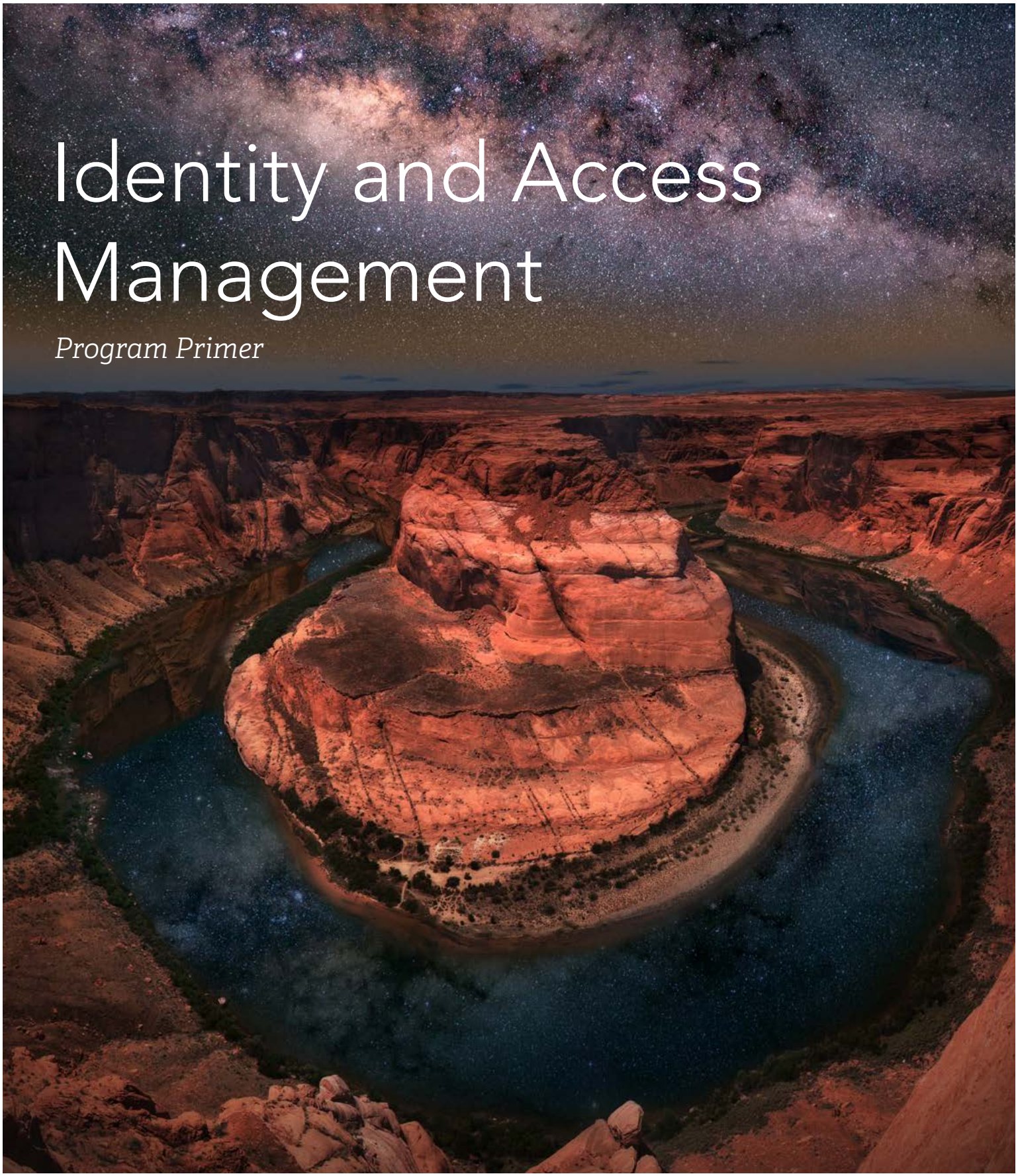
Identity and Access Management

Program Primer



OPTIV

Executive Summary

The role of identity in the modern enterprise has been steadily growing in importance over the last decade. As the enterprise technology stack continues to explode from a handful of on premise applications to thousands of business-critical apps across corporate data centers, mobile devices and clouds, the management of identities and access to sensitive company information has become monumentally difficult.

The taxonomy of identity and access management spans a number of areas, including program management, identity data management, access management, access governance, identity management, privileged access management, and data security and analytics. Each of these areas have related pain points, objectives, business drivers, with supporting people, process, and technologies, and deserve careful examination and prioritization for your organization.

One of the major end goals for many organizations is to have workflows and supporting solutions in place to allow new employees to be provisioned for access to the applications and systems they will need to do their job in a semi-automated or fully automated fashion, based on the functions that new hire will perform. Unfortunately, even in large organizations, many legacy applications and systems still require manual provisioning with ad-hoc access requests, where there is no pre-determined function or role definition.

During the lifecycle of any given user they will typically have many roles and access to many systems and applications. It is inevitable that where manual processes exist a user will accumulate many unneeded identities and maintain access to applications and systems they no longer require for their job. Even when users leave the company these identities and legacy access can persist, creating substantial security related risks to the organization.

Enterprises do not solely manage the identities of their employees: most companies also manage identities for their partners, contractors, vendors, and many must manage customers, along with perhaps students, faculty, nursing staff, and more, leading to a complicated web of workflows and solutions. Almost every company now has hundreds or even thousands of third parties who connect into their IT systems or have physical access to their facilities. All of these third parties must be carefully restricted to the appropriate level of access to systems and applications they require to perform their duties. Contractors are an especially difficult challenge due to the high frequency for turnover, the decentralized way they are managed, and the lack of authoritative sources for their identity data.

Each different type of identity will have subtle differences in policy, accessibility to critical systems and data, and the type of standard lifecycle changes that must be managed in a cohesive fashion. The administrative overhead this can cause is significant, so careful and thoughtful strategic planning is necessary.

For these and many other reasons, for many organizations, managing identities independently across potentially thousands of systems and applications has become a seemingly impossible feat creating an environment that lends itself to intellectual property theft, misuse or destruction by employees, partners, providers, customers or attackers.

Without a centrally managed identity store, identity federation, role definition, and auditability, enterprises will struggle to hold their users with valid identities accountable while maintaining the type of visibility necessary to keep data safe. The balance of accessibility against security is a struggle every organization must continue to tackle, and taking a strategic approach is key to supporting business enablement while reducing risks.

Today more than ever before a programmatic approach to identity and access management is singularly important to the safety and security of your organization and critical assets. Relying upon an outcome-driven program built using a well-defined set of capabilities, security leaders can build repeatable, measurable and accountable identity and access management programs that deliver real business value.

Program Clarity

The scope of this research addresses IAM from a security program development perspective. IAM can encompass multiple types of relationships between an organization and its stakeholders, including business-to-business (B2B), business-to-consumer (B2C), as well as the relationship held with internal users, which could include employees, contractors, vendors, students, faculty, researchers, business partners, affiliates, franchisees, and more. Any type of relationship an individual might have can be controlled and the associated risks mitigated through robust and thoughtful IAM programs. The below research focuses on those internal user relationships, but many of the concepts and maturity gains can be applied to these other relationships.

At Optiv, we define IAM as the people, processes, and technology used to create, manage, authenticate, control, and remove the permissions a user has and the way data is accessed throughout an organization. This is further broken down into the core functions described in the following sections

Program Strategy Approach

Although enterprise IT and security organizations may take different approaches to IAM, their end goals are similar: provide visibility, improve productivity and manage users and their data access privileges, resulting in an improved overall security posture, reduced risk, and increased business value through enablement.

Unlike some security related programs, IAM technology decisions in the context of user lifecycle management and access management are generally focused on the solution's ability to solve business problems and enable end users, while core security and risk mitigation is the key center point with privileged access management, data security, and identity governance. With IAM, the associated business problems are not only to cut cost through automation, but also to facilitate the execution of strategy while enhancing the user's experience.

In the following pages, and more in-depth in the IAM Blueprint, we will further define, explain, and recommend steps to mature all of these core functions across six effective levels of maturity and provide the guidance necessary to plan, build, and run a successfully business-aligned identity and access management program.

Model Driven Program Development

Optiv's research and subsequently the approach taken within Optiv's IAM practice focuses on the following:

- Core Functions of IAM
- IAM Maturity – Current and Desired Future State
- Outcome Oriented IAM Program Development
- Laying the Foundation for a Successful IAM Program

Core Functions

Building Blocks of Program Development:

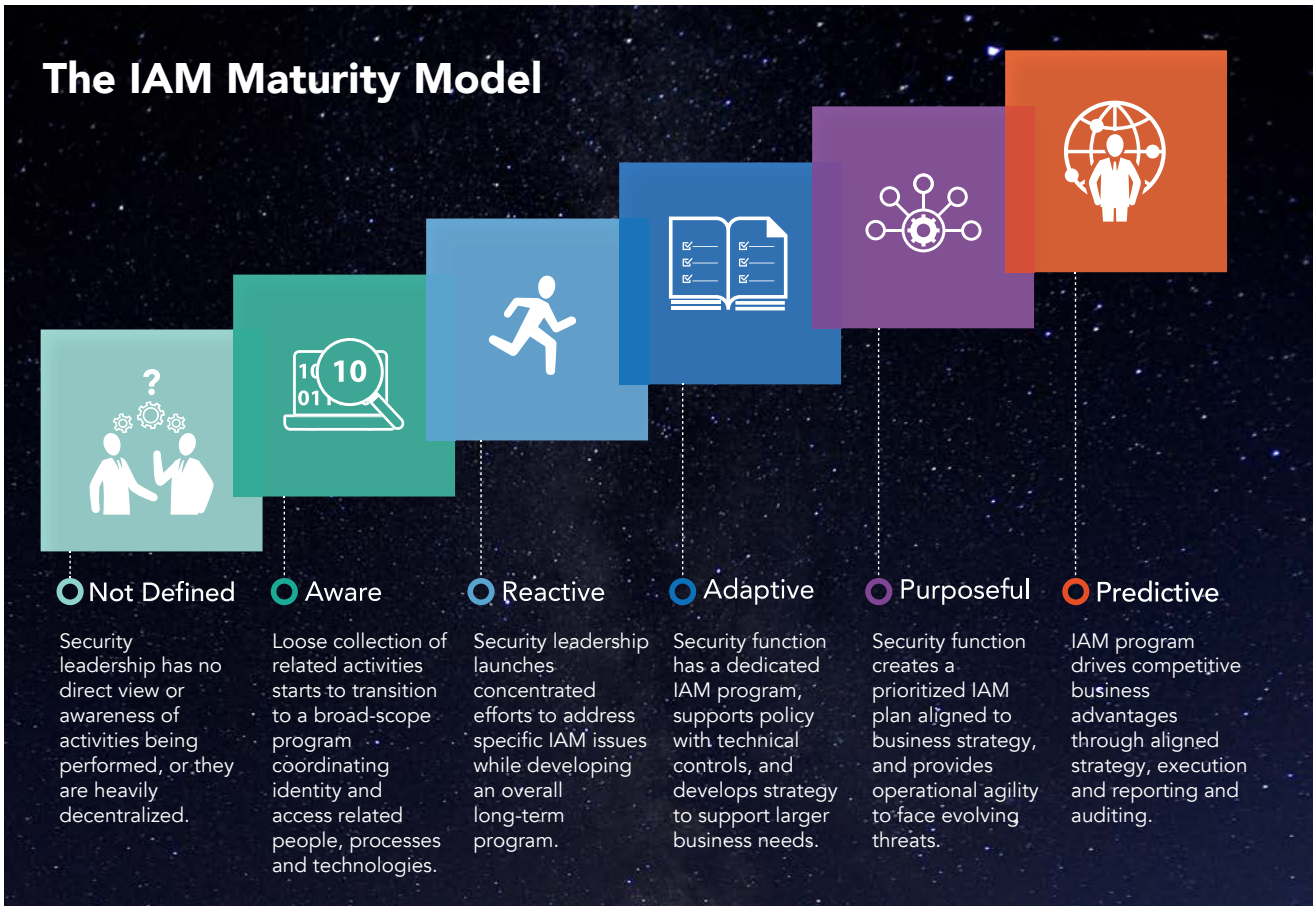
Core functions are the essential building blocks of every Identity and Access Management program. These are attributes that every program we studied and analyzed contained in various forms. Additionally, input from various industry and Optiv experts was used to normalize and evaluate each core function.

IAM Program		
How the organization, it's executive stakeholders, and its subject matter experts approach IAM pain points, drivers, and the supporting people, process, and technology changes.		
Identity Data Management	**Access Management**	**Access Governance**
The control and management of identity-related data, the systems that house the data, and how the data is processed across the organization	Supporting authentification mechanisms, including single sign-on (SSO), multi-factor authentification (MFA), federation, and password management	Policy-based activities enabling the definition, enforcement, review and audit of IAM functions and policy compliance
Identity Management	**Privileged Access Management**	**Data Security and Analytics**
Core user lifecycle and self-service management of end user accounts, administration and entitlements	Supporting the processes and technical controls related to elevated permission accounts	The ability to provide data classification, identification and user analytics to support data security programs

Core functions are broken down further by related use case or functionality:

IAM Program		
Plan	Build	Run
Identity Data Management	**Access Management**	**Access Governance**
• Authoritative Sources • Identity Data Model • Identity Master Data Management • Identity Data Governance • Identity Correlation Keys	• Authentication • Strong Authentication • Federation • Password Policies • Self-Service Password Reset	• Role-Based Access Control • Access Certification • Segregation of Duties • Audit • Reporting
Identity Management	**Privileged Access Management**	**Data Security and Analytics**
• User Onboarding • User Termination • Access Requests • Delegated Administration • User Information Self-Service	• Privileged Credential Vaulting • Privileged Session Management • Local Admin Management • App to App Credential Management	• Data Classification and Identification • Data Access Governance • Data Loss Prevention

Optiv's Program Maturity Approach and Model



Outcome-Oriented Program Development

Program development at Optiv is outcome-based, meaning we first model the end results an organization is working to achieve and are then capable of working backwards to determine the necessary capabilities and supporting resources. In order to accurately show directionality and achievement to leadership – we focus first on outcomes.

Outcomes are modeled in two ways to provide direct value at either a high level strategic vision, or at a more tactical plan, build, and run capacity. At the highest level, outcomes are modeled on a vision for each maturity level. The best way to look at these is that they address the net result of successfully reaching each maturity level.

At a more tactical level, we look at plan, build and run and how an identity and access management program will manifest at each of these three lifecycle stages in an enterprise IT organization.

Strategic Maturity Overview:

Maturity Level	Strategic outcome
0 - Not Defined	Security leadership has no direct view or awareness of activities being performed, or they are heavily decentralized and not understood.
1 - Aware	Loose collection of related activities starts to transition to a broad-scope program coordinating identity and access related people, processes, and technologies.
2 - Reactive	Security leadership is able to launch concentrated efforts to address specific IAM issues while developing an overall long-term program.
3 - Adaptive	The security function has a dedicated IAM program, supports policy with technical controls, and aligns strategy with larger business needs.
4 - Purposeful	The security function creates a prioritized IAM strategy that is aligned with the larger overarching business strategy, and provides for nimble operations to face evolving threats.
5 - Predictive	The IAM program deploys strategy, produces reporting and provides services that drive competitive business advantages while supporting business enablement through aligned program initiatives.

Tactical Phase Overview:

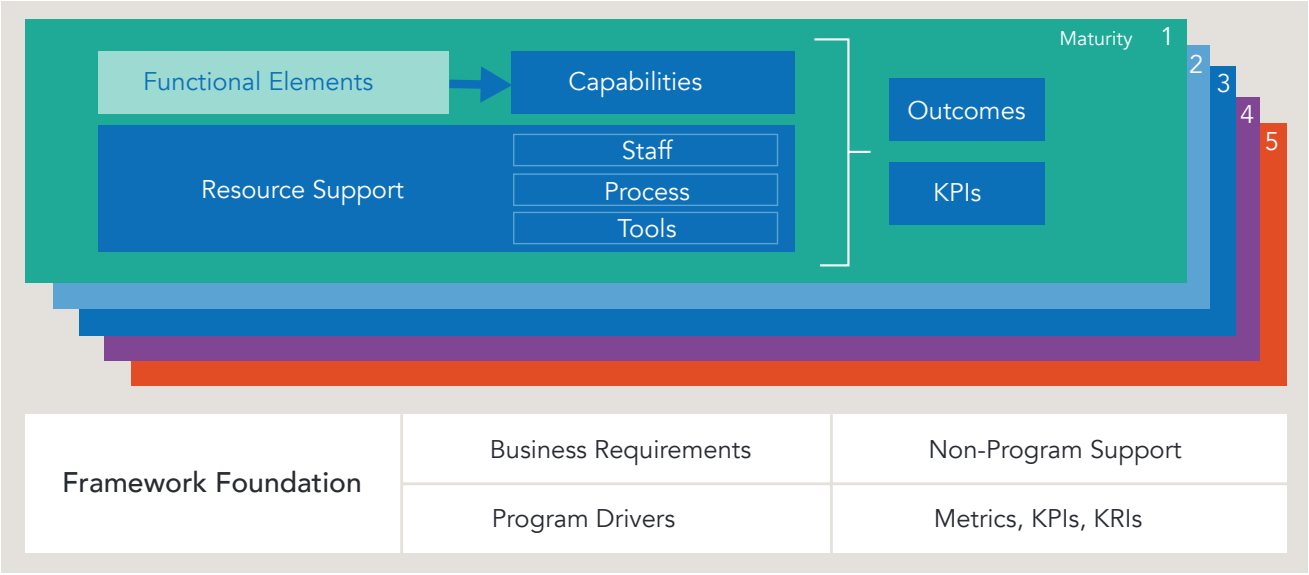
Phase	Description
Plan	The manner in which an organization defines and designs the program, aligning it to IT capabilities and business need
Build	The manner in which an organization deploys and implements the program into the organization
Run	The manner in which an organization operationalizes and maintains the program to continuously adapt to and serve business need

Tactical Maturity Levels:

	0 - Not Defined	1 - Aware	2 - Reactive	3 - Adaptive	4 - Purposeful	5 - Strategic
Plan	Leadership not involved in planning	Leadership aware but not core stakeholder	Responds to incidents, very tactical, little planning	Identifies needed changes, implements centrally but tactically	Routinely evaluating needs and defining vision with involved SMEs	Strategic, prioritized business enablement and enterprise needs
Build	Ad-hoc, decentralized, no governance or awareness	Ad-hoc, decentralized leadership told as "FYI"	Centralized but "exception" based testing and other SDLC processes minimal	Effective reactions and implementation	Integrated change management, awareness, and prioritization is effective	Cross-enterprise integration and compatibility fully built into stack
Run	Ad-hoc, decentralized, no governance or awareness	Decentralized, leadership can provide thoughts on approach	Standard but stagnant, changes only from issues/ incidents, training occurs later	Adaptive techniques, effective training, involved leadership	Purposeful support, maintenance, and training, improved SLA's	Products/ training continuously examined and enhanced

Laying the Framework Foundation for Success

The Framework Foundation is comprised of the four foundational elements of each IAM program we studied that was successfully implemented and deployed. The foundation ensures that the program is business aligned (program drivers), stakeholder driven (business requirements), appropriately supported from the rest of the organization (non-program support) and measurable to the appropriate stakeholders (metrics, KPIs and KRIs). Together these components bring grounding to the program and give security leadership peace of mind.



Program Drivers

When developing the programs Framework Foundation, our research team looks to understand motivations from a business perspective. Why an organization invests resources in any particular initiative is important and can be modeled to deliver insight to security leaders. This provides those whom have not had clear direction from their leadership with some potential ideas on what the expectations of their programs could be, and how to align to their generic business profile and operational goals. While we understand that what drives one company does not necessarily translate to another – general themes based on company profile (maturity, market-segment, etc.) provide well-grounded guidance. Our Program Drivers provide this insight from one on one interviews and focus groups.

Business Requirements

The purpose of Business Requirements is to ensure stakeholder needs are being addressed. During the course of research, our team spent time with security leaders and program managers to understand what the motivations of their key stakeholders were – and how they addressed these issues through the development and maturation of their IAM program. Business requirements ensure that input from both technology (IT) and business leaders is taken into account when choosing appropriate solutions, and prioritizing, designing and developing the program goals and roadmap.

Non-Program Support

Non-Program Support addresses all those bits and pieces that are critical to the success of an IAM program, but are out of the direct control of the program manager or security leadership. IAM is spread across various operations and support functions inside companies and relies heavily on human resources and other departments to provide support. Processes like onboarding, profile management and off-boarding are typically not processes owned by IT or the security team, but are integral parts of the overall IAM program goals and maturity. The Non-Program Support items are meant to help security leaders and program managers figure out what is needed from the parts of the business they do not directly control or influence. Cross functional governance teams can be established to help provide a cohesive vision that will work for the organization as a whole, while meeting the security team's objectives.

Metrics, KPIs and KRIs

One of the most significant portions of the Identity and Access Management program framework is being able to research and deliver real metrics, such as KPIs and KRIs. As a program grows in maturity there is an undeniable need to report progress and success – measurement is one of the key parts of that message and reporting. But not every program reports the same things at every maturity stage. In response to this, our research team gathers and refines the various metrics, key performance indicators and key risk indicators that organizations across varying maturity and market segment produce and track – to help demonstrate progress and success – in order to provide those collective insights directly to you.

Optiv measures an organization's IAM maturity in detail across each of the core functional areas, in order to help understand current state and prioritize the roadmap approach.

Assembling the Program

Bringing the program together to support success during implementation phases involves a four-phase process – building an enterprise profile, assessing current capabilities, identifying desired outcomes and building out the strategy and roadmap for achieving the desired result.

Whether you are planning on building a program from scratch, improving an existing program or auditing an existing capability for maturity – the Optiv program framework approach provides ultimate flexibility based on research you can trust. Start with the end in mind and decide on the type of business-aligned outcome your organization wants to achieve. Once those goals are set, it's time to assess capabilities and identify gaps. Where there are gaps, Optiv's team is here to assist you in creating a prioritized, strategic roadmap to develop your necessary capabilities utilizing our research model to define the staffing, process and technology requirements to support your program development efforts. Because setting goals and starting is not enough, our model will assist you with identifying the most appropriate metrics, KPIs and KRIs to demonstrate progressive achievement and desired success.

Get started today, take the **free self-assessment** at app.snapapp.com/IAM_Assessment and let Optiv be your strategic advisor.

Research Principal
Rafal Los
Managing Director
Solution and Program Insight, Optiv

Program Expertise
Janel Schalk
Senior Director
Strategic Consulting, Optiv

Executive Sponsor
Bryan Wiese
Vice President and General Manager
Identity and Access Management, Optiv

1125 17th Street, Suite 1700
Denver, CO 80202
800.574.0896
www.optiv.com

Optiv is a market-leading provider of end-to-end cyber security solutions. We help clients plan, build and run successful cyber security programs that achieve business objectives through our depth and breadth of cyber security offerings, extensive capabilities and proven expertise in cyber security strategy, managed security services, incident response, risk and compliance, security consulting, training and support, integration and architecture services, and security technology. Optiv maintains premium partnerships with more than 350 of the leading security technology manufacturers. For more information, visit www.optiv.com or follow us at www.twitter.com/optiv, www.facebook.com/optivinc and www.linkedin.com/company/optiv-inc.

5.17 | F1