protiviti®
*Face the Future with Confidence*

# Five Common Identity and Access Management Pitfalls

Identity and access management (IAM) is at the forefront of each organization's overall security strategy. Effective organizations ensure that regulatory compliance and risk management drivers are balanced with business-friendly and effective processes in order to provide users with access to the right resources at the right time.

Organizations that struggle with IAM often do not treat it as an ever-living component of their business. Too often, IAM needs are handled as one-off IT security initiatives due to specific triggers, such as closing an audit finding or improving on a particular business inefficiency. Mature IAM capabilities help meet the demands of initiatives from business and application teams and can potentially reduce costs associated with managing identities and access.

Organizations that treat IAM as a project or series of projects, rather than an ongoing internal service offering, often face issues such as a lack of long-term executive sponsorship, ownership for ensuring the continuous improvement of IAM services and focus needed from multiple parts of the organization to solve complex IAM problems. Performing one-off IAM initiatives may close gaps in the short term, but doing so leads to decentralized services and potential resurfacing of root causes. Organizations should establish an internal services team or organization with the mission to continuously improve IAM services to better serve business needs pertaining to risk, compliance, efficiency and competitive advantage to achieve the long-term benefits from the investments made in managing IAM.

In this paper, we discuss five common IAM pitfalls organizations run into today: lack of an effective operating model, lack of meaningful metrics, lack of an IAM roadmap, insufficient business analyst involvement in IAM and technology as the primary focus of IAM investment.

## 01 Lack of an Effective Operating Model to Ensure Organizational Alignment to Continuously Improve IAM Services

A fundamental mistake for organizations when handling security needs is performing individual, one-off projects to address IAM concerns. Individual projects often lack centralized leadership and provide only temporary solutions to the issue at hand. While a one-off initiative may temporarily close a pointed gap for a specific business area, it may not always align with the enterprise IAM program vision.

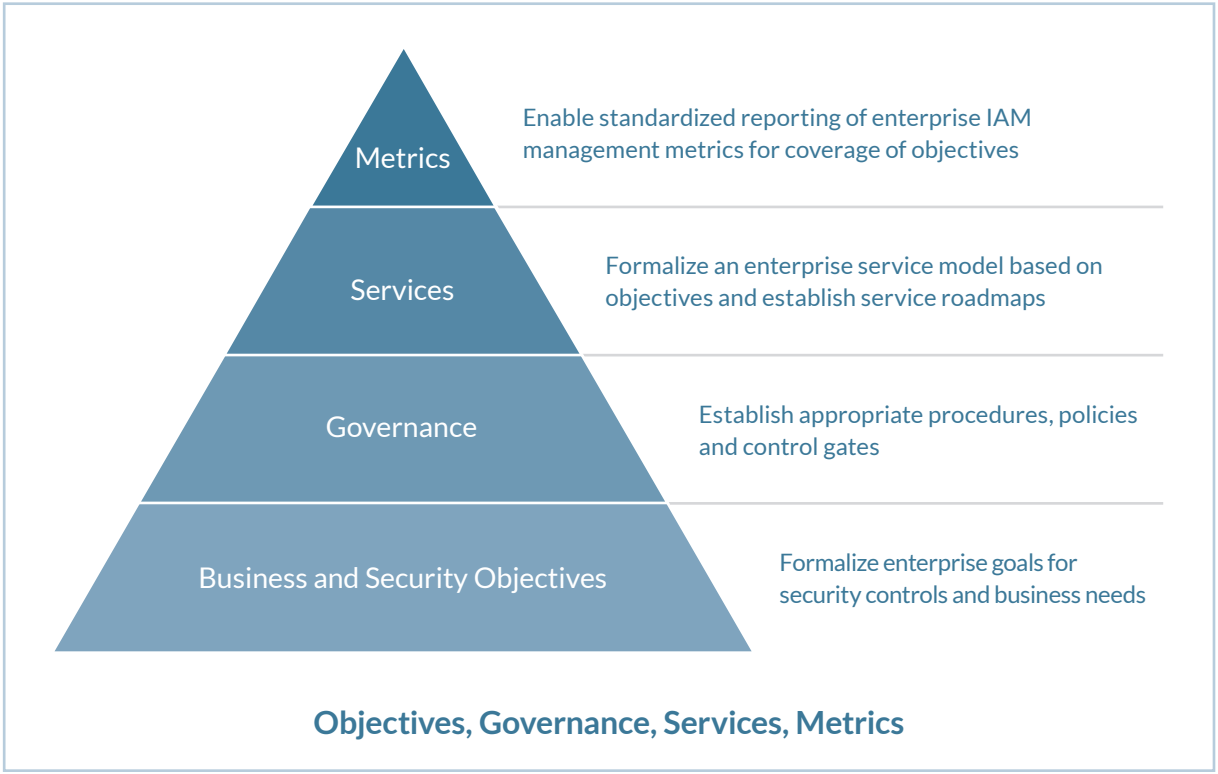
A successful organization treats IAM as an ongoing internal service to the organization. Setting up an IAM operating model, along with a dedicated internal services team, helps establish IAM as an ongoing service, manage demand from the business and IT, prioritize initiatives, and gauge IAM progress and maturity. An IAM operating model consists of four elements: formalizing enterprise goals and control objectives; establishing procedures, policies and control gates to drive governance; formalizing an enterprise service model; and standardizing reporting of enterprise IAM management metrics.

## 02 Lack of Meaningful Metrics

Many organizations lack defined metrics that report on the status and maturity of an IAM environment, such as enterprise service usage and enterprise control objective compliance. Successful IAM programs put focus on common business and security control objectives. The IAM team must work with the business, risk and compliance, and IT teams to define business objectives that will meet the demands of application teams, HR and other business units. Similarly, aligning security control objectives with industry frameworks, such as NIST and ISO, helps define control objectives. (See the first layer of the operating model in Figure 1.)

With these enterprise objectives, an IAM program will be able to effectively report on current status, work in progress and what still has to be done. Executive- and board-level utilization of compliance and coverage metrics will enable better decision-making around investments at tactical and strategic levels and will demonstrate how risk and operational effectiveness are being addressed. Having the ability to measure the progress of IAM initiatives against these objectives is

### Figure 1: Protiviti IAM Operating Model



paramount in helping manage the program and deliver services across the organization to drive risk reduction, regulatory compliance and business efficiencies.

Coverage metrics help show conformance to enterprise goals and compliance progress by risk level. Business-objective coverage metrics serve to show progress toward meeting business needs throughout the organization, and they tell you which applications are using IAM services and identify gaps in your IAM efficiency. Control-objective coverage metrics, on the other hand, serve to show compliance of applications and systems against IAM control objectives. They tell you which applications are compliant with which control objectives and which risk levels are lagging behind with control compliance.

Performance metrics provide transaction-level reporting to measure efficiency of services and projects. They tell you which IAM services are being used effectively and where improvements can be made to IAM systems or processes.

## 03 Lack of an IAM Roadmap with Effective Ongoing Demand-Management Practices

Organizations often lack mature roadmaps, creating point-in-time roadmaps but not actively managing or working from them over time. (In other cases, organizations lack a roadmap at all.) A point-in-time roadmap does not accurately reflect ongoing or completed projects, recently adopted technology, or other dependencies. Without a continually updated roadmap, an organization's IAM team provides limited demand management and reacts to business needs only as they arise. The lack of demand management leads to IAM investment that is not aligned with true business needs. In order to make the roadmap effective, a demand-management function is needed.

Organizations should look to invest not only in updating a roadmap but also establishing the ongoing demand-management capability to keep the roadmap refreshed over the long term. Managing IAM can be significantly improved with the continual refresh of a mature roadmap that accounts for initiatives in process and governance, enhancements to existing services, and establishment of new services. A roadmap needs to be actively maintained and used to guide initiatives.

Different IAM services should have product managers in place to manage the lifecycle of the service. A product manager is responsible for the management and demand of his or her particular IAM service and managing inputs to the broader IAM roadmap. The manager becomes a key stakeholder involved in maintaining the overall IAM roadmap and works closely with the team delivering IAM services.

## 04 Insufficient Business-Analyst Involvement in IAM

Organizations often hire technical staff who lack experience in requirements gathering or managing identity services to implement IAM systems. Although technical staff are needed to deploy and maintain the technology, lack of business analysts with IAM teams results in ineffective system deployments that often do not solve the root cause of business needs. Successful IAM programs look to invest in business analysts who work with the business to understand the issue at hand and work alongside technical staff to implement and manage IAM services.

It is important for organizations to have IAM staff who understand how to interface with the business to solicit and document requirements, support testing, and provide education and awareness (training). Good business analysts understand identity and access lifecycles, know how to interface with nontechnical business stakeholders, and work efficiently with the product manager and technical staff.

A business analyst also helps manage the demand pipeline for IAM services and conduct ongoing demand-management activities with business and IT stakeholders. He or she has the ability to understand the needs of applications and identify whether business and security control objectives can be met using existing services, or whether additional investment may be required. The addition of business analyst personnel significantly improves the effectiveness of an IAM program and its ability to provide services to meet business needs.

## 05 Technology as the Primary Focus of IAM Investment

Finally, when IAM issues arise, organizations often lean too heavily on implementing technology with the idea that it will solve all issues related to identity and access. This leads to short-term solutions with an incomplete understanding of the real business need and accompanying requirements, and issues often resurface. Organizations investing too heavily in technology often have a limited view on the overall business value of IAM initiatives and thus struggle to realize maximum gains. Successful IAM programs look to focus efforts on the strategy, process and governance of an IAM program first, then tackle technology with all the right requirements in place.

Effective process and governance helps remediate elements outside of technology, such as organizational structure, risk management, and standard procedures and processes. Complying with existing IAM standards, such as managing privileged accounts through an enterprise IAM tool, can be enforced without the use of technology by utilizing existing enterprise gates, like change management processes, release management or a system development lifecycle. Root problems often lie within the process and governance in place (or the lack thereof), which make up organizations' IAM. Increasing the focus on establishing IAM methodologies and governance frameworks, reengineering processes, improving standards, and employing playbooks will have long-term benefits to organizations.

## How Protiviti Can Help

Protiviti has proven IAM methodologies and frameworks to help organizations avoid common IAM pitfalls and establish IAM as an ongoing service. These frameworks include setting up an operating model, establishing business and security control objectives, developing key metrics, establishing and maintaining a roadmap, and prioritizing investments to reach a mature IAM environment and long-term goals.

## Contacts

**Todd Musselman**
+1.972.489.3532
todd.musselman@protiviti.com

**Matthew Kotraba**
+1.703.299.3503
matthew.kotraba@protiviti.com