

Don't Let The Circus Distract You



BY ARCHIE REED

With all the noise around compliance in the identity management market today, you could be forgiven for thinking the circus has come to town. Every vendor is touting their solutions as being able to deal with your compliance needs today – even mine. While compliance is certainly the big stick to drive justification of Identity Management, however, assuring success requires that the traditional goals for Identity Management not be forgotten when justifying delivery.

*Welcome back my friends, To the show that never ends,
We're so glad you could attend, Come inside, come inside,
There behind the glass, is a real blade of grass, Be careful as you pass,
Move along, move along.
We would like it to be known, the exhibits that were shown,
Were exclusively our own. All our own, all our own.*

- Emerson, Lake and Palmer, 1972

The new Identity Management Circus is in town, and continues to add attractions. Now, center stage, our most feared, yet most popular attraction so far: Compliance. Beware... this beast can bite, you could lose a limb. It takes a trained professional to understand how this beast thinks. But with help, you can get close and learn more.

This is how I feel sometimes as I read the press, and wander through shows like the February 2005 RSA Security show. Every man and his dog, vendor, consultant, analyst, and journalist owe the new compliance initiatives a great deal of thanks for providing a raft of justifications to push solutions into organizations. The barkers are announcing their compliance initiatives and enticing customers with a lot of

good commentary, yet there are numerous sideshow tricks being employed as well to get you in the door.

Perhaps that's where the analogy falls down, because vendors actually want to get in your door. Yes, I work for a vendor and I am in the mix, but please bear with me. The intent of this discussion is to take a brief look at the noise around compliance, why is it there, and how it is playing out on a worldwide stage. I'll conclude with the key approaches to justification for Identity Management, and key considerations around including compliance deliverables in such a project.

Avoid Fear Based Perspective

Some observe the fallen idols of compliance such as Enron, WorldCom or

continued on page 67



Don't Let The Circus Distract You

continued from page 80

similar. Perhaps it is the prophets of compliance, the great Gramm, Leach, Bliley, Sarbanes or Oxley, with their great tomes in which they write great words of requirements. Certainly that is initially a US centric viewpoint, so don't forget the worldwide initiatives around privacy and electronic commerce. Corporate Governance initiatives worldwide are increasing as more governments and industry groups are defining requirements for organizations to incorporate into their internal policies and processes.

It's About Business Processes

Many organizations have identified compliance as a critical initiative, yet consider it a pure money-pit. Things such as internal processes should be able to be short circuited to support business requirements, but that is exactly what regulatory compliance prohibits. Good compliance initiatives, however, are founded in good business processes. So compliance is not necessarily the burden it appears. Thankfully it does offer significant value to organizations – beyond just getting some projects approved.

Security and IT buyers today are also using compliance initiatives to support their own initiatives – modifying the goals or deliverables to fit their needs so they can get the dollars. The key here is to ensure that while you deliver on compliance requirements, other benefits are also illustrated.

Good compliance initiatives are founded in good business processes. So compliance is not necessarily the burden it appears.

The reason for this is that sometimes all compliance objectives are not met initially in an identity management initiative, and it pays to have other success metrics to justify the project. Beyond compliance driven by regulations and corporate governance, the basics count including: security; cost reduction; revenue enhancement; and better, faster integration of partners and customers.

Kevin Kampman of Burton Group notes “Don't bank on any single one of these elements to justify Identity Management initiatives.” Critically, the observation is that “Organizations need to carefully balance the right drivers – more than one – to ensure measurable success.”

Compliance Plus Productivity

While Identity Management helps organizations improve their compliance levels, it also helps streamline the ongoing compliance efforts. As noted by Jonathan Penn of Forrester, “IT itself is often viewed as a cost center – IT security even more so, and compliance even more so. Therefore, the same ‘selling’ techniques that made provisioning attractive as a way to wring efficiencies (i.e., cut costs) from IT security administration can be very neatly applied to compliance.”

While there is a definite focus on the US and Europe in many of these compliance objectives, the reality is that this is a worldwide phenomenon. The interesting thing is that Kampman's comments around identifying the “right drivers” are especially true when you consider the goals of geographically or vertically specific organizations.

A Worldwide Opportunity (or Challenge)

I've just completed a security road show tour of Asia, India and Australia. My experiences there and my trip last year to Europe make it clear that corporate governance and regulatory compliance is a world-wide challenge. However, while the results need to be almost the same, the reasons are different depending on the region.

In Europe, there is considerable effort going into similar financial reporting reforms as in the US. Europe, Japan, Canada and Australia are also heavily focused on privacy management for the moment. For example, the European Data Protection Directive mandates the handling of all types of personal data. Traditionally the US has had less regulation around privacy, until HIPAA, although recent issues such as the ChoicePoint privacy breach in the US may change regulatory focus.

In India and China, for example, there is little reason for organizations to implement identity management based on cost reduction concerns. This type of justification generally revolves around reducing the number of staff involved in processes, and decreasing the inaccuracies associated with provisioning efforts. The reality is that India and China have a good supply of very reasonably priced labor.

So why do countries such as India and China need to meet compliance initiatives? Quite simply, they need to be



able to deliver to their partners worldwide a level of certification and confidence around their processes. As more data – primarily personal or intellectual property – moves off-shore, those companies providing services need to be able to attest to the same level of policy and process enforcement that their customers do. Customers in these cases are those that have chosen to outsource business functions.

To take a case in point, India has a number of laws dealing specifically with security and privacy. For example the Indian Information Technology Act of 2000 makes unauthorized use of data a punishable offense. This should make it easier for organizations to be comfortable with a partnering or outsourcing effort with an Indian company.

However, the reality is that validation, let alone enforcement, of the laws is difficult. By all accounts, the Indian legal system runs at a glacial pace. Because enforcement rarely comes until after due process, the proverbial “cat is out of the bag” and would have long since left the building by the time it occurs.

Additionally, even Indian companies outsource (or sub-contract) work, yet often do not inform their partners or customers of that fact. Now however, contracts are being written to take these issues into account, and my experience talking to Indian organizations suggests that the driver for compliance is definitely aligned with customer requirements and satisfaction rather than any cost related imperatives. This is happening because the companies are not only being asked to attest to compliance, but also provide proof.

Compliance is not the only driver for Identity Management projects today. Don't forget the ROI based reasons for identity management in your planning.

Avoid Too Narrow a Focus

Interestingly, doing an audit against one particular regulation or standard is not enough. For example, in a SOX assessment, a significant security failure in the network might be identified. However, it might be classified as being isolated to a part of the network that does not affect the core financial systems, or associated data feeds to those financial systems. As a result, it won't be in scope for a SOX assessment or report, and ultimately not dealt with at the time.

The key challenge is adequacy of controls on all of the systems that feed financial reporting data, not general network security. So you must work with auditors to identify the scope of the assessment and then focus on relevant controls.

So, focusing on just the financial systems could, potentially, create a solution that requires greater change later on to incorporate additional compliance and security requirements. How do we deal with this?

Good Process, Good Frameworks.

There is a huge list of standards out there from various organizations such as Information Systems Audit and Control Association and Foundation (ISACA) – www.isaca.org, British Standards Institute (BSI) – www.bsi.org.uk, International Organization for Standardization (ISO) – www.iso.org, National Institute of Standards and Technology (NIST) – www.nist.gov, IT Infrastructure Library (ITIL) – www.itil.co.uk, and others.

One of the key tenants I always recommend as part of any identity management initiative is to get all the stakeholders together and obtain agreement on a common vocabulary. The potential for a common vocabulary comes from using common models or frameworks to help formalize such projects. The most common models to use for compliance initiatives – especially SOX and GLB – are:

- COSO – The Committee of Sponsoring Organizations of the Treadway Commission – www.coso.org
- CobiT – Control Objectives for Information and related Technology – IT Governance Institute – www.itgi.org and Information Systems Audit and Control Association – www.isaca.org
- SysTrust – AICPA American Institute of Certified Public Accountants – <http://www.aicpa.org/assurance/systrust/princip.htm>

SOX details a large number of requirements and many have little to do with technology. Real SOX compliance requirements are therefore very broad and not IT specific at all.

SOX details a large number of requirements and many have little to do with technology. Real SOX compliance requirements are therefore very broad and not IT specific at all.

The big external auditors (Deloitte, E&Y, KPMG and PwC) have their own compliance assessments. The Public

Company Accounting Oversight Board (PCAOB) & US Securities and Exchange Commission (SEC) both recommend COSO as a control framework for SOX compliance. Unfortunately, like SOX, COSO is broad.

The Control Objectives for Information and related Technology (CobiT) is then more commonly used to provide further granularity for IT specific controls. CobiT covers more than what is really needed by SOX for IT controls, however. The IT Governance Institute (ITGI) has a definitive document on IT Control Objectives for SOX and you can find it on the ITGI site link above. This document provides IT assessment guidance for SOX compliance.

SysTrust offers an additional step that organizations can take to provide an “assurance service in which a system is

evaluated and tested for reliability when measured against four essential principles: availability, security, integrity and maintainability.”

Now, while there is a common basis for both CoBiT and SysTrust, there is no direct link. So it is again up to you, or a hired gun, to make those links to ensure that all requirements are met.

Conclusion

Compliance is not the only driver for Identity Management projects today, yet the noise around compliance is huge. I don't think this is something anyone is unaware of, however if you believe the hype, it is the big stick. Pushing Identity Management as a “compliance only” initiative, however, can cause it to become yet another white elephant for IT. Don't forget the ROI based reasons for identity management in your planning.

Relative to compliance, there were existing frameworks and approaches which were not being utilized, enforced or acknowledged in some cases. Understanding and actually using these frameworks allows you to talk with the business and an auditor about what it is you are trying to achieve, and create a common vocabulary across the organization.

It also allows you to better compare identity management vendors' solutions, and better assure a successful outcome. ■

Archie Reed is Director of Strategy at HP and member of the Digital ID World Industry Advisory Board. He is the author of several books on identity topics including *Implementing Directory Services* (McGraw-Hill) and *The Definitive Guide to Identity Management* (Realtimepublishers.com).