

Identity Governance Program

Topics

01

Overview

02

IGA Program Pillars

03

Benefits, Business Case, Scope of Services

04

Roadmap

05

Roles & Team Structure

Overview

Many organizations have made significant investments in the technology supporting Identity and Access Management. A managed security service program wraps that technology investment with a robust Identity Governance and Administration program to achieve the following:

- ❖ Create an **“Identity-first”** security approach that makes identity-based standards and controls a foundational element of the organization’s cybersecurity architecture.
- ❖ Establish a comprehensive framework for managing **all digital identities, access privileges**, and compliance & standards across the organization.
- ❖ Centered on standard **IGA pillars** and address gaps within each
- ❖ Enable secure, efficient, and compliant identity operations (JML lifecycle)
- ❖ Focus on standards, process excellence, accountability and stakeholder engagement
- ❖ Strategic objectives support achieving Capability Maturity Model (CMM) Level ‘Managed’ (i.e. Capable)



PROGRAM PILLARS

IGA Program Pillars



Identity Governance & Strategy



Lifecycle Management



Access Management



Privilege Access Management



Access Governance



Identity Analytics



User Experience/
Business Enablement

Establish clear ownership, accountability, and alignment with business & regulatory

- IAM Policy & Standards Alignment
- Role Definition/ SOD
- Compliance Alignment
- Metrics & KPIs
- Maturity Model
- Communication Standards
- IGA 3 year Roadmap

Manage digital identities from onboarding to offboarding

- Technology has matured the tech supporting lifecycle
 - Joiner
 - Mover
 - Leaver
- Unified approach to identities & access – not just human identities
- Directory Svcs integration & operating model

Control and enforce how users authenticate and what they can access

- Modern Authentication standards across enterprise
- Role-based (RBAC) fully enforced
- Single Sign-On (SSO) integration and mgmt.
- Session Management: PAM, UBA/anomaly detection

Protect and monitor high-risk accounts with elevated privileges

- Incorporate PAM Cred. Vault into the IGA program
- Just-in-time access
- Session Recordings
- Break-glass procedures
- Integration opportunity for SIEM and other security tools

Provide visibility, oversight, and control over who has access to what

- Access Reviews and Certifications
- Role Mining & Optimization
- Segregation of Duties
- Auditing & Reporting

Detect and respond to anomalous identity behaviors

- Lifecycle Analytics
- UBA and integration with SIEM/ SOAR
- Address trends while acknowledging deviations (inform tech backlog)

Balance security with usability and productivity

- Onboarding refinements
- Self Service Capabilities
- Integration with SNOW
- User Authentication Standards

Continuous Improvement and Automation



BENEFITS, BUSINESS CASE, & SCOPE OF SERVICES

Overall Benefits

In today's world identity is core to the digital fabric of all business functions. The governance and administration of these identities is at the center of an organizations' operations and their information security foundation.



Enhanced Security

Identity theft, spoofing, AI threats, etc... highlight the need to administer and manage identities in a secure and controlled manner. Enhancing identity security overall.



Regulatory Compliance

Enrich the ability to meet regulatory compliance with ease as all components of the IGA program live and operate together.



Improved Operational Efficiency

Creating and enforcing standards, reducing exceptions, deepening partnerships, and creating clarity in the organization will further operational efficiencies that the technology platform doesn't address.



Risk Management

Continuous monitoring and governance of identities can help identify and mitigate risks associated with excessive permissions or inappropriate accounts, improving the overall security posture.

Organization-Specific Benefits

Most organizations have specific items to be addressed that are current gaps in their IAM Program.



Close Integration & Visibility Gaps

Expand on the technology investments by enforcing identity standards for all digital identity types. Creating operational efficiencies & analytics to create a truly managed program.



Compliance and Co-Ownership

Accountability with Application and Infrastructure teams regarding all digital identities. Improving visibility and compliance overall.



Mature Partnerships

Build partnerships with internal and external stakeholders:
Internal: Infrastructure, Applications Teams, etc.
External: HR, Affiliates, Hiring Managers, etc.



Governance based outcomes

Ensuring full management, administration, and compliance of all digital identities with analytics and KRI's monitored and managed.

What's the Difference?

Today's IAM Capabilities

- IAM is focused on Identity life cycle management for human identities only (leaving a large gap)
- Application Provisioning via automated connectors
- Access request processing and workflow orchestration
- Limited Access certification (aka attestation/ review)
- Dynamic Role based Access for some user populations
- Basic reporting and analytics

Tomorrow's IGA Program

- ✓ Overarching program to incorporate and govern people, process and technology surrounding identities
- ✓ Comprehensive identity lifecycle management including non-human identities: e.g. cloud, services, RPA, etc.
- ✓ Incorporate PAM and access management
- ✓ Advanced analytics to for visibility, but also to inform rapid improvements, technology backlog, or SIEM/SOAR.
- ✓ Partnerships with key stakeholders including ongoing operations and communications
- ✓ Breadth, Depth and Insight overall

IGA Strategic Objectives



Identity Governance & Strategy

- IGA standards communicated and enforced
- Identity Steering Committee formed and operated quarterly
- Standard Operating Procedures assessed, revised and enforced
- Define Co-Ownership of identity governance with key internal IS stakeholders
- Influence IT policy adjustments



Lifecycle Management

- Evaluate AI Opportunities for workflow enhancements
- Unified approach to identities & access:
 - Cloud
 - MFA Access
 - Machine/SVC
 - AI Agents/Bots
- Align with the broader enterprise identity program and modernize
- RACI/Ops model with key stakeholders
- Manage backlog for enhancements



Access Management

- Explore integrations with SSO and other Auth-based tools
- Create Auth standards across the enterprise
- Refinements to affiliate identity approach; who does/does not get accounts and what access



Privilege Access Management

- Incorporate PAM Cred. Vault into the IGA program
- Integration opportunity for other security tools: i.e. SIEM
- Break-glass procedures



Access Governance

- Add Compliance Campaigns for disconnected systems
- Role Mining analysis
- Mock Audits
- Improve compliance and auditability with documentation and processes



Identity Analytics

- Build/Refine KRIs and support with analytics
- UBA reporting and integration with



User Experience/ Business Enablement

- Advance partnership with HR
- Create white glove programs where needed; i.e. Physicians
- Expand and advance user training and awareness

Achieve Capability Maturity Model (CMM) Level 'Managed' within 24 months



ROADMAP

3-YEAR ROADMAP

0 – 6
MONTHS

6 – 12
MONTHS

YEAR
2

YEAR
3

PLANNED ACTIVITIES

- Establish IGA program governance and sponsorship
- Technology stabilized with core internal team
- Address communication gaps
- Establish partnerships with key stakeholders
- Build first phase of Analytics
- Assess current IAM practices, standards, procedures, and technology

PLANNED ACTIVITIES

- Enforcement of Co-Ownership of Identities with App & Infrastructure Teams
- Plans to incorporate full identity populations: Cloud, PAM, Svc, RPA, etc..
- Plans to incorporate Auth
- Implement physician white glove program*
- Evaluate AI opportunities
- **Assess MSSP relationship and review/revise roadmap**

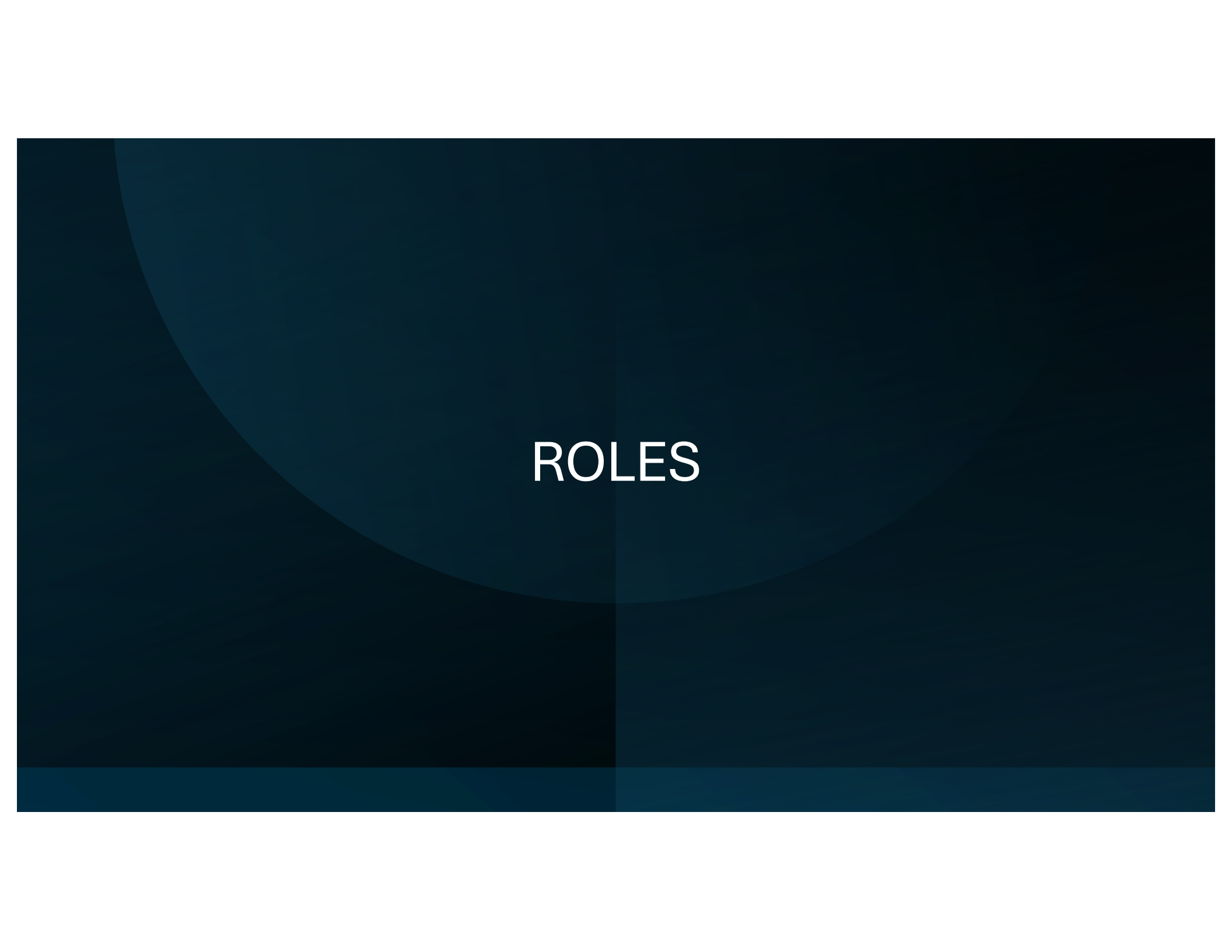
PLANNED ACTIVITIES

- Align with enterprise identity program, retire legacy tech*
- Compliance campaigns expand to add't systems*
- Incorporate all digital identities into IGA
- Incorporate Auth (SSO, MFA)
- Additional Application Connectors*
- Advance analytics

PLANNED ACTIVITIES

- Incorporate AI into workflows
- Governance optimization
- Conduct mock-audits
- Additional Application connectors
- **Decision on MSSP continuance or return to internal business units**

*May require capital investment by the organization



ROLES

Role Definitions

	MSSP Resource	Client Resource	Function
IGA Program Director	X		Oversight for IGA program. Serves as an advisor to senior leadership on IAM trends and innovations, threat mitigation strategies related to access control, and ensuring alignment with organization cyber goals. Serves as the liaison and key communications resource between business operations & key stakeholders. Create & maintain 3-year roadmap,
Process & Workflow Expert	X		Create and reinforcement organizational process changes related to identities (i.e. OCM) . Serves day-to-day for standard operating procedures, efficiencies, data trends, groom technology backlog, and escalation point. Ensures documentation is current & available.
Data Analytics	X		Creates and produces regular reporting which informs KRIs, trends, anomalies, and integrates as needed with other systems: e.g. SIEM, UBA, etc.
Identity Fulfillment		X	Lifecycle management of user identities to be expanded to address IGA gaps & partner with key stakeholders
Compliance Enforcement		X	Compliance campaigns and co-ownership of identities
IAM System Admin/Engineer		X	Manages the IAM platform, data sources, and connected systems to support automation and governance
IAM Build Team	TBD	TBD	Customize the IAM platform to meet needs of the IGA program – can be internal or outsourced

IGA Structure

