THE BUSINESS VALUE OF IDENTITY AND ACCESS MANAGEMENT

ABSTRACT

This white paper explains the types of business value that a well-run Identity and Access Management (IAM) program can provide. First it explains the functional components that typically make up an IAM program, and then it explores how each of them can contribute value to the line of business.

RSA

INTRODUCTION

In recent years, Identity and Access Management (IAM) solutions have increased in maturity and scope, and information security practitioners have grown in their level of experience and expertise. As a result, we've witnessed many ways in which well-executed IAM programs have delivered benefits to enterprises, including improved compliance, increased security, and cost savings via automation of IT activities.

However, there's an additional angle to the value that IAM programs can provide, which forward-looking organizations have begun to place at the forefront of their IAM planning, evaluation, and program efforts: the business value that IAM can deliver to an organization. In this whitepaper, we'll explore the different types of business value that a well-executed IAM program will provide, and hopefully spark your thinking about how your organization could similarly benefit.

For the purposes of this whitepaper, we'll be exclusively focusing on the *qualitative* value that an IAM program can provide to the business. We're not taking a *quantitative* approach, or attempting to calculate the ROI of IAM – there are other resources available that do a good job of exploring, explaining, and modeling those.

BUSINESS VALUE

In general, modern IAM solutions not only help automate and streamline IT activities, but they deliver business value. They do so by helping the line of business (LOB) become involved in making access decisions, by making these access decisions simple for the line of business to make, and (yes) by automating IT activities behind the scenes. We'll explore some of the areas of business value in this whitepaper, but let's first define the scope of an IAM program, and the type of processes that it can help improve.

Today's IAM programs are typically scoped to be responsible for the much of the identity lifecycle – starting with creating (or detecting) a new user and provisioning their initial access, managing the addition (or change) of access while they're active, and removing their access at the end of their relationship with the organization. It also comprises security and risk-related areas, such as definition and enforcement of access policies, the administration of access reviews (also known as access certifications), and the operation of an Access Request portal, with an associated set of approval processes. The typical IAM program scope is summarized in the table below:

Functional Area	Description
Identity Data Collection	Collecting detailed data about users, accounts, roles, and application entitlements, and unifying them in a centralized identity store
Data Analytics (Identity Intelligence)	Providing visibility across this identity store – reports, dashboards, and analysis of identity-related status and trends
Access Reviews	The business process whereby supervisors review what access their team members have, and confirm (certify) that it's correct. Also refers to other types of reviews, such as reviews by application owners.
Policy Management	The ability to define policies (such as Segregation of Duties policies), to detect violations of policies, and to initiate remediation processes
Role Management	The capability to mine, define, and maintain roles, which consolidate entitlements into more easily managed chunks
Access Request Management	Providing users with an easy-to-use web-based portal for requesting new (or changed) access, as well as password resets. Behind the scenes, this element executes a request approval workflow, routing requests to the right person.
Provisioning	A system driven by the IAM business processes that executes changes to people's access in IT systems. Typically this will exercise application APIs, or make API calls into directory systems to make the access changes, automatically.

Given this broad functional scope, and the types of business processes we've discussed, it should be clear that there is plenty of opportunity for IAM to add business value. We'll explore some of the areas next.

ACCELERATING ACCESS REVIEWS

Access reviews are typically not anyone's favorite activity. Organizations are usually driven to perform them because they're required to do so by compliance or security guidelines. Although they clearly add value – and improve security, which everyone agrees is an important goal – they're typically viewed by the line-of-business as a task that must be endured. While a modern IAM platform won't push access reviews into the same league as, say, an enjoyable summer picnic, it can at least simplify, streamline, and accelerate the tasks.

Specifically, organizations can significantly reduce the amount of time and effort required to perform access reviews – often by 40-50% - while simultaneously improving their effectiveness. This will make everyone happy, and will free up line of business users' time for more valuable and strategic business activities.

ENFORCING ACCESS POLICIES

Access policies (also referred to as Rules) are an interesting area, since well-run IAM programs will define and enforce a mixture of security and business policies. From the line-of-business perspective, policies can help ensure smooth and reliable business operations. Security concerns aside, line of business managers and business application owners are typically very attentive to the rights that users have within key business applications, and how this access relates to their key business processes. Users with inappropriate levels of access can cause business problems with significant impacts. And as the LOB revises and changes business processes, which happens on an ongoing basis, they need to do so with the support of the underlying IT systems, and with correct changes to users' access.

ROLES

From a business perspective, roles bring a lot of benefits. Primarily, they simplify nearly all the business processes and line-of-business interactions with IAM systems. Whether performing an access review or requesting new access, everyone likes to work with a nice, chunky role (like "Financial Analyst Level 2", or "Clinical Technician 3"), rather than the typically dozens of fine-grained entitlements that comprise the role.

Specifically, when role are developed as a partnership between IT/InfoSec and the Line-of-Business, they can live up to their full potential – simplifying business tasks and improving the types of access that people, by ensuring that roles include all relevant entitlements, and exclude unnecessary ones.

ENABLING SELF-SERVICE ACCESS REQUEST

Access Request Management at its heart provides value to the line of business – enabling users to log in to a friendly web portal to request additional (or changed) access for themselves, or for people who work for them. And, since most requests for access will require manager or resource owner approval, it must also manage the routing and execution of these approval requests. Finally, it may also include self-service password reset capabilities, which clearly delivers value to all users, at least those of us who occasionally mix up our dozens of passwords.

While on its surface these may appear to be simple tasks, to do them well requires a solid foundation of IAM capabilities. Specifically, it requires broad visibility of user entitlements (and roles, if applicable) across all key business applications – if the request portal only includes a subset of key business apps, it'll diminish its value for users. It must also understand the organizational structure, and who has responsibility for which application resources, in order to properly route approvals to the appropriate people.

Ultimately, these access request capabilities are what underlie efficient and effective Joiner and Mover processes, which the lines of business execute every single day. A well-run access request system can, without a doubt, deliver substantial business value.

RELIABLY PROVISIONING USER ACCESS

Behind the business processes described above, there is some sort of provisioning system – or, at its most basic, a manual provisioning process. By provisioning, we mean the execution of changes to people's access within the underlying IT systems. This may constitute adding someone to a directory group, creating an application account, or adding/removing application entitlements from an existing user's account.

Clearly, there are significant IT benefits that are gained when this type of work is migrated from being manually performed to being automated. But how does that benefit the business? Actually, there are two reasons that the line-of-business might be interesting in encouraging IT to automate provisioning across all key business systems. First, automated provisioning is *faster* than manual

provisioning, which means that people's access changes happen faster. Whether adding new access for a new employee, or removing access for a departing employee, speed is critical. But the second reason is potentially even more interesting – automated provisioning is *more reliable* than manual provisioning. That is, these access changes happen at a predictable speed, and with a consistent level of quality. This ensures that business users will get precisely the access they need to be productive, in a predictable amount of time. That's definitely appealing to the business.

CONCLUSION

While IAM programs are typically fairly broad in scope – and potentially *very* broad in scope within more mature organizations – it should be clear that even at lower levels of maturity, IAM programs can deliver substantial business value. More mature IAM programs can help the organization achieve *business agility* – which can unlock huge business value. For example, it can give IT the ability to say "yes" to the LOB when they ask for something access-related, such as:

- Enabling partners to access a previously internal application
- Supporting a smooth federation between you and trusted suppliers
- Enabling an acquisition to be integrated quickly

Even for everyday activities, the business benefits that IAM can deliver are compelling: Imagine that hiring managers can request access for new employees, and have it correctly provisioned within 24 hours, every time. Imagine that new users automatically get all their appropriate system access, based on their job role. Imagine that all users remain in compliance with security and regulatory policies because the system continually enforces access policies, and prevents users from obtaining inappropriate access.

These are the kinds of benefits that organizations can obtain today, with a well-managed IAM program based on a modern IAM foundation. What kind of impact would this have on your business?