

# Compliance Ignites the **IDENTITY** **MARKETPLACE**



Identity management is in the midst of more deployment and change than it has ever seen, and the rates are accelerating. Technology is changing, understanding of its use is changing, and the concept of where it applies is changing. There is also a wave of innovation taking place in identity technology and methods. What has ignited this marketplace activity? The first universal application for identity infrastructure – an application that every business will have to deploy eventually – automating regulatory compliance.

**E**very company has an “identity management system.” The only question is how much of it is manual and how much is automated. In 2004 most large companies went through the painful process of documenting their controls and systems in preparation for compliance auditing. This compliance driven documentation process made it impossible to ignore “messes” in internal identity life cycle processes, and process issues such as multiple users that share network identities in their daily work. This visibility, coupled with its impact on the ability to demonstrate compliance, has created awareness that is spurring identity initiatives.

By year end, the realization was dawning that compliance is not a one time event, but rather it is a recurring process. This is bringing the

true recurring cost of manual compliance auditing into focus – and creating an imperative that they be reduced in out years. This also has identity management sales ramping.

## **The Universal Identity Application**

The emergence of regulatory compliance as a driver marks the most significant change yet for identity – the emergence of a universal application. Until now, identity products couldn’t be packaged much beyond being an easy to deploy toolkit for building relatively custom projects. Deployments usually required more money to be spent on professional services than on software and hardware. This was true because every identity deployment had a somewhat different mission from the rest. Now compliance has created a nearly universal application for identity infrastructure.



This doesn't mean that identity management products will all become the same – far from it. Every company needs an accounting system, for example, but that has certainly not become a one size fits all

growth and technology evolution is occurring because of it.

### **Driving Deployments**

The demand to automate compliance is driving deployment of identity management solutions. “There are lots of reasons for bringing identity management infrastructure into play,” said Pat O’Kane, Chief Identity Architect at Unisys. “Operational efficiency, general security, productivity, and business agility among others. But the compliance issues have really focused the discussion in the last year. With Sarbanes-Oxley, the first round of reports from the auditors are coming in and [companies] are realizing that they have a lot of identity issues in their environment. Because SOX is such a driver at such a high level in many of these enterprises, the identity management aspect of addressing the issues that are brought out by the auditors is getting a lot of visibility. Higher visibility within the company means that projects will be better funded and actually take off.”

“Compliance is driving the majority of spending in security and risk,” said Paul Proctor, VP and Analyst in the Security and Risk Strategies practice at Meta Group. “The secret of regulation is it does not tell you what you need to do, you have to figure it out yourself. You must select reasonable and appropriate controls to address reasonably anticipated risks to your organization and you have to build a program that embodies all of those controls.”

“We observe three basic requirements in all regulatory rules,” said Proctor. “Accountability – who did what and when, and who was responsible. Transparency – you have to be able to see inside the process to be able to understand it. And Measurability – you have to be able to say here’s how good we were at doing it. It will not all be based on identity, but identity is absolutely one of the



---

**With the emergence of a universal application for identity will come an acceleration in the integration of identity technologies, as well as in their ability to integrate with whatever legacy identity environment they find themselves deploying into.**

---

market. However, such a universal need does create a minimum set of requirements that all deployments must meet, and this is now in the process of happening with identity and compliance.

The kinds and magnitude of identity technology change that the appearance of this universal application will drive are widely underestimated today. However 2005 will be the year that the impact of compliance on identity begins to clarify. It will take a couple of years for the effects of compliance on technology and market uptake to clearly sort out, but things are now in motion to define and package the compliance automation identity application. And explosive market

---

## At the low end, compliance seems likely to create opportunity for identity products focused on smaller businesses.

---



cornerstones. You will not be able to do anything unless you know who was assigned what privileges, and what privileges they should have been assigned.”

“Over the last twelve months the understanding has matured that identity is in fact central to compliance,” said Sara Gates, VP Identity, Sun Microsystems. “There is a patchwork quilt of technology that will make up an enterprise’s entire compliance automation, not just identity, but there’s [a growing] knowledge of the collision of identity management and compliance. The primary phase one [identity] project is de-provisioning when people leave, and reporting on who has access to what.”

### A Force for Change

Compliance is creating a much larger market for existing identity products, but it will also be a driver that creates changes in that technology. With the emergence of a universal application for identity will come an acceleration in the integration of identity technologies, and in their ability to integrate with whatever legacy identity environment they find themselves deploying into. Products will become dramatically more lightweight and flexible. Packaging will begin to emerge that allows easier incremental deployment without disrupting the fabric of a company’s computer systems and business processes.

We are already seeing the integration of formerly disparate technologies. On the outward facing side of identity management, we are seeing rapid growth in the use of federation to link identities across administrative domains. The emergence of SAML 2.0, with its convergence of the SAML and Liberty Alliance ID-FF proto-

cols, has sparked the integration of such technologies as Web services gateways and SSL VPN gateways into a larger identity infrastructure. The variety of technologies that are becoming “SAML enabled” illustrates how widely the integration of identity infrastructure will ultimately spread in the enterprise.

This integration to create an identity and policy driven view across technologies is destined to continue, driven by compliance. Because compliance requires the ability to attest to who has access to information, and often who did access it and for what purpose. “You will start to see interesting [identity based] technology integrations,” said Sara Gates. “Security event monitoring, RFID, and document rights management.”

Document rights management is an area of identity technology that should be spurred by compliance. Robin Bloor, President of Bloor Research, calls this Data Identity Management. “Sarbanes-Oxley makes the CFO and CEO responsible for the accuracy of the corporate accounts,” said Bloor. “Which in turn makes them responsible for keeping such data safe. This means safe from being altered fraudulently, and also safe from being distributed illegally.” Once the basics of access auditing are automated, Bloor sees compliance driving documents rights management. “You might say that you don’t care about data identity management right now,” said Bloor, “But you will, because the pressure for compliance is building.”

This should create impetus for identity based rights management systems like Microsoft’s RMS (See Digital ID World Mar/Apr 2004 issue,) Adobe’s new Policy Server, and products like those from

Liquid Machines. These products have struggled to gain acceptance because of their limitations in identity integration, but are starting to mature significantly.

### Lighter Weight, Looser Coupling

Technologies such as virtual directories (See Digital ID World Sep/Oct 2004 issue,) Federation, (See Digital ID World Jun/Jul 2004 issue,) and standards such as SAML, XACML, WS-\* and SPML are creating more loosely coupled and lighter weight identity solutions that remain enterprise class in capability. The trend towards viewing identity infrastructure as a network of interoperable products will grow, as compliance forces integration across ever an ever increasing scope.

At the low end, compliance seems likely to create opportunity for identity products focused on smaller businesses. All public companies must demonstrate Sarbanes-Oxley compliance, for example, no matter their employee size. An article in the December 9, 2004 USA Today noted that the burden this imposes on smaller companies, those with 500 or less employees, can be crippling – amounting to as much as 10% of their top line revenue. This can’t continue year after year, without making many businesses non-viable. We would expect to see smaller scale identity systems arise to provide compliance automation for this scale of business at a reasonable price.

### Legacy Identity Infrastructure

Despite the changes in technology and the appearance of new technology, it is clear that we will not rip and replace what is already deployed in identity any more than we did elsewhere. Rather, a lot of current identity technology will become

“legacy identity infrastructure.” This existing identity infrastructure will become integrated into a more flexible, easily deployable, less expensive architecture the same way that mainframes and their applications got integrated into remote access, client server, web portal,

policy. Compliance is all about assuring that policy is followed with respect to who does what, or who is allowed to do what with what data. To fully automate compliance to these policies across decoupled network systems, such as Web Services or applications that integrate with partners across administrative boundaries, policy will have to become federated.

It has been difficult enough for companies to reach agreements on liability sharing, and dispute resolution cost apportionment with respect to implementing identity federations. But once those agreements are hammered out, the technology must to become able to express them in its policy to assure automated enforcement of compliance with the agreements across all participants in the federation.

For this to occur across domains, methods of federated provisioning and federated policy expression will have to be developed. These will bring with them issues of privacy and security that must be solved, as well as issues of policy translation into different domains.

Currently, identity data tends to be replicated on all sides of a federation, allowing the issues of common (or translatable) policy expression and provisioning work flow policy automation to be finessed. But that isn't a long term sustainable model. As federations grow and truly cross management domains, identity technology will have to learn how to make policy able to be created in one domain, applied in another domain, and then enforced in yet another domain without manual intervention to set this up. Development of methods to federate policy in this way will ultimately be forced by compliance automation.

### **Compliance and Trust**

Ever since the early days of PKI, the technology industry has spoken of creating an



---


**Document rights management should also be an area of identity technology that gets spurred by compliance.**

---

and even Web services infrastructures as technology evolved. Techniques such as virtualization will evolve to handle this type of legacy identity integration into a larger network of loosely coupled identity infrastructure.

### **Federating Policy**

Another issue that compliance automation will ultimately require technology to learn how to handle is the federation of



---

## The necessities of compliance automation will force the deployment of identity technology, and also force change and evolution in identity infrastructure, technology, and methodology.

---

environment of trust in networked computing. Usually this was discussed at a level far below what is actually required to accomplish this – one that could even be called naive. Automating compliance will force the development of methodologies and technologies that truly do create trust, since trust emanates from knowing that the infrastructure is reliably assuring compliance with agreed upon policies.

Automating compliance will thus force evolution of technology in the areas of how policy truly should be expressed to be automated in a distributed fashion. Issues of complexity, such as how to get sufficient granularity without losing manageability, must be addressed. Issues of policy translation also arise, such as how do policies created at a corporate level translate into an environment such as an SAP application setting without having to be tediously recoded at each boundary.

Today, portions of the same policy tends to be implemented manually in multiple places, each translated there by hand. Long term, for policy to pass muster with auditors, these error prone steps will have to be eliminated. This is a very significant problem, requiring innovations in how policy can be expressed for algorithmic use. But once solved, this will make identity infrastructure far more agile with respect to changes in business or application infrastructure.

### Security and Identity

It also seems likely that automating compliance will reveal more fully the interactions between identity and security. This will cause identity to become seen in a larger context, touching many technologies that have not been previously seen as

identity related. This is starting to happen on its own a bit, with many “security” products becoming SAML enabled, LDAP enabled, or AD enabled. Even as they extend hooks out to enterprise identity stores, many people still don’t see these as identity products, or their missions as part of the identity infrastructure. But if it needs access to identity or policy to operate, then it is ultimately part of the identity infrastructure. Automating compliance will make this clearer with time.

### In This Issue

Provisioning technology has changed significantly over the past few years, making it much easier to deploy and integrate. Provisioning: The Foundation of Compliance Automation examines why compliance is driving provisioning deployments, and also how compliance is already starting to change provisioning by altering it to allow automated enforcement of such concepts as segregation of duties.

Looking a bit to the future, Why Compliance Will Change Identity Management examines the changes that have already occurred in products to address the needs of automating compliance, as well as the trends that compliance seems likely to create in identity technology. This article also examines whether compliance will be a long term driver for identity, or whether it is creating a short term burst of activity that will fade.

Our identity case stories in this issue all focus on deployments that used identity to automate compliance. In Affymetrix Adds Identity to IT’s DNA we see examine a case where identity management was originally deployed for security and

management reasons, but showed its effectiveness when compliance issues arose. Sarbanes-Oxley gets a large share of the compliance focus today, but HIPAA and other regulations are also becoming identity deployment drivers. In California Pacific Medical Center Fingers Compliance we explore how a hospital used identity to achieve HIPAA compliance. Our case story SSHA Deploys Managed Identity Service looks at how the Canadian province of Ontario is building a managed network to integrate its health care service information and created an identity service to help applications comply with PIPEDA.

Compliance will drive the need to link identity to context, so that policy can be integrated across domains. Michel Prompt explores how new virtualization techniques might be employed to accomplish this in The Second Wave: Linking Identities To Contexts. And in the midst of the compliance hype, Archie Reed warns us not to forget the lessons already learned about identity management in his article Don’t Let The Circus Distract You.

The necessities of compliance automation will force the deployment of identity technology, and also force change and evolution in identity infrastructure, technology, and methodology. The marketplace for identity management is currently estimated by analysts to grow to over \$10 billion in the next three years. But as dramatic as this inflection point will be, it will still be just the start. For once these platforms get deployed, they will begin to be leveraged to use identity to integrate, manage, and secure network data and applications in a much more integrated way. ■