Communications of the Association for Information Systems

Volume 28 Article 11

3-2011

The Identity Management Challenge

Heather A. Smith
School of Business, Queen's University, Kingston, Ontario, hsmith@business.queensu.ca

James D. McKeen
School of Business, Queen's University, Kingston, Ontario

Recommended Citation
Smith, Heather A. and McKeen, James D. (2011) "The Identity Management Challenge," *Communications of the Association for Information Systems*: Vol. 28 , Article 11.
DOI: 10.17705/1CAIS.02811
Available at: https://aisel.aisnet.org/cais/vol28/iss1/11

Communications of the Association for Information Systems

CAIS

The Identity Management Challenge

Heather A. Smith

School of Business, Queen's University, Kingston, Ontario

hsmith@business.queensu.ca

James D. McKeen

School of Business, Queen's University, Kingston, Ontario

Abstract:

As organizations extend the online delivery of services and data across departmental, organizational, and even jurisdictional boundaries, they must trust that they can identify and authenticate the customers, businesses, employees, and third parties using them. Traditional approaches to identity management (IDM), such as documents, clearly don't work in the online world, yet to date there is no online equivalent of the passport or photo-id. Instead, organizations have established their own identity management practices. As a result, IT managers are looking for more holistic and standardized IDM practices that could simplify access to multiple services and enable organizations to collaborate and cooperate across global organizational boundaries, as well as keep identity information secure and private. This article explores these IDM challenges and how managers are approaching this issue. It discusses the key *management* components of IDM looking first at the basic concepts of IDM, its essential elements, and organizational stakeholders. Next, it examines why IDM is increasingly a *business* concern, in addition to an IT concern and describes the key IDM challenges facing IT managers. It then distils key principles of effective IDM and makes recommendations for how IT managers can improve on their current IDM efforts.

Keywords: identity management, federated identity management, authentication and authorization, identity standards, deperimiterization, identity life cycle

Volume 28, Article 11, pp. 169-180, March 2011

I. INTRODUCTION

As organizations increasingly extend the online delivery of their services and data across departmental, organizational, and even jurisdictional boundaries, they must trust that they can identify and authenticate the customers, businesses, employees, and third parties using them. Traditional approaches to identity management, such as documents, clearly don't work in the online world, yet to date there is no online equivalent of the passport or photo-id. Instead, each organization and sometimes individual programs within organizations, have established a variety of identity management practices, such as passwords or "shared secret" questions.

However, as the integration of data and services progresses, IT managers are trying to grapple with more holistic and standardized approaches to identity and authentication that could simplify access to multiple services and enable organizations to collaborate and cooperate across global organizational boundaries to deliver services. As well, since all organizations must be concerned with identity theft and fraud, managers are continually challenged to implement practices that keep identity information secure and private.

Identity management (IDM) typically includes controls to prevent, detect, or correct harmful events and steps to: identify a user; authenticate or prove the user is who he says he is; authorize what types of information can be accessed; and account for what a user does. Effective identity management is, therefore, widely seen as being an essential component for the safe and secure delivery of online information and services. Furthermore, as work extends to mobile and virtual activities, more and more identity management frameworks and standards need to integrate with a variety of devices, platforms, and protocols.

To explore the challenges of IDM that organizations are currently facing and to better understand how they are approaching this issue, both internally and collaboratively with other organizations, the authors convened a focus group of senior IT managers from organizations in a variety of industries. In preparation for this session, we asked them to consider a number of questions about IDM in their organization. These questions included: the scope of IDM; the business case for IDM; how it is organized and governed; the roles and responsibilities that are involved; key challenges and major obstacles; and best practices or principles of effective implementation.

This article discusses the key *management* components of IDM, as opposed to its *technical* components. It looks first at the basic concepts of IDM, its essential elements, and organizational stakeholders. Next, it looks more deeply into why IDM is increasingly a *business* concern, in addition to an IT concern. Third, it describes the key challenges facing IT managers as they try to address the rapidly evolving needs for IDM in their organizations. Fourth, it distills some key principles of effective IDM, and, finally, it makes several recommendations for IT managers about how they can improve on their current IDM efforts.

II. IDENTITY MANAGEMENT (IDM) BASICS

Almost all of us recognize and are familiar with some of the basic concepts of identity management, even if we are not aware of it. Most IDM frameworks recognize three main components [Smith, 2007; Allan and Perkins, 2009; Aitoro, 2008]:

1. *Registration or Identification.* These are processes that answer the question: "Who are you?" Whether we are employees, customers, or citizens, we are constantly being asked who we are by the systems we use. Typically, we are given a unique username for each system we use, often leading to confusion when we forget who we are in a particular situation!

2. *Authentication.* These processes answer the question: "How do I know it's you?" At a minimum, we are required to provide a password, which may be as simple as our phone number but may also be a complex combination of letters and numbers that we are required to change on a regular basis. Other, less commonly used methods of authentication include: shared secrets (i.e., questions about yourself); biometrics (i.e., fingerprint or iris scans); or a file or swipe card that works in combination with a password.

3. *Authorization.* These processes answer the question: "What are you allowed to do or see?" and validate that the user has the right to access a specific resource. As more and more detailed information is being made available online (e.g., banking, medical records, intellectual property), this is becoming a crucial question for both individuals and organizations. Companies and governments are now bound by legislation (varying in

different parts of the world) to protect the information they collect, while individuals need to know that their personal information is protected and will not be used for purposes they did not authorize. Both want to ensure that criminals, profilers, hackers, and other unapproved users do not gain access to their information.

What is often less well-understood is the foundation of people, process, and technology on which identification, authentication, and authorization are built. This provides the basis for trust in the IDM process itself and assurance that the proper protections are in place [Doctorow, 2007]. Without trust that the IDM process provides effective identification, authentication, and authorization, companies and individuals will not want to conduct business online. Until quite recently, this organizational infrastructure has been buried deep within most IT organizations and their applications. IT has been responsible for creating the processes, implementing the technology, and providing the staff to undertake:

- *IDM Administration.* A large part of IDM work has traditionally involved registering and deregistering users of IT systems and managing their passwords [Allan and Perkins, 2009]. For example, it has been estimated that one-half of all Help Desk calls are for password resets [Waters, 200]. Administration also includes determining what systems and information an individual is entitled to access and monitoring usage to ensure that no unauthorized transactions take place.

- *Information Privacy.* Protecting personal privacy is closely linked to access control. Organizations need practices in place to assure individuals that their information will be protected and ensure that it will be used only when and where needed by persons authorized to do so.

- *Security.* Organizations must also protect their data from being lost or fraudulently accessed [Suess and Morooney, 2009]. A strong identification, authentication, and authorization process can prevent most unauthorized access not only to personal data, but also to corporate intellectual property by persons or companies not known to the organization and to the applications that actually run the company. However, it cannot prevent access by persons who are authorized to see this information and who use it inappropriately or by unauthorized persons who get physical access to it (e.g., by walking into an office or hijacking an identity). Thus, physical and virtual security goes beyond basic IDM practices.

- *Risk.* All IDM practices should be based on an assessment of the risk involved to both individuals and organizations. The more electronic access an organization provides, the greater the risk of theft, fraud, and disruption [Small, 2006]. Focus group members pointed out that the biggest risks are from insiders and problems often arise through error rather than deliberate action. “This is why we need to have very specific access controls,” said one. “There should be no generic internal IDs for anyone.” Clearly, there are levels of risk based on a combination of the type of information involved, who is accessing it and under what circumstances. There is little risk associated with a competitor accessing a company’s cafeteria menu and high risk in the same individual accessing its employee or client list. Thus, appropriate IDM needs to be linked to the level of risk involved to provide the assurance that the right information protection is in place without causing undue irritation or frustration with the controls being used.

- *Regulatory Compliance.* Finally, all organizations have legal responsibilities to properly identify and authenticate users of their data and applications as well as those accessing their services [Smedlinghoff, 2008]. Compliance becomes increasingly challenging when companies hire external third parties to do work for them. One manager noted that his company has to have legal oversight for all external access provided to vendors and partners because his company is legally responsible for what happens to its data. Other managers noted that they are legally required to review key transactions done by their employees, to have all staff review acceptable use practices and to separate roles and responsibilities with respect to key transactions.

While organizations still typically undertake their own identification, authentication, and authorization services, as well as the underlying administration and other assessments, there is much discussion about how IDM could be done differently and more effectively. Federated IDM is an approach that suggests that companies could agree to trust their partners’ IDM services and vouch for each other’s users [Waters, 2007; Smedlinghoff, 2008]. Many of the companies in the focus group are exploring doing this on a case-by-case basis, because managing identities internally is becoming increasingly complex and challenging [Fest, 2008]. “It’s becoming unfeasible to own the identity repository for every individual accessing our data,” said one manager. “We need identity federation because we don’t want identity management to be our primary focus.” Other companies are exploring turning identity services over to a trusted third party which would be able to develop a standardized approach to federation on behalf of a number of companies. Unfortunately, there are still serious legal concerns to federation which have inhibited its use.

The legal and compliance issues associated with federated IDM underscore one of the biggest challenges involved in implementing any effective IDM—the complexities arising from the multiple interests of the stakeholders it serves. Within a single organization, IT, legal, HR, and individual business units are all involved in its governance in the focus group companies. Stakeholder considerations multiply exponentially when an organization opens itself up to external access of any type. As one researcher notes: "[IDM] is an intricate mix where … [p]arties might be influenced by privacy desires and regulations, legal liability, security vulnerabilities…, enjoyment or productivity, profit motives, application flexibility, and more. Some goals sit in uneasy tension with others" [Maler, 2009].

III. IDM AS A BUSINESS ENABLER

In the past IDM has been largely a technical matter and considered an internal IT function of limited interest to the business. Today, however, IDM has become an essential business enabler, and with this transition has come not only greater visibility for IDM but also a host of new issues for business and IT managers to collectively address. Unfortunately, most business leaders are unaware of how much the IDM environment has changed recently [Kalin, 2005; Small, 2006; Neuenschwander, 2006]. "For many years, identity management was exclusively an enterprise proposition with an emphasis on security, authorization for resource access and institutional control of all aspects of identity provisioning and usage" [Maler, 2009]. As a result, IDM has largely been seen by business as a technical issue rather than as a business one [Wagner and Allan, 2009]. This perception is now slowly changing as businesses run up against their internal IDM limitations, and IDM practices have been unable to respond effectively to new business needs [Kho, 2009].

The focus group was unanimous about the need to see IDM as a business enabler. "The business climate is changing rapidly with competition from different sources, globalization and a mobile workforce. We need to be more flexible about how we work with people and we need to work in ways we haven't before. So IDM is really a foundation piece to enable business transformation," said one manager. Another explained, "The ROI for IDM is not great, but we just need to do it; it's 'table stakes' for us." A third noted, "Our failure to address the limitations of our legacy IDM processes has become a real barrier to business transformation."

Unfortunately, the strong technical focus of many IDM specialists has obscured business' understanding of this issue. As with other infrastructure projects, the need for funding has too often focused on nitty-gritty details without explaining in business terms *why* IDM is so important [Kalin, 2005]. Focus group managers recognized this problem. "We need an alternative approach to IDM based on business value," said one manager. "IDM is a 'huge dilemma' for us. Business is not taking ownership for it and IT is having to fund it on its own. But traditional approaches simply don't work today," said another.

What IT managers and increasingly, business leaders, are coming to understand, is that effective IDM, in collaboration with security, is the means whereby organizations can balance their risk and flexibility needs and make appropriate business decisions as they become more mobile, global, digital, and interconnected with customers and other companies [Small, 2009; Shuey and West, 2006; Wagner and Allan, 2009]. In the risk:flexibility equation, the *risks* of poor identity management are much better-known and described than the flexibility component. IDM risks include fraud or identity theft; privacy and regulatory noncompliance; reputational loss resulting from information loss or theft; and financial loss if customers and partners lose trust in an organization's ability to protect their information [Shuey and West, 2006; Allan et al., 2009; Britt, 2009; Perkins, 2009]. The risk component of IDM was also more widely incorporated in the practices of the focus group organizations as well. For example, one large organization now has a Chief Information Security Officer who is responsible for IDM at the enterprise level. Another has implemented processes to manage identity risks across several initiatives. Legal departments of their organizations are also active in providing oversight for external partnering arrangements because companies are concerned about who is using their data and who has access to their intellectual property. In short, as one manager stated, an important organizational priority is to "develop IDM capabilities that will enable us to work together without sacrificing security or productivity."

Beyond risk management however, business enablement/flexibility is an equally important component of the IDM value proposition. One manager stated, "We need to be more flexible about how we work with people and to work in ways we haven't worked before." A composite list of business needs that require strong IDM compiled from the focus group includes:

- Support for a more mobile and global workforce
- Speedier mergers and acquisitions
- Increased linkages with partners and suppliers
- The ability to deal with increasing volumes of information and present a consolidated view of data from across many different systems
- Protection for massive amounts of data moving around the world and between companies

- Improved online customer service and customer access to information
- Increased collaboration
- More rapid access to external capabilities (e.g., outsourcing)
- Addressing complex external relationships (e.g., a partner one day and a competitor the next; a partner in one area and a competitor in another)

Table 1 illustrates how one focus group manager views the IDM risk:flexibility equation with respect to enabling collaboration. Note that there is not a one:one correspondence between the services enabled and the risks involved, further complicating the equation.

Table 1: Effective IDM Balances Business Flexibility and Risk Management

Enabling Collaboration	Managing Risk
• Give users access to the resources they need to be productive • Link business processes across security boundaries • Quickly roll out new services to customers and partners	• Ensure individuals are efficiently granted appropriate rights to resources and services • Ensure ONLY authorized individuals are granted access rights • Monitor what authorized users are doing with their access to identify insider threats • Be able to monitor, audit and report on the implementation and effectiveness of controls for compliance and regulatory purposes

Other business IDM needs relate to cost containment and productivity. In many cases, users are frustrated with multiple sign-ons and complex and time-consuming security access processes that do not appear to add value [Perkins, 2009; Kho, 2009; Maler, 2009]. Finally, many organizations want to provide improved customer experiences, build customer and partner ecosystems, and facilitate new ways of working and remote access [Allan et al., 2009; Small, 2009; Kho, 2009].

IV. IDM CHALLENGES FOR IT MANAGERS

Each of these business needs represents a series of IDM challenges for IT managers. Whereas in the past, IT has been able to limit access to data and applications through building a secure firewall around an organization and thus prohibiting external access, today's organizations are increasingly becoming more porous and are heading toward complete deperimiterization [Maler, 2009]. "As we increase the number of our strategic partnerships, IT becomes a barrier without effective IDM," said one manager. "We don't want to become identity managers for everyone who accesses our data," said another. "Therefore, we need to do IDM differently than we have been."

Managing IDM in a deperimiterized world means moving away from an IDM approach that is data and application-centric. In the legacy environment that most IT managers have inherited, IDM is managed on a system-by-system basis [Waters, 2007]. As a result, users often have many usernames and passwords. One study found that 37 percent of enterprises have between seven to twelve passwords per employee and 12 percent have twelve or more [Kho, 2009]. Thus, it is no surprise that even internally, managing user identities and entitlements has become increasingly complex and that IDM in many organizations has become siloed and fragmented [Allan et al., 2009]. Furthermore, legacy systems often have numerous vulnerabilities and flaws, given that they were designed for a firewalled world [Aitoro, 2008]. One focus group manager described her company's current state of IDM as follows:

> *We have no consolidated view of which employees have access to which assets. We cannot validate access rights and privileges. Access is not revoked in a timely fashion when an employee changes jobs or leaves. Our user administration is complex and overlapping and pre-employment checks cannot be confirmed prior to granting information access to workers.*

Many organizations are struggling with elevating IDM from being done by individual systems to being managed at an enterprise level. As a starting point, focus group members were trying to develop enterprise policies and procedures for both internal staff and external access. Developing the right processes and governance is critical, they stressed, because of the risk:flexibility trade-offs involved. "Our goal is to develop a single, enterprise ID," said one manager, "and to have one integrated, automated IDM lifecycle."

Unfortunately, such an integrated, enterprise process is still more of a goal than a reality. Organizations are hampered in developing it by a number of factors. First, as noted above, there is limited business understanding of the business benefits of effective IDM and thus, limited funding available for building the infrastructure and staffing the process [Kho, 2009]. Second, governance is typically fragmented among IT, the business, HR, and legal

departments [Maler, 2009; Wagner, 2009]. Third, current IDM practices and processes are often manual [Small, 2006]. Fourth, the security risks are increasing rapidly [Nash, 2009; Kho, 2009] and fifth, the number and type of devices not provisioned by an organization (e.g., cell phones or laptops) and the number and type of remote or external users needing access is increasing exponentially [Waters, 2007].

While IT managers are working on these internal challenges, they are poorly supported by the available technologies, standards, and legal frameworks. Although IDM is about more than technology, tools can be useful in many aspects of the lifecycle, including: administration, audit and analytics, authentication, and authorization. Unfortunately, the available tools do not map well to these IDM functions, and there is considerable confusion about their capabilities [Kreizman et al., 2009]. Many tools are proprietary, making it difficult to easily deploy IDM across enterprise boundaries [Kho, 2009; Saran 2007]. These problems are exacerbated by a lack of common language, standards, and accepted best practices in IDM [Neuenschwander, 2006; Kho, 2009]. As one focus group manager noted, "Without common standards and a common understanding of IDM principles, it is very difficult for organizations to move forward and engage in federated IDM, though that is what we would all like to do."

Most countries' legal frameworks are also woefully lacking in numerous ways. One study found that there are no universally-accepted standards of identity-proofing or common standards of what attributes should be used to identify an individual or a business [Smith, 2007]. This means that every organization, and its legal department, is left to determine what attributes it should collect for appropriate access control. Thus, in most focus group companies, every external relationship must be manually configured and legal approval sought. "We are held to be legally accountable for who is using our data," said one manager. Another noted, "We must assess each vendor individually regarding their standards and practices." In some cases, organizations' legal obligations are unclear and, in others, companies appear to be over-regulated, resulting in considerable confusion [Saran, 2007; Neuenschwander, 2006; Smith, 2008]. Finally, for global companies, the challenge is even greater as they must factor different countries' privacy laws into their access equations. "In many cases, we must control what data leaves a country, preventing global service providers from accessing certain kinds of data," explained one manager. The overall result is that legal concerns have meant that federated IDM has been much slower to take off than initially expected and external access to company data and processes is still limited and largely manual.

Overall, managing access across an enterprise of any size at any deeper level than coarse access control is "a herculean effort" [Neuenschwander, 2006]. What's needed, according to the focus group, is a different approach to IDM. "At present, we have point products, point problems, fragmented policies and processes that simply don't work for our business environment," explained one manager. Others agree, "the increased scale of network access today exceeds the original models of IDM" [Small, 2006]. "[The current] fragmented, siloed approach cannot meet the needs for business agility in enterprises with ever-increasing numbers of internal and external users across heterogeneous legacy, client/server, web and service-oriented architecture environments" [Allan et al., 2009].

V. PRINCIPLES OF EFFECTIVE IDM IN THE FUTURE

Newer approaches to IDM are by no means well-established and there are still many gaps in our understanding about how these might work. However, there are several principles to guide this development that are quite widely accepted. These include:

- *Approach IDM Holistically.* Focus group managers agree that IDM should be an integrated part of an organization's overall security framework that consists of several layers, each of which work together to create an environment of trust and protection (see Figure 1). A layered approach provides multiple forms of back-up protection in case vulnerabilities are detected, while integration ensures that practices are as efficient as possible from both a user and a cost point of view. A comprehensive framework should support both internal and external access, address governance and process as well as technical concerns, and integrate IDM into policy-setting [Wagner and Alan, 2009; Suess and Morooney, 2009].

- *Focus on Business Value.* As noted above, the business-enabling elements of IDM can often get lost in the technological jargon that too-often characterizes IDM plans and discussions [Smith, 2008]. There are several elements of business value that should be considered in developing an IDM framework. First, IDM should be designed to help make effective business decisions and manage the flexibility:risk trade-offs that are involved [Small, 2006; Allan et al., 2009]. Second, it should reduce the cost of providing effective IDM [Small, 2009; Perkins, 2009]. Third, it should increase trust both internally and externally in an organization's IDM practices [Smith, 2007]. Fourth, it should support the development of electronic services, virtual and remote work, and global sourcing [Wagner and Allan, 2009]. Finally, by streamlining IDM practices, it should enhance productivity and adherence to acceptable-use policies [Maler, 2009; Kalin, 2005; Small, 2006].

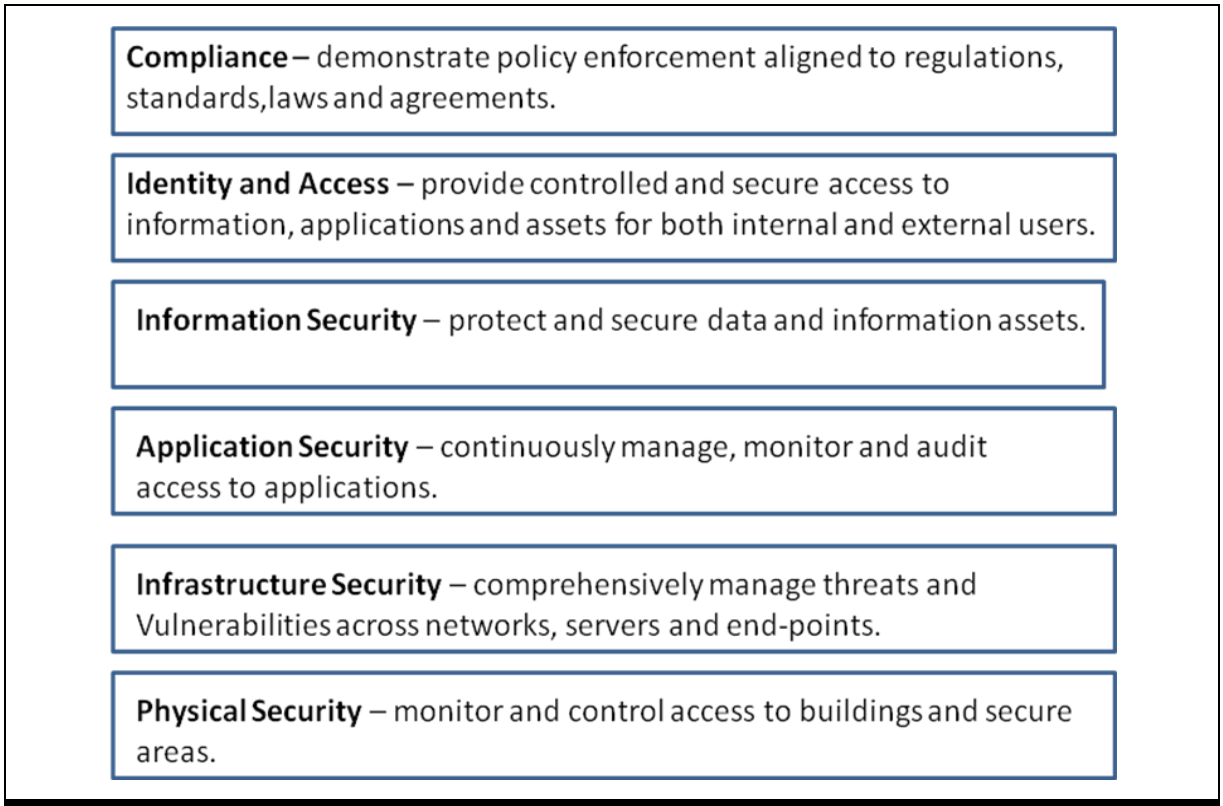

Figure 1. IDM Is Part of a Holistic Security Framework

- *Adopt Standards Wherever Possible.* It was widely-recognized in the focus group and elsewhere that enterprise IDM should adhere to open standards in order to facilitate provisioning of cross-enterprise services [Smith, 2008]. However, these standards are just beginning to be developed and are still far from being broadly accepted [Saran, 2007; Kho, 2009]. Thus, at present, companies must largely create their own standards—either on their own or within their industry. Several members of the focus group are participating in standards-creating bodies that are designed to create small federated IDM environments in order to be able to trust identities created within them. Similarly, other third party IDM services are beginning to emerge [Neuenschwander, 2006; Fest, 2008]. It is, therefore, important for IT managers to monitor these developments and to adopt standardized approaches as they become available.

- *Develop a Roadmap.* IDM is a rapidly evolving field [Allan et al., 2009]. Moving from traditional approaches to newer and more effective ones will take time and require vision and the development of a roadmap [Smedlinghof, 2008; Allan et al., 2009]. Such a roadmap would not only create the framework, policies, and standards for IDM, it would also develop the processes and infrastructure required to achieve it. Streamlining processes to structure IDM activities more effectively and eliminate duplication of effort is a good first step [Allan et al., 2009]. Improved integration of business and IT IDM processes is another [Shuey and West, 2006]. Finally efforts need to be made to simplify security technology such as: developing a single sign on for systems that links to user roles; segmenting data to enable more granular access; and improving monitoring and reporting [Small, 2006; Kreizman et al., 2009]. Focus group members were at different stages of developing such roadmaps but all were actively working on them.

- *Decouple IDM—from Applications, Environments and Companies.* The goal of newer approaches to IDM is to abstract it from specific entities. Clearly, it must be decoupled from individual applications so that it can be managed holistically. However, it must also make identities portable across systems, technical environments, and devices [Smedlinghoff, 2008; Small, 2006]. And, it must be designed to rapidly connect (and disconnect) users and partners as required [Perkins, 2009; Wagner and Allan, 2009]. Some newer approaches to IDM are user-centric, putting customers at the centre of IDM by making them owners of their own data rather than many different companies. These approaches use identity management services that act as identity containers and provide proof of identity to companies as permitted by a customer, who can choose what information to release to a company [Maler, 2009]. While there is agreement that such IDM services are not yet practical for most companies, decoupling IDM as much as possible from proprietary practices is good

preparation for the direction that most observers (and the focus group) believe that IDM is headed [Maler, 2009; Kho, 2009; Djordjevic and Dimitrakos, 2005].

VI. MOVING FORWARD WITH IDM: ADVICE FOR IT MANAGERS

No IT manager or business leader should ever underestimate the challenges involved in IDM as the field struggles to keep up with our increasingly networked, global, and mobile world. Members of the focus group had several recommendations for other IT managers about how to begin moving toward the next level of IDM. These include:

- *Identify IDM Needs and Set Policy.* An important step in evolving IDM is to better understand the organization's needs for IDM both internally and externally. As noted above, there is no standard list of identity attributes or an external identity management body, so organizations are forced to fend for themselves in determining acceptable internal and external authentication; layers of authentication, such as situational or corporate access; IDM triggers, such as changing jobs or adding a new vendor; and the level of granularity of access that is desirable. Understanding IDM needs is fundamental to establishing access policies and to developing effective IDM processes, stated the focus group managers.

- *Address IDM Process and Governance.* It is widely accepted that many organizations have inadequate and immature IDM processes [Allan et al., 2009; Kho, 2009; Suess and Morooney, 2009]. Many focus group members were in the process of assessing the current state of their IDM and determining their strategy and vision for adapting it to meet their needs. One manager explained her organization's IDM goals as: "We want to have one enterprise ID; one integrated, automated full lifecycle process; one (or a very few) sign-ons; one book of record; and improved compliance, service, and productivity." Other focus group managers were concentrating on improving the process for external access. "We need a process for assessing vendor IDM practices," said one. Another was looking at how to recognize external identities from trusted third parties. All these processes need governance, and business ownership of IDM was viewed as essential to making the right decisions about how the flexibility:risk tradeoffs are handed. "The trouble in our organization is that we have no overall owner," said one manager. "Ownership is split between IT, operations, and our lines of business." A single leader and clarity about roles and responsibilities was deemed essential to improving. Another manager added, "We need to make process changes to get the sequence of events right, and we need to reengineer our workforce management process to better integrate with our IDM process." Viewing IDM as a lifecycle can be useful in helping to develop and manage an improved process (see Figure 2).

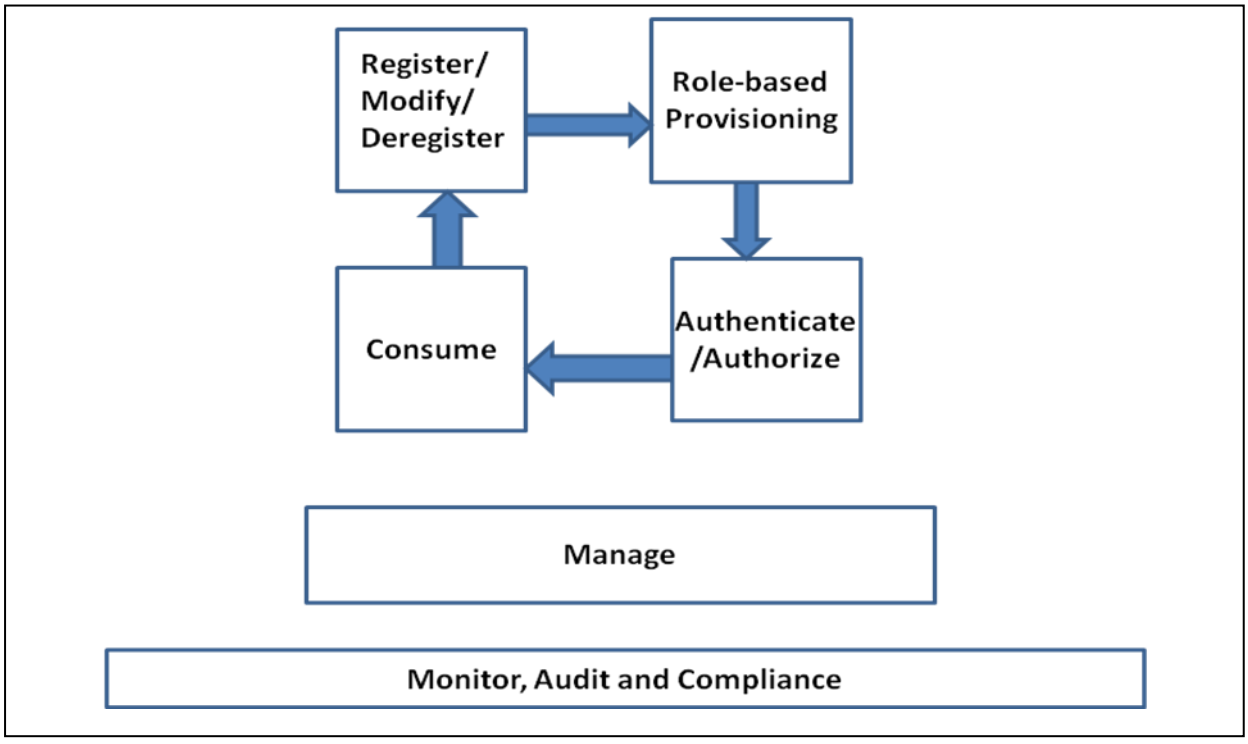

Figure 2. The IDM Lifecycle

- *Integrate IDM with Architecture.* IDM technology is an important component of any organization's approach to IDM, stated the focus group, but only if it is combined with effective processes and behavioural changes. Most of the technical challenges involved stem from poor systems integration and a lack of standards. These can best be addressed by an organization's architecture group as it plans and designs how applications and infrastructure will evolve. Clearly, IDM should also be integrated with the organization's security framework and many enterprises are working to extract IDM from their applications and develop a single enterprise sign-on that is linked to access and other controls. In the longer term, most focus group organizations are hoping that IDM will eventually become a service that is provided by a third party or which is jointly owned by a federation of related organizations. While this has not been widely implemented at present, architects and security specialists should be aware of standards developments and any initiatives in their industry to share identity information.

- *Incorporate Traceability and Auditability.* What is often overlooked in considering IDM is the back end of the lifecycle process, including monitoring accounts, user activity and compliance reporting. Increasingly, these activities are becoming part of legal and regulatory best practices. Focus group managers noted that a significant amount of their time is now devoted to this work and that new tools and policies are needed in this area. "The top three threats to enterprise security are insider-related," stated one manager. These include employee error, data theft, and insider sabotage. Overall, insider fraud costs U.S. companies over $600 billion annually [Small, 2009]. To address these risks, many managers have been given new oversight roles and responsibilities but inadequate processes and tools to help them. "IDM has created work for me that I never expected," explained a manager. "I now receive several messages a day to revalidate transactions that are being done by my staff. Every executive has a responsibility to review what is being done." Some of the monitoring that is now considered important includes monitoring the volume of user activity, monitoring the types and locations of activities, and ensuring activities are properly segregated to prevent fraud. Finally, reports must also demonstrate compliance with all regulations and laws. Ideally, as much of this work as possible should be automated, while governance and processes also need to be designed to effectively incorporate these new requirements for IDM.

VII. CONCLUSION

Identity management is a huge and constantly changing challenge for organizations. IT managers must balance the substantial risks involved in becoming increasingly networked and opening their firewalls to clients and partners with the resulting business value delivered. Like so much else in IT, effective IDM must be viewed from both a business and a technical lens and requires business leaders to be actively involved in taking ownership of the decisions involved. There is no straightforward and easy-to-implement solution for IDM. As a result, IT managers are all too often caught between a rock and a hard place—either being seen as the obstacle to business transformation or having to take "bet the company" risks with inadequate data and access controls. However, they do themselves no favour by failing to articulate IDM issues in business terms when speaking with business leaders. It is, therefore, incumbent on all organizational leaders to work together to continuously evolve a practical and holistic framework that will ensure that their IDM practices keep up with both the opportunities and the risks of a transforming world.

REFERENCES

Editor's Note: The following reference list contains hyperlinks to World Wide Web pages. Readers who have the ability to access the Web directly from their word processor or are reading the article on the Web, can gain direct access to these linked references. Readers are warned, however, that:

1. These links existed as of the date of publication but are not guaranteed to be working thereafter.
2. The contents of Web pages may change over time. Where version information is provided in the References, different versions may not contain the information or the conclusions referenced.
3. The author(s) of the Web pages, not AIS, is (are) responsible for the accuracy of their content.
4. The author(s) of this article, not AIS, is (are) responsible for the accuracy of the URL and version information.

Aitoro, J. (2008) "Identity Management", *Government Executive* (40)7, pp. 30–33.

Allan, A., E. Perkins, and T. Scholtz (2009) "Gartner Identity and Access Management Program Maturity Model", *Gartner Research*, #G00170668, October 8.

Allan, A. and E. Perkins (2009) "Key Issues for Identity and Access Management, 2009", *Gartner Research,* #G00165392, March 6.

Britt, P. (2008) "Taking the Byte Out of Cybercrime", *Information Today* (25)11, p 50-51.

Djordjevic, I. and T. Dimitrakos (2005) "A Note on the Anatomy of Federation", *BT Technology Journal* (23)4, pp. 89–106.

Doctorow, C. (2007) “A Conversation with Cory Doctorow and Hal Stern”, *ACM Queue* (5)3, pp. 16–23.

Fest, G. (2008) “Identity Management: The Lure and Peril of Open ID”, *Bank Technology News* (21)4, pp. 10–11.

Kalin, S. (2005) “How to Tackle Identity and Access Management”, *CIO Magazine,* www.cio.com (current Dec. 1, 2005).

Kho, N.D. (2009) “The Changing Face of Identity Management”, *EContent* (32)3, pp. 21–25.

Kreizman, G. et al. (2009) “Gartner Identity and Access Management Capability Models, 2009”, *Gartner Research*, #G00166023, March 10,.

Maler, E. (2009) “The Design of Everyday Identity”, *Online Information Review* (33)3, pp.443–457.

Nash, K. (2009) “Tough Work Ahead to Defend Digital Infrastructure; Review of Security Needs Provides a Long List of Issues to Address”, *CIO Magazine* (22)15.

Neuenschwander, M. (2006) “Identity Management Market Shifts—Who’s Out There?” *Network Security*, 12, December, pp.7–10.

Perkins, E. (2009) “Cost Cutting in Enterprises and Six Ways Identity and Access Management Programs Can Help, 2009 Update”, *Gartner Research*, #G00167403, April 20.

Saran, C. (2007) “Lack of Interoperability and Liability Hold Back Identity Management IT”, *Computer Weekly,* November 13, p. 16.

Shuey, R. and A. West (2005) “Building a Balanced Identity Management Infrastructure”, *EDUCAUSE Review* (41)5, pp. 138–139.

Small, M. (2006) “Unify and Simplify: Re-thinking Identity Management”, *Network Security,* 7, July, pp. 11–14.

Small, M. (2009) “Keeping the Bad Guys Out: Keeping the Customers Happy”, *The British Journal of Administrative Management,* Summer, pp. 32–33.

Smedlinghoff, T. (2008) “Legal Obstacles Delaying Federated Identity Management”, *CIO Magazine*, www.cio.com (current Jan. 30, 2008).

Smith, D. (2008) “The Challenge of Federated Identity Management”, *Network Security,* Vol.4, pp. 7–9.

Smith, H.A. (2007) “Identity Management and Authentication: A Fundamental of Improved Service Delivery”, Report of the IDMA&A Task Force to the XI Lac Carling Conference, Niagara Falls, ON.

Suess, J. and K. Morooney (2009) “Identity Management and Trust Services: Foundations for Cloud Computing”, *EDUCAUSE Review* (44)5, pp. 25–42.

Wagner, R. (2009) “Roundup of Identity and Access Management Research 3Q09: Core IAM and IAM Governance”, *Gartner Research,* #G00170862, September 24.

Wagner, R. and A. Allan (2009) “Highlights from the Gartner European Identity and Access Summit, 2009”, *Gartner Research,* #G00167237, April 17.

Waters, J. (2007) “ID Management Definition and Solutions”,, *CIO Magazine,* www.cio.com (current May 2, 2007).

ABOUT THE AUTHORS

Heather A. Smith (hsmith@business.queensu.ca) has been named North America's most published researcher on IT and knowledge management issues. A senior research associate with Queen's University School of Business at Kingston, Canada, she is the co-author of four books: *IT Strategy in Action; Management Challenges in IS: Successful Strategies and Appropriate Action; Making IT Happen: Critical Issues in IT Management;* and *Information Technology and Organizational Transformation: Solving the Management Puzzle.* A former senior IT manager, she is currently co-director of the IT Management Forum and the CIO Brief, which facilitate inter-organizational learning among senior IT executives. She is also a senior research associate with the Society for Information Management's Advanced Practices Council. In addition, she consults, presents, and collaborates with organizations worldwide, including British Petroleum, TD Bank, Canada Post, Ecole des Hautes Etudes Commerciales, the OPP, and Boston University. Her research is published in a variety of journals and books *including MIT Sloan Management Review, Communications of the Association for Information Systems, Knowledge Management Research and Practice, Journal of Information Systems and Technology, Journal of Information Technology Management, Information and Management, Database, CIO Canada,* and the *CIO Governments Review.* She is also a member of the editorial board of *MISQ-E*.

James D. McKeen is a professor of IT Strategy and Distinguished Research Fellow in MIS at the School of Business, Queen's University at Kingston, Canada. Jim received his Ph.D. in Business Administration from the University of Minnesota. He has been working in the IT field for many years as a practitioner, researcher, and consultant and is a frequent speaker at business and academic conferences. Dr. McKeen co-facilitates the networking of senior executives in the IT sector through two well-known industry forums: the IT Management Forum and the CIO Brief. He also has extensive international experience, having taught at universities in the U.K., France, Germany, and the U.S. His research has been widely published in various journals including the *MIS Quarterly*, *Knowledge Management Research and Practice*, the *Journal of Information Technology Management*, the *Communications of the Association for Information Systems*, *MIS Quarterly Executive*, the *Journal of Systems and Software*, *the International Journal of Management Reviews, Information and Management*, *Communications of the ACM*, *Computers and Education*, *OMEGA*, *Canadian Journal of Administrative Sciences, Journal of MIS*, *KM Review*, *Journal of Information Science and Technology,* and *Database*. Jim is a co-author of three books on IT management with Heather Smith, the most recent being *IT Strategy in Action* (Pearson Prentice Hall, 2008). He currently serves on a number of editorial boards.

Communications of the Association for Information Systems

ISSN: 1529-3181