



Provisioning: THE FOUNDATION OF AUTOMATING

Automating compliance begins with knowing who has access to what and implementing procedures that assure it. This moves provisioning front and center in the race to find ways to automate compliance. In fact, many of the evolving efforts at compliance automation are growing directly out of provisioning's identity life cycle management and workflow automation technologies.

The concept of automating compliance is relatively new to enterprise. "2004 was the year that most organizations got it into their heads that they needed to address compliance," said Paul Proctor, VP and Analyst in the Security and Risk Strategies practice at Meta Group. "But they focused on process and getting their houses in order. Coming out of their first round of SOX audits they are now saying, 'what can we do to make that easier next year?' And they are realizing that it's twofold – they've got to get their act together with respect to identity, then they have to start automating some of those processes."

But having gone through that pain, most companies are not yet looking to technology to help automate their compliance processes. "It will be a little bit better this year because they're

not starting from scratch," said Proctor. "[Last year companies] threw the people together, spent the effort in downloading all the reports from the machines, looking through them manually and deciding where the risks were. Because they went through that once it will be easier to go through it a second time. But they weren't thinking about what they could change to make it easier, they were just focused on getting it done."

Even though compliance is already driving a marked increase in identity management sales, we are only at the beginning of the up tick. "2005 is going to be the year that people start looking at the automating technologies," said Proctor.

Starting With Identity

Regardless of the regulation, compliance is about knowing who did what when; having processes in place to

assure that only the proper people can do what when; and being able to prove that those processes are being followed. To automate compliance then, you must have access to a well maintained identity store – one where you know that policies

that we have today, user provisioning is a key technology,” said Mark Ford, Principal, Enterprise Risk Services, Deloitte. “Public companies are investing in processes and technology that authorize a person to have access to critical transaction processes. They are also looking to automate the ability to completely manage the process when that user moves from one job to the next so that they gain new privileges, and lose the old privileges. Finally, they are looking to automate the termination process. A provisioning system is a technology that can help companies solve that problem today.”



Coming out of their first round of SOX audits companies are now saying, ‘what can we do to make that easier next year?’

were correctly followed to set up users and create or modify their access privileges. This process, known as identity life cycle management, is at the heart of identity management.

Modern provisioning technology combines the policy driven management of identity life cycles with the automated propagation of that identity information to the locations required to put the desired access authorization policies into operation. Provisioning products vary architecturally (and significantly) as to how they implement these functions, but they all implement identity life cycle management and deploy the result to the systems that require it.

“In trying to automate some of the [compliance] processes with the technology

In many ways the driving force behind provisioning as a first step for compliance automation is actually de-provisioning – removing user access rapidly and with assurance it has been removed in all appropriate locations. “In the last twelve months, there’s been a shift in what’s the most urgent project,” said Sara Gates, VP Identity Management, Sun Microsystems. “The primary phase one project now is de-provisioning when people leave, and reporting on who has access to what.” Gates indicates this shift has been driven by compliance audits. “Big companies have been grappling with what do they have to prove to auditors. They’ve got these manual, cobbled together, expensive processes that are barely holding on and it’s absolutely not sustainable. Making compliance sustainable is critical this calendar year.”

Creating the Foundation

“There are certain capabilities of identity management, some of them new, some of them existing, that customers are looking for when we say automation,” said Gates. “The foundation would be a report of who has access to what, by business manager. Send it quarterly, make the approval and authentication an audited event, and keep it in an audit log for seven years. That’s a real simple example where you



are attesting once a quarter in an automated fashion instead of a manual fashion ‘who has access to what’ and making approvals part of that cycle.”



People have always had to do these things, they just did them manually and inefficiently.

Most provisioning systems are capable of this level of compliance automation. Simply centralizing provisioning of access into such a system creates a single place to pull the current status of who has access to what. However, the heart of “making the approval an authentication and audited event” is the provisioning system’s life cycle management workflow capability, and here there is significant variation among product features and capabilities.

The Importance of Workflow

Compliance policies will spell out who in the company has the authority to

grant access to various resources. In some cases, there will be a policy involving multiple approvals that must be followed to grant a person access to a resource. Robust workflow capability in a provisioning product is the key to being able to automate these policies without involving IT people directly (unless the policy calls for that.)

Workflow rules take the approval process and implement it as a set of automated rules. These rules allow anyone to request access to a resource, and then automatically stage the approval process to the proper people within the company. If there are multiple approvals required, workflow may first automatically send the request to a department manager for approval, then when the manager approves the request it may be sent on to the application’s owner for further sign-off before access is granted. Sophisticated workflow systems can allow intricate rules about things like automated escalation of non-responses from approvers (who may be sick or on vacation) as designated by the policy.

Workflow systems can not only automate access approval policies, they can log for audit purposes what has happened, who granted approval when, perhaps even adding notes about why if the approval is exceptional to the policy in some way. This type of audit trail forms the basis for automating the first level of compliance verification. The policy itself is approved, the auditors are shown how that policy was converted to an automated set of rules that implement it in workflow, and the audit trails verify that the policy is being followed.

Workflow and Compliance

“The underpinnings of compliance are really geared to ‘can you show me that you’ve got a process in control to manage the risk in these types of activities,” said

The heart of “making the approval an authentication and audited event” is the provisioning system’s life cycle management workflow capability.

Kurt Johnson, VP Corporate Development, Courion. “And the second piece is ‘can you prove it?’ By automating these things through [provisioning] you can say [to an auditor] here’s our process and here it is automated. [Then] they know you can’t get outside the boundaries any more because you’ve automated that process, and the reporting functionality and the ongoing access validation and verification prove it.”

Courion has extended the concept of workflow policy specifically to handle compliance. As part of their Compliance Courier product they have added to the specific access authorization workflow a layer of global compliance policy checks for things like the Segregation of Duties requirements of Sarbanes-Oxley. This added, decoupled, policy layer checks access approvals that would otherwise be within company policy to see if they would violate compliance policies. If they do, then alerts can be sent, the workflow can be modified, or the approval can be routed to a different workflow or simply denied as desired.

The Next Level

The reports that provisioning can generate, and the policies around granting access that workflow can automate, form the foundation for compliance automation. Now that compliance automation is starting to be considered more deeply, however, we are starting to see products that leverage provisioning infrastructure to go further. Courion’s Compliance Courier – released last July - grew out of a customer’s compliance needs.

“The driver was the merger and acquisition activity [of a financial services

customer],” said Johnson. “The [regulators] were on them to ensure they had processes in place for managing accounts, privileges and access because there were such diverse operations from so many different factions of the consolidation happening. People have always had to do these things, they just did them manually and inefficiently. In their case they were pouring out reams of reports that by the nature of the reports and how they were being processed weren’t really meeting their business requirement. It wasn’t effectively clamping down on this process.”

“All the information was there within our product and how our product was being used,” said Johnson. “We have information on who had access to what, we’re setting up roles and rules to define what people should have access to, and we can we compare those things. So we started to extrapolate all this data and run some comparisons.” That’s where Compliance Courier was born. In July 2004 the company released a productized version.

Sun’s recent Identity Auditor product developed from an integrated look at the problems of compliance automation. “We think a lot about the identity and what compliance is bringing to identity management,” said Sara Gates. “You’ve got to be able to look at multiple systems in the context of a single policy violation. The starting point is scanning multiple applications for separation of duties, general ledger access, unauthorized general ledger access, and some other very basic foundational elements. And that’s where we see people today. This last twelve months their pain comes from the fact that

they’re writing scripts to scan logs and correlate, they’re manually looking across access control lists and seeing where their policy applies. It’s a nightmarish situation in terms of not being automated, and the lack of that automation really taking unbelievable man hours.”

Sun’s response was their Identity Auditor product. Built on the foundation of the provisioning experience brought by the Waveset acquisition, Identity Auditor integrates across the wider set of Sun’s identity products to provide a deeper automation of compliance.

Summary

The process of using identity to automate compliance begins with provisioning. “About six months ago, we started seeing people put provisioning in place for critical apps for two reasons,” said Gates. “So you can hook into HR and revoke access close to immediately and so that you can do reporting on who has access to what and make it an attestation process.”

The next process is to start to automate scanning across systems for more global compliance violations such as segregation of duties. “Starting late last year and early this year was the need to scan across those systems for policy violations. Because de-provisioning and reporting establish a baseline for compliance.”

Compliance automation technology is destined to evolve significantly in the years ahead. But it seems certain that provisioning will remain its foundation. ■