WHITE PAPER

excelgens

The Identity and Access Management Imperative: Securing the Enterprise

excelgens

Table of Contents

excelgens

Overview

This white paper discusses a set of recommendations and best practices methodology that facilitates the successful delivery of projects in the complex world of Identity and Access Management solutions implementation. The objective of this paper is to outline and discuss three essential elements that enable the effective delivery of an Identity and Access Management solution in a client environment.

In the past, IAM was focused on establishing capabilities to support access management and access-related compliance needs. The solutions were often focused on provisioning technology and were poorly adopted; they also resulted in high costs and realized limited value. Organizations often struggled to meet compliance demands during this period, and the solutions were deployed to manage very few applications and systems. Centralized, standardized, automated identity management services designed to reduce risk, cost, improve operational efficiency continued to be elusive.

The IAM challenge for executives

The digital world is creating shifts in the way business gets done, resulting in both exciting but often troubling times for executives. What was once an intimate corporate network is now a globally connected web of people and devices. More employees work remotely, carrying sensitive data on notebooks and PDAs. Partners and suppliers are invited inside the corporate walls to interconnect their own systems and share information. Vendors and contractors are trusted with access to sensitive data.

Many C-level executives may not know for certain that their information is secure—that only the right people are gaining access to the appropriate applications, networks, and data. And now with the introduction of cloud-based services, mobile devices, and remote users, there are even more connections to critical data and applications both inside and outside of the enterprise.

Identity and access management (IAM) is the security discipline that authorizes users to access corporate systems and information. It helps prevent fraudulent access and use of data that could potentially impact the business, its partners, or even worse, its customers.

The majority of organizations haven't been able to realize the full promise of IAM—to secure the enterprise information in a cost effective and compliant manner. Many have implemented components of IAM, some even accomplishing the elusive "single sign-on," but often fall short in other areas.

This failure is evident as research from Business investigations shows 75% of breaches went undetected for weeks or even months.

IAM Life Cycle Phases

The management of identity and access permissions can be viewed as multiple stages. The IAM life cycle illustrates the stages that users proceed through when joining a business workforce and obtaining access to the tools and assets necessary to do their job. The IAM life cycle also includes stages to ensure that employees maintain appropriate access as they move within the organization with access being revoked or changed when they separate or change roles.

An IAM program requires a well-defined strategy and governance model to guide all the life cycle phases.

User access request and approve

Definition objective:

- Gaining access to the applications, systems and data required to be productive.

Common challenges:

- Processes differ by location, business unit and resource.
- Approvers have insufficient context of user access needs —do users really need access to private or confidential data.
- Users find it difficult to request required access.

Reconcile

Definition objective:

- Enforcing that access within the system, matching approved access levels.

Common challenges:

- Actual rights on systems exceed access levels that were originally approved /provisioned.
- There is no single authoritative identity repository for employees/non-employees.

Review and Certify

Definition objective:

- Reviewing user access periodically to realign it with job function or role.

Common challenges:

- Processes are manual and differ by location, business unit and resource.
- Reviewers have insufficient context of user access needs.

excelgens

Top 3 Drivers for a successful IAM Solution

Every organization has different business drivers for determining and implementing an Identity and Access Management Solution. To ensure the greatest possible chance for success, strategy must align with business goals in order to drive business results.

1. **Analyze existing access to various systems and consolidate them into Roles and Policies.**
   - Review existing access control lists across all the namespaces.
   - Develop Roles and Policies.
   - Import of Existing Roles from an Authoritative Source
   - Role vs. Actual Analysis
   - Rule Based Roles assignment.
   - Associate Roles to Users
   - Alert all concerned parties of the change.

2. **Process employee related feeds coming from reliable sources like HR to update user records.**
   - Understand data formats used in HR data feeds
   - Map HR Feed data attributes to the User attributes
   - Ensure account data is correct and complete
   - Push changes to multiple systems seeking Identity Data

3. **Implement Workflow/Approval process and Self Service portal**
   - Design Workflow/Approval flow chart from beginning till the end
   - Assign Manager/Business Approver to the respective users
   - Handle account change requests (create, modify, revoke etc)
   - Route change request to all concerned parties for approval.

Manage risk and address information security compliance requirements

Meeting standards and regulations can be tricky, especially as organizations expand access beyond their firewalls to customers, partners, suppliers, and applications in the cloud. It's difficult enough to manage systems within the corporate domain but even more difficult when accounting for access across a firewall. Therefore, it's vital to centrally manage user access and easily provide reports for compliance assessments.

IAM takes time to implement and working with the service provider's team of experts helps organizations quickly deploy solutions and meet security compliance requirements. Hosted IAM can be set up in a fraction of the time it takes to deploy IAM internally. It can also provide a centralized solution that's easy to manage and delivers policy enforcement rules that afford the same rights to users as if they had signed on to the individual systems directly.

When considering the effort needed to manage the security compliance requirements within regulations and standards such as PCI DSS, Basel II, and HIPAA, it's important to use a hosted IAM provider that thoroughly understands regulation requirements and provides reporting functionality.

The service provider can also analyze the enterprise IT environment and provide expert advice on security gaps and remediation steps, helping both the business and the IT department address its security compliance requirements.

The potential for risk can be seen in many business arrangements—particularly one as common as offshore partnerships. Consider a pharmaceutical company that adds an offshore partner to gain cost savings and speed time

to market for a new product. To realize the advantages, significant data sharing between the two companies must happen. For example, the partner may need access to a critical data center that contains sensitive patient research covered by HIPAA regulations. The right IAM solution makes it possible to quickly add partners in a secure manner and helps demonstrate compliance through auditing and reporting.

Speed implementation and control costs

When employees leave, partner and supplier relationships change, or companies merge or divest, all of those user connections must be managed. This is an area of concern for many organizations as they expend significant resources to try and adapt to their changing user base.

Just developing an IAM solution can take many months. It takes time to create a work plan, locate hardware, purchase software, install and configure the system or systems, train administrators, create connections to other systems, and test the application. And these are just a few of the tasks required.

Hosted IAM eliminates the need for businesses to purchase expensive IT infrastructure hardware and software. It also allows organizations to get up and running quickly on systems that have the most up-to-date, leading IAM applications. Increased scalability also provides an extremely short time to productivity, which means that contractors and partners are able to begin work and access resources quickly and efficiently.

Conclusion

Identity and Access Management solution implementations can be a complex projects but they do not necessarily have to be expensive and disruptive. In fact, implementing an Identity Management Solution can be easily accomplished, provided the top three drivers presented in this paper have been identified and designed into the implementation process.

This solution can lead to recognizing other benefits including improved efficiency, secure confidential information, and integrity of financial information.

Here are some guidelines for success:

- Develop a strategy that is aligned to the needs of the business and considers people, processes and technology issues
- Don’t think of IAM as an IT-only initiative, especially when it addresses business usage and regulatory requirements
- Be strategic, not tactical, when planning and designing a solution
- Because IAM is pervasive, be prepared for objections and concerns during any transformation process
- Avoid the “Big Bang” approach; use a risk-based, phased implementation approach to ease the integration and adoption of IAM changes
- Don’t rush to buy and implement a tool without first considering the necessary business and process transformation requirements — tools do not guarantee enhancements in maturity
- Creating an inventory of applications, systems and definition of business-friendly access roles (profiles) are critical activities to ensure success of an IAM program and will take longer than expected
- Don’t expect 100% assignment of access through roles; start with enterprise-level roles first, then move to business-unit-level roles and allow for exceptions.

About ExcelGens

ExcelGens, a Woman-Owned Minority Business Enterprise (MWBE) was formed to address specific IT services needs of enterprises of all sizes. Our team of industry veterans who have more than 60 years of diversified industry experience came together to service enterprises that are getting ready for tomorrow's challenges.

Contact Us

To learn more about how ExcelGens services and solutions help solve your business and IT challenges contact your ExcelGens representative or visit us at www.excelgens.com.

USA

New Jersey (Headquarter)

2001, Route 46, Waterview Plaza, Suite 310, Parsippany, NJ 07054

Chicago

30 South Wacker Drive #2200, Chicago, IL

Minneapolis

820 Marquette Avenue, Minneapolis, MN 55402

California

2478 Via Espada, Pleasanton, CA 94566

INDIA

Gurgaon

Udyog Vihar, Gurgaon, 122001, Haryana, India

Dehradun

Patel Nagar, Dehradun, India