

# Human Resources: A Key Partner in Successful Identity Management Initiatives

**Human Resources: A Key Partner in Successful Identity Management Initiatives**

**Table of Contents:**

- 2** . . . . . The Expanding Role of HR
- 2** . . . . . Why Is Identity Management So Critical to Organizations?
- 4** . . . . . Common Issues Related to HR's Involvement in IdM Initiatives
- 5** . . . . . Strategies for HR Involvement
- 6** . . . . . HR and IdM: Your Enterprise Wins



# The Expanding Role of HR

**For identity management solutions to be effective, enterprises require a strong partnership between HR, IT and other business stakeholders in both the planning and implementation of IdM initiatives. Many organizations stumble with IdM because of the lack of a broadly shared vision and agreed-upon responsibilities.**

Human Resources (HR) leaders have long held that people are a company's greatest asset. Now it is becoming clear to many organizations that people's identities are valuable asset as well, especially when it comes to managing how employees within a company, as well as external people such as partners, customers and suppliers, interact with an organization's systems, applications, information and computing assets.

When viewed in this manner, HR's role expands beyond the traditional responsibilities of screening, on-boarding, paying, developing and separating employees. At a strategic level, this role now includes helping to vet, create and manage unique and well-defined identities for all employees as well.

In this light, the HR function becomes a critical business partner in helping to initiate and manage the complete lifecycle of workforce identity information. Additionally, some HR functions are also stepping up to take responsibility for the creation and management of non-employee identities, such as contractors, temps and other business partners

No doubt, HR's role is multifaceted in today's complex business environment of globalization, flexible workforces, increasing regulatory requirements, extended business ecosystems and growing security risks. This is why HR is increasingly a critical business partner in helping to initiate and manage the complete lifecycle of workforce identity information.

This paper examines the expanded role of HR as it relates to identity management (IdM), which is essentially the capability to assure trust and compliance as it relates to accessing an organization's systems, information and assets. For identity management solutions to

be effective, enterprises require a strong partnership between HR, IT and other business stakeholders in both the planning and implementation of IdM initiatives. Many organizations stumble with IdM because of the lack of a broadly shared vision and agreed-upon responsibilities.

## Why Is Identity Management So Critical to Organizations?

In many of today's enterprises, system administrators maintain user names, IDs and identity-related credentials in multiple specific-purpose directories, most of which are treated as stand-alone identity stores. While flexible, this distributed approach results in redundant, inconsistent and incomplete views of identities. As a result, identity administration and maintenance is costly and complex, plus it makes audit and compliance activities difficult as well.

An identity management solution can consolidate and reconcile distributed identities by synchronizing identity data across multiple directories, providing a unified and accurate view of identities distributed across the enterprise.

This approach retains much of the flexibility of distributed administration, while providing significant efficiency and auditing capabilities through the use of automated rule-based and role based approval work flows for account management.

Why is well-managed identity information so important? Identity information controls users' access to platforms and applications and all the information that resides in an organization's systems. Organizations must make sure the right people have access to

the right information at the right time while preventing unauthorized or unneeded access.

In an era of increasing security risks and privacy concerns, it is critically important to make sure the right people have access to the right information at the right time, while ensuring that controls are in place to prevent unauthorized or unneeded access. This is especially important in light of regulatory requirements related to information privacy, security and integrity. Effective access management relies primarily on knowing who

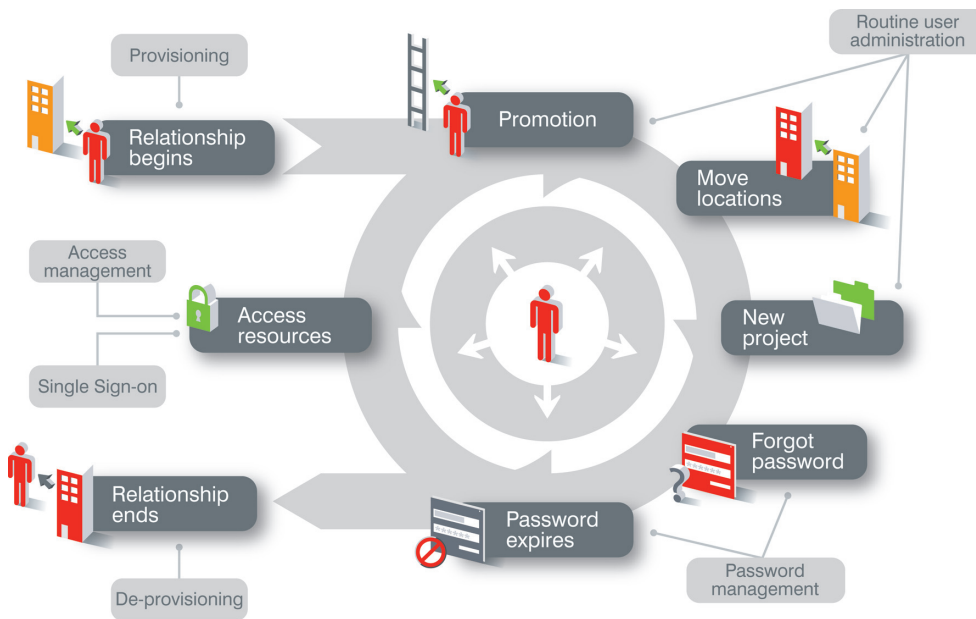
is authorized and who is not, which in turn relies on trusted, unique and accurate identity information.

But the status of users of information is not static, which is why HR is such a crucial partner in most IdM infrastructures. New users join the organization, others leave and existing users change jobs and roles. These “trigger events” are most logically and efficiently captured in HR systems, making them ideal authoritative sources for timely and accurate employee identity information.

**In an era of increasing security risks and privacy concerns, it is critically important to make sure the right people have access to the right information at the right time, while ensuring that controls are in place to prevent unauthorized or unneeded access.**

## Identity Lifecycle

The diagram below depicts the lifecycle of an identity: it is established, provisioned and eventually terminated, and ends with the de-provisioning of access rights. This identity lifecycle corresponds closely to the traditional employee lifecycle that HR manages—a clear rationale for HR’s role as an authoritative source for employee identities.



## The need to control HR-related costs can seem to conflict with the investment in changing HR-related methods and processes that may be required to successfully leverage IdM solutions.

From a security perspective, it is even more critical to get timely separation triggers when people leave the company so their access rights can be revoked as close to “real time” as possible.

### Common Issues Related to HR’s Involvement in IdM Initiatives

Given the high degree of overlapping interests, why do IdM initiatives sometimes face challenges in forging strong partnerships with HR? And what are the consequences if those partnerships are not created? First, it is important to understand that very rarely do IdM implementations encounter intentional barriers. Most issues arise from goal misalignment, planning disconnects, inadequate awareness-building or insufficient communication.

Goal misalignment can occur in organizations that tend to plan in silos, where each department sets its own direction, objectives and initiatives. For example, a common objective for HR is to minimize the costs associated with managing an organization’s workforce. The need to control HR-related costs can seem to conflict with the investment in changing HR-related methods and processes that may be required to successfully leverage IdM solutions. When this is the case, it is helpful to view costs from a corporate-wide perspective rather than a functional one. The total costs associated with regulatory compliance, for example, can be quite significant, given such regulations as Sarbanes-Oxley and the Health Insurance Portability and Accountability Act (HIPAA) in the U.S. and other data privacy regulations globally.

Today, HR essentially has a fiduciary responsibility to make sure that changes in employee status are captured and communicated so

that access privileges can be appropriately changed. So initiatives like IdM that facilitate compliance and reporting provide significant return on investment, regardless of the functions involved.

The nature of the organization itself can also create IdM implementation challenges. Companies that have chosen a highly decentralized structure may tend to resist enterprise-wide or cross-functional initiatives which may be seen as leading to a loss of local autonomy. For example, corporate HR departments often encounter resistance to the idea of a companywide HR information system. Various business units and geographies may have a comfort level with their existing HR systems and processes, feeling that a “one size fits all” system may not meet their needs.

These types of ownership and control issues, often labeled as “politics,” must be addressed by IdM planners and stakeholders when proposing to implement enterprise-wide IdM initiatives. The implication is that senior managers must have an informed view of IdM-related issues, benefits and implications and must then supply the necessary organizational incentives—and perhaps disincentives—to create alignment among stakeholders.

A related situation sometimes arises when a company already has invested significantly in an enterprise-wide HR information system (HRIS) HR stakeholders may not be anxious to undertake the additional tasks or responsibilities necessary to integrate HR with IdM architectures. Whether the resistance comes from politics, territoriality or simple task overload, it can sometimes be difficult to orchestrate the interdependencies associated with enterprise IdM requirements. Additionally, some HRIS applications may be seen as too rigid and complex to adapt to the specific workflow and business processes associated with proposed IdM solutions.

When such disconnects occur, the result may be sub-optimization of some IdM benefits. For example, in some organizations, the average time required to fully provision new employees with all the access rights they need to be productive can be a matter of weeks, clearly a productivity issue. This can arise because of shortcomings associated with current processes that make it difficult to get timely hiring event data.

From a security perspective, it is even more critical to get timely separation triggers when people leave the company so their access rights can be revoked as close to “real time” as possible. Again, root causes may be current business processes that do not provide timely separation event data. Clearly, these dependencies require the active support and sponsorship of HR leaders to change HR-related methods and processes in order to optimize IdM capabilities.

Another area of HR coordination with IdM initiatives involves the concept of employee roles. A key IdM best practice is managing access to resources based on an individual’s role. For example, a marketing analyst may need view-only access to a module in the company’s Customer Relationship Management (CRM) system that contains customer contacts; however, a sales executive may need to have both read and write rights in order to create or change customer data. The use of roles greatly simplifies provisioning and creates a higher level of information security. However, many HR departments have not created and managed job titles and functions with access provisioning in mind. In these cases, aligning and engineering useful roles across the enterprise requires active involvement from HR from both a role design and role ownership perspective, another area where collaboration with HR is a critical success factor for IdM effectiveness.

## Strategies for HR Involvement

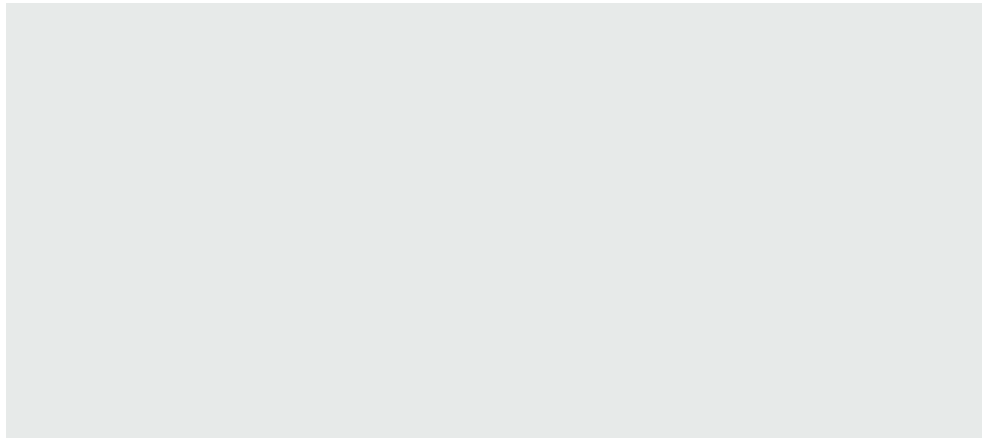
Because of the strategic nature of HR in successful IdM rollouts, collaboration and goal alignment should begin early in the IdM discussion phase. It is particularly important that this early collaboration focus on IdM education and awareness building for key members of the HR community. For companies that have solid IT planning and oversight mechanisms in place, this process may involve building cross-functional stakeholder support for IdM during periodic cross-functional planning sessions.

These awareness-building efforts should focus on IdM benefits such as compliance, security, productivity and efficiency. These discussions should also stress that IdM capabilities can help attain shared goals of increasing employee satisfaction through faster access to resources and mechanisms such as employee self-service. Identity services can confirm user identity when employees interact with online services to manage contact information, reset passwords, request resources or interact with systems.

For organizations with less formal cross-functional IT planning processes in place, it will be necessary to engage HR leaders one-on-one in discussions explaining the strategic significance of IdM, its business benefits, its interdependencies with HR and common goals. The key here is timeliness. Begin these discussions when IdM planning begins, not when implementation begins.

In fact, a best practice for successful IdM implementations is a solid front-end planning and roadmapping engagement which involves all key stakeholders, not just the IT community. Such an engagement has as key deliverables a go-forward road map that has been prioritized and phased to best leverage IdM

**A best practice for successful IdM implementations is a solid front-end planning and roadmapping engagement which involves all key stakeholders, not just the IT community.**



[www.novell.com](http://www.novell.com)

benefits based on the needs of the business. It includes involving stakeholders in creating a common vision for identity services, developing guiding principles and establishing shared goals.

Ideally, HR involvement continues beyond the planning phase. HR subject-matter experts should be engaged throughout design, testing and roll-out to ensure that processes are aligned and optimized from both an HR and IdM perspective.

### **HR and IdM: Your Enterprise Wins**

It is important for IT leaders to understand that IdM is not simply a technology imple-

mentation. Identity services are foundational enterprise capabilities, and as such will have a ripple effect throughout an organization. Orchestrating a successful IdM roll-out will require engaged sponsors from HR, IT and business teams to drive direction setting, planning, change management and assimilation. In our experience gained through planning and implementing numerous IdM initiatives across a broad spectrum of industries, organizations that have active sponsorship from the HR community have greater IdM implementation success. This is why we believe that securing HR's early and active involvement is a key task for IT leaders who wish to deploy enterprise identity services.



Contact your local Novell® Solutions Provider, or call Novell at:

1 800 714 3400 U.S./Canada  
1 801 861 1349 Worldwide  
1 801 861 8473 Facsimile

**Novell, Inc.**  
404 Wyman Street  
Waltham, MA 02451 USA