



# MOVING FROM MANDATE TO DIFFERENTIATOR

**THE RIGHT IDENTITY, ACCESS AND SECURITY MANAGEMENT TECHNOLOGY  
ENABLES EASIER COMPLIANCE AND COMPETITIVE ADVANTAGE FOR THE BUSINESS.**

Compliance doesn't have to be daunting. The best identity, access and security management technologies help companies establish the controls and business structure that enable governance. And, with that in place, compliance comes naturally, putting CSOs in the driver's seat with automated, on-demand compliance capabilities to make audits more effective and efficient.

It's no secret that security and compliance violations today can prove disastrous. Corporate fumbles can quickly become headlines, thrusting customers into the waiting arms of the competition. Well-thought-out governance, risk and compliance (GRC) strategies help companies large and small avoid those nasty entanglements.

Compliance is no longer the dreaded topic that it used to be, a mandate imposed by outside forces. "Today, compliance is more often self-imposed," says Ross Chevalier, CTO Canada for Waltham, Mass.-based Novell. "It's a differentiator, an opportunity to prove trust and competence."

Perhaps that change in mind-set stems from the fact that getting the corporate house in order and preparing for audits don't have to be as convoluted as once expected. "If we achieve our security goals, proving compliance is simple," says Mike Johnson, security architect for Ingersoll Rand.

According to a recent survey by IDG Research Services, that's exactly what smart business and IT leaders are doing. This report sheds new light on why many companies are implementing identity, access and security management technologies to automate the compliance process. Key findings of the research include:

- Risk management and compliance rate high as drivers of identity, access and security management.
- The ability to "prove" compliance is considered the top benefit of implementing identity, access and security management solutions.
- When it comes to successfully identifying and

managing risk, many companies score lower than one might expect.

## Security Tops the List

In today's digital economy, security and risk management are a priority for most organizations. The right processes and systems safeguard intellectual property, protect private customer information, and keep companies from crumbling under the negative press that inevitably comes with security violations. Perhaps more important, they put the necessary controls and business structure in place to prove compliance—if or when the need arises.

In the IDG survey, more than three-quarters of respondents assign a critical or high priority to their companies' ability to identify and manage risk. At the same time, a majority consider the ability to prove compliance, secure access for remote employees and 24x7 security monitoring as critically important.

Addressing those priorities may seem complicated, but several key components make for a practical strategy, which can be delineated as such: Security management is a holistic view of "how security is done" within an organization. Identity management is a standard around which the question "who are you?" can be answered. Access management is a standard that helps define which identities are granted usage of assets. Although these are discrete disciplines, together they comprise a complementary set of technologies that contribute to good governance.

"We must be able to tell 'who that is' and manage the 'what and when' parts of administration," says Johnson. "Without identity and access management, there is no way we could achieve our goals." He believes identity and access management are foundational building blocks that help ensure that "the right people have the right access to information."

**Novell**® **CSO**  
Custom Solutions Group



The majority (71 percent) of survey respondents are already using security management solutions at their companies, 66 percent are using access management and 62 percent identity management solutions.

#### **It's All in the Proof**

GRC is the main driver behind identity, access and security management implementations. In fact, 81 percent and 77 percent of respondents, respectively, indicate high significance for risk management and compliance as drivers, while 64 percent give equally high marks to business governance.

"One of the greatest challenges under GRC is not that you say it's so, but that you can show it is so," Novell's Chevalier says. "Identity, access and security management provide proof points in the context of authoritative data so you can do just that."

This certainly comes to bear in the research findings. Respondents point to many of the benefits one might expect, such as secure access for remote employees, centralized access management and easier implementation and enforcement of IT policy. However, the most commonly referenced benefit, as indicated by 63 percent of respondents, from implementing identity management, access management and security management solutions is the ability to "prove" compliance.

"Trying to achieve compliance without putting all your ducks in a row is a frivolous activity," says Ivan Hurtt, senior product marketing manager at Novell. Focusing on security naturally leads to the ability to prove that what you say is so, really *is* so.

"The IT industry needs to realize that compliance isn't quite the bogeyman that it used to be," says Johnson at Ingersoll Rand. "With a good security program, compliance follows." Indeed, he says, the best way to build a bad security program is to make compliance the objective.

#### **Success Me Not**

From a trenches perspective, Gary Meech, CISSP manager of information security and privacy with American Airlines, says identifying and managing risk can be likened to "climbing a high mountain in the dark without safety ropes." Creating a process to provision accounts and providing access with the right levels of security by identifying all the different people in the organization, he says, is very challenging.

## **Identifying and Managing Risk: Getting It Right**

The IDG Research Services survey revealed an alarming gap between the high priority respondents place on identifying and managing risk and the low success rate they think their companies have achieved to date. For those caught in the gap, here are a few remedial steps that can help put success within reach:

- Make it a corporate initiative, complete with senior executive sponsorship. IT can't do it on its own.
- Work in smaller groups; they are more conducive to getting things done than large committees.
- Break down the initiative into doable chunks, focusing on high-visibility outcomes with a short term to value.
- Implement a system that can aggregate multiple identities into a single entity. This is critical for manageability, security and cost-efficiency.
- Automation is key. Manual processes are time-consuming and error prone; automation capabilities can be the difference between passing and failing an audit.
- Don't try to answer the big question of compliance. Rather, implement systems so the answers are there when needed.

"Above all," says Novell's Ivan Hurtt, "remember that with the right security in place, compliance will follow naturally."

Perhaps this explains why respondents rate their companies' success at such tasks as relatively low—especially considering the high priority ratings they give to identifying and managing risk. Although the ability to identify and manage risk is a top priority for 77 percent of respondents, just 34 percent say their companies are extremely or very successful at doing so.

Whether risk has been mitigated is not a black-and-white issue, and most CSOs have nothing by which to compare success. Novell's Hurtt contends that



the difficulty lies in aggregation and analysis. CSOs must look for anomalies over a variety of systems and then look at that information holistically. Additionally, manual processes and application silos make it nearly impossible to correlate data. So, it's the lack of visibility and correlation of information, he says, that prevents companies from proving compliance—that is, verifying that violations are not happening—and achieving success.

Still, success boils down to one thing: Are you able to identify where you have security anomalies and policy violations? That's a question that can't be answered without "virtualizing" a user's multiple identities down to one entity, Hurtt states. A user is a single person, but companywide, he may have different identities across 150 unrelated systems. CSOs need visibility into the big picture, and must be able to aggregate user data across the entire corporate landscape.

In addition, separation of duties and the ability to manage identities over their entire life cycle is core to proving compliance. "[Identities] are doorways into your information systems, so provisioning them correctly—giving just the right amount of access—is critical to ensuring separation of duties," says Meech. When an employee leaves the company, his account must be disabled in a

timely manner, he says, especially given litigation e-discovery rules CSOs will be hard-pressed to accomplish any of this without identity, access and security management technology.

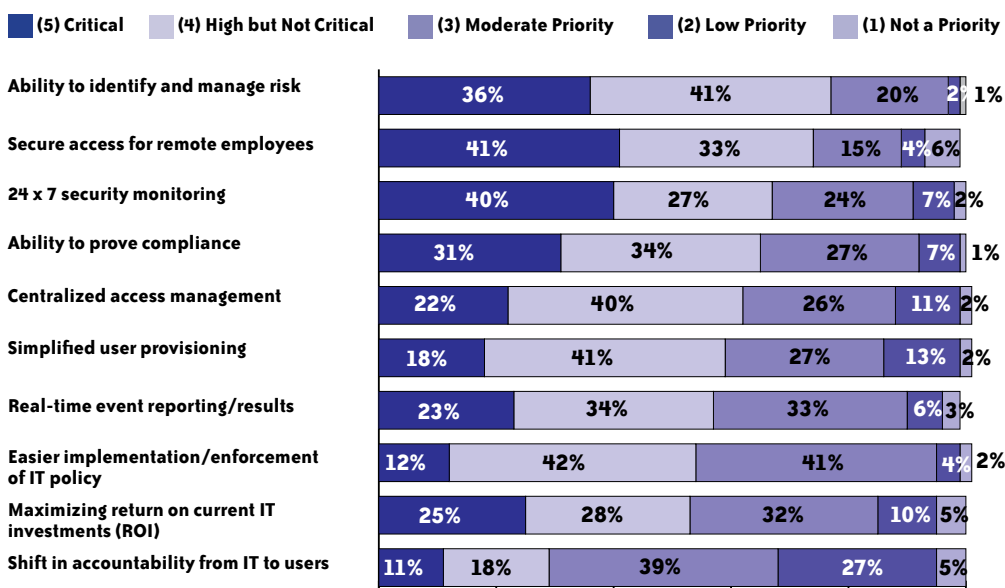
### Automate, Automate, Automate

Automation is one sure route to compliance because it forces better management of identities, separation of duties, consistency in policy enforcement and, more generally, good governance. And automation offers "compliance on demand," Chevalier says.

That gives CSOs control. They can license compliance monitoring tools, responding to audit requests with a push of a button. Or, when requests come in, they can bring business to a standstill while the IT department scrambles to construct each compliance entity. The work required could take an entire IT group off-line until it's complete because the amount of data that must be gathered and analyzed is enormous. "It's the audits and the follow-on questions—not the fines and judgments—that can put you out of business," says Chevalier.

In the end, it's far easier for auditors to believe that the people involved in a manual process could make a mistake than to believe there could be a glitch in an automated process.

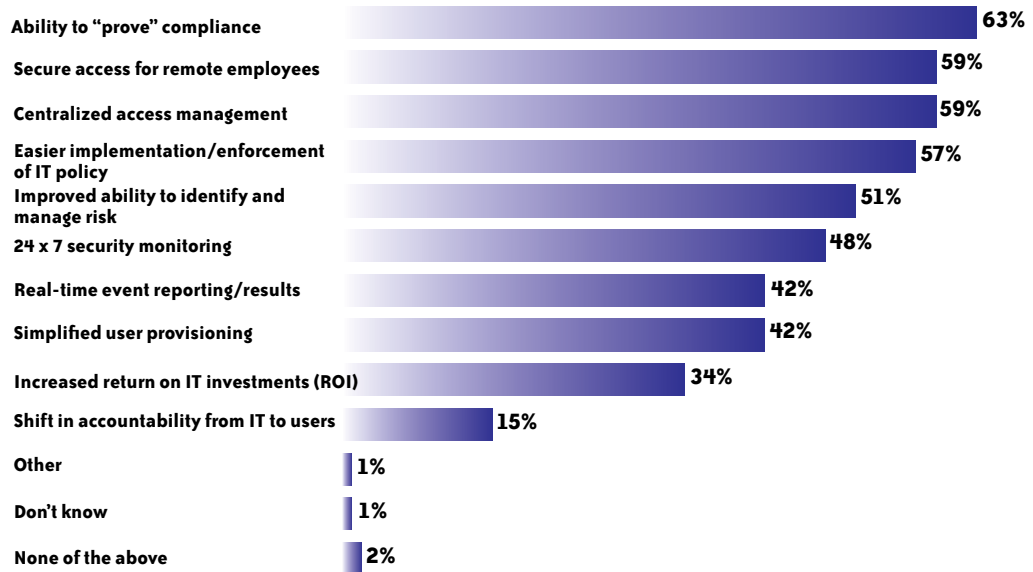
## Importance of Outcomes During the Next 12 Months



Source: IDG Research, 2007



## Benefits Experienced as a Result of Implementation of an Identity Management, Access Management or Security Management Solution



Source: IDG Research, 2007

### Paying the Price for Compliance

However one gets there, compliance may still be perceived as a must, rather than an opportunity. So is it really worth it to put all these pieces in place? "Yes," says Chevalier. "There are controls and business structure that come with it, so there is definite value to be had."

That value comes in a variety of forms. Better user life cycle management means companies are more likely to be on top of employee changes, ensuring that access privileges are accurate and timely. Enhanced password management means fewer passwords for users to remember, and codes that can be more complex and changed more frequently. And simplified sign-on—as the name suggests—simplifies work processes, making users more productive.

Indeed, operational efficiency is something companies don't necessarily expect to achieve. Considering the potential reduction in overall IT costs, implementing identity, access and security management technology "is a smart decision even if you take compliance out of the equation," says American Airlines' Meech. With these solutions, companies gain streamlined management and automation, in addition to savings from simply re-

ducing password resets, which may cost companies upwards of \$80 per occurrence.

The real value, however, comes from protecting the corporate brand and reputation. Of course, customer value is a complicated differentiator that varies with every company, but compliance is a tool that facilitates the creation of trust and competence. Compliance is therefore important, not just because it's required, but because it can and should be used for competitive advantage.

In the end, simply ignoring compliance could put an organization in a precarious position. "Many of our clients realize that if they don't use compliance-oriented technology they can effectively be putting themselves out of business," says Chevalier. So putting the right identity, access and security management technology in place would seem to be a no-brainer.

To learn more about how you can leverage automated compliance as a point of differentiation for your business, go to [www.novell.com/identity](http://www.novell.com/identity)

Copyright © 2008 Novell, Inc. All Rights Reserved. Novell, the Novell logo and the N logo are registered trademarks of Novell, Inc. in the United States and other countries. \*All third-party trademarks are the property of their respective owners.