Choosing Identity Management Solutions: Why, How, and What
Security & Risk Strategies, Security Infusion
Earl Perkins

FOCAL POINT
As identity management needs rise in priority for enterprises, many seek approaches to (1) justifying a business case for it; (2) starting such an effort once requirements have been identified; and (3) finding currently available solutions for such needs.

CONTEXT
Why Identity Management Is Important
Ironically, identity management as we currently know it suffered an identity crisis during its early formation several years ago (see Figure 1). In an attempt to put a name to a set of critical business drivers facing enterprises worldwide, vendors, analysts, and journalists aggregated together a collection of functions, processes, services, and infrastructures under a common logo that sometimes confused customers as often as assisted them in solving critical business issues. What organizations really saw and understood about identity management was manifested in day-to-day issues, such as how difficult it was to get timely new-employee access to computer services, how many passwords employees had to remember, or how each kind of privileged access to resources was handled differently, with time-consuming procedures and delays for changes. Other enterprises became concerned about how identities of individuals who were not employees would be managed securely, how compliance to new government regulations could be assured, how revocation of access rights on employee termination could be improved, and how both old and new IT systems could use any new solutions to manage identity.

Fortunately, it was such drivers that served to focus much of the security and identity vendor market strategy during the past two years in terms of product development, prioritization of features and functions, positioning of access management and provisioning/workflow, and merger/acquisition decisions (see Figure 2). It is also such key business drivers that IT organizations ([ITOs] and coalitions of IT and user management groups with identity needs) use as a starting point when building justification messages for identity management solution purchases.

Drivers That Justify Identity Management Solutions
Justifying significant investments in a solution for identity management for most current production deployments falls into four major categories in the order they are most frequently used:

• **Compliance:** Currently, the most frequent business driver for identity management investment is addressing the need for compliance — whether for concerns outlined by auditing reviews as mandated by documented controls or increasingly by governmental regulations driven by data protection, privacy, financial integrity, and related laws. Few drivers are more compelling than staying out of prison or avoiding severe financial penalties, and legal counselors have assessed the risks on behalf of their enterprises as significant enough to warrant investigating potential mitigating technology solutions. The extent of that technology need is still very much up to interpretation.

**META Trend:** Driven by compliance and cost, organizations will focus on identity as a business asset. Identity management will continue to confuse, but grow, as more organizations spawn projects around identity infrastructure (e.g., enterprise directories, Web SSO) and user life-cycle management. Web services (2005/06) will expand identity to non-person users and exacerbate the need for identity solutions. Identity infrastructure will be incorporated into application infrastructure “stacks,” incorporating finer-grained authorization (2004-06), and cease as a standalone market (2006/07). User life-cycle management will draw closer to other operations functions (2006/07).
• **Security:** Closely allied with compliance is the security card. With the overall threat index rising for most enterprises on access to valued resources, increasing pressure is being applied by some business owners to increase the level of protection for such assets. This can be done in numerous ways within the identity infrastructure or with more effective identity management and administration. Some organizations are choosing the latter or a two-pronged approach to the concern. Not surprisingly, this driver usually originates with information security presence in the enterprise or through business elements allied with information security.

• **Cost savings:** There is a return on investment argument for some elements of identity management, primarily in the operational administration area of password resets, synchronization, and management. This usually represents the entry point for most enterprises starting an identity management effort, and most can quickly show real savings. In some areas such as Europe, organizational culture (e.g., federated structures limiting levels of centralization that can be achieved) and employment laws that impede resource reduction may result in lower-than-expected cost benefits. Other investment returns can be shown with methodical process improvements that result in time of delivery for services that affect bottom-line operational expenditures through provisioning and workflow system deployments. However, these tend to take longer to realize such returns. Identity management represents one of the few areas within the information security umbrella that can actually show some form of investment return, albeit moderate. Information security as a whole is primarily about information insurance.

• **Productivity:** Sometimes confused with cost savings, this driver is used in conjunction with a major enterprise application deployment, or the deployment of a “consuming service” that needs identity management and calls on the infrastructure for services that it clearly cannot provide. This requires the IT infrastructure to step up and request some form of management capability to be productive and to address that requirement. There may also be requirements given to an ITO that drive the complexity of the existing identity infrastructure past a “tipping point” where it is unable to sustain the build-out of the new service. The organization must request some build-out of the identity management capability to address it.

“Eating the Elephant”

Although it may be possible for an enterprise to recognize the symptoms of an “identity crisis” and take action to resolve it, many are unsure of the first steps necessary to initiate an identity management program. Where does the organization start? Although there are many variations based on industry sector, enterprise size, application portfolio, and other factors, general guidelines that may be useful when developing an identity management plan including addressing the following issues.

• **What do major business or customer representatives recognize as primary business drivers for identity management?** These include drivers such as compliance, security, cost savings, and productivity. Consideration must be given to any particular order of priority, and the circumstances behind each driver. This information will be needed later when aligning the right initiatives to be delivered.

• **Where is the pain?** For each active driver that results in enterprises initially considering identity issues, there are simmering aches within the applications and the infrastructure fabric. Some are merely reflections of the drivers already outlined and provide definition and granularity that can be used to build a business case beneath the banner of the drivers. Others require definition so that they can be prioritized in the context of the drivers for identity management.

• **Are there existing projects or initiatives already underway that involve identity or access elements — single sign-on initiatives, directory, or metadirectory deployments?** What about Active Directory rollouts? Could such initiatives be consolidated or leveraged in fulfilling one or more of the major drivers? Many enterprises find to their surprise (or their chagrin) that they already “have” identity management and are unaware of it, or they have not aligned it with addressing the strategic drivers of the enterprise.

• **What is the state of existing identity infrastructure in the enterprise?** An effective identity management program’s chances markedly improve if it has a relatively robust, consistent, and mature identity infrastructure as a basis (see Delta 2317). History shows that if some of the basic problems found in identity infrastructure are solved first (e.g. directory structure, consolidation, authoritative use, integration, authentication services deployment), this usually leads to an easier time with more complex
identity management deployments. At a minimum, identity management planning must include identity infrastructure considerations.

- **Who is involved in the effort?:** Major functions of identity management include the ability to secure application access quickly and effectively and to integrate multiple disparate stores of credentials and services involved in that effort. As a result, application development and information security play critical roles in decision making for strategic identity management solutions. That is not always apparent at first glance. Other decision makers include IT infrastructure (e.g., network, server) architects, human resources, and IT administration. The key role is played by the customers of IT, who lead the effort in every respect. They literally own the identities that will be managed before, during, and after deployment. Where possible, they should play leadership roles in planning and deployment.

### Risks and Pitfalls of Implementation

Once a decision is made to initiate some form of identity management program within an enterprise, there are challenges. In the early days, more than half of all major identity management initiatives failed for different reasons. Some of the pitfalls sound painfully familiar to any major effort that has pervasive impact to IT infrastructure and applications.

- **Political infighting:** Identity management deals directly with human resources, privacy, access privileges, permissions, security, and secrets across all multiple enterprise divisions, multiple infrastructures, multiple vendors, and multiple cultural environments in multinational corporations. It represents a very challenging exercise in diplomacy-alone discussions regarding process or organization impacts as a result of its introduction.

- **Scope creep:** As seen from the drivers previously mentioned, identity management has some compelling starting points. Once initiated, it can assume a life of its own, and unless carefully bounded, can grow into a program bureaucracy that is unable to meet realistic expectations or timelines.

- **Program paralysis:** The opposite effect may occur for enterprises that may try to solve some of the more fundamental problems, such as a common role-based authorization model for all applications or consolidating all application authentication repositories down to one. Such efforts may end up taking so long to plan and to gain the approval of the parties involved that they become unrealistic or outdated.

- **Vendor domination:** Although identity management is still in a relatively early phase, it remains tempting to enable systems integrators or vendor coalitions to sometimes have too powerful an influence in establishing identity management architecture, technology, and configuration decisions, instead of enabling such decisions to be driven by business needs. Let the buyer beware.

### What Is the Current Market for Identity Management?

In mid-2004, the identity management market consists primarily of two categories of solution providers.

- **Suite/stack vendors:** These are identity management vendors that have assembled a complete set of identity infrastructure, access management, and identity management components and have achieved a significant degree of integration between such components. Suite vendors are more accurately characterized as identity and access management vendors because they have user provisioning, workflow, delegated administration, and Web single sign-on capabilities. Examples of suite/stack vendors include IBM Tivoli Identity/Access Manager, Novell Nsure solutions, and Computer Associates eTrust.

- **Component vendors:** These are identity management or access management vendors that address some or most of the major services of identity or access management, but they usually do not possess identity infrastructure or software foundation platform systems. Examples of component vendors include BETA Systems SAM, BMC Control SA, Netegrity IdentityMinder eProvision, Thor Technologies Xellerate, and Courion AccountCourier.

Some confusion remains among ITOs about identity management versus access management and the vendors that address them. Most access management vendors now label themselves as identity management vendors, though many do not have provisioning and workflow solutions of their own and depend on partnerships to provide them.
This raises another important question among customers: Which is better to buy — suite/stack or component when constructing an identity management solution? An identity management provisioning METAaspectrum, due to be completed year-end 2004, will provide better insight into this question. However, general guidelines from existing deployments show that business drivers, coupled with prioritizing the specific needs for identity management of most enterprises, are still favored at this time, and choice often favors component vendors. However, it is important to note that suite vendors are aware of this and have been aggressive with pricing, configuration, and feature options as a counter to this component vendor advantage.

**Bottom Line**

Justifying identity management for enterprises is possible but not easy. Organizations must band together with the business or the customer and use compliance, security, cost savings, and productivity arguments as starting points. The identity management planning cycle has many roots in IT and benefits from a good identity infrastructure. However, organizations must prioritize the pain and consider implementing services in stages if they are unable to justify large-scale programs. Many are not. The vendor market is still in an early phase with a crowded set of suites, stacks, and components. Enterprises must let business drivers remain the guide for constructing the solution set rather than suite, stack, or alliance stories. They are useful in the selection process, but the organization has to live with the final result.

*Business Impact:* Identity is a strategic corporate asset and a reusable key to access the information resources of the enterprise. Identity management is the system used to care for and secure that asset and ensure its authorized use according to corporate policies and controls.
Many vendors delivering identity and permissions (e.g., directory, metadirectory, Web single sign-on) infrastructure from 1999-02 are now declaring themselves identity management vendors. Vendors providing administration and management applications (e.g. delegated administration, workflow, password management) during the same period are now claiming identity management status. Who is correct, and what comes first? One method for securing enterprise identity addresses three major areas.

- The primary functions of identity services (e.g., authentication, authorization, credential storage)
- Major infrastructure components to support the delivery of such functions (e.g. directories, metadirectory utilities, Web single sign-on, operating system authentication)
- The management, administration, and security “umbrella” covering the infrastructure that delivers identity services includes:
  - User provisioning
  - Delegated administration
  - Password reset/synchronization/management
  - Self-service
  - Integrated workflow
  - Auditing, logging, and reporting
  - Integration (e.g. metadirectory services)

Separating function from infrastructure and infrastructure from management is key to developing a prioritized plan to address identity security and choosing the right partners to deliver and manage it.

Source: META Group
### Figure 2 — Leading Identity Management Vendors

<table>
<thead>
<tr>
<th>Vendor</th>
<th>Product</th>
<th>Web Site</th>
</tr>
</thead>
<tbody>
<tr>
<td>Beta Systems</td>
<td>SAM</td>
<td><a href="http://www.betasystems.com/e_beta.nsf/(Docs)/024001000">http://www.betasystems.com/e_beta.nsf/(Docs)/024001000</a></td>
</tr>
<tr>
<td>BMC</td>
<td>Control SA</td>
<td><a href="http://www.bmc.com/products/proddocview/0,2832,19052_19429_22855_1587,00.html">http://www.bmc.com/products/proddocview/0,2832,19052_19429_22855_1587,00.html</a></td>
</tr>
<tr>
<td>CA</td>
<td>eTrust Admin</td>
<td><a href="http://www3.ca.com/Solutions/SubSolution.asp?id=4348">http://www3.ca.com/Solutions/SubSolution.asp?id=4348</a></td>
</tr>
<tr>
<td>Siemens</td>
<td>DirXmetarole</td>
<td><a href="http://www.siemensenterprise.com/prod_sol_serv/solutions/categories/id_manage_solutions.shtml">http://www.siemensenterprise.com/prod_sol_serv/solutions/categories/id_manage_solutions.shtml</a></td>
</tr>
</tbody>
</table>

Source: META Group