

# IDENTITY MANAGEMENT: EASING THE COST OF COMPLIANCE

Corporations have spent billions in the past few years on regulatory compliance—and research shows there's no end in sight. Many are now turning to **identity management technology** to ease the burden.

It's difficult to recall a time when companies were subject to so many regulations. Due to the need for greater data security and demands for improved corporate accountability, the federal government and certain industries have developed a series of laws and regulations guiding many corporate processes that previously were not deeply scrutinized. And as Congress considers even more regulations governing issues such as consumer privacy, it's likely that the compliance burden will only get heavier for many businesses.

In the past few years companies have had to comply with a string of regulations covering multiple aspects of their operations. Among the key mandates that have had a big impact on businesses and IT functions are the Health Insurance Portability and Accountability Act (HIPAA), a law designed to secure electronic patient information; the Sarbanes-Oxley Act (SOX), which requires all public companies to substantiate financial statements with proof of the procedures and controls in place; the Gramm-Leach-Bliley Act (GLBA), which requires banks and financial services firms to protect customer data; and Basel II, which stipulates conditions for adopting more risk-sensitive minimum capital requirements for banking organizations.

## High Costs, High Risks

So it's little surprise that the cost of compliance is high. A study by AMR Research in 2005, *Spending in an Age of Compliance*, predicts the cost over the next five years will hit \$80 billion. The report by the Boston firm, based on a survey of 225 business and IT leaders on their compliance spending priorities, estimated that organizations will spend nearly \$15.5 billion on compliance-related activities in 2005 alone.

Financial Executives International (FEI), a Florham Park, N.J., group representing corporate financial managers, reports that public companies' total costs for the first year of SOX Section 404 compliance averaged \$4.36 million—39 percent higher than the \$3.14 million companies

expected to pay. The data is based on a survey of 217 public companies with average revenues of \$5 billion.

In addition to the added costs, the compliance effort is requiring more staff time and resources, especially within the IT department. According to a survey conducted by *CIO Insight* magazine earlier this year, companies expected to devote about 12 percent of IT staff and 8 percent of IT budgets to regulatory compliance work in 2005.

Much of that time and resources have been focused on learning exactly what the regulations mean to the enterprise and the business impact. In many industries there is still a lack of understanding of what companies need to do to comply and how peers are addressing the compliance challenges.

The complexity is increased as different auditing firms emphasize different controls, so organizations in the same industry might be getting different advice than other companies. In many cases, the process of becoming compliant is much more complex than financial and technology executives anticipated. The amount of documentation, time and effort required to comply with Sarbanes-Oxley, for example, can be staggering.

While many companies have learned a lot in the first year of SOX compliance, quite a few are still seeking guidance and input from the Securities and Exchange Commission on how to proceed.

Despite all the costs and aggravation of compliance, the penalties for not complying are even higher. Failure to abide by the rules could result in possible jail time for CEOs, CFOs and other senior executives. Organizations could incur steep fines as well as criminal and civil prosecution.

Then there's the cost of negative publicity surrounding a lengthy investigation that could result if a company is caught failing to comply. The bad press could lead to lost business, as customers and partners take their business elsewhere. The bottom line: regulatory compliance isn't going away, and companies must find a way to deal with it effectively or bear the risks.

## The Identity Management Solution

As part of compliance efforts, many companies are turning to identity management technology to meet data security requirements. Identity management enables organizations to better control who gets access to what systems and applications at any given time. Compliance-level accountability demands this kind of control over access to information, and the ability to prove that controls exist and are enforced.

Identity management provides accountability through single sign-on, authentication, federation, user provisioning, and identity administration capabilities. It allows enterprises to centrally manage users' identities and access rights; enforce segregation of duties; restrict access by maintaining tight control over user permissions and privileges; and automate processes and reporting.

Organizations that deploy identity management are able to automate, control, track and document processes from beginning to end—a key requirement for compliance. For identity management systems to be effective they must be comprehensive, end-to-end solutions. If organizations are to comply with regulations, they need to have control of the entire life cycle of each individual identity.

Large, global organizations typically manage thousands of identities and access privileges across various enterprise applications and resources. This underscores the need for a heterogeneous identity management solution that can plug into all these disparate resources.

Access to corporate information also changes in response to business events, such as mergers and acquisitions, employee hires and moves, and the addition of new business partners. An identity management solution must be able to support these changes.

Oracle delivers all these ID management capabilities with Oracle Identity Management, a comprehensive, end-to-end identity and access management infrastructure solution that protects information, critical business systems and applications against unauthorized access. Oracle Identity Management, which is part of the Oracle Fusion Middleware family of products, includes a suite of identity management functions that are fully integrated into a broader framework that can be leveraged throughout an enterprise—dependent of

application, directory and platform.

Organizations using Oracle Identity Management realize several key benefits. As the technology enforces consistent business rules and practices, enforces control over access to applications, and provides reports and auditing on identity life cycle events,

organizations can enhance enterprise-wide compliance.

Another benefit is reduced operational costs. Identity Management automates life cycle management for potentially millions of users, delivering single sign-on to improve user productivity and decrease password-reset costs. And the software helps strengthen security by eliminating delays in the setting of access privileges after identity and policy changes.

### Steps to Success

To help ensure a successful identity management strategy, technology executives should take these steps:

- **Take a "top-down" approach.** That means getting buy-in for an identity management rollout from senior business executives, line-of-business heads and technology managers in the organization. Agree on current and future business goals related to the identity management initiative.
- **Think long term.** The identity management solution put in place must be adaptable to new applications and allow companies to keep up with new regulations and changes in existing laws.
- **Evaluate your environment.** Make business goals, not existing infrastructure, the determining factor in decision-making about identity management. Consider the strategy within the context of a services oriented architecture/ Web services environment. Take into account products, customers, and points of distribution.
- **Test, test, test.** Deploy the technology, then test and review its performance on a scheduled basis or whenever regulations or business conditions change, such as a merger or acquisition.

Systems, applications and information are far too critical to business operations to be left unprotected, and that's especially true in this new age of regulatory compliance. A comprehensive, end-to-end identity management solution can go a long way toward helping an organization control access and comply with the rules. ■

## THE HIGH COST OF COMPLIANCE

### \$15.5 BILLION

Amount organizations will spend on compliance-related activities in 2005

Source: AMR Research, "Spending in an Age of Compliance," 2005

### 70,000

Additional man-hours spent by large firms on SOX compliance

Source: Deloitte

### 2/3

Percentage of compliance budgets spent on internal staff and external consultants

Source: AMR Research ("Compliance Spending Soars," searchCIO.com, April 27, 2005)

### \$2.4 MILLION

Average amount paid by companies for audits, in excess of what they had anticipated

Source: FEI

### 70%

Percentage of reported SOX 404 deficiencies directly related to ineffective identity and access management practices

Source: Ernst & Young Engagement Analysis, June 2004