investments: The BRiCE Framework

Operationalizing identity maturity requires **strategic prioritization**, as organizations cannot address all domains simultaneously.

The BRiCE framework provides a structured approach to evaluate identity initiatives across four dimensions:

Business Value → Alignment with business goals and digital initiatives

Risk Impact → Reduction in identity-related threats

Cost → Implementation and operational investment

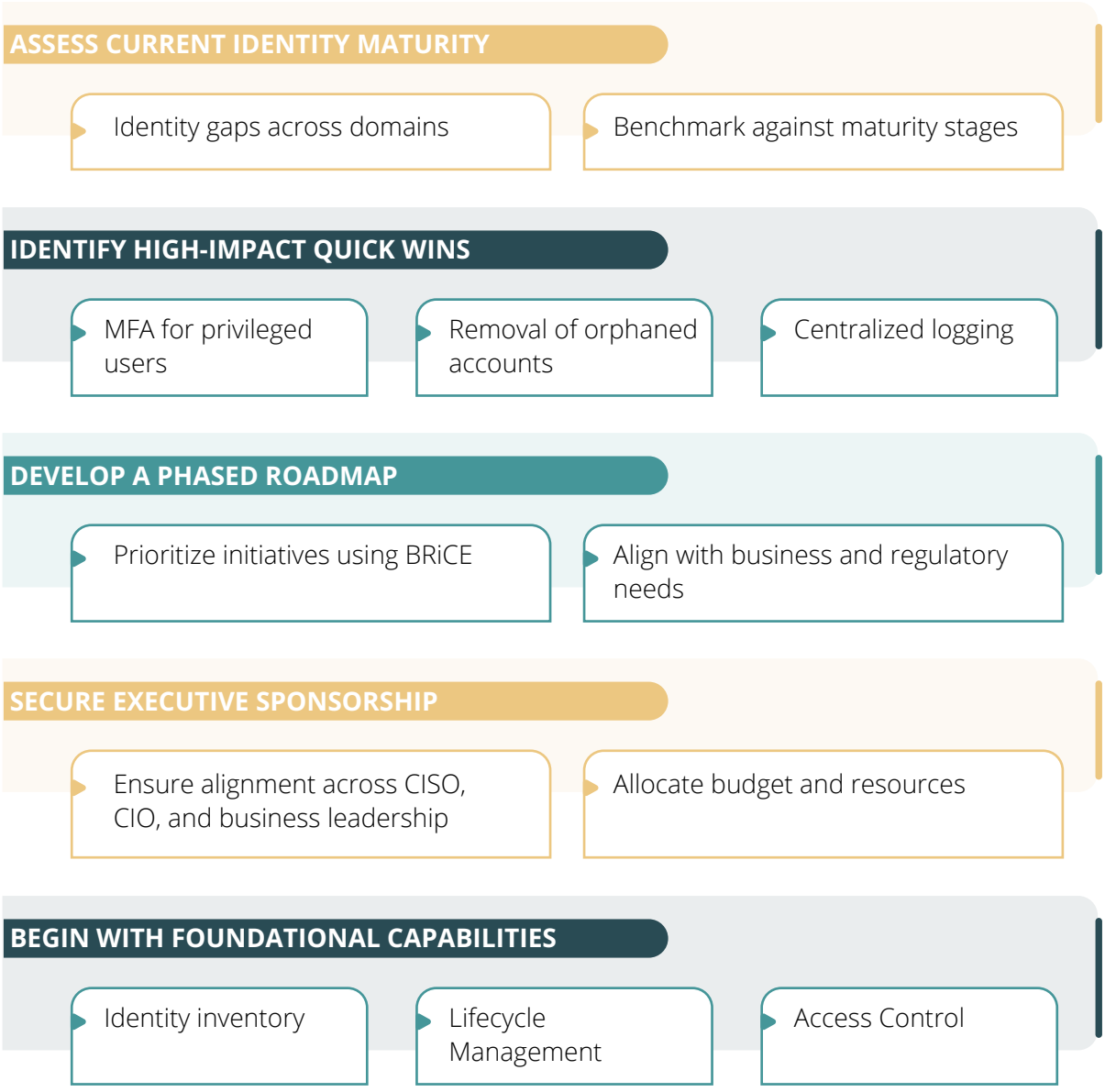
Effectiveness → Expected improvement in identity maturity

Organizations should compute a composite score:

BRiCE Score = [(Business Value × Risk Impact) / Cost] × Effectiveness

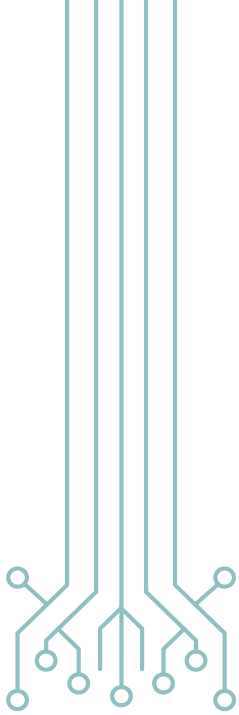
Higher BRiCE scores indicate initiatives that deliver stronger business value and risk reduction relative to implementation cost, while also contributing significantly to identity maturity. Organizations can use the score to comparatively prioritize IAM initiatives, enabling CISOs and leadership teams to focus first on investments that provide the greatest strategic and security impact.

Operationalizing identity maturity begins with **focused, actionable steps**:



Identity maturity is not a fixed destination but a **continuous journey of evolution**. Identity is the foundation of trust, resilience, and digital innovation.

The Future of Identity Access Management: Autonomous, Intelligent, and Trust-Driven



The future of identity security will be defined by how effectively organizations can manage **scale, autonomy, and intelligence** across a diverse and expanding identity landscape.

Identity as Digital Infrastructure

Identity will become as foundational as networks, compute, and data. It will function as the underlying trust fabric that enables secure interactions across increasingly distributed and interconnected environments.

Identity must be designed as a persistent and interoperable layer across systems, a real-time control plane for enforcing trust decisions and a shared infrastructure that supports internal operations and external ecosystems.

Autonomous Identity Management

Given the scale and velocity of modern identity interactions, it is essential to focus on **autonomous identity systems** that can manage identity lifecycle, access, and risk.

However, autonomy introduces a new strategic requirement: **trust in the system itself**. Organizations must ensure that autonomous identity systems operate within clearly defined guardrails, with transparency, auditability, and human oversight.

The future operating model will evolve towards: Human-on-the-loop governance, where systems execute at scale and humans define intent and boundaries.

AI-Driven Identity Governance

AI will not only consume identity systems, but it will redefine how identity governance is executed.

Static policies → **Dynamic, context-aware policy frameworks**

Periodic reviews → **Continuous access validation**

Manual analysis → **Predictive and prescriptive decision-making**

The future of governance will not be about controlling access statically, but about **orchestrating trust dynamically across systems, identities, and decisions**.

Identity Intelligence and Behavioral Security

As identity becomes the primary attack surface, the ability to understand identity behavior in real time will define the effectiveness of security programs.

Identity intelligence will evolve into a **core decision-making engine**, integrating **behavioral analytics, risk scoring, threat intelligence and contextual signals across devices, networks and applications**. This enables a shift from:

Authentication as a one-time event → **Continuous identity validation**

Rule-based controls → **Behavior-driven enforcement**

In the future, identity system will not just verify who a user is, it will continuously assess whether the behavior aligns with expected patterns and when access should persist, be restricted, or revoked. Hence, it becomes important to balance when to leverage intelligence for precision and speed, as well as, avoiding over-dependence on signals that may create noise or false positives. Organizations that successfully operationalize identity intelligence will move toward **predictive identity security**, where risks are mitigated before they materialize.

Human-Machine Identity Continuum

The distinction between human and machine identities is rapidly dissolving. Enterprises are moving toward unified identity ecosystems, where humans initiate actions, machines execute processes and AI agents make decisions. Therefore, it becomes essential to:

- Treat all identities as first-class entities within IAM
- Apply consistent governance across identity types
- Establish clear ownership and accountability, even for autonomous systems

This convergence will require organizations to rethink identity not as a user-centric model, but as a **system-wide trust model spanning all actors**.

Building a Resilient Identity Ecosystem

Resilience will be the defining characteristic of future identity systems. As identity becomes central to both security and operations, any failure in identity can have **system-wide impacts**. A resilient identity ecosystem must be – Adaptive, Scalable, Integrated, Intelligent, and autonomous.

Foundations of a Resilient Identity Ecosystem

Autonomous

Independent operation within defined policy boundaries.

Adaptive

The ability to respond to evolving threats in real time.

Intelligent

Data-driven operations and continuous learning.

Integrated

Seamless connectivity across identity, security, and business systems.

Scalable

The capacity to support growth in exponential identities and transactions.

Ultimately, resilience is not just about preventing failure, it is about ensuring that identity systems can **support continuous innovation without compromising trust**.

The future of identity security is not an extension of current IAM practices, it is a **re-architecture of how trust is established, enforced, and evolved** in digital systems.

In this emerging paradigm, identity is no longer a checkpoint, it is the **continuous, adaptive fabric that enables secure and scalable digital enterprises**.

Reference

[1] Passwords Alone Are Not Enough to Mitigate Credential Harvesting Risks, Gartner

[2] Managing Identity in the Age of AI – A practitioner's guide to the future of identity, Oleria and SINET

[3] Managing Identity in the Age of AI – A practitioner's guide to the future of identity, Oleria and SINET

[4] Verizon DBIR 2025: Credentials Are Still #1 Threat

[5] Verizon DBIR 2025: Credentials Are Still #1 Threat

Authors

Jagadeesh Kunda
Co-founder & COO, Oleria

Didier Vandenbroeck
Vice President Security & IT, Oleria

Abhishek Singh
Senior Product Manager, Oleria

Neha Mishra
Lead – Research and Insights, DSCI

Anuprita Singh
Senior Associate – Research, DSCI

Editor

Jahnab Bharadwaj
Senior Associate – Marketing and Communications, DSCI

Data Security Council of India (DSCI) is a not-for-profit, think tank on data protection, cyber security and critical technologies in India, setup by Nasscom, committed towards making the cyberspace safe, secure and trusted by establishing best practices, standards and initiatives in cyber security and privacy. DSCI works together with the Government, law enforcement agencies, defense, industry sectors including IT-BPM, BFSI, CII, Telecom, and other think tanks for public advocacy, thought leadership, capacity building and outreach initiatives.

Oleria is an AI-native identity security and governance platform that continuously governs and enforces access across human, non-human, and AI identities. As enterprises sprawl across cloud, SaaS, and on-prem systems, legacy IGA stitches point tools into stale snapshots that miss hidden access risk.

Oleria takes a different approach: a single AI-native access graph, built across hundreds of integrations with MCP-enabled connectors that let AI agents reason over live access data.

It unifies posture management, governance, and incident response in one platform, reaching full identity visibility in under an hour, eliminating over-privileged access, and governing AI agents, all at far lower TCO than legacy IGA.

For more information, please visit: www.oleria.com

DATA SECURITY COUNCIL OF INDIA
Nasscom Campus, Fourth Floor, Plot. No. 7-10, Sector 126, Noida, UP - 201303
+91-120-4990253 | info@dsci.in | www.dsci.in

DSCI_Connect dsci.connect dsci.connect data-security-council-of-india dscivideo