

## Identity Management - A Good Investment for Today's Economic Times

By Tom Patterson & Ryan Rubin  
Deloitte & Touche

Financial officers have a duty to help their organization manage costs by using all of the tools at their disposal. One new tool in the financial arsenal is a comprehensive program of Identity Management. Organizations old and new, across Europe and around the world, are saving money, streamlining business, enhancing employee productivity, increasing customer self-service, and reducing their overall risk profile. While the tools to make all of this happen fall in the category of information security, it is primarily these business drivers that make the difference. First some background.

Imagine having only to remember one username and password to access all your business applications. Imagine only ever logging into your office computer once in the morning and not having to log on again for the rest of the day or until you leave your desk. Imagine your customers navigating from business partner web sites to yours without the need to re-validate their credentials. Imagine your IT department being able to control access to users, customers and partners from one central point and a couple of mouse clicks.

The number of ID's a user needs to access company IT resources has become a barrier to their use and an ever-increasing security threat to the overall environment. Identity management or ID Management provides a solution to address this problem.

ID management is a *strategic decision* and direction that many organisations need to start thinking about today. It makes good business sense as it involves consolidating IT infrastructures and streamlines business processes. It reduces support overheads and relieves the burden that users put on helpdesk operators. It can also assist in tracking internal users who use business applications and provides a customised and tailored user experiences for enterprise users. ID Management projects have a demonstrated Return on Investment (ROI) by significantly reducing operational/ recurring costs and . enabling and supporting business initiatives such as portal implementations or B2B interactions.

ID management assists with overall *risk management* as the number of unused accounts on key systems can be reduced and effectively managed if employees leave or change roles within the organisation. It also provides several benefits for others parts of the organisation. For example, from a financial perspective it provides ROI which can be measured using quantifiable factors such as reducing staff support time and effort required, improving productivity and reducing unnecessary user software licenses. For audit and security divisions it provides a centralised method of providing access control and authorisation in a controlled and auditable manner.

Identity Management is changing the way organisations think about and manage their internal and external user bases. Application functionality and

access control can be directed through an identity centric model enabling an organisation to be in better control and in touch with an individual's behavior within an organisation's IT environment. It helps organisations to track where users go, what users see and how they are presented with information that is especially directed at them.

Companies are investing heavily in technologies that either do not fit in with the organisation's strategic plans or are ineffective of providing a complete strategic solution required by that organisation. Some have been known to purchase solutions that are in their infancy in terms of operational effectiveness and robustness. Whilst other solutions land up as shelfware because they did not fully meet business requirements. Many tactical solutions have had to be "thrown out" due to organisations realising that a more effective strategic direction was required.

The key for organisations to make Identity Management a success is to conduct an initial analysis of the organisation to see which technologies will best fit the profile of the organisation. Furthermore, unless the organisation is 'identity centric ready' in terms of business process alignment, technology won't go very far down the value chain that Identity Management provides.

Three critical aspects of any business should be considered when introducing security solutions to an organisation: people, process and technology. The technology often gets most of the attention while the people and processes fall behind. Unfortunately, with provisioning and identity management tools, if rules governing access control and are not clearly defined and communicated, and the authorisation logic created does not reflect how business accurately flows through the organisation, the likelihood of a successful deployment is low. In fact, it will simply highlight the procedural shortcomings the organisation must resolve and could result in costly re-engineering exercises. Customers report that the more time they spend in the planning stages of the project, the more successful the implementation.

Security investments can provide a quantifiable ROI, especially if they reduce administrative costs. However, most enterprises lack the capability to capture the metrics needed to show the cost-benefit of such solutions. Justifying the cost of a Identity Management solution can be addressed in a number of ways to show a benefit to the enterprise. Examples include cost avoidance and cost reduction .

Before embarking on your Identity Management mission, ensure that you've taken into account areas highlighted in this article. As there is a strong business case, measurable metrics should be put in place to track the progress of your project. Take care to choose the appropriate technology that meet your business requirements and fit within your organisation. Finally ensure that your people and underlying processes are also aligned to embrace this new challenge. This is an area that requires leadership from the financial professionals, with the benefits to be realized across the organization in lower costs, more efficient operations, and an overall reduction in risk.

Tom Patterson is the Partner In Charge of Security Services for Deloitte & Touche – EMEA. Tom is based in Frankfurt Germany, and can be reached at 49 69 75 695 523, or at [tompatterson@deloitte.com](mailto:tompatterson@deloitte.com)

Two Graphics to be placed within the article:

### Top Ten Identity Management ROI Metrics

1. Lower Security Administration Head Count.
2. Turnaround Time in Processing Access Requests.
3. Fewer Errors that Require a Second Processing of a Request.
4. Fewer Number of Emergency Calls for security related events.
5. Fewer Number of Password Reset Calls.
6. Faster On-boarding of Employees
7. Faster shut-down of redundant or terminated staff.
8. Increased secure customer self-service access.
9. Better integrated supply chain information.
10. Easier and faster merger/acquisition processing

### Road Map: An Identity-centric model is the cornerstone of your future security strategy

