

# Identity Management: Tackling the 400-Pound Gorilla

By Richard E. Mackey, Jr.

In the past, many organizations shied away from the daunting task of addressing their identity management issues in a consistent and integrated way. Managing the many accounts across applications and systems and ensuring that people are accorded appropriate privileges in the face of new hiring, job changes, and departures is just hard. Adding to this challenge is the complexity of differences in policies and approval requirements across departments and divisions, geographical distribution of offices, and independence of administrative groups. Many organizations find the problem easier to ignore than to tackle.

***Regulations, like Sarbanes-Oxley (SOX), are forcing companies to ensure that their user communities are well controlled, well audited, and appropriately provisioned. Furthermore, the same regulations require a documentation path for all the approval and auditing activities. Meeting these stringent requirements with a patchwork of different identity management solutions is challenging at best and in large organizations, an exercise in futility.***

Fortunately or unfortunately, depending on your viewpoint, companies are finding they just don't have the luxury of ignoring this problem anymore. Regulations, like Sarbanes-Oxley (SOX), are forcing companies to ensure that their user communities are well controlled, well audited, and appropriately provisioned. Furthermore, the same regulations require a documentation path for all the approval and auditing activities. Meeting these stringent requirements with a patchwork of different identity management solutions is challenging at best and in large organizations, an exercise in futility.

## How Identity Management Systems Help

While many organizations, particularly those in the financial sector, have been dealing with strict audit requirements for user accounts, SOX is forcing a much larger group of companies to confront this issue. Financial firms have been going through the exercise of "recertifying" all their accounts for years. Recertification, typically an annual process, requires coordination of supervisors and administrators to validate the accounts across the firm. This is time consuming and difficult and leads many people to think about automation. However, companies are finding that while a clean automated integration of all the identity systems would be ideal, what is really required are consistent policies, practices, and documentation of all the processes surrounding identity management. In other words, the most important aspect of an identity management solution (at least where compliance is concerned) is making sure that all account approval, account creation, modification, and review are performed in a consistent manner and that the activities are captured for audit. Two distinct problems need to be solved: automating the workflow of notification and approval, and automating the administration of account creation, modification, and removal. The good news is that workflow automation is a relatively straightforward problem to solve and there are products that can facilitate much of the necessary work.

The main drive of regulatory compliance in the identity management space is ensuring that an organization knows who has access to what. That means that when an account is created, the right people—namely supervisors, system owners, and information owners—need to sign off. It also means that throughout an account's lifecycle, the account must be reviewed by the same parties to ensure only appropriate people have access to information and systems. Identity management systems can be configured to require this periodic review, handling the notifications, providing the interface for approval, and capturing the logs of the events.

Another important part of identity management and regulatory compliance is ensuring that duties like requesting privileges and approving privileges or operating on an account and auditing the activity are separated. Identity management systems can help to enforce separation of duties by enforcing authorization policies and requiring multiple parties in the approval process.

## Automation

We have said the most important part of identity management, at least for compliance, is the automation of workflow and logging. However, this doesn't mean that automation of administrative tasks isn't important. Obviously, the more systems that can be integrated with a centralized identity management system the better. Any identity management solution worth considering includes automated administration of the usual sus-

pects, namely, Windows Active Directory, LDAP directories, popular database products, Novell, Email systems, and Unix variants. Integration of these systems usually helps companies take a significant step toward easing the overall administrative burden.

Companies need to bear in mind that integration can be a difficult process. The issue is not usually the technical integration but the fact that differences in policies, naming standards, and service configurations can be different between different organizations within an enterprise. Combining divisions under a single identity management scheme forces organizations to resolve these differences prior to deploying the technology. It is easy to underestimate the impact of directory structure changes, development of approval workflow definitions, and the effort involved in education and training when rolling out new processes and technology to a department or division.

***The complicated nature of identity management itself and the differences from department to department and division to division are the most troublesome part of rolling out a solution. With this in mind, the best approach is to attack the problem one step at time, building on small successes.***

### **Deployment Strategy**

The complicated nature of identity management itself and the differences from department to department and division to division are the most troublesome part of rolling out a solution. With this in mind, the best approach is to attack the problem one step at time, building on small successes. For example, rather than attempting to deploy a centralized management system to an entire corporation, some organizations choose a smaller division with relatively straightforward requirements as their pilot site. The best guinea pig for this exercise is an organization with relatively new, homogeneous, technologies, not one contaminated with years of legacy systems and services. Furthermore, it's advantageous to choose an isolated organization that doesn't require tight integration with others.

Even with this approach, the deployment will surface problems in workflow, administration automation, notification, and communications. However, it is better to get these relatively straightforward problems ironed out in a controlled environment. It's best to face the fact that rolling out such a significant component of the enterprise infrastructure will require some amount of pain. The most prudent path is to plan for it and avoid losing support for the program in its early stages.


### **Thinking About The Cost Of Identify Management**

Before the regulatory requirement of Sarbanes-Oxley began to bear, many companies recognized both the need and the benefits of integrated identity management. However, few organizations made significant

progress. In almost all cases, the cause was the *perception* that solving the identity management problem would cost too much.

What is wrong about that conclusion is that the cost of the integrated solution was viewed as an entirely incremental cost. In fact, enterprises spend enormous resources today in managing identities in an ad-hoc manner, but those costs are largely invisible. Organizations that implement integrated identity management actually save money while benefiting from consistent controls.

### **Beyond Compliance**

Ideally, security technology and security projects serve as business enablers, providing previously unavailable services, streamlining processes, or reducing costs. Integrated identity management falls into that category. After reaping the benefits of low cost and consistent account administration, organizations are leveraging their identity management systems to support broader provisioning initiatives. The same policies, approval, and workflows that underlie the identity management system can be used to support other employee-oriented services. For example, a new employee may not only need accounts and privileges on production systems, he may also need office space allocated, an email account created, a corporate credit card, and a portable system. The integrated identity management system underpins the automation of these extended services. 

---

*Richard E. Mackey, Jr. is Principal of SystemExperts Corporation ([www.systemexperts.com](http://www.systemexperts.com)), a recognized leader in network security. He is a regular contributor to The ISSA Journal.*