

# Compliance: The Key to “How” May Be “Who”

BY SARA GATES

Now that the processes have been laboriously documented and manually verified once, it is becoming clear that the key to maintaining ongoing compliance at a reasonable cost is the automation of some or all of the compliance auditing process.

How can that task best be approached? Since the answer lies in knowing who does what in your systems – identity is the key.

**I**n just the last few years, compliance has become one of the most pressing business challenges for organizations in a multitude of industries. Since the passage of legislation such as the Sarbanes-Oxley Act of 2002, the Healthcare Insurance Portability and Accountability Act and the Gramm-Leach-Bliley Act, companies are scrambling to meet new requirements for protecting the integrity and privacy of critical business information.

Billions of dollars are being invested and millions of hours spent on the effort to achieve compliance. The need for a cost-effective and sustainable approach to the



---

## Unlike Y2K or other major IT initiatives of the past, compliance involves not just one large project, but a continuing effort to comply and to demonstrate compliance to auditors – making identity auditing part of the everyday fabric of business.

---

challenge is becoming increasingly apparent. Identity management and, specifically, identity-based auditing are key to enabling ongoing compliance, and a strong case can be made that they are one of the most important components of any cost-effective, sustainable approach.

### **Identity's Central Role in Compliance and Corporate Auditing**

When you consider the obvious questions associated with compliance, one theme emerges over and over: “Who?” Who has access to critical data? Who has access to financial systems? Who has access to the systems that feed the systems that report on the health of the business? The importance of “who” makes it clear that identity is an essential component of compliance. And that makes it critical to be able to keep track of identity information.

Consider the Sarbanes-Oxley Act of 2002 (SOX), which mandates that, as part of the effort to ensure that financial statements are accurate and complete, publicly held companies must establish adequate internal controls around financial reporting. Establishing these controls requires implementing financial reporting processes and protecting the information that goes into those reports. Compliance thus requires knowing who has access to this information, wherever it is. Proving compliance requires tracking and archiving that access on an ongoing basis.

As organizations work to achieve these objectives, the costs will be significant. Gartner surmised early on (in the October 2003 report “You’ll Have to Spend to Attain Sarbanes-Oxley Compliance”) that large and midsize enterprises would spend

up to \$2 million each through 2005 to become compliant, thus bringing the total costs into the billions. And just last November, AMR Research projected that spending on SOX compliance would grow to \$5.88 billion in 2005.

Whereas SOX mandates how corporate financial information is handled, the Health Insurance Portability and Accountability Act (HIPAA) and the Gramm-Leach-Bliley Act (GLB) require that individual health and financial information, respectively, be kept private by healthcare-related organizations and financial institutions. As with SOX, complying with these mandates requires knowing where the information is, who has access to it and when it’s being accessed. At least one industry analyst predicts that financial-industry spending on GLB compliance will reach \$170 million in 2006.

But if the cost of compliance is high, it’s nothing compared to the cost of noncompliance. Penalties for noncompliance with SOX and HIPAA include both hefty fines and possible jail time. And in the first cases brought by the Federal Trade Commission for GLB violations, two mortgage companies are being required to submit to rigorous regular audits of their information security programs for the next ten years. What will be the cost to these organizations of getting through these audits successfully? What will it cost them if they fail?

### **Identity and the Never-Ending Nature of Compliance**

Identity management and identity-based auditing can enable ongoing compliance and help avoid audit failures effectively

and cost-efficiently—by meeting head-on two specific aspects of the challenge. First, they address the fact that achieving compliance is an ongoing process that must be sustainable in practical ways over the long term. Second, they deal with the problem of the identity-related information required to achieve compliance existing in a potentially unlimited number of places throughout the enterprise.

Ongoing compliance. Unlike Y2K or other major IT initiatives of the past, compliance involves not just one large project, but a continuing effort to comply and to demonstrate compliance to auditors. Day in, day out, organizations must be aware of who has access to what information and track that access in accordance with compliance requirements. Managing the identity lifecycle is central to achieving this, and it provides a good example of just how challenging ongoing compliance can be. After investing a tremendous amount of effort in data-cleansing and reviewing user access privileges to get to an initial state of compliance, the enterprise then has to continually re-check those privileges and ensure that access stays appropriate for every user – because responsibilities are continually changing as people change job roles or end their relationships with the enterprise.

Manually monitoring user access controls to maintain ongoing compliance is costly and labor-intensive, not to mention inefficient and error-prone. But it appears to be the route many organizations are taking: According to AMR, the largest category of spending for compliance in 2005 will be internal labor/head count, accounting for 42% of the total

that is expected to be spent. As compliance pressures increase, it seems likely that this will prove unsustainable.

Alternatively, identity management technology can address the ongoing need for compliance by automating – and thereby making more efficient and cost-efficient – the provisioning and other processes that are related to monitoring and controlling access to information. This will reduce the need for ongoing expenditures for staffing and services.

While identity management in general can be used to automate information access-related processes, maintaining and demonstrating compliance requires a more specific capability. Identity-based auditing can provide the insight into access and access violations that is necessary for staying in compliance. It can define why access is granted on any given occasion, detect violations and potential violations of access policy and take steps to remediate and mitigate in the event of a violation. Perhaps most important, identity-based auditing can take the information from identity management processes and use it to create a comprehensive and ongoing trail of accountability that demonstrates compliance.

Infinite sources of information. Identity management and identity-based auditing centralize control over information access to overcome the otherwise overwhelming challenge of gathering identity and access data from multiple sources and resources throughout the enterprise. They provide a central point through which to determine and report on who has access to what at any given time, streamlining the otherwise laborious process of pulling information together from many disparate places.

---

## Identity-based auditing can take the information from identity management processes and use it to create a comprehensive and ongoing trail of accountability that demonstrates compliance.

---

Having a central point of control is important because, at any given time, a user may have accounts on many different applications and operating systems. To check for compliance without such centralization, audits have to sample the accounts associated with each system and manually inspect the various access permissions to see that there are no conflicting permutations. To complicate matters, if there are policy exceptions, the auditor has to painstakingly retrace the steps by which the user gained access and establish a trail of approval. That trail is likely to be based on little more than email accounts and paper forms filled out by administrators who approved the changes. This manual process is time-consuming and risky. If the trail is not sufficiently traceable, it could become evidence of a compromised control environment – which could lead to an even longer and more invasive audit.

Identity-based auditing can drive the effectiveness and efficiency of compliance by automatically scanning for policy violations and audit exceptions across heterogeneous applications and systems enterprisewide. Identity-based auditing solutions that also automate the process of remedying exceptions as they are detected provide the added advantage of addressing the legal culpability associated with reacting to the potential for fraud in a timely way.

### Summing up the Value Proposition for Identity-Driven Compliance

An identity-driven approach to compliance moves an enterprise from relying on manual, fragmented processes to maintaining a monitored, optimized state of compliance.

This helps not only to enable successful compliance, but also to control the ongoing cost associated with compliance efforts.

A comprehensive identity management and identity-based auditing solution can:

- enable repeatable, sustainable and cost-effective compliance with existing and emerging mandates for protecting the integrity and privacy of information
- make compliance proactive by automating identity management processes, including the detection and remediation of problems and the creation of audit trails
- operate across, and centralize control over information from, multiple applications and resources throughout the IT environment

It's worth considering, too, that however challenging compliance may seem already, it's likely to get even more daunting. More regulations will be defined. Additional compliance deadlines will arrive. New audit requirements will be announced. Meanwhile, enterprises are still catching their breath from meeting some of the SOX and HIPAA deadlines that came in 2004. Who knows what's next? The best bet is to be prepared now. ■



Sara Gates is Vice President of Identity Management for Sun Microsystems. She may be reached via email at [Sara.Gates@Sun.com](mailto:Sara.Gates@Sun.com).