

# COMPLIANCE WEEK

## Take Five: Keys to Identity Management

By Todd Neff – January 15, 2008

The field of identity management is enduring a bit of split personality these days.

On one hand, business software giants are gobbling up small companies that provide ID management solutions, to cobble together comprehensive offerings compliance and IT departments can tailor to their specific needs. At the same time, the overall need for ID management is growing ever more sophisticated, giving rise to powerful tools like federation and enterprise role management.

Sarbanes-Oxley compliance has led auditors to insist on proof of who accessed which system at what time. Then there are the more prosaic reasons driving companies to pay more heed to ID management: “staying out of jail, staying within budget, and not being embarrassed by big data exposures,” as Steve Steinke, an IT security analyst with the 451 Group, likes to put it.

Others cite organizational efficiency and easier (read: cheaper) audits, and, yes, opportunities to profit. Whatever the motivation, taking action in identity management can be daunting. Here are five things you should think about before you do.

### Think Beyond Straight Identity Management



Identifying users on your IT system should only be a starting point, says Kevin Kampman, a senior analyst for the Burton Group covering identity management. He sees three key technologies emerging to think of ID management in broader terms: enterprise role management, identity audit, and entitlement management.

“People are realizing you can’t manage individuals; you have to start aggregating them into business responsibilities,” Kampman says. That has led to the rise of managing a person’s access to data based on what he does (that is, his enterprise role) rather than who he is. The benefits, Kampman says, range from disaster recovery to better alignment of business goals and IT infrastructure.

That change stems from a basic fact of modern corporations: While companies tend to organize roles in terms dictated by either the human resource or IT departments, neither reflects what roles people actually play in a business.

Identity audit software, meanwhile, lets companies define, implement, and show control around identities and access. Large identity-management systems have some of this built in, and specialist software companies such as Aveksa and SailPoint offer their own solutions.

Kampman says identity audit’s rise is fueled by gaps in user-ID provisioning and access management across audited systems, and largely manual access approval and auditing procedures. Such software fills those gaps and add controls like segregation-of-duties policies, risk analysis, and automated access review and certification, he says.

Entitlement-management systems take authentication deep into a software application. Where traditional access controls cease once you’re through a software application’s front door, entitlement management tracks who gets to do what once you’re in the house. It has the potential to ease SOX and other compliance burdens, Kampman

says.

## Federate and Open Up

Federated identity-management systems keep track of identity across organizational boundaries, allowing users to sign onto internal and external corporate systems with a single password. Firms upgrading identity-management systems should insist on compatibility with SAML 2.0—Security Access Markup Language—which is shaping up to be the lingua franca across diverse corporate identity-management systems.



“One needs to be compliant with the generally accepted infrastructure in this globally connected world,” says Roger Sullivan, vice president of Oracle Identity Management and president of the Liberty Alliance Project. The Liberty Alliance developed and oversees the SAML standard.

Sullivan  
a quiet period?”

Among other things, SAML 2.0 provides a mechanism to limit a person’s access to certain periods of time. That satisfies a huge requirement of SOX compliance, says Sullivan: “That is, who had access to what data when? Did this marketing person gain access to privileged financial information during

Steinke says that federated identity management has the potential to enable collaboration among trusted partners where “you’re not only saving money, you’re enabling an application and relationships between customers.”

Open standards don’t stop with federated identity management. Kampman cites yet another acronym—XACML, or eXtensible Access Control Markup Language—as a promising, flexible standard for the fine-grained authorization inherent in entitlement-management systems.

## Put Process Before Technology

This bit of conventional wisdom applies to about any IT project, but perhaps doubly so with identity management systems. Mark Ford, a partner in Deloitte & Touche’s security and privacy practice, sums it up as, “Don’t try to automate chaos.”

The success of an identity-management system hinges on hard up-front thinking about the roles within an organization, and what those roles dictate for access privileges. Companies that spent the time to do this have been successful, he says.

Kampman says companies must remember that identity management has evolved beyond a simple administrative tool that adds, removes, or changes user IDs; today, the function ties into compliance and audit requirements at a deep level. “So it’s important to understand what the business relationships are and what the processes are that you’re trying to integrate this with,” he says.

## Implement Smart

This, too, sounds obvious, but identity management carries some specific wrinkles in implementation. Idan Shoham, chief technical officer of identity-management software company M-Tech, says phased implementations are the way to go: Turn on the easy stuff first, then roll out elements requiring deeper business-process analysis and systems integration.

Deloitte takes the same approach.

“Don’t try to do the Big Bang,” Ford says. “If you try to set the architecture up and roll it out across the enterprise, you will fail.”

Shoham says simple password management should happen before more complex access management and user provisioning. Likewise, a manual system of streamlined, centralized user provisioning should be in place before

---

**“One needs to be compliant with the generally accepted infrastructure in this globally connected world,”**

— Roger Sullivan,  
Vice President,  
Oracle Identity Management

---

launching automated workflow and rules-based provisioning.

Shoham also stresses the need for strong leadership in identity-management projects, since they spill across many corporate fiefdoms. Finally, he says, a system's value "should be measured, not promised," meaning companies should track effects on administrative labor and the reduction in orphan accounts.

### **Forget About ROI (Sort of)**

Some benefits of identity management you can measure. Others, you just can't.

One area where ROI can be measured, Ford says, is in simpler audits. With a steady level of trust in identity-management systems, auditors can focus on one central system rather than plowing through every access control across the company, he says.

Also—particularly with large-scale implementations—savings can be significant when streamlined identity-management processes cut human administrative overhead.

But, Kampman argues, identity management's value is deeper. It is a fundamental part of clarifying an organization's operational nature, which has become blurred through years of cobbling together systems and responsibilities based on the latest pressing need.

"I think the return on investment is return on organization, because you need to understand what your business is about," he says. "We've created infrastructure we don't understand."

---

Compliance Week provides general information only and does not constitute legal or financial guidance or advice.