Achieving cost efficiencies in Identity and Access Management

CISOs are seeking opportunities to contain the costs of their cyber security programs. This follows a period of significant investment in cyber security, during which organizations rapidly matured their cyber security capabilities to maintain pace with the evolving threat landscape. The transitioning of funding, from investment budgets into operational budgets, has resulted in greater scrutiny on program operational effectiveness and efficiency.

The urgency of cost takeout has recently been exacerbated by the COVID-19 global lockdowns. Many businesses have experienced a significant drop in sales, and are now struggling to manage their cost base. Businesses must streamline their operations and cyber security programs cannot expect to be shielded from this—despite the rise in fresh threat vectors associated with virtual working and the emergence of some opportunistic adversaries.

A core component of all cyber security programs is Identity and Access Management (IAM). Over the past few years, significant investments have been made in this space—resulting in regulatory pressure, incidents involving inappropriate access rights, and CISOs effectively articulating the commercial benefits of a leading IAM capability. This investment has taken various forms but typically involves buildout of tooling and processes. In many instances, this expansion was done piecemeal (an inevitability associated with annual budgetary processes). Wherever there is fragmentation, unnecessary complexities, or underutilized resources in the IAM capability, there is opportunity to create efficiencies.

This paper focuses on three incremental approaches to cost rationalization:

1. **Operational enhancement.** This involves stitching together historically tactical initiatives to create a more strategic approach to managing IAM.
   - *Example levers: Tool rationalization, organizational rightsizing, and selectively engage Managed Service Security Providers (MSSP)*
2. **Process automation.** This entails the focused use of technology to accelerate tasks that are currently performed manually.
   - *Example levers: Workflow automation, user entitlement automation*
3. **Continuous improvement.** This approach draws on kaizen, the Japanese philosophy of continuous improvement. In the digital age, this often means managing costs while simultaneously improving speed, accuracy, and control.
   - *Example levers: Role engineering, Risk-based entitlement management*

Note that these levers should not be viewed in isolation. For example, organizational rightsizing is unlikely to be achieved without an increase in automation.

It is crucial that cost takeout initiatives do not result in threat exposures. Clearly, preventative capabilities have a significantly lower financial impact than the impact of a cyber security incident. Large enterprises, which may typically spend $4 million annually on cyber security awareness training, will find this well below the $13 million average cost of a data breach.

Operational enhancement
As organizations have built out their IAM capabilities, they will inevitably have taken a number of tactical steps to address immediate business requirements or unanticipated emerging threats. Operational enhancement requires CISOs to reevaluate their IAM capability with a strategic lens. Outlying processes and tools may prove superfluous to requirements—and provide the opportunity to achieve cost savings.

How to identify opportunities for operational enhancement?

When processes and tools are deployed in silos, there is a risk that overlaps will inadvertently have been developed. Mapping process flows and tooling specifications may illuminate overlaps in the IAM capability, which can be rationalized as part of cost-cutting initiatives.

Similarly, there may be some overlap in the specific roles that IAM resources perform. For example, different people and teams may duplicate the execution of controls and the completion of assessments. This is typical when certain IAM roles or functions are duplicated across lines of business.

This can be solved by analyzing and restructuring the organizational structure to pull capabilities back into centralized functions (or geographic locations).

Some organizations may find themselves over-reliant on IAM resources in higher cost locations. Offshoring job roles creates an opportunity for labor arbitrage.

Conversely, pivoting in the opposite direction—i.e., towards a slimmed down higher cost, higher skill IAM resource base—may enable the achievement of cost savings when combined with a concerted technology uplift. This becomes particularly relevant where IAM resources responsible for task monitoring, tool maintenance, access review support, etc. have been offshored to a country which has since experienced wage inflation.

At the end of the spectrum, some organizations may seek to move to a manged services model for common IAM operational processes. Managed service providers deliver on an outcome-based model, and this enables organizations to be flexible in their volume of IAM related tasks.

How can operational enhancement takeout costs?

Taking a strategic lens to the existing IAM organization enables CISOs to focus on the actual business need and threat exposure. In this way, the IAM strategy can be embedded into the broader operational strategy.

Converging siloed capabilities and processes for example, enables deeper streamlining of the IAM organization and limits spend overlap. Similarly, optimizing solution deployment enables organizations to limit licensing spend on unutilized features.

How have we helped clients enhance their IAM operations?

Tool rationalization
We have worked with clients to review the product specifications of their IAM tools. In this way we have identified (1) unused functionality, (2) overlapping functionality, and (3) incomplete rollouts. In some instances we have observed that clients may be utilizing as little as 10 percent of their tool's functionality such as rolling out a solution to act as the Identity Repository and Access Certification launcher without fully utilizing its Access Request, Approval, Provisioning and Advanced Analytics potential. We have also delivered gap analyses on existing specifications against industry-leading specifications, to demonstrate where there is room for enhancement.

Organizational rightsizing
We have analyzed IAM roles and responsibilities to identify opportunities for convergence. We have also benchmarked organizational structure against peer organizations of a similar size and risk profile to identify efficiency opportunities.

To enable a more flexible IAM organization, we have supported clients with Identity-as-a-Service strategy and implementation. Identity-as-a-Service provides clients with on-demand, precisely targeted, plug-and-play solutions that provide increased agility and flexibility to organizations.

Managed services delivery
We provide managed services across vendors and solutions by an experienced team. Our approach could reduce operational costs by 10–30 percent and move the headache of resource management to KPMG.

We also provide an outcome based model based on executing activities for a predicable monthly fee versus paying for resources.

KPMG

Process automation
The flow of IAM processes does not necessarily require fundamental reorientation to leverage the benefits of leading IAM tools. Often organizations are saddled with manual processes that have calcified into business-as-usual workflows with numerous manual steps. Identifying these repetitive tasks and automating them frees up human time and intellectual capital, so they can focus on the issues that truly introduce risk to the organization.

How to identify opportunities for process automation?

Organizations often fall into operational patterns that, over time, become business as usual. When people new to the organization look at a process and ask, "Why do we do things that way?" there is a good chance they have recognized an inefficiency that can potentially be automated.

Processes that are candidates for automation include workflows that are conducted the same way, every time, with no variation, but still require some type of intervention by a person or software.

When the outcome is always identical, the intermediate steps can be automated as much as possible. Today's leading IAM tools have deep functional capabilities that include scripting, rules engines, conditional workflow, and connectors to applications and APIs—these features can be leveraged to automate repetitive activities , for example Cloud Identity Governance and Access Management.

How can process automation take out costs?

The largest advantage to automation is the time saved by an organization on manual processing of steps in a workflow. Consider an example of an IAM analyst that needs to manually add user entitlements for an application. These manual processes add up to hundreds of hours in a year where the analyst could be focusing on application onboarding, but instead completes the same task over and over again.

If there is enough workload, perhaps the organization requires additional headcount just to make sure there is enough capacity to complete the repetitive activity, as well as anything else that arises. If there is some exigency that must be handled, it is also possible that the repetitive task gets delayed—if the task could be automated, however, the organization could be assured in its completion, on time.

In addition to saving of time (and potentially headcount) from automation, organizations benefit from reducing mistakes from manual errors. If incorrect access is provisioned or deprovisioned, then there is lost productivity while the mistake is corrected and the impacted employee is unable to complete their normal job role.

How have we helped clients automate their IAM processes?

Workflow development
We have worked with clients to consider the often underutilized technical automation capabilities of their existing IAM tools in the context of their IAM workflows. We analyze where buttons are clicked, phones are called, emails are sent, and tickets are generated—determining where and how we can automate those tasks with the tools they already have. By doing so, we can save time, reduce mistakes, and reduce the need for "human APIs".

User entitlement automation
We have reviewed user entitlement review programs and organizational roles with clients to help determine where risk is concentrated in the organization. Too often, managers spend hours downloading, reviewing, clicking, and emailing approvals for the same very-low-risk entitlements for more than one of their direct reports.

We have helped identify these very-low-risk roles and entitlements, grouping them together in easy-to-view summary that can be easily approved once or auto-approved depending on conditional logic. What used to take managers hours can now be completed in minutes, enabling a focus on the true risk areas.

KPMG

Continuous improvement
Organizations may enhance processes and also may automate them in one-off initiatives. But what if they continually reviewed how well processes operated—always training an eye on inefficiency and encouraging everyone involved in a process to identify where time is wasted or mistakes are made? This is the core of "Kaizen"—a Japanese philosophy of continuous improvement.

How to identify opportunities for continuous improvement?

Organizations often launch initiatives to enhance or automate their processes. Typically, these projects are one-offs, and although perspectives may be solicited from the employees conducting the activities, after the project has ended the process returns to a static state (even if it has been much improved).

With continuous process re-engineering, the process improvements are never static. Instead, employees involved in the process are empowered to raise their hand when they identify an inefficiency. Their feedback, comments, pain points, and ideas are tracked and actioned throughout the year.

Continuous improvements may be changes in workflow steps, reduction of duplicative activity, or automation of repetitive tasks. Any process can benefit from continuous re-engineering as long as management provides full support for enabling employees to help improve the process.

How can continuous process improvement takeout costs?

Because continuous process re-engineering has no end state, the costs of lost productivity due to inefficient use of time or mistakes can be reduced throughout the year instead of just once during a top-down initiative.

When end users, IAM practitioners, and managers are all empowered to look at a process with a critical perspective, organizations get the benefit of diverse experiences and thought patterns—yielding innovative solutions that can be celebrated in the organizational culture as changes for better.

When machine learning and sophisticated cognitive solutions are also leveraged for their analytical horsepower, decision-making for continuous improvement is further supplemented.

How have we helped clients continually improve their IAM processes?

Role engineering
We have worked with clients to implement continuous role engineering programs, where advanced IAM solutions can actively monitor and report on combinations of roles that are underprovisioned, overprovisioned, or not used at all. Combined with regular stakeholder workshops, the role analytics can keep the available roles streamlined and effective—reducing entitlement sprawl, provisioning confusion, and residual risk from over-permissive roles.

Risk-based entitlement management
We have worked with clients to evaluate their entitlement management programs from a risk-based perspective. We first use stakeholder interviews combined with cognitive analytics tools to obtain a baseline of where the highest-risk entitlements are concentrated. Concurrently, we work with business unit leadership to understand how critical processes are actioned (and what the risks are from inaction or error).

Once our risk baselines are established, we can begin to dynamically trigger workflow based on risk events, for example, new joiners, changes in role, changes in data classification handled by an app, or changes in role combination. Typically entitlement review would occur on a scheduled basis, but with continuous process re-engineering, we can help clients manage risk every day—not just once a quarter.

100-day plan

1–30 days: Raise awareness, align functions, and mobilize resources, including a strong sponsor

— **Engage and align expectations:** Raise awareness across the enterprise of the need for cost-focused change in IAM, and define who will lead the charge.

— **Identify existing transformation initiatives:** Consider all existing IAM programs to reduce any business disruptions.

— **Identify your change evangelists:** A core, blended delivery team is essential in establishing the tools and methods that will enable your IAM change program.

30–60 days: Assess initial opportunities and conduct a proof of concept.

— **Decide on a methodology, from assessment to deployment:** Agree on a methodology that will work in your organization to assess opportunities for achieving cost efficiencies.

— **Create a matrix for assessing and prioritizing transformation levers:** This will help you identify quick wins and deliver value early using predefined prioritization criteria.

— **Conduct a technology capability assessment:** Review the existing technology landscape in detail to prepare your infrastructure.

— **Define your target IAM operating model:** Agree on how you will structure your IAM capability.

60–100 days: Assess proof of concept results, define your framework, and build a roadmap to begin development at scale.

— **Define and start building your IAM Center of Excellence:** The new digital operation will require a framework for governance and change.

— **Deploy a proof of concept to assess suitability:** Test to see whether the initiative is fit for purpose, robust, and scalable across your IAM function.

— **Deploy infrastructure requirements:** This will become a critical element to move into production at scale, beyond the first 100-day period.

— **Develop an adoption roadmap:** Outline what your automation journey looks like based on your defined case for change and business priorities.

— **Define and manage a baseline for outcomes:** Build a baseline of outcomes delivered per month and adjust if needed prior service level objectives are enforced.

KPMG

Connect with us

Jim Wilhelm
Principal, Cyber Security Services
T: 215-913-8440
E: jameswilhelm@kpmg.com

Debbie Patterson
Alliance Senior Director
T: 512-423-6150
E: deborahpatterson@kpmg.com

Some or all of the services described herein may not be permissible for KPMG audit clients and their affiliates or related entities.

kpmg.com/socialmedia