

IDENTITY AND ACCESS MANAGEMENT SOLUTIONS

Help Ensure Success in Moving from a Tactical to Strategic IAM Program

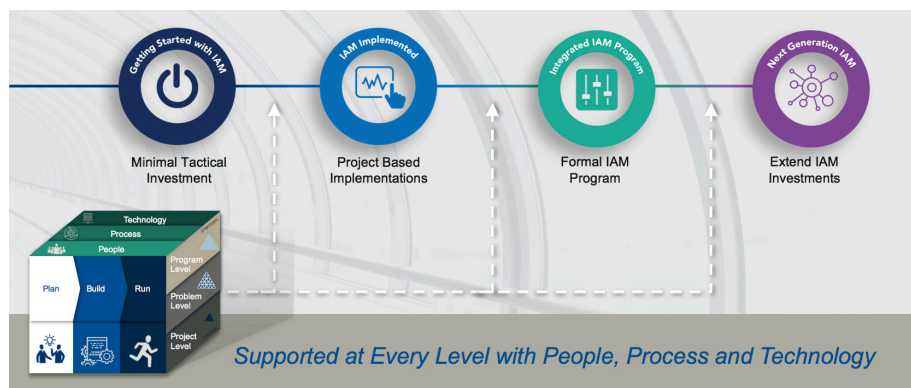
Overview

While identity and access management (IAM) provides many benefits to your organization that ultimately increase revenue, reduce costs and minimize risk, IAM projects have consistently proven to be challenging. The typical organization takes a technology centric view of IAM, implementing projects in a silo by focusing on a single project or business problem. To make matters worse, skilled security professionals, and specifically IAM experts, are a scarce resource.

Identity and Access Management is an Evolution

We believe that achieving success with IAM is an evolution that is driven by the maturity of your IT organization and the complexity of your requirements. Aligning key stakeholders and business initiatives, and partnering with experts in the leading IAM technologies are keys to transitioning from tactical project to strategic program.

Through our experience in working with hundreds of clients, we defined four stages of this evolution used to evaluate your current state before deciding on next steps.



Because no two clients are the same, we customize your journey leveraging strategic consulting and implementation services, leading IAM vendors and Optiv developed technologies, staying focused on people, process and technology.

Our IAM services include:



Workshops and Assessments



Implementation and Integration



Program Governance

Why choose Optiv for IAM?

- Complete IAM-focused solution offering
- Repeatable approach tailored to client requirements
- 100+ IAM strategic advisors and delivery experts
- Access to a collaborative team of IAM specialists
- Dedicated Centers of Excellence for leading IAM vendors



IAM Strategy Workshop

Wide ranging one or two-day working session overview of IAM trends and vendors, client business drivers and challenges. Workshops can be tailored based on your budget, timing and expected business outcomes.



Outcomes:

- Assess current state, including key stakeholders, client pain points and high level goals
- Develop an IAM maturity model and identify potential risks to success
- Create recommendations and next steps toward a mature IAM program



Identity Centric Security Workshop

Wide ranging one or two-day working session overview of IAM trends and vendors, client business drivers and challenges.



Outcomes:

- Prioritize ICS goals based on tactical business objectives
- Assess current state environment(s), current state pain points, organizational challenges and “red flags”
- Create recommendations for a customized ICS roadmap and implementation plan



IAM Assessment

Broad tactical or enterprise assessment and discovery to understand current state intricacies and challenges.



Outcomes:

- Document current and future use cases and detailed requirements
- Identify progress toward a mature IAM program
- Create short-term and strategic roadmaps, as driven by specific business needs and requirement



IAM Compliance and Identity Management Readiness

Thorough analysis of identity related data, reducing risk of failed audits.



Outcomes:

- Assess targeted systems and evaluate role model
- Identify patterns and dirty data
- Develop recommendations for clean-up before moving forward with implementing an IAM solution

IAM Role Assessment

Thorough analysis of role data, promoting visibility and awareness into users' access.



Outcomes:

- Identify current state access profiles and patterns
- Leverage role definitions defined through a best practice approach and proven methodology
- Build foundational role models that set the stage for automation

Active Directory Assessment

Comprehensive review of Active Directory, including the underlying security and governance of your directory infrastructure.



Outcomes:

- Assess current state, including infrastructure, management processes, and governance
- Identify access security issues associated with group management, stale users, elevated privileges and admin password violations
- Create roadmap that defines remediation path to achieve a healthy environment and tools and best practices for maintaining it

Unstructured Data Risk Assessment

Comprehensive view of the location of sensitive unstructured data and who is accessing it and evaluation of the overall health of Active Directory permissions.



Outcomes:

- Identify access security issues associated with the access controls and authorization process, privileged and end user monitoring, and Active Directory structure
- Discover location of unstructured data files, including those that contain regulatory data such as SOX, HIPAA, PCI, GDPR and BLG, as well as stale files that should be archived or deleted
- Create roadmap that defines remediation path addressing data security risk issues and establishing an approach for governing sensitive unstructured data

IAM Health Checks

Complete evaluation of vendor implementations, validating against business requirements. Available for CyberArk, Ping Identity, RSA and SailPoint.



Outcomes:

- Review current architecture, hardware and application performance
- Examine integrations with other technology components and existing processes
- Document findings and develop recommendations to improve operational effectiveness of deployments

IAM Implementation and Integration Services

Definition, design, development, test and deployment of IAM technology solutions for leading IAM vendors. Our expertise includes access management (single sign-on, federation, multi-factor authentication, privileged access management), identity administration, identity governance and security and analytics.



Our Services Include:

- Implementation Quick Starts
- Architecture development and design support
- Product installation and configuration
- Implementation and engineering support
- Customization management
- Staff augmentation

IAM Technology Selection and Sourcing

IAM solutions advisors guide you through the process of selecting the right technology to meet your business goals and technical requirements.



Our Services Include:

- Share perspective on industry research in relation to client environment
- Manage the vendor interactions, pricing and process
- Assist with IAM vendor selection and RFP process
- Evaluate vendor solutions and responses
- Provide or facilitate vendor demos and POCs

Optiv Developed Technologies

Integrations, tools and extensions that enhance the value of your IAM investments and customize deployments to your requirements.

- Point solutions and integrations that create one “cyber security” fabric
- Tools and technologies that help migrate legacy IAM technologies to next-gen, protecting existing investments
- Extensions and enhancements of commercial off-the-shelf (COTS) technologies to meet your unique needs



Optiv Developed Technologies Include:

- Ping Identity Integration Kits: SiteMinder, Axiomatics, HitachiID, Netskope
- RSA SecurID Suite Integration Kits: CyberArk, Microsoft Office365
- Legacy WAM (including Oracle Access Manager and SiteMinder) to PingAccess Migration
- RSA SecurID Access Manager and L&G Custom Integration and Extensions
- Unix Access Governance Tool that collects and correlates Unix access information

Identity Centric Security Solutions

Combination of technology and services that integrate existing cyber security and IAM technologies based on the use cases defined by the Identity Defined Security Alliance (IDSA).



Our ICS Services include:

- Ping Identity - Netskope Integrated Solution: Combines the intelligence of Netskope with the centralized authentication of PingFederate to enable context-based authentication and access policy enforcement as defined by the IDSA

Privileged Access Managed Service

Comprised of an extensive team of privileged access management engineers and threat analysts, Optiv can help control costs, increase security and reduce risk by protecting and managing your critical privileged access environment.



Our Services include:

- High Availability and Performance - system and connection monitoring and backup and recovery assurance
- Administration - privileged account, password vault user access, password vault user group and policy target account platform management
- Release Management - updates, upgrades and patches, security recommendations and change management
- Reporting - service management, operation and audit and compliance reporting

IAM Program Governance

Project or program management oversight giving your IAM project more visibility across key stakeholders and integration with compliance and security programs.



Our Services include:

- Provide project management expertise focused on IAM service delivery management, planning and oversight across a single project or an entire program.
- Integrate your IAM program with your internal oversight and compliance functions
- Educate governance and steering committees on the integration of IAM across the business to meet compliance and security requirements

We provide implementation and integration services for the following leading IAM vendors:

