Pioneering the Next Era of Security

Transforming Identity & Access Management

Fatima Hoblos
Identity & Access Management
Kmart Group

Why IAM Matters NOW?

Beyond the Perimeter

Identities are now the primary control plane, replacing network perimeters in modern security architectures.

Evolving Threat Landscape

Attackers are targeting credentials directly through ransomware, supply chain intrusions, and identity-based breaches..

The Digital Imperative

Rapid innovation demands agility without compromising security. IAM is the foundation for secure digital growth.

As organisations accelerate digital transformation initiatives, identity has emerged as the crucial element that can either enable or undermine security efforts. The stakes have never been higher.

What is Identity and Access Management (IAM)?

> IAM is the framework of policies and technologies ensuring that the **right individuals** have the **right access** to the **right resources** at the **right time** for the **right reasons**.

The Four Pillars of IAM

- Identification: Who are you?
- Authentication: Are you who you say you are?
- Authorization: What are you allowed to do?
- Auditing/Accounting: What did you do?

Key IAM Capabilities

- Authentication: Secure sign-in, SSO, MFA
- Access Management: User provisioning, external users, RBAC
- Governance: Access reviews, SoD, auditing
- Privileged Access Management (PAM): Credential management, session control, JIT access

Beyond Passwords: Modern Authentication

The Password Paradox

- Most breaches involve weak or stolen credentials
- Password reset requests account for 20-50% of all IT help desk tickets
- Complex password requirements often lead to insecure practices

Adaptive Authentication

- **MFA:** Reduces account compromise risk by 99.9% (Microsoft)
- **Biometrics:** Fingerprint, facial, voice recognition with <1% false acceptance
- **Passwordless:** FIDO2/WebAuthn, certificate-based
- **Contextual factors:** Location, device, behavior patterns, time of access

Implementing Adaptive Authentication: Start with enforcing MFA for all users, prioritizing privileged accounts. Then introduce risk-based authentication that adjusts requirements based on login context (unusual location/device triggers stronger verification). Finally, pilot passwordless options with specific user groups before broader rollout.

The Operational Core: Automating Identity Governance

The Cost of Manual IAM

- Significant delays in access provisioning
- Manual access reviews have high error rates
- Many audit findings relate to access control deficiencies
- Typical enterprise spends 5,000+ hours annually on access management tasks

Automated Governance Benefits

- **Efficiency:** 85% reduction in provisioning time
- **Accuracy:** 95% decrease in access control errors
- **Compliance:** 70% reduction in audit preparation time
- **Cost Savings:** significant savings per provisioning request

Key Automation Priorities

Access request workflows, approval chains, provision/de-provision processes, periodic access reviews, anomaly detection, and compliance reporting

Integration Requirements

HR systems, directory services, cloud IAM providers, application-specific access controls, privileged access management, and security monitoring tools

User Lifecycle Management

1

Onboarding

- Automated account provisioning
- Role assignment based on job function
- Birthright access

2

Changes & Transitions

- Role changes and promotions
- Access recertification
- Temporary privilege elevation

3

Offboarding

- Immediate access revocation
- Account deactivation
- Archiving of user data

4

Continuous Governance

- Regular access reviews
- Orphaned account detection
- Privilege creep prevention
- Compliance monitoring

Access Control Models: RBAC vs. ABAC

1

Role-Based Access Control (RBAC)

Pros: Simple to understand, widely implemented, clear governance

Cons: "Role explosion," limited flexibility, potential over-privileging

Best for: Smaller organizations, stable environments, clear role boundaries

2

Attribute-Based Access Control (ABAC)

Pros: Highly granular, adaptable to change, supports Zero Trust

Cons: Complex implementation, requires robust attribute management

Best for: Large enterprises, regulated industries, dynamic environments

3

Hybrid Approaches

Benefit: Balances security granularity with operational efficiency

Implementation: Start with RBAC, gradually incorporate attributes

Fortifying Resilience: IAM for Disaster Recovery

The Critical Role of IAM in Crisis

When disaster strikes, identity becomes the key to recovery:

- Identity services are often the first requirement for restoring operations
- Access management prevents security shortcuts during recovery
- Emergency access protocols balance urgent needs with security
- Identity-based recovery prioritization ensures critical services first

Key DR Strategies for IAM

- **Redundancy:** Geo-distributed identity stores, multi-region deployment
- **Backup procedures:** Regular backups of identity data, configurations, policies
- **Failover mechanisms:** Automatic switching to secondary identity providers
- **Break-glass procedures:** Emergency access with strict controls and auditing
- **Regular testing:** Simulated failures to validate recovery procedures

From Reactive to Proactive: AI's Role in Modern IAM

1

Anomaly Detection

AI algorithms identify unusual access patterns and potential threats by establishing behavioral baselines and flagging deviations.

Example: Detecting when a user accesses systems at unusual hours or from unexpected locations.

2

Risk-Based Authentication

ML models dynamically adjust authentication requirements based on real-time risk assessment.

Example: Requiring additional verification when login context suggests elevated risk.

3

Behavioral Analytics

AI systems establish user behavior patterns to detect potential account compromise or insider threats.

Example: Identifying when a user suddenly accesses sensitive data they've never touched before.

4

Role Mining & Optimizsation

ML algorithms analyze access patterns to suggest optimal role structures and identify excess privileges.

Example: Recommending role consolidation by finding access pattern similarities across users.

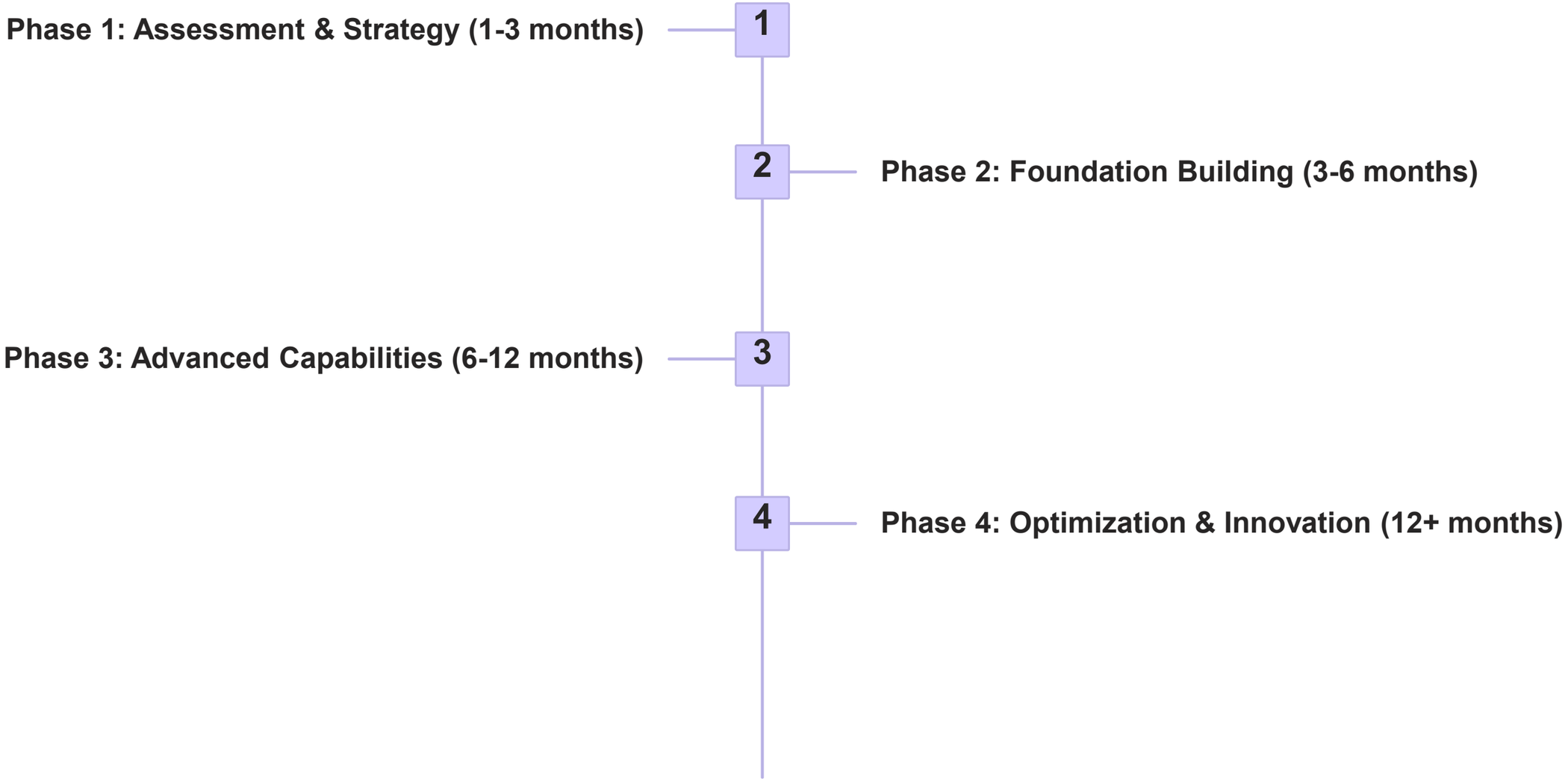
5

Automated Access Reviews

AI assists in access certification by prioritizing high-risk access for human review and handling routine certifications.

Example: Pre-approving low-risk access while escalating unusual privilege combinations.

The Roadmap Forward: Strategic IAM Implementation



Let’s connect!

fatime.hoblos@kmart.com.au