THE BEGINNER'S GUIDE TO IDENTITY AND ACCESS MANAGEMENT

What Every CIO and CISO Needs to Know About Identity Security

INTRAGEN.
by nomios

Contents

EXECUTIVE SUMMARY 1

WHY IDENTITY IS NOW A STRATEGIC PRIORITY 2

AI IS CHANGING THE IDENTITY EQUATION 2

WHAT IAM ACTUALLY IS 3

THE IDENTITY SECURITY LANDSCAPE EXPLAINED 3

IDENTITY GOVERNANCE AND ADMINISTRATION (IGA) *4*

ACCESS MANAGEMENT (AM) *4*

PRIVILEGED ACCESS MANAGEMENT (PAM) *4*

IDENTITY SECURITY POSTURE MANAGEMENT (ISPM) *4*

NON-HUMAN IDENTITIES (NHI) *5*

CUSTOMER IDENTITY AND ACCESS MANAGEMENT (CIAM) *5*

A PRACTICAL EXAMPLE: WHAT GOOD LOOKS LIKE 6

THE FOUR-STEP IDENTITY MODEL 6

WHERE MOST IAM PROGRAMMES STALL 7

TURNING IDENTITY RISK INTO BUSINESS VALUE 7

IDENTITY SECURITY AS A MANAGED BUSINESS CAPABILITY 8

WHAT TO DO NEXT 8

EXPLORE YOUR IDENTITY SECURITY MATURITY 9

EXECUTIVE SUMMARY

Identity now sits firmly within the remit of the CIO and CISO.

Cloud adoption, hybrid work, regulatory scrutiny, the rapid growth of machine identities and the emergence of enterprise AI have made access control one of the most critical operational disciplines in the organisation.

AI systems are now:
- Accessing enterprise data
- Generating decisions
- Acting autonomously within workflows
- Integrating through APIs across core platforms

Yet in many organisations, AI activity is not governed with the same discipline applied to human users. This creates a new identity challenge:

Who is accountable for what AI can access, what it can do, and how its activity is monitored?

At the same time, Identity and Access Management remains:
- Fragmented
- Tool-driven
- Reactive
- Poorly understood outside IT

This guide provides a practical introduction to Identity and Access Management in plain language.

You will learn:
- What IAM actually covers
- How AI and Non-Human Identities change the access landscape
- How the major identity components fit together
- Where governance gaps typically emerge
- What good looks like when Identity Security is run as a managed business capability

IAM is not just about login screens and passwords. It is the control layer for human, machine and AI-driven access across the enterprise.

WHY IDENTITY IS NOW A STRATEGIC PRIORITY

Every organisation is expanding digitally.

New cloud platforms. Remote employees. Third-party collaboration. Automation and service accounts. Customer portals and digital products. Every one of these depends on identity.

The question is no longer: "Do people have accounts?"

The question is:
- Who has access to what?
- Why do they have it?
- How long should they keep it?
- Can we prove it?

When identity is unmanaged or fragmented, organisations experience:
- Slow onboarding and offboarding
- Audit friction
- Over-privileged access
- Limited visibility into machine credentials
- Unclear ownership of identity risk

Identity Security brings structure, visibility and accountability to this landscape.

AI IS CHANGING THE IDENTITY EQUATION

AI is no longer experimental in many enterprises, it is embedded in:
- Productivity platforms
- Customer service workflows
- Security tooling
- Software development pipelines
- Data analytics platforms

AI systems do not simply "read" data they:
- Retrieve information across multiple systems
- Execute actions through APIs
- Generate content and decisions
- Trigger downstream workflows

Each of these actions requires identity and access. The governance challenge is not whether AI is secure, it is whether AI access is:
- Deliberate
- Scoped
- Monitored
- Auditable

Without structured Identity Security:
- AI systems may inherit excessive privileges
- Service accounts may expand without visibility
- API access may persist without lifecycle control
- Accountability for AI-driven actions may become unclear

AI amplifies whatever access model already exists. If governance is strong, AI operates within guardrails. If governance is weak, AI accelerates inconsistency.

Identity Security is therefore the foundation for responsible AI adoption.

WHAT IAM ACTUALLY IS

Identity and Access Management can be summarised in one sentence:

Right people. Right access. Right time. Right reason.

But that sentence carries significant operational weight. Identity is more than a username.

An identity can be:
- A person - employee, contractor, partner, customer
- A role or function - such as “Project Manager in Finance”
- A system or machine - service accounts, bots, scripts, APIs

In modern organisations, Non-Human Identities often outnumber human ones by a significant margin.

Access is more than login.

Access includes:
- Applications you can open
- Files you can read or edit
- Permissions inside systems
- Privileged actions on infrastructure
- Machine-to-machine credentials

The more powerful the access, the more important it is to control and record it.

IAM is the discipline that ensures access is deliberate, traceable and aligned to business purpose.

THE IDENTITY SECURITY LANDSCAPE EXPLAINED

IAM is not one product. It is a landscape of capabilities, each solving a distinct problem.

Understanding this landscape helps executives ask better questions and avoid fragmented investments.

IDENTITY GOVERNANCE AND ADMINISTRATION (IGA)

Business question: Who should have what access, and can we prove it?

IGA provides:
- Joiner, mover and leaver automation
- Role modelling and birthright access
- Access request and approval workflows
- Access certifications and recertifications
- Segregation of duties controls
- Complete audit trails

Identity Governance and Administration ensures access decisions are intentional, documented and defensible.

It transforms access from a ticketing process into a governed lifecycle.

ACCESS MANAGEMENT (AM)

Business question: Are you really who you say you are?

AM handles:
- Single sign-on
- Multi-factor authentication
- Adaptive access policies
- App integrations
- Workforce lifecycle synchronisation

Access Management connects people securely to applications while balancing security and user experience.

PRIVILEGED ACCESS MANAGEMENT (PAM)

Business question: Who controls the most powerful accounts?

PAM governs:
- Administrative accounts
- Vaulted credentials
- Just-in-time elevation
- Session monitoring and recording
- Break-glass procedures

Privileged accounts concentrate operational and regulatory risk. Privileged Access Management ensures that high-impact access is tightly controlled and auditable.

IDENTITY SECURITY POSTURE MANAGEMENT (ISPM)

Business question: Where are the gaps across the whole identity landscape?

ISPM provides:
- Cross-system visibility
- Risk scoring
- Toxic combination detection
- Stale and orphaned account discovery
- Continuous posture monitoring

Identity Security Posture Management gives leadership a consolidated view of identity risk rather than isolated system snapshots.

NON-HUMAN IDENTITIES (NHI)

Business question: What about the machines?

Non-Human Identities include:
- Service accounts
- API keys
- Secrets in code
- CI and CD pipeline credentials
- Cloud workload identities

These identities are often unmanaged and over-privileged.

Governance of Non-Human Identities is now a strategic priority as automation and AI adoption accelerate.

AI agents, automation scripts and machine-learning workflows operate through service accounts, APIs and delegated permissions. These identities often outnumber human users and can accumulate broad access if not actively governed.

Identity Security must extend equally to human users, machine identities and AI-driven processes.

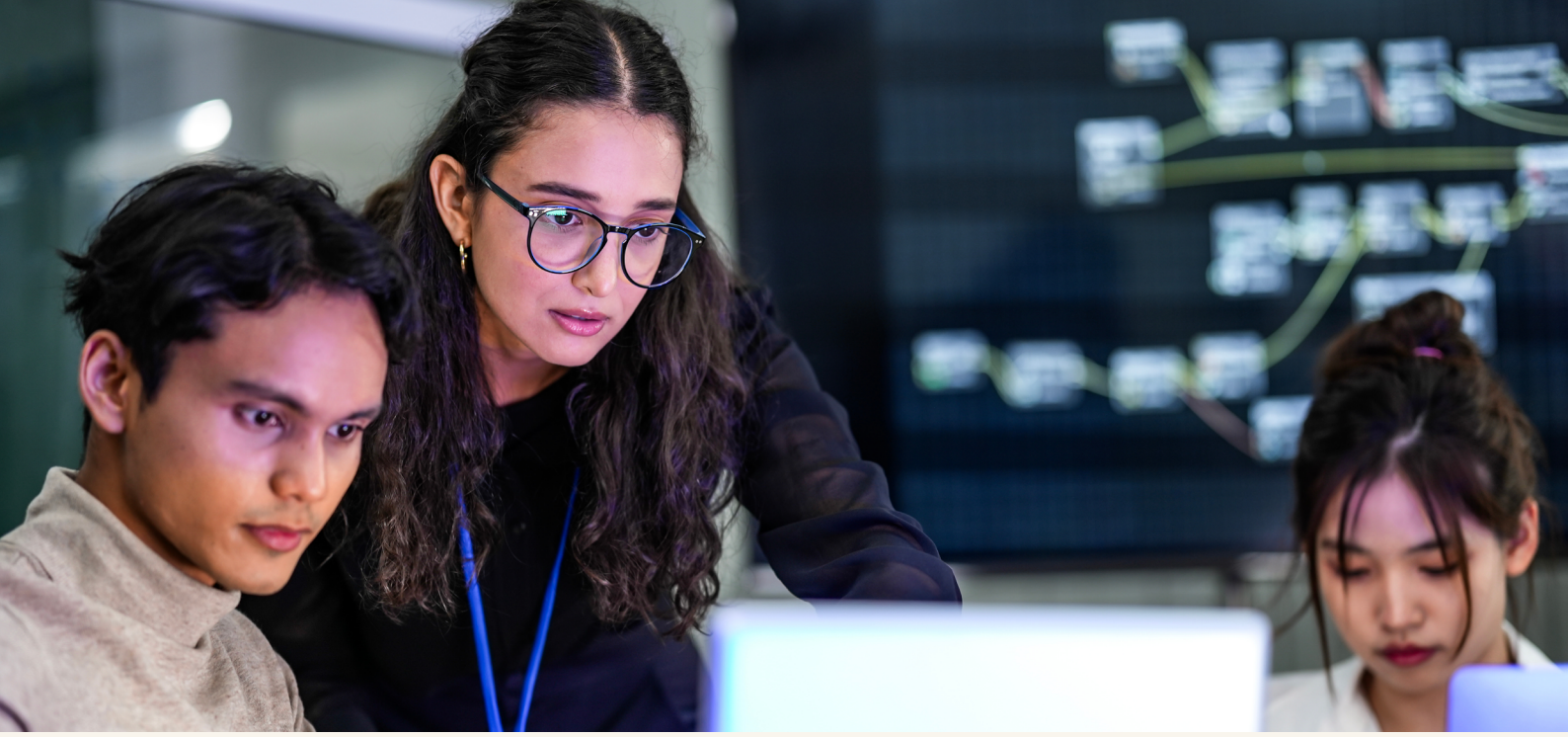
CUSTOMER IDENTITY AND ACCESS MANAGEMENT (CIAM)

Business question: How do we securely onboard and authenticate customers at scale?

CIAM focuses on:
- Self-service registration
- Social login
- Passwordless authentication
- Consent management
- High-scale performance

Workforce identity tolerates friction. Customers do not.

Customer Identity and Access Management ensures security without damaging digital experience.



A PRACTICAL EXAMPLE: WHAT GOOD LOOKS LIKE

Consider a new employee joining on Monday.

HR creates their record. Birthright access is assigned automatically. Project access triggers an approval workflow. Single sign-on provides seamless application access. Multi-factor authentication activates when working remotely. An IT administrator configures their laptop using a monitored privileged session.

The employee sees none of this and that's the point! Well-run Identity Security operates in the background, enabling productivity while producing continuous proof.

THE FOUR-STEP IDENTITY MODEL

Every access event follows the same pattern:

Identify → Authenticate → Authorise → Audit

- Identify — Who or what is requesting access?
- Authenticate — Are they who they claim to be?
- Authorise — What are they allowed to do?
- Audit — What did they do, when and why?

This simple framework helps executives assess maturity across systems.

If any step is inconsistent or manual, risk increases and evidence weakens.

WHERE MOST IAM PROGRAMMES STALL

Many IAM initiatives struggle not because of technology, but because of operating model gaps.

Common patterns include:

- Tool-first thinking without governance design
- Siloed deployments across AM, PAM and IGA
- No defined ownership after implementation
- Manual workarounds outside formal workflows
- Limited visibility into Non-Human Identities
- Identity treated as a project rather than a capability
- AI initiatives deployed without corresponding identity governance design

IAM does not end at go-live. It must be run. Identity Security delivers its full value only when treated as an ongoing managed business capability.

As AI adoption accelerates, many organisations introduce new automation and data access patterns without adjusting their identity operating model. This creates governance gaps that only become visible during audit or incident review.

TURNING IDENTITY RISK INTO BUSINESS VALUE

When Identity Security is structured correctly, organisations gain:

- Faster onboarding and role changes
- Cleaner offboarding
- Reduced audit preparation effort
- Clear visibility of access rights
- Measurable control over privileged activity
- Structured governance of machine credentials
- Executive-level reporting on identity posture

The proof is not a separate project.

It is the byproduct of running identity correctly every day.

IDENTITY SECURITY AS A MANAGED BUSINESS CAPABILITY

Identity is not a one-time implementation.

It is an operational discipline that spans:
- HR
- IT
- Security
- Compliance
- Application owners
- Infrastructure teams

Running IAM effectively requires:
- Governance design
- Platform expertise
- Continuous optimisation
- Ongoing monitoring
- Structured change management

Many organisations do not want to build this as a permanent in-house function.

A Managed Service model enables:
- Faster time-to-value
- Reduced internal complexity
- Access to specialist expertise
- Continuous improvement
- Clear accountability

Identity Security becomes predictable, measurable and aligned to business objectives.

Discuss your Identity Security with our experts here.

WHAT TO DO NEXT

If Identity now sits within your remit, the next step is clarity.

- Where does your organisation sit today?
- Which parts of the identity landscape are mature, and which are fragmented?
- How are Non-Human Identities governed?
- Is your IAM programme delivering proof by design, or relying on manual effort?
- How is AI access governed across your enterprise?
- Do AI agents operate under least-privilege principles?
- Can you trace and evidence AI-driven actions?

A structured assessment can provide a clear, prioritised roadmap without disruption.

EXPLORE YOUR IDENTITY SECURITY MATURITY

Discover how Identity Security can be delivered as a managed business capability with fast time-to-value.

Learn where you are today. Understand what good looks like. Build a roadmap that aligns security, productivity and compliance.