BUSINESS-DRIVEN IDENTITY AND ACCESS GOVERNANCE: WHY THIS NEW APPROACH MATTERS

ABSTRACT

For years, information security and line-of-business managers have intuitively known that identity and access governance (IAG) must be driven by business requirements. After all, business managers know best "who should have access to what." This white paper explains why taking a business-driven approach to IAG can enable organizations to easily prove compliance, minimize risk and enable the business to be productive.

TABLE OF CONTENTS

ABSTRACT 1

EXECUTIVE SUMMARY 3

TODAY'S REALITY: FAILED IDENTITY MANAGEMENT 3

THE IMPORTANCE OF BUSINESS CONTEXT 3

PHASED APPROACH TO BUSINESS-DRIVEN IDENTITY AND ACCESS GOVERNANCE 4

SUMMARY 5

EXECUTIVE SUMMARY

For years, information security and line-of-business managers have intuitively known that identity and access governance (IAG) must be driven by business requirements. After all, business managers know best "who should have access to what."

But all too often, organizations' tools and processes don't reflect this "business context." These systems typically lack support for a business view of users' access and their business roles and responsibilities. They also generally don't reflect fine-grained entitlements that determine specifically which actions users may take within applications. This is usually due to organizations attempting to use technical, IT-focused identity and access management (IAM) tools to attempt to solve business-focused governance problems.

Business context is the sum total of everything an organization knows about its users, their job responsibilities, and the information, applications and entitlements they need. While some context is contained within IT-managed systems (such as directories and HR applications), additional context is also held by the managers who supervise users or by the owners of business functions, applications and data, not by the IT or security staff.

This white paper explains why today's identity management systems fail to properly reflect business context, why embracing a business-driven approach to identity and access governance reduces costs while increasing security, and describes a step-by-step methodology for implementing it.

TODAY'S REALITY: FAILED IDENTITY MANAGEMENT

Today's organizations face more security threats and regulatory challenges than ever, not to mention an exploding user population, the proliferation of mobile devices, and the potential damage to shareholder value and reputation that would result from a data breach. Yet, not only are traditional identity and access governance (IAG) systems failing to keep up, they are falling behind the need to proactively manage an ever-changing risk and threat landscape. Traditional IAG architectures are fragmented, complex, and ill-equipped to deal with the pace of change in an organization, from simple employee transfers to restructuring, new regulatory requirements and mergers and acquisitions. In addition, traditional identity systems have consistently been prohibitively expensive to deploy and operate, limiting their breadth of coverage and effectiveness.

Cloud computing increases complexity by creating a new application silo (and more administrators with privileged access) for every new cloud application and cloud service provider. It also increases the rate of change, as lines of business obtain new services, often without informing the central IT or security groups. Mobile computing and the "bring your own device" trend create yet more identity and access governance silos to accommodate each new platform.

The result is that even as organizations need easier, faster and more consistent IAG, the pace of change makes their compliance and risk posture ever less certain. Relying on siloed, reactive, incomplete systems make it even harder to discover and apply the business context needed for each application or group of systems, and the lack of a single, central IAG infrastructure even more critical. Organizations need to easily prove compliance, minimize risk and enable the business to be productive.

In the face of all these challenges, the key to solving these problems is to leverage a centralized, modern identity and access governance system built around business context.

THE IMPORTANCE OF BUSINESS CONTEXT

Business context is the often-forgotten, but key ingredient to assure effective, enterprise-wide IAG. It is often overlooked because IAM and IAG are usually handled by the CIO, CISO, VP of Security or Director of Security. None have the business context required for efficient, effective enterprise-wide access governance. Most of this business context lies instead with the supervisors and other business managers who understand the specific responsibilities various users have, and the access each requires.

Consider, for example, a finance department with five employees, each with Analyst Level 2 job codes. The IT department might conclude each should have the same access rights and entitlements. However, their supervisor knows who is responsible for travel and entertainment spending, and who monitors telecommunications and utility expenses, and can thus make more accurate access and entitlement decisions for them. Different members of a clinical drug trial team might have the same job titles, but require different levels of access to test data depending on their seniority, training, or project assignments.

Business application owners are also well-equipped to understand how applications or data resources are used and what access and entitlement policies are appropriate for them. Application owners, along with risk, audit and compliance teams, have the best context for setting IAG policies specific to various business applications or industry domains. And data resource owners know best who should have access to sensitive or regulated data.

To apply this context most effectively, organizations must enable business managers, business application and data owners, and the audit, risk and compliance teams to drive access-related policy requirements. IT must then translate those requirements into

operational activities. Achieving this business-driven identity and access governance requires new processes and new technology, and it requires the business to partner with IT.

BUSINESS-DRIVEN IDENTITY AND ACCESS GOVERNANCE REQUIREMENTS

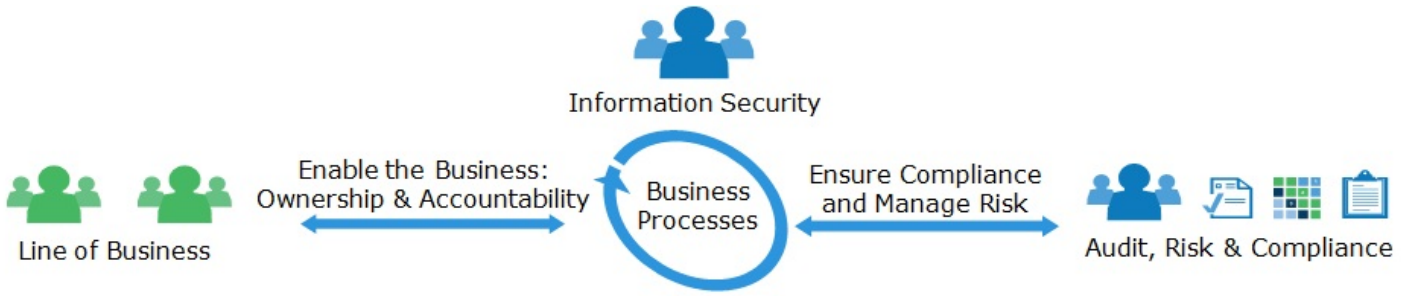
To bring business context into the IAG process, IT must transform the cryptic jargon of application and infrastructure entitlements into a business-friendly view of access and give business managers a simple, intuitive way to make IAG decisions throughout the identity and access lifecycle.

Business-driven IAG also requires that the lines-of-business (LOBs) take ownership of the tasks that they have the context for, and become accountable for them. Audit, risk and compliance teams must be able to create requirements, measure results and institute controls. IT security and operations teams must have visibility into and control over how IAG activities are conducted, since they are ultimately responsible for carrying out the decisions made by LOBs.

Organizations must be able to easily define policies which leverage business context, assuring compliance in areas such as segregation-of-duties (SOD) or access request and approval. Once a policy has been instantiated, it can be applied automatically and violations dealt with automatically. Since the contents of these policies will be familiar to LOBs, IT Security and Operations, Audit, Risk and Compliance teams, this is a very effective way to engage them in the IAG process.

Automating the fulfillment of access changes can significantly reduce cost and effort, because to date, organizations have typically struggled to achieve the required automation with IT-focused tools from traditional identity management vendors. A truly business-driven approach to IAG provides a simple access change management mechanism that keeps business logic separate from application-specific integration logic. It also enables policy-based access changes, using rules and workflows to deliver quicker access in line with established policies. This enables a cost-effective and rapid method for on-boarding applications from a change fulfillment perspective.

All of this requires an automated, centralized identity and access governance platform, which gives business owners a simple view of identities and access, enables automated, policy-based access controls, fulfills IAG change requests, and builds proactive access compliance into the fabric of the organization. Figure 1 illustrates how such a platform enables an organization to establish business processes to accomplish all of these activities.



PHASED APPROACH TO BUSINESS-DRIVEN IDENTITY AND ACCESS GOVERNANCE

Business-driven IAG is best made operational by implementing discrete, measurable business processes in a step-by-step phased approach that delivers value in each phase. The steps are:

Visibility and Certification: This repeatable, sustainable process automatically collects and cleanses identity and entitlement data to obtain a single unified and normalized view of current access rights. This technical view of access is transformed into a business view so that LOB managers, such as supervisors or business owners of resources, can become accountable for reviewing access rights. This happens via a business user-friendly access certification process (also known as an access review), where people's entitlements are reviewed and approved (or revoked) by a supervisor or application owner.

One important additional step, which is also a good example of establishing business context, is identifying the business owners of data resources (such as file shares, or SharePoint sites), as well as any metadata that defines its business purpose and risk classification.

Policy Management: Capturing decision-making context and business logic in a set of policies defined as rules is an excellent way to automate security and compliance controls. Having rules trigger workflows provides process and policy automation, and reduces costs.

For example, the identification of a new employee can trigger a multi-step process that includes creating accounts for the employee, providing her with appropriate group memberships, assigning the accounts appropriate entitlements to applications and data and obtaining the necessary approvals.

Role Management: Roles enable business managers to more easily manage entitlement changes. Consider the role of Bond Trader Level 2. A user in this role might be entitled to 35 different fine-grained entitlements (such as the ability to make trades up to a certain limit) across several applications. Rather than requiring a manager to review and evaluate each of the 35 entitlements, the manager can simply verify that the role is correct for the person. This is an easier and more natural way for the manager to apply the needed business context because they are thinking about the role played by a specific person, not about a detailed list of application entitlements.

Roles also simplify Joiner, Mover and Leaver processes and make it easier to assign users additional access. They also make it more efficient to review, validate or test user access to simplify compliance and risk management and speed up fulfillment.

This phase also produces processes for lifecycle management of directory groups, which are often used to govern access (especially to data resources) in much the same way as roles.

Often, organizations do not want to dive right into creating and managing Roles. Another alternative to consider is using suggested entitlements, which can provide choices to a business manager about what entitlements similar users have during the Joiner or Mover processes.

Access Request Management: Once a business view of access and the abstractions to simplify and automate access management are in place, an organization is in a good position to establish a self-service access request front-end for business users, and an auditable and policy-compliant change management engine for IT on the backend. This process empowers LOBs to invoke access requests without any knowledge of the infrastructure and details involved in servicing the requests, therefore easing the access request process. It also provides proactive compliance by enforcing policies before access is granted.

Change Fulfillment (Provisioning): Business-driven changes to identity and access result in actual modifications to user accounts, group memberships and entitlement assignments in systems, data resources, directories, applications and access control solutions. Change fulfillment – which may be referred to as provisioning -- is a process that usually exists in some form before an organization embarks on any of the phases mentioned here. The challenge is typically about evolving the process so that it is consistent, policy-driven, at the entitlement level and as much as possible, automated.

There are several mechanisms for fulfilling access changes. A simple task notification, such as an email to a system administrator, is often the easiest and most straightforward approach to change fulfillment. Creating a ticket in a service desk is a more consistent way to track requests, responses and confirmations, and can leverage an existing enterprise change management system. However, the associated time lag, cost and error rate often drive organizations to automation. An automated fulfillment solution delivers operational efficiency and timely changes, and ideally supports the rapid on-boarding of new applications.

Traditional provisioning engines make it difficult to onboard (connect to) more than a few applications because these older systems combine the business logic that defines governance policies with the logic required to integrate with each application. This requires expensive custom coding for each new connection, and whenever policies change. Traditional provisioning engines also tend to focus on account-level or group-level provisioning, which doesn't provide the necessary level of visibility or access requirements. Modern, business-driven IAG systems maintain the policy-related business logic at a higher level, making this "last-step" integration much easier and less expensive. And modern business-driven IAG systems focus on deep provisioning with the ability to view and change fine-grained entitlements in applications.

SUMMARY

Organizations cannot afford to spend any more than they must on identity and access governance. Nor can they afford the regulatory, legal or intellectual property risks of not properly managing identity and access governance. The road to the most efficient and effective identity and access governance runs right through the owners of the business processes, applications and data. It uses the rich "business context" about which users require what access and entitlements as the foundation for automated, business-driven identity and access governance that delivers the maximum business value at the lowest cost.

WWW.RSA.COM