



**Identity and access management:
uncovering the secrets to successful
implementations.**

Contents

2 Overview

2 *IAM is more critical than ever*

4 *Many IAM projects are fraught with difficulties*

5 *Understanding IAM*

7 *Separating fact from fiction*

9 *Prescription for success*

13 *Successful IAM in action*

16 *Summary*

16 *IBM and identity and access management*

Overview

As today's business climate demands greater efficiency, security and regulatory compliance, the need for effective identity and access management (IAM) has never been more pressing. However, just the idea of IAM can strike fear in the hearts of line-of-business and IT executives. This is not surprising; IAM projects have a reputation for being complex and expensive, and it can be difficult to achieve their intended objectives.

However, with the right approach, an identity management project can produce significant benefits, including lower costs, enhanced security, better compliance, and increased end-user productivity and satisfaction. This white paper presents an overview of key IAM challenges, debunks common IAM myths and outlines an approach for making IAM projects successful.

IAM is more critical than ever

Ten years ago, IAM was tackled by relatively few leading-edge companies. Today, it has become an imperative for almost all enterprises. Regulations such as the Sarbanes-Oxley Act, the Payment Card Industry Data Security Standard, the Gramm-Leach-Bliley Act, the Statement on Auditing Standards No. 70, Basel II, and the Health Insurance Portability and Accountability Act now require that companies and their officers be accountable for lack of proper data security. Companies must implement comprehensive security controls to protect critical data and ensure privacy of sensitive information, and they are subject to material financial and legal liabilities if appropriate steps are not taken to protect relevant data. This applies to more than just access to financial information; it's also about who has access to business information, a broad group that can include the majority of an enterprise's employees.

As the regulatory hurdles continue to multiply, business complexity is also increasing dramatically. Technologies such as service-oriented architecture (SOA) enable deeper lines of automation and integration, both within the enterprise and across corporate boundaries. Compounding the IAM challenge is the constantly evolving and increasingly complex threat environment. IT security departments today must be concerned not only with external threats of

Highlights

Manual processes related to identity and access management are typically costly and inefficient.

Enterprises are turning to IAM projects to improve security, reduce costs and improve employee productivity.

terrorism, Internet-borne viruses and worms, and identity theft, but also with the growing insider threat problem. According to a recent survey from the Computer Security Institute, insider abuse of network access or e-mail edged out virus incidents as the most prevalent security problem, with 59 and 52 percent of respondents reporting each respectively.¹

Addressing IAM challenges by adding more operational staff to execute manual processes is not an option for most companies, as manual processes are usually costly, inefficient and risky.

- *A significant percentage of calls to IT help desks are typically related to password and access issues.*
- *Only 17 percent of companies labeled by Aberdeen as “Industry Average” claimed they had no orphaned accounts (accounts with access that should have been revoked).²*
- *Some organizations take more than 30 days to decommission accounts, and others have no defined process to discover if orphaned accounts even exist.³*
- *Errors in paperwork and manual processing of access and provisioning activities often require rework.*

Given these factors, it is not surprising that IAM has moved from the periphery to front-and-center focus, prompting many more enterprises to put IAM projects on their priority lists. As adoption of IAM has increased, companies that have successfully tackled IAM have realized a multitude of benefits, including:

- *Improved compliance posture with centralized views and business processes for verifying identities and granting access rights*
- *Reduced costs resulting from the sunset of separate, custom identity administration solutions*
- *Improved security and reduced cost as a result of having fewer employee logins and employee credentials*
- *Improved productivity and employee (or customer) satisfaction through single-sign-on (SSO) experiences and on demand access provisioning*

Highlights

IT executives are often reluctant to tackle IAM for several reasons.

Many IAM projects do not achieve their stated goals.

Failed technology is rarely the cause of unsuccessful projects.

- *Improved business flexibility resulting from a faster time to market and a centralized, standardized security infrastructure*
- *Centralized audit views of runtime authorization events, allowing for easier detection of malicious behavior.*

Many IAM projects are fraught with difficulties

Although the number of IAM implementations is growing as more IT executives recognize IAM's importance and potential benefits, an IAM initiative can be one of the most dreaded projects on the IT landscape, with good reason. Many IAM projects end up behind schedule and over budget and deliver significantly less than the projected return on investment. As a result, the vision that many line-of-business and IT executives had in mind at the start of the project never comes to fruition, and organizations are often saddled with significant ongoing expense as well as audit exposure.

The symptoms of poor or incomplete IAM implementations can be seen clearly in these statistics:

- *Fifty-eight percent of companies surveyed by Ponemon Institute report using mostly manual processes for monitoring identity controls.⁴*
- *Only 13 percent of companies surveyed by Ponemon Institute describe their company's approach to identity compliance as centralized.⁵*
- *Only 10 percent of companies surveyed by Aberdeen have a single identity store, while 8 percent have more than 100.⁶*

While the reasons behind ineffective implementations are varied, most are not a result of failed technology but instead can be attributed to the following factors:

- *Too large of a scope initially—trying to do it all at once*
- *Early short cuts that ultimately lead to problems later*
- *Lack of expertise and insight regarding the current state of IAM policies, procedures, standards, best practices and costs*
- *Limited understanding of IAM technologies*
- *Lack of expertise to integrate IAM technologies with existing IT infrastructure*
- *Insufficient executive participation, validation and buy-in*

Highlights

Developing a logical, phased approach to IAM increases the chance for success.

Identity management is the process of managing information used to identify users, control user access, determine user privileges and delegate administrative authorities.

In contrast, companies that thoroughly understand their current situation, the unique capabilities and constraints of their organization, and the various IAM technologies are more likely to be successful. These companies take the time to develop a logical, phased approach to IAM where each phase builds on previous phases, creating a more security-rich and efficient enterprise with each progressive step.

Understanding IAM

The first step toward a successful IAM implementation is to understand the basics of IAM, which are sometimes misunderstood. Although potentially complex in application, the essence of identity and access management is fairly straightforward: Determine who should have access to what applications and resources (and who shouldn't) according to business rules.

Identity management

Identity management is the process of managing information used to identify users, control user access, determine user privileges and delegate administrative authorities. When it comes to end users, one size does not fit all. User lifecycles are in constant motion because people's roles and responsibilities often change. As employees are given new responsibilities or transfer within the organization, their access privileges need to be reviewed, approved and updated to match their new responsibilities. At the same time, previous access privileges may need to be suspended, removed or reviewed. Customers that are granted access to applications can also have profiles that evolve. For example, auction-site power sellers or stock investors who reach a specified trade volume need their profiles and authorizations to be updated seamlessly.

Although accurate authorization is important, the speed of that authorization is just as critical. For example, until new employees can access business or e-mail applications, they may not be able to start work—so the process for setting up new accounts and passwords must be timely.

Highlights

Access management is about managing consistent sets of access control policies across enterprise systems.

Access management solutions are integrating with broader service management solutions.

Security policies are dynamic, too, so identity management solutions should include tools that streamline policy creation and allow administrators to assess the potential impact of policy changes without introducing them to a production environment.

Oversight and governance requirements for security place importance on the ability to manage identity and access data. Predefined reports and audit events should allow auditors to quickly gain an accurate view of an organization's security posture and state of compliance.

Access management

Access management is the ability to manage consistent sets of access control policies in line with security policies and compliance regulations across enterprise systems, including policy administration, monitoring and enforcement.

Access management solutions manage the day-to-day access of resources by authorized persons. Effective solutions integrate formal security policies into the access management workflow to automate the management of access to operating systems, networks, servers, storage devices, databases, desktop applications, online commerce systems and enterprise applications. At the core of access management is the unification of the many user names and passwords that users typically have to remember (or write down on unsecured notes) into a single, security-enhanced authentication and access process (typically via use of SSO technologies).

Web-based SSO and distributed Web-based administration have almost become the standard. Moving to greater control and centralization requires identity and access management solutions that are much more encompassing, including integration with physical access control processes.

Access management solutions are also trending toward integration with broader service management solutions to more closely associate IT processes and events with user identities. It's not enough to simply allow or deny access to applications; you have to know who is making the request to access a resource, and why.

Highlights

Understanding the myths of IAM can help set realistic expectations.

Separating fact from fiction

With a basic understanding of IAM fundamentals in mind, the next step toward a successful implementation is to dispel the myths and misconceptions regarding IAM that can make it difficult for IT and line-of-business executives to understand how to plan and prioritize.

What follows is a sampling of common IAM myths and their realities based on IBM's experience in the marketplace.

Myth: A massive process reengineering effort is required before my organization can benefit from identity management.

Reality: While it is true that process change is often a required part of an IAM project, many benefits can be realized with a minimal amount of process reengineering. In fact, most successful enterprises do not take on process reengineering as an initial step in an identity management implementation. By first taking interim steps such as establishing central administration of IDs across platforms/business units and implementing self-service features such as password resets, organizations can quickly begin realizing some concrete benefits from IAM. In parallel, organizations can take the time to secure the correct level of business involvement and gain a full understanding of affected processes to enable a sensible and prioritized approach to automation.

Myth: Our human resources database is the only authoritative data source we need.

Authoritative data sources are required to support effective IAM.

Reality: While a human resources database is often a good start, we have found that many companies' databases have a significant amount of out-of-date or missing information. Examples of shortcomings include:

- *Lack of information on contractors and other non-employee personnel*
- *Out-of-date information on organizational affiliations/roles*
- *Lack of information on reporting lines*
- *Incorrectly defined job titles*
- *Delays in populating information about new hires.*

Highlights

Concentrate efforts on projects that create the most value and avoid automating every process.

Role management is ongoing, because role definitions constantly shift.

Without quality information from an authoritative source, IAM projects cannot be very successful. As a result, an initial effort to establish data integrity in an authoritative source is often required.

Myth: The goal of an IAM project should be full automation of all identity-related processes.

Reality: It is rarely cost-effective to automate all identity-related processes. When considering whether to automate, organizations need to conduct a clear cost-benefit analysis that considers the number of IDs being managed as well as the cost of current identity-related processes. For example, it may not be worthwhile to automate access to an application that has only a handful of users in the application identity repository. Instead, it may make more sense to consolidate the business functions for small applications or to consolidate the identity information onto a centralized identity repository. Leveraging multiple IAM strategies based on business needs and priorities can keep an IAM project on time and on budget while creating an IAM infrastructure that is more flexible and scalable.

Myth: If we have a role-based access control system, we can start automating access based on roles in our IAM project.

Reality: Role-based access control on its own is usually not sufficient for automation, because roles are typically very loosely defined. Leveraging roles to enable effective automation requires a comprehensive role management system that helps enterprises discover, certify, compare, consolidate and deploy role definitions. Role management needs to be ongoing, because role definitions constantly shift based on application development, organizational changes, and merger and acquisition activity. Leading IAM solutions are designed to integrate with enterprise role management solutions in the marketplace today, allowing enterprises to approach the automation phase in IAM projects more effectively and efficiently.

Highlights

IAM software vendors are focusing efforts on ease of implementation and management.

An assessment and planning exercise is the first step.

Myth: IAM software products are inherently complex to implement.

Reality: While many early IAM products were difficult to implement, the marketplace has matured in the past few years, and software vendors are focusing significant efforts on improving the ease of implementation and management. This is particularly true in the marketplace for SSO products and is also becoming increasingly true in the provisioning space. Some of the key usability features being incorporated into newer versions of IAM products include:

- *Task-oriented wizards that simplify configuration and minimize the need for scripting*
- *Preconfigured application programming interfaces (APIs)*
- *User-friendly processes for defining approval workflow*
- *User interfaces that are easier to use and more customizable.*

Prescription for success

With the fundamentals in mind, the next step is to create the blueprint for the IAM initiative. Just as a blueprint is critical when you are building or remodeling a house, it is critical to start an IAM project with a well-structured plan in hand. This plan must define not only the end goal (what the finished “house” will look like), but also the specific steps to achieve that goal.

Just as building a house without a well-thought-out plan would likely result in poor construction, an IAM project without a plan usually leads to unsatisfactory results. Companies that don’t have a blueprint or that are unsure whether their existing blueprint is sufficient should start by performing an assessment and planning exercise to ensure that they are getting their IAM project off to a good start.

Creating the blueprint

An IAM strategy assessment should include the following elements:

- *Identity data quality assessment*
- *Identity lifecycle assessment*
- *Definition of architectural principles*
- *Solution roadmap*

Highlights

An identity data quality assessment can determine if a foundation exists to support data quality.

Identity data quality assessment

For most companies, the drivers behind an IAM implementation are to automate manual processes, reduce costs and increase security. However, process automation must be built upon a set of good data. By first undertaking an identity data quality assessment of identity and access information, companies can ensure that they have the right foundation needed to support data quality. An identity data quality assessment helps identify areas of concern within the enterprise and provides a roadmap to begin implementing controls that help improve IAM data quality.

A comprehensive identity data quality assessment should address the following areas and answer a number of key questions:

- *Audit: Is information access and modification auditable?*
- *Access: Is information protected with proper access controls?*
- *Compliance: What are the potential impacts of having bad data? What are the privacy and compliance requirements around IAM data?*
- *Accountability: Who is responsible for ensuring data integrity?*
- *Validation: How is data validated?*

An identity data quality assessment can also be a mechanism for supporting business buy-in because it makes business owners aware of the importance of IAM-related information management and the impact it can have on business operations.

Identity lifecycle assessment

Each company has a unique set of processes that affect the management of identities throughout the identity lifecycle. Before automation of these processes is attempted, it is important that they first be well understood, well documented, effective and efficient.

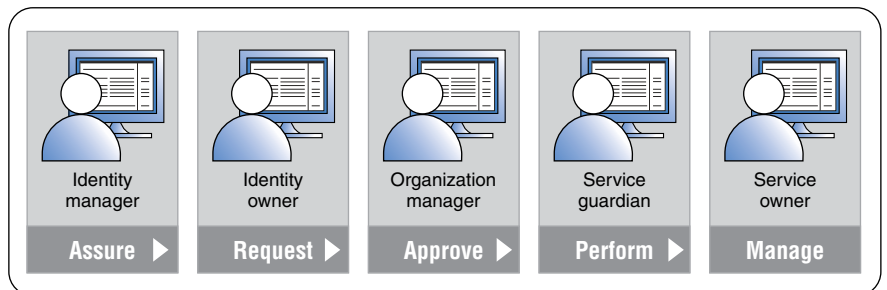
An identity lifecycle assessment discovers the processes associated with identity.

Highlights

Unfortunately, business processes around identity lifecycle management are often overlooked. As a result, organizations can end up with technology that does not work for their business processes—because their chosen solution was not designed to complement and optimize business processes. For example, if a business process does not make information on new hires immediately available, automating that “as-is” process will not produce satisfactory results because information will still not be up to date.

To avoid such wasted efforts, enterprises can undergo an identity lifecycle assessment to help identify events that lead to identity and access information changes, such as hiring a new employee, transferring an employee to a new job or terminating an employee. An assessment offers the guidance needed to establish sound business processes that, in turn, help drive a successful IAM project.

Example: Identity lifecycle view



The biggest challenge with many IAM projects is creating a consistent approach toward application integration.

Definition of architectural principles

The biggest challenge with most IAM projects is creating a consistent approach toward application integration. To overcome this hurdle, organizations can leverage IAM architectural principles—a prescriptive set of best practices that help establish a standardized approach for application integration.

Highlights

Defining a set of consistent architectural principles can help lower IAM costs and complexity.

Development of a detailed solution roadmap can help prioritize efforts and spending.

Architectural principles for an identity management solution should:

- *Be flexible enough to support different platforms*
- *Be an integral part of business processes*
- *Provide an incremental migration approach for application integration*
- *Be treated as part of a mission-critical infrastructure*
- *Support regulatory compliance requirements.*

By defining a set of consistent architectural principles, organizations can help streamline and simplify this challenging aspect of identity management, helping to lower costs and complexity.

Solution roadmap

An IAM strategy assessment should include development of a detailed solution roadmap that outlines a clear and logical path toward enhancing IAM maturity levels. This roadmap should include the definition of foundational projects that must be completed in order to pave the way for successful IAM technology implementations. For example, if consistent identity management standards do not exist, they must be developed early on to establish an appropriate framework for later efforts.

Once these foundational projects are complete, enterprises can begin implementing technologies to automate and streamline IAM. While the timing and sequencing of these projects will vary based on each company's unique business needs and objectives, there are common paths that many enterprises follow. For example, many enterprises invest in single sign-on projects early on because they can show clear business value through reduction of help-desk call volume and increased end-user satisfaction. Similarly, enterprise role management streamlines identity lifecycle automation and is most effectively addressed prior to implementation of provisioning technologies.

Highlights

A large retailer needed to streamline its IAM processes.

A phased approach allowed the client to prioritize investments.

Successful IAM in action

IBM's experience with a large retailer demonstrates the advantage of this approach.

The client had historically taken a very loose and decentralized approach to identity and access management. Identities were typically created at the store level, and often a set of generic IDs were issued at each store to give employees access to systems such as point-of-sale systems, time and attendance applications, and inventory management systems. However, with the advent of regulations such as the Sarbanes-Oxley Act, the need to assign individual IDs and verify each employee's access to systems became necessary. At the same time, the company was in the process of implementing a vendor portal, which required the creation and management of even more IDs to enable external users to access the retailer's systems.

Defining a solution that addressed these pain points was challenging. The size of the enterprise and the high rate of employee turnover compounded typical IAM issues. Additionally, the retailer had plans to expand rapidly.

The client initially approached IBM to help with implementation of an enterprise directory. However, based on IBM's experience with other clients in the retail industry, it was able to demonstrate the benefits of tackling a more comprehensive IAM project that would include not only the creation of an enterprise directory, but also automated, role-based provisioning, stronger access controls and self-service features such as password reset.

With guidance from IBM, the client developed a phased approach that allowed it to quickly address key compliance issues while also reducing costs and improving operational efficiency. This solution leveraged industry-leading software from IBM, as well as IBM's consulting and implementation services.

Highlights

Phased implementation approach for a large retailer

	Stage 0 ▶	Stage 1 ▶	Stage 2 ▶	Stage 3 ▶	Stage 4 ▶
	Isolated silos	Central administration	User self-service	Role-based access control	Integrated user management (in process)
Properties	<ul style="list-style-type: none"> Each system administered separately Generic user IDs used by multiple individuals Inability to validate individual access to systems 	<ul style="list-style-type: none"> Central creation and deletion of accounts Central data storage and administration for security-relevant data 	<ul style="list-style-type: none"> Users are partially responsible for administration of their data 	<ul style="list-style-type: none"> Definition and use of universal, on-system-specific roles Automation of roles assignment (dynamic roles) 	<ul style="list-style-type: none"> Identity management as a central service Only one point of data storage (single point of truth) SSO Influence on application source code
Results	<ul style="list-style-type: none"> Inconsistent states Limited security Large administrative overhead 	<ul style="list-style-type: none"> Reduced cost through consolidated administration Improved security through timely deprovisioning 	<ul style="list-style-type: none"> Reduced cost and administrative effort (previously 40% of all calls related to password resets) Improved service for employees 	<ul style="list-style-type: none"> Reduced administrative costs Accelerated adoptions Improved security 	<ul style="list-style-type: none"> Reduced application development costs Complete consistency Faster time to market for vendor/ intranet applications

Centralization of administration reduced cost and risk while improving security.

A self-service password reset solution reduced the volume of calls to the help desk.

In stage one, the client implemented a limited deployment of IBM Tivoli® Identity Manager, IBM Tivoli Access Manager and IBM Tivoli Directory Integrator software. This enabled the client to establish centralized administration of key platforms, thereby reducing costs and reducing business risk. Connections were established from the provisioning system to the human resources system, IDs were linked to individual employees, and basic access rights were established for administrators. At this stage, provisioning activities remained essentially manual to allow the client time to conduct a more detailed review of existing processes for account creation and deletion. During this phase, IBM assisted the retailer with an assessment of current business processes and mapping of new processes required to establish “adequate internal controls” as required by Sarbanes-Oxley.

In stage two, the client deployed a self-service password reset solution that empowered end users to reset their own passwords without calling the internal help desk. This reduced previously long wait times and the number of help-desk calls related to password resets, which had accounted for approximately 40 percent of call volume. At the same time, the company implemented password synchronization on multiple target systems and established standard management practices to control password quality against organizational password policies.

Highlights

A role-based access control solution gives fast access rights to users based on changes in their job functions.

Automation of IAM processes has saved the company time and money.

In stage three, the client implemented user administration policy automation through a role-based access control solution. This enabled the company to grant access rights based on assignment to a defined role in the organization and to fully automate provisioning/deprovisioning of accounts for store employees based on role and human resources activities such as new hire, change and termination. Access rights are dynamically and automatically updated based on changes in user roles, resulting in huge efficiency gains – what once required a three-week manual effort by six full-time employees is now an automated process that takes less than three hours.

As the client continues its journey toward fully integrated user management, it is currently integrating the employee store portal for role-based access and providing dashboard access to critical applications. Additionally, more critical business applications are being integrated into the system to enable automated access and provisioning.

As a result of the initiative, the company has realized several benefits, including:

- *Reduction of daily administration and help desk costs*
- *Automated self-registration for vendors*
- *Automated notification of profile updates for accounts inactive for more than 90 days*
- *Simplification of security audits for governance/compliance*
- *Consolidation of the control of user administration processes*
- *Elimination of inconsistencies across multiple platforms caused by human error*
- *Enablement of more granular access control for stores through use of role-based access control*
- *Automation of routine manual user administration and processes across applications*
- *Significant reduction in reaction times after user status updates and timely access removal per established business processes (e.g., e-mail file retention per audit guidelines after user access removal).*



Summary

As risk management and compliance have come to the forefront of business, identity and access management have come to the forefront of IT.

When approached in the appropriate manner, identity and access management can allow your business to respond to change, reduce management costs and protect its most valuable information assets.

IBM and identity and access management

For organizations that require security-rich, controlled access, IBM products and services are designed to protect assets and information from unauthorized access without affecting business productivity. IBM solutions for identity and access management can help companies address their enterprise security needs while supporting compliance and business requirements.

In 2007, IDC ranked IBM as the worldwide revenue share leader in the identity and access management software marketplace.⁷ And IBM is a leader in SOA and the service management approach to IT.

For more information

To learn more about how security solutions can help you provide access to resources while helping to secure them, contact your IBM representative or IBM Business Partner, or visit:

ibm.com/itsolutions/security

© Copyright IBM Corporation 2007

IBM Corporation
New Orchard Road
Armonk, NY 10504
U.S.A.

Produced in the United States of America
12-07
All Rights Reserved

IBM, the IBM logo and Tivoli are trademarks of International Business Machines Corporation in the United States, other countries, or both.

Disclaimer: The customer is responsible for ensuring compliance with legal requirements. It is the customer's sole responsibility to obtain advice of competent legal counsel as to the identification and interpretation of any relevant laws and regulatory requirements that may affect the customer's business and any actions the reader may have to take to comply with such laws. IBM does not provide legal advice or represent or warrant that its services or products will ensure that the customer is in compliance with any law or regulation.

1 Computer Security Institute, *2007 CSI Computer Crime and Security Survey*, Robert Richardson, 2007.

2,3,6 Aberdeen Group, *Identity and Access Management Critical to Operations and Security*, March 2007; Copyright © 2007, Aberdeen Group.

4,5 The Ponemon Institute, *Survey on Identity Compliance*, March 2007.

7 IDC, *Worldwide Identity and Access Management 2007-2011 Forecast and 2006 Vendor Shares*, www.idc.com/getdoc.jsp?containerId=207609