Identity Management Framework:

Delivering Value for Business

By Srinivasan Vanamali, CISA, CISSP

With the advent of web-enabled technologies, extranets for partners and federated networks for business units, organizations are moving away from a closed business model to a more open model. This has resulted in complexity dealing with users and managing their access to systems. There is also increased risk due to ineffective controls in managing user identities, establishing trust, enabling privacy, and complying with legal and regulatory requirements. Identity management (IM) deals with these risks. Identity management, in a nutshell, is a convergence of business processes and technology to provide security, trust and privacy by identifying users and authorizing access to identity-based systems, information resources and applications.

Identity management is often perceived to be the panacea for all issues related to an open model, identity-based system. However, more and more organizations deploy identity management solutions from a tactical perspective—isolated technology initiatives to solve technical issues or deal with compliance requirements—rather than from a strategic point of view, which is business-driven and outcome-based.

As pointed out in Burton Group analyst research, "…historically, enterprises have made attempts to treat the symptoms of the identity management problem with point solutions."[1]

It is further noted in the research, "Many enterprises make the mistake of rushing to implement directories, security systems and other IM components before they evaluate how they're storing, managing and distributing identity information."

This has resulted in:

- Fragmented point solutions
- Failure to deliver real business value
- Failure to leverage existing investments and infrastructure
- Dilution of identity management initiatives over time
- Increasingly difficult funding for further initiatives

For identity management to thrive organizationwide and deliver business value, it is important to establish a framework that acts as a term of reference for all identity management initiatives.

What Is Identity Management?

Today, organizations have many *ad hoc* processes and tools to manage and provision user identity information from human resources (HR) systems to other systems and applications. Identity management streamlines various business processes that deal with managing all forms of identities in an organization—from enrollment to retirement.

Critically important in the emerging model is the ability to integrate business processes and technology to provide fine levels of granularity in terms of linking people to systems and services. One of the key objectives of identity management is to centralize and standardize this process so that it is provided consistently as a common service across the organization.

Identity management is comprised of many components that provide a collective and common infrastructure, including directory services, authentication services (validating who the user is) and authorization services (ensuring the user has appropriate privileges to access systems based on a personalized profile). It also includes user-management capabilities, such as user provisioning and deprovisioning.

Approach to Identity Management

Under the prevailing business environment where IT budgets are ever shrinking, organizations are reluctant to spend on new initiatives that will solve only technical problems. Today's approach is "business-driven IT," where IT solutions go beyond solving technical issues to enabling the business. Identity management initiatives reflect the fundamental change in the role of IT within organizations. The premise is that identity management solutions deliver real business value with tangible benefits. This occurs by improving responsiveness to the business with solutions like delegated and self-service administration, which reduces the reliance on support organizations. Identity management also delivers a measurable return on investment by means of reducing cost and improving productivity. For example, an automated workflow system could streamline the user provisioning process and eliminate the need for a number of silo administrators managing different systems and applications. Users self-managing their accounts, resetting their passwords and unlocking their accounts through a portal will also improve productivity.

For this reason, identity management initiatives must be approached from a strategic point of view with a high level of clarity on objectives and clear measurable outcomes, such as improved business process and enhanced user experience.

Why a Framework?

The scope of identity management is broad and affects all facets of the business. It is important to understand that identity management needs to be pervasive to be effective, and it is easy to be overwhelmed by all the jargon, technologies and products. This often seems to be the case when identity management is approached from a technical perspective.

As further noted in the Burton Group research, "…most of today's IM infrastructures are ad hocracies, built one application or system at a time, rather than created within an enterprisewide framework. The result is a spider web of overlapping repositories, inconsistent policy frameworks and process discontinuities. The resulting systems are error-prone, expensive to manage and riddled with security loopholes."

To address this scope and complexity, a simple model is required—a framework that can be used to discuss the major business issues and how to deal with them effectively and efficiently. A framework will serve as a basis for vital understanding between business management and technical managers on all identity management initiatives.

Identity Management Framework

An identity management framework helps align identity management initiatives with the organization's business goals and security strategy. It also focuses on issues related to:

- Delivering business value
- Data confidentiality and integrity
- Nonrepudiation
- Authentication and authorization
- Provisioning and deprovisioning
- Audit
- Compliance and monitoring

Figure 1 outlines the key components of the framework based on a top-down approach where each layer of the pyramid relies on the one above.

The key components of the framework are security vision, IM strategy, policies and standards, IM architecture, IM specifications and IM road map. Each is described in detail in the following sections.

Security Vision

Organizations must have an executive-sponsored security strategy based on current business and IT strategy. Identity management initiatives must closely align with the organization's security initiatives and subscribe to the information security management system (ISMS) scope, security principles and values.

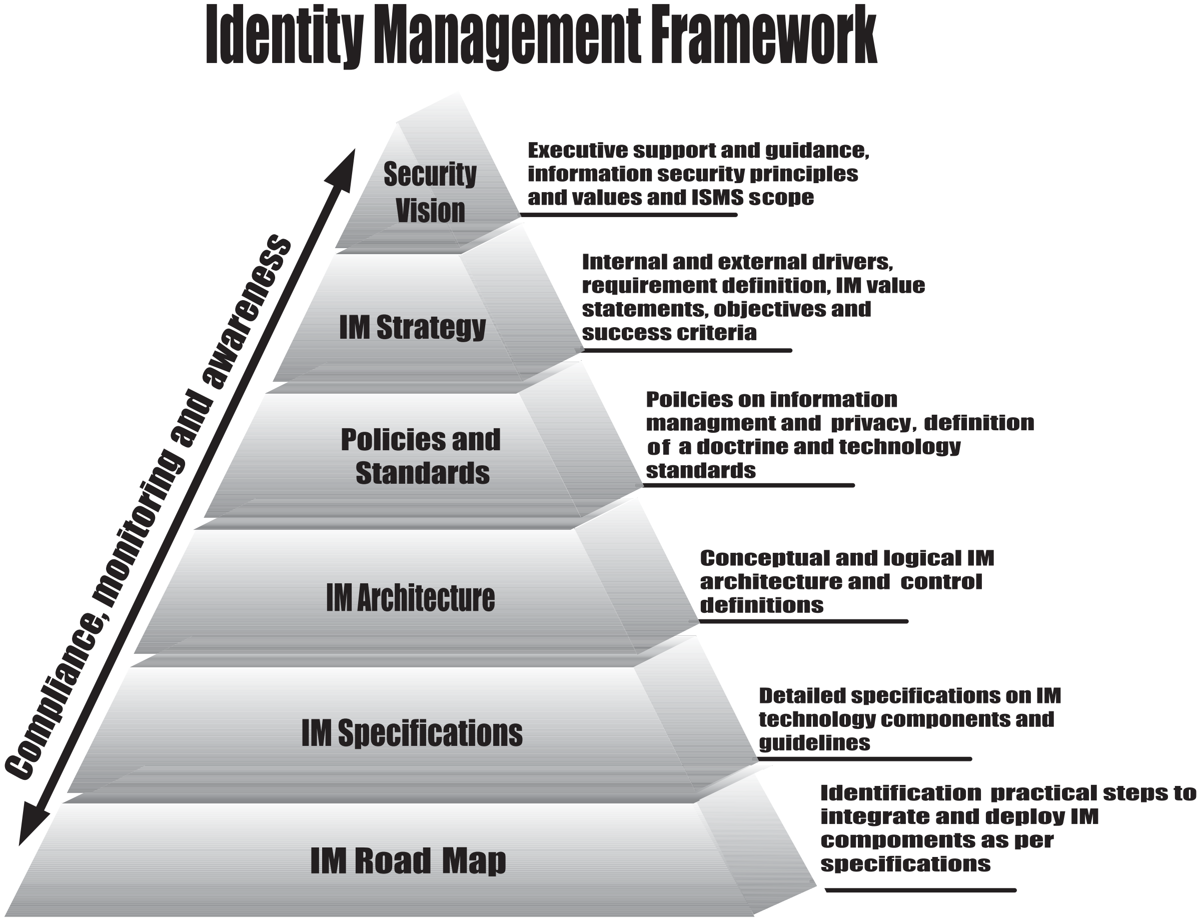
An organization's security vision statements must include:

- Importance of information security to the organization
- The need for information assets to be secured
- Description of how these assets will be managed
- A risk management approach to mitigate perceived risks

Identity Management Strategy

An identity management strategy is a key component of the framework and must align closely with the organization's business and IT strategy. The strategy should be based on

Figure 1—Key Components of the Identity Management Framework


Identity Management Framework
Security Vision
Executive support and guidance, information security principles and values and ISMS scope
IM Strategy
Internal and external drivers, requirement definition, IM value statements, objectives and success criteria
Policies and Standards
Poilcies on information managment and privacy, definition of a doctrine and technology standards
IM Architecture
Conceptual and logical IM architecture and control definitions
IM Specifications
Detailed specifications on IM technology components and guidelines
IM Road Map
Identification practical steps to integrate and deploy IM compoments as per specifications
Compliance, monitoring and awareness

business drivers[2] and must clearly define the key drivers both internal—such as reducing IT costs and improving security—and external—such as regulatory requirements and audit requirements—to the organization.

The strategy clearly identifies the:

- Objectives of identity management
- The success criteria against which any initiatives will be measured. These should include success factors to measure the degree to which each objective is met. For example, an audit report identifies a security risk that user accounts are not removed as soon as they leave the organization. Implementing a user-provisioning system that automatically removes the user IDs pertaining to a former user mitigates the risk and fulfills the audit requirement.
- Overall business benefits anticipated, such as improved process, reduced cost, improved service delivery and improved productivity. For example, deploying self-manage services as part of a corporate portal allows users to reset their locked accounts based on a "challenge and response," which results in a reduced number of calls logged through the help desk. This translates to improved service delivery and productivity gained, as the users are able to get back to their tasks without unnecessary delay caused by the help desk process.
- Inherent risks of the strategy, which are often related to reengineering the business processes, which requires organizational change from a political and cultural perspective. Also, cross-organizational cooperation required to implement the strategy needs to be evaluated.

The strategy can be used to redesign processes and workflows, identify opportunities for automation, correct control weaknesses, and define and consider alternative solutions.

Policies and Standards

The framework must outline a set of policies for identity management. These policies should cover a range of levels from organizationwide to system-specific and even to issue-specific.

The framework defines a set of standards to which identity management initiatives have to adhere. Some examples include:

- Defining minimum authentication levels and methods, such as using two-factor authentication as a minimum requirement to perform administrative tasks
- Defining acceptable levels of encryption
- Defining directory standards and approaches, such as the role of a metadirectory or how to integrate existing directory servers into a common backbone
- Defining data exchange formats and methods, such as SPML, SAML, XML and DSML

One of the key requirements of the standards section of the framework is to define an information management doctrine or terms of reference on how to deal with privacy, trust and regulatory requirements on audit and compliance. Identity management initiatives become part of common infrastructure. This provides a consistent approach that is applied to all initiatives and can be leveraged for new identity management initiatives.

Identity Management Architecture

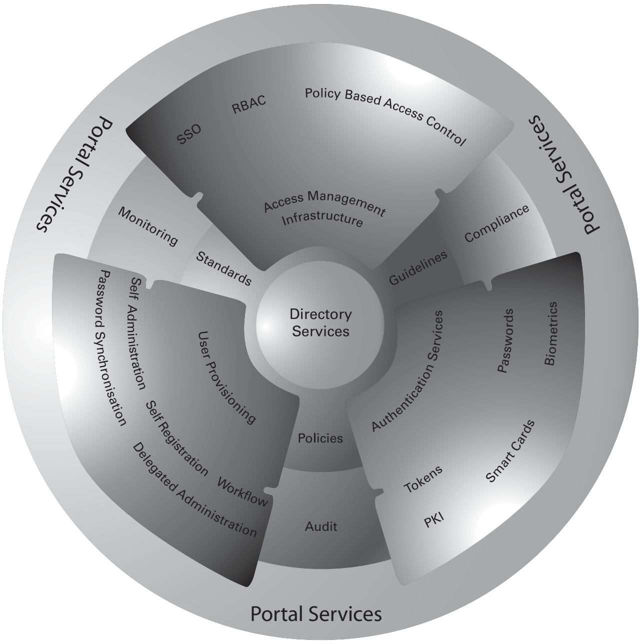
Organizations should have an enterprise architecture encompassing the security architecture. The identity management architecture must align with the security architecture and must identify the key components of identity management and provide effective measures to manage security across the organization.

The objectives of the identity management architecture are to:

- Serve as a model and act as a blueprint to adopt and follow for current and future identity management initiatives
- Be practical, effective, consistent and manageable

Figure 2 depicts the key components of an identity management solution.

Figure 2—Key Identity Management Components



The control functions specified in the architecture must support the design, implementation, maintenance and management of the identity management infrastructure.

The key identity management components in **figure 2** are:

- Directory services—Built on a name-based object model, directory services is the most critical component of identity management. It acts as a repository for user ID and user profile information, and it plays a key role in user authentication and enabling on-demand service delivery.
- User provisioning—A role-based approach driven by a directory, user provisioning helps oversee end-to-end user life cycle management from enrollment to retirement across different name-based systems and applications.
- Authentication services—This component helps identify the user through various authentication methods, including digital certificates.
- Access management infrastructure—Based on a defined policy, access management infrastructure controls and authorizes access to information systems and applications.
- Portal services—These act as a presentation layer providing a single interface to all web-enabled systems and applications, as personalized to the user profile.

Identity Management Specifications

The detailed specifications guide technology choices based on required functionality. A key requirement is an understanding of how each component fits into the identity management architecture and its role as part of the overall solution.

The specifications also cover evaluation criteria for acquiring or integrating identity management solutions, along with guidelines for effective implementation. The identity management infrastructure is a loosely coupled technology driven by a set of business processes. For example, a detailed specification for a user provisioning system addresses evaluation criteria to meet technical and business objectives of the proposed solution. If the solution has an impact on an existing business process, the specification must address how to deal with the impact and what is required to reengineer that business process.

Identity Management Road Map

Defining a road map is a critical component of the framework. One of the challenges often faced by organizations is where to start and how to go about delivering a solution. A typical road map must identify practical steps to deploy and integrate identity management components in line with the organization's identity management specifications, architecture, policies and standards, and identity management strategy.

The road map must also identify low, medium and high priorities based on short-, medium- and long-term strategies, driven from a business impact and value proposition.

For example, consider an organization that has too many help desk calls logged due to different user IDs and password combinations for each application. While the organization's long-term strategic approach is to move toward web-enabling applications with a directory-centric security framework, which will reduce the number of IDs, it may take two years to achieve. In the meantime, it can look at a short-term solution of providing a self-service function where users can reset their password and unlock accounts. This approach is based on a high priority but a short-term strategy to address a business-critical issue, which will improve the user experience and productivity.

Conclusion

While identity management solutions are becoming a popular response to security challenges, organizations must carefully consider how to ensure benefits and value to the business. Identity management initiatives are often diluted over time as organizations fail to leverage their existing technology and intellectual property investments, and instead reinvent the wheel.

Organizations can demystify the technical hype and approach identity management from a business-driven IT perspective by following an identity management framework. The framework should carefully consider and clearly define business goals, strategy, policies and standards, along with detailed identity management architecture, specifications and a road map. This provides a basis for successful, business-driven and clearly understood identity management.

References

[1] Lewis, Jamie; "Enterprise Identity Management: It's About the Business," vol.1, 2 July 2003, Burton Group Directory and Security Strategies Research Overview, *www.burtongroup.com*

[2] Ahuja, Jay; "Identity Management: A Business Strategy for Collaborative Commerce," *Information Systems Control Journal*, vol. 6, 2003

Srinivasan Vanamali, CISA, CISSP
is the senior consultant, enterprise security, for Computer Associates in Melbourne, Australia. He has more than 16 years' experience in a variety of IT management and technical roles and has worked in a variety of industries including government, banking, energy and health. For the past six years his focus has been information security management based on industry standards such as ISO:17799 (NZS/AS:7799) and COBIT, with a specialty in information assurance process, security audit and assessment, security architecture and information risk management (assessment and mitigation). Over the previous four years, Vanamali has been focused on delivering identity management solutions primarily in the finance sector working with banks in Australia, New Zealand and the US. He has also engaged in a number of security audits, assessments and information security assurance reviews in Australia and New Zealand. Vanamali has developed an information security framework model based on standards and has written a white paper called "Identity Management Framework: Delivering Business Value."

Information Systems Control Journal, formerly the IS Audit & Control Journal, is published by the *Information Systems Audit and Control Association*, Inc.. Membership in the association, a voluntary organization of persons interested in information systems (IS) auditing, control and security, entitles one to receive an annual subscription to the *Information Systems Control Journal*.

www.isaca.org