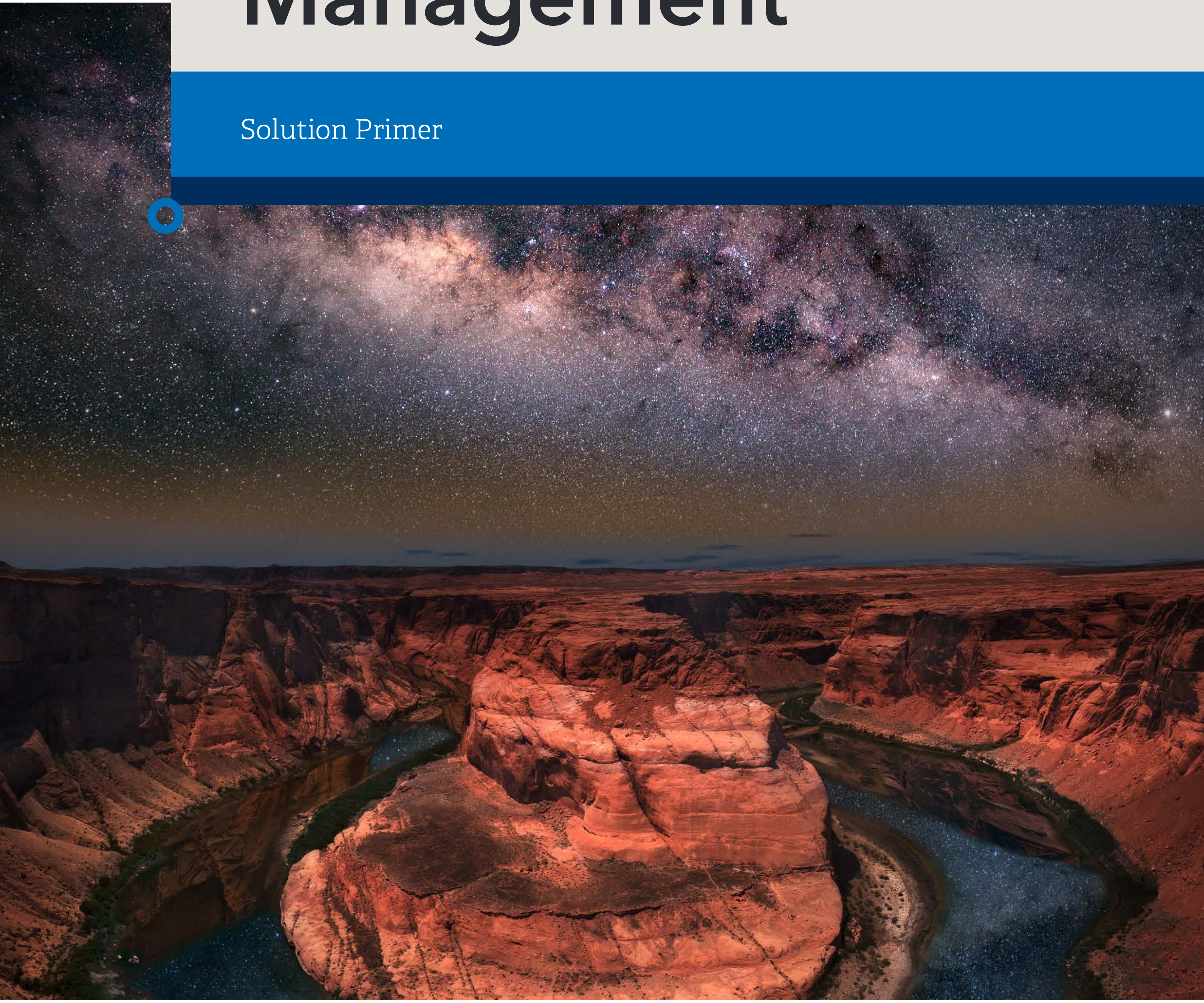
Identity and Access Management

Solution Primer



OPTIV

Executive Summary

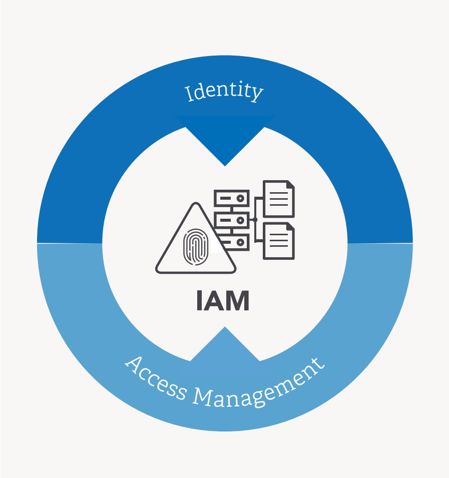
Identity and Access Management (IAM) is so difficult, because it "touches everything." It's a consistent message from CISOs across the country. To make matters worse, the enterprise perimeter is dissolving, compliance mandates are becoming increasingly detailed, intellectual property is going digital and there is a persistent risk of data theft. Failing to address these emerging realities with a holistic strategy cripples security performance, increases IT overhead, and adversely affects profitability.

IAM presents a broad range of capabilities and technical functions, when coordinated, protect the data that organizations care about the most. The transformation of IAM teams from keepers of the user lifecycle process, to leaders in providing security program maturity requires the automation of routine tasks, new skillsets developed through hiring and training, and maximizing technology investment through gains in maturity.

The path to maturity goes well beyond IAM technology investment alone. It may not require a new team of people, but it will at least require a coordinated plan, as well as a set of recurring processes. Managing IAM-related roles and processes. can offer a portable control set, ready to protect your organization wherever your critical assets reside.

Program Clarity

The scope of this research addresses IAM from a security program development perspective. Using IAM maturity to benefit the wider information security program, such as what is suggested by Identity Defined Security™ (IDS) research, is a related issue but not heavily addressed here. Also, IAM can include three main sets of relationships between an organization and its stakeholders: business-to-business (B2B), business-to-consumer (B2C), and business-to-employee (B2E). This research focuses on B2E relationships, but many of the concepts and maturity gains can be applied to these other relationships.



We define IAM for the purpose of this research as follows:

Identity management:

The processes, people and technology used to create the assertion of a unique identity for a user or system based on a set of credentials, identifiers and attributes.

Access management:

The controls that enable organizations to dynamically specify which users or systems can access other systems or facilities, what resources those users or systems can access, what operations they can perform, and what accountability is required for their actions.

Program Strategy Approach

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

Unlike most security related programs, IAM technology decisions in the context of IAM should always be focused on the solution's ability to solve business problems. With IAM, the associated business problems are not only to cut cost but to facilitate the execution of strategy and enhance user experience.

In shaping the IAM program, each of the following five functional elements should be addressed: 1) Program Governance 2) Identity Management 3) Identity Data Management 4) Access Governance, and 5) Access Management. In the following pages, we will further define, explain, and recommend steps to mature all five of these functional elements. In short, they can be understood as follows:

1 **Program Governance** — The oversight and risk management functions related to the IAM program. Roles associated with governance inform strategy creation, program direction, stakeholder communication and risk posture analysis.

2 **User Administration** — The consolidation and standardization of processes related to user lifecycle management, access request management and password management.

3 **Identity Data Management** — The consolidation, control and use of data related to identities and includes the architecture of identity stores under various deployment models.

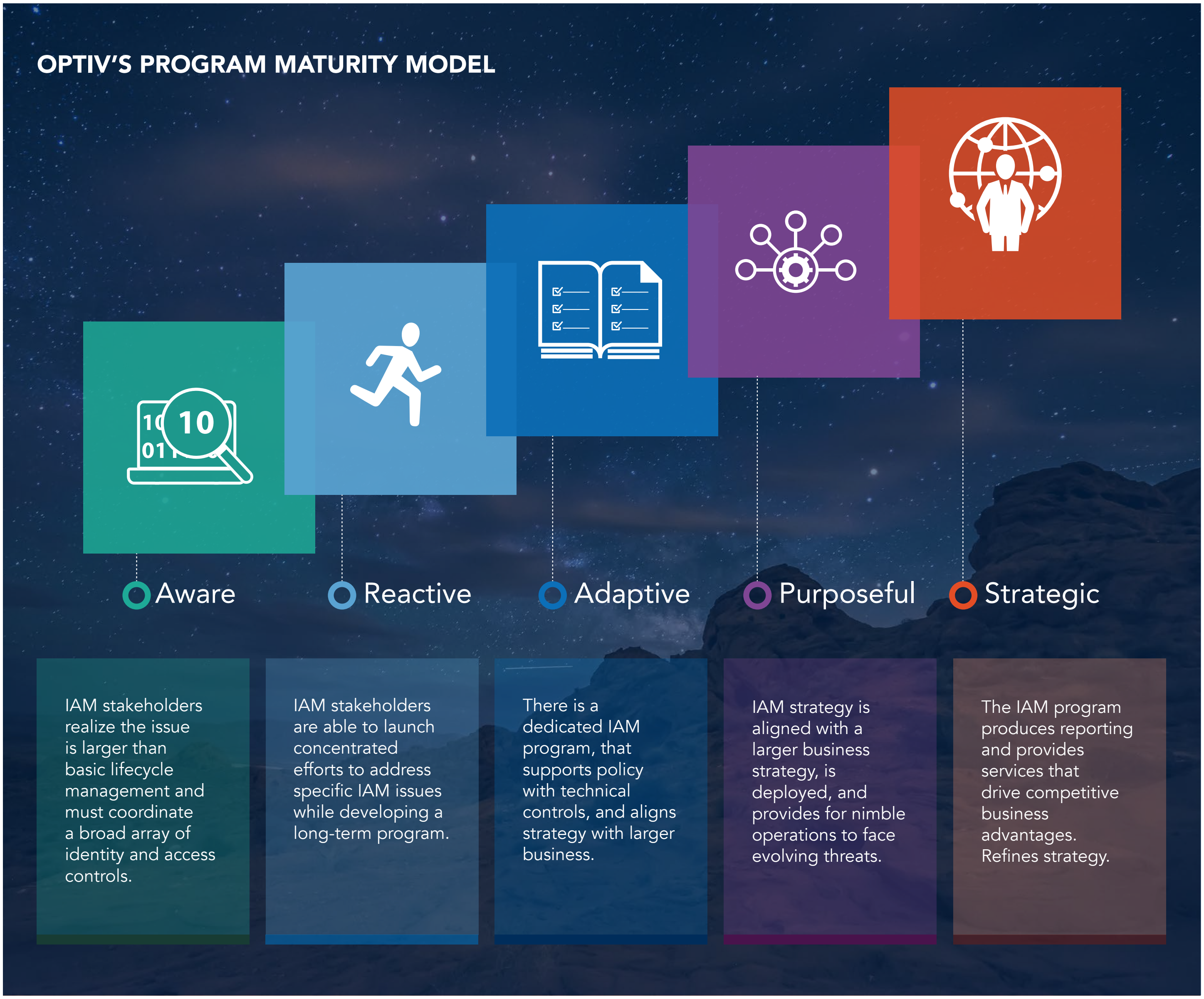
4 **Access Governance** — The development of flexible, yet effective roles, implementing risk-based decisions about access control, access certification, segregation of duties and access reporting.

5 **Access Management** — The execution of access governance at run time, using various architectures and protocols to enforce access governance under a variety of deployment models.

Model Driven Program Development

A properly constructed maturity model is built around outcomes, helps organizations to understand their current level of maturity, and aligns future state guidance with realistic, business-aligned capabilities. In order to understand the areas of focus, they must first understand the problem they are trying to solve and their own capabilities, resources and business climate.

The Optiv enterprise security maturity model is split up into five phases, based on unique characteristics and outcomes. The maturity model is linear in progression in that each maturity phase builds upon the accomplishments and outcomes of the previous.



OPTIV'S PROGRAM MATURITY MODEL

Aware

IAM stakeholders realize the issue is larger than basic lifecycle management and must coordinate a broad array of identity and access controls.

Reactive

IAM stakeholders are able to launch concentrated efforts to address specific IAM issues while developing a long-term program.

Adaptive

There is a dedicated IAM program, that supports policy with technical controls, and aligns strategy with larger business.

Purposeful

IAM strategy is aligned with a larger business strategy, is deployed, and provides for nimble operations to face evolving threats.

Strategic

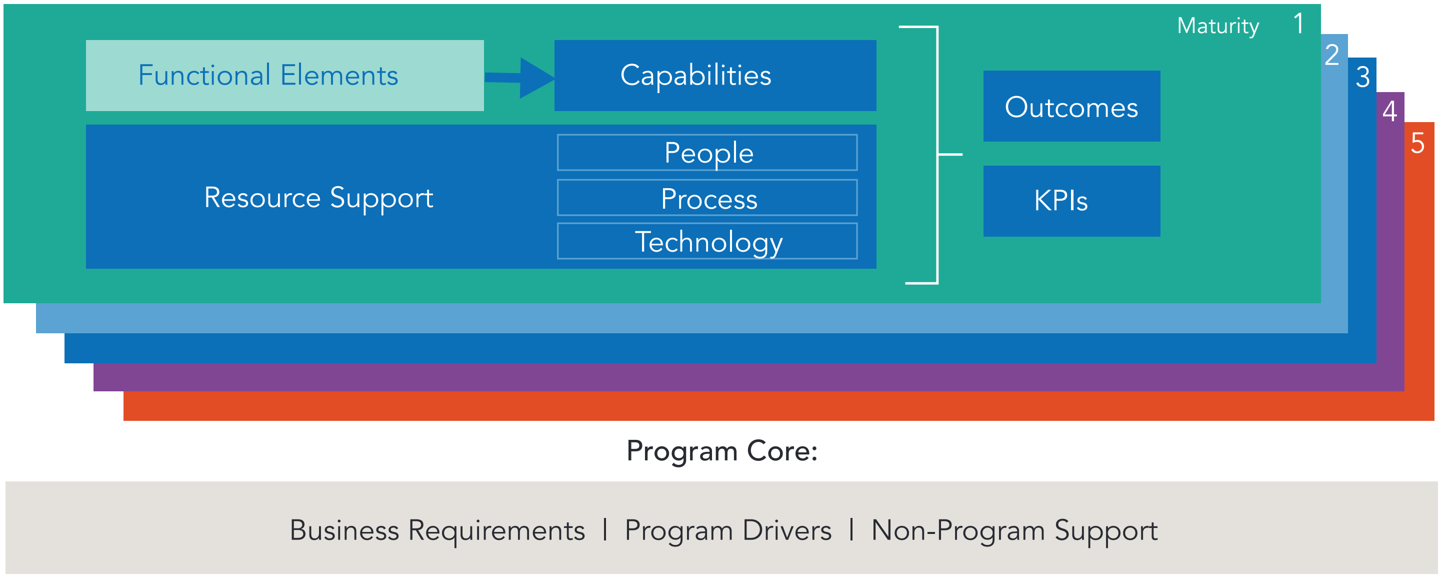
The IAM program produces reporting and provides services that drive competitive business advantages. Refines strategy.

Model Driven Program Development

Program Core

Defining business requirements means The Optiv Solutions R&D maturity model is built with two primary components. The **program core** which makes up the base of the overall model across all maturity levels and the **functional maturity level** that describes the effectiveness of the maturity level and its attributes. The **program core** is made up of three key elements – 1) drivers, 2) business requirements, and 3) non-program support.

Each **maturity level** is made up of five attributes – 1) functional elements, 2) resource support, 3) capabilities, 4) outcomes and 5) KPIs. These define the attributes of each maturity level and provide the building blocks to understand, build and measure desired outcomes at each maturity level based on industry-leading practices and field research.



Business Requirements

The business requirements establish the relevant, vetted business requirements from key stakeholders driving the creation of the program guidance. The key question to ask is "What are the stakeholders expecting of this program?" Another way to look at program requirements is to ask the question: "What are the goals?" Below are likely business requirements:

- Desire for more integration of current IAM resources
- Desire for an IAM program that enables key business functions at acceptable cost
- Risk management capability that balances access needs and control requirement

Program Drivers

These program drivers are the reason(s) for the investment of company resources to define, design, deploy and mature the program. The key question we answer is "What business factors or forces are driving the organization to develop this program element?" Another way to look at program drivers is that they answer the question: "Why are we building this program?" Below are likely program drivers:

- An internal or external security incident with IAM implications
- Audit concerns and findings
- Lack of internal skills or time to effectively manage IAM projects with current maturitys

Non-Program Support

Non-program support addresses the support infrastructure that is outside the program purview, but is still critical to the development of the program. The key question to ask is "What is needed from the business in order to succeed?"

For IAM, these vital stakeholders will likely include:

- Human Resources
- Service Management Managers
- Role Owners
- Resource Owners
- Security Operations Managers
- Mobile Device Managers
- DLP Program Managers

Model Driven Program Development

Outcome-Oriented Program Development

The outcomes described below outline what the IAM strategy is trying to achieve broadly. These are the executive, high-level operating goals of each maturity level. The Optiv maturity model focuses on outcomes because these outcomes are what will ultimately define success for the business overall.

Outcome	Description
Communicate Need	Ability to raise awareness and inspire action related to IAM strategy objectives.
Coordinate Resources	Ability to maximize the use of existing resources so that processes don't duplicate efforts.
Provide Control	Ability to implement a strategy that provides the desired risk posture.

Relating Outcomes to Maturity

Maturity Level	Communicate Need	Coordinate Resources	Provide Control
Aware	Governance and measurement are unstructured.	Governance and measurement are unstructured.	Potentially unreliable identity data, variable accountabilities, multiple authoritative identity stores. Access is managed informally and according to each application.
Reactive	Strategy developed with aid of executive sponsorship, focused on comprehensive coverage of IAM program scope.	Broad set of stakeholders engaged in order to manage IAM-relevant resources across the business.	Process and policies are defined, but uneven deployment and enforcement. Identity data and access still variable.
Adaptive	All stakeholders receive reporting and provide insight on the status of strategy deployment.	Governance and measurement strategy implemented, focused.	Policy and process supported by standard technical controls. Identity data stores.
Purposeful	Governance and measurement strategy fully operationalized across business.	Broad stakeholder group focused on refining processes, establishing risk tolerances and enhancing program communications.	Centralized infrastructure leveraged to standardize controls. Technical controls mature to automate governance of identity data and access.
Strategic	Governance and measurement strategy refined to provide executive-level reporting on adoption and basic measurements.	Reporting aids future decision-making and converge, access is centrally managed.	Technical controls mature to automate governance based on dynamic risk posture. Identity and access is managed in a variety of deployment models.

Functional Elements – Building Blocks of Program Development

Functional elements are the categories of capabilities needed for any given program at each maturity level in order to reach the desired outcomes. While each maturity level is made up of the same functional elements (the operational pieces of the security program), different functional elements may be activated at different maturity levels. Not all functional elements, even though present, will be evident or the focus of every maturity level.

Functional Element	Description
Governance	The oversight and risk management functions related to the IAM program. Roles associated with governance inform strategy creation, program direction, stakeholder communication and risk posture analysis.
Identity Management	The consolidation and standardization of processes related to user life-cycle management, access request management and password management.
Identity Data Management	The consolidation, control, and use of data related to identities include the architecture of identity stores under various deployment models.
Access Governance	The development of flexible, yet effective roles, implementing risk-based decisions about access control, access certification, segregation of duties and access reporting.
Access Management	The execution of access governance at run time, using various architectures and protocols to enforce access governance under a variety of deployment models.

Assembling the Program

Enterprise security organizations' need for management and governance of user identities and privileges has never been greater. As the consumerization of IT continues to evolve and the enterprise IT environment becomes more fragmented and distributed, sufficient protection is obviously not going to be provided by perimeter-centric security programs alone. The risk of data loss and security breaches increases the pressure on security organizations to quickly respond and adapt.

Taking a focused approach to IAM allows organizations to enable new technologies while maximizing legacy solutions and increases the likelihood that IAM will evolve to help achieve business goals and achieve desired protections in a highly decentralized infrastructure and data environment.

Taking a holistic approach that safeguards critical data, systems, and applications goes well beyond IAM technology investment alone.

Setting up for IAM maturity gains may not always require a new team of people, but it will at least require an investment of time and resources coordinated through a strategy. A set of recurring processes will need to be managed by and a stakeholder group dedicated to creating more confidence in a highly connected world. **The result of this IAM strategy can be the positioning of IAM as a pillar of the entire security program and help the business remain nimble and maximize its most precious assets; its people and innovations.**

Want to learn more?

Insight on IAM is an ongoing series of thought leadership at Optiv. Click the links below to download other corresponding materials on the subject.

OPTIV

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.

Supported at Every Level with People, Process and Technology

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 Service Guide

Heath Nieddu
Senior Research Analyst, Solutions Research and Development
Office of the CISO, Optiv

Key Contributor:
Robert Block
Vice President of Strategic Solutions, IAM
Optiv

OPTIV

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

Optiv is the largest holistic pure-play cyber security solutions provider in North America. The company's diverse and talented employees are committed to helping businesses, governments and educational institutions plan, build and run successful security programs through the right combination of products, services and solutions related to security program strategy, enterprise risk and consulting, threat and vulnerability management, enterprise incident management, security architecture and implementation, training, identity and access management, and managed security. Created in 2015 as a result of the Accuvant and FishNet Security merger, Optiv is a Blackstone (NYSE: BX) portfolio company that has served more than 12,000 clients of various sizes across multiple industries, offers an extensive geographic footprint, and has premium partnerships with more than 300 of the leading security product manufacturers. For more information, please visit www.optiv.com.