The Impact of Governance on Identity Management Programs

Rafael Etges, CISA, CRISC, CIPP/C, CISSP, is the director for security consulting services at TELUS, directing the organization's governance, risk and compliance (GRC) and identity and access management consulting practices. He is a member of the ISACA Toronto (Ontario, Canada) Chapter.

Anderson Ruysam, CRISC, CISSP, ITIL, is a senior IT risk advisor at the Government of Ontario, Canada, specializing in IT GRC and business management. Ruysam brings more than 14 years of extensive experience in IT governance, risk management and security operations.

Recently, the interest of organizations in identity and access management initiatives has increased dramatically, mostly led by the government, retail and financial sectors' concerns with data leakage, fraud and regulatory compliance and by management's interest in optimizing IT processes and reducing spending. The benefits associated with role and identity programs include improved management of access to information systems (IS) and data, which leads to better security and risk management; portability and reusability of role definitions across the organization; an ability to meet and demonstrate regulatory compliance; improved business continuity; and, equally important, cost efficiencies in administration and integration of business applications.

As the average annual budget required by enterprises to deploy identity management (IDM) solutions approaches the seven-figure range,[1] significant management involvement and diligence is vital to properly allocate resources. In addition to the business justification for such an investment, solid IDM governance must be applied to ensure that the relevant stakeholders are involved in the definition of principles and goals governing how business roles are managed within the organization. The ongoing message must be that IDM is a business issue affecting compliance, risk, privacy and cost-efficiencies, and that the main driver remains the proper management of business roles and processes supported by complex technology—and not the opposite.

This article focuses on two questions: What are the governance elements required to ensure the success of an IDM deployment in a complex enterprise environment? What is the bottom-line impact of having—or not having—these elements in place?

IDM, ROLE AND ACCESS GOVERNANCE

The identity and access governance discipline is rapidly evolving, and best practices and standards are still being developed.[2] Discussions among industry leaders are taking place, and best practices are being promoted by research institutes such as Forrester,[3] the Burton Group[4] and Gartner,[5] which further expand on specific approaches, solutions and products that address these new requirements and their respective areas of value.

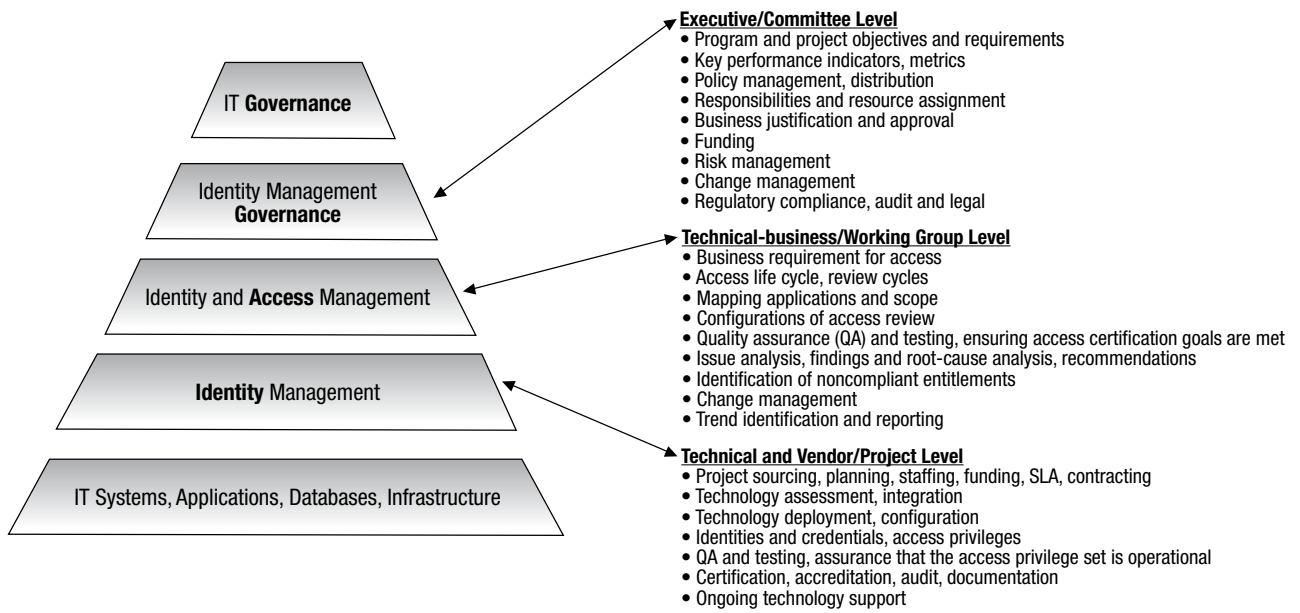
Different terminology is being created and used as the industry practices evolve around the management of roles, access and identities. In general, "role" represents a set of responsibilities needed to conduct business operations or transactions, "access" represents the privileges and resources used by someone within a role, and "identity" represents someone with a given role at a certain point in time.[6] The clear distinction among these terms is paramount since the management of each of these elements is evolving into discrete disciplines of their own. While identity management solutions focus on the automated provisioning and deprovisioning of identities/access to system resources, they have little to offer in terms of access governance (which roles should be granted access to what resources and how) or identity governance (how the organization defines roles and identities with the involvement of business leaders responsible for operations and revenue streams that rely on those roles to function).

Figure 1 shows a sample framework used to differentiate these elements and address the needs and requirements at each level.

THE BENEFITS OF GOVERNANCE

Different entities and individuals tend to defend different views and definitions of governance. A complete and impartial definition of "enterprise governance" reads: "Governance is the framework, principles, structure, processes and practices to set direction and monitor compliance and performance aligned with the overall purpose and objectives of an enterprise."[7]

Figure 1—Sample Role and Identity/Access Management Framework



Organizations that originally deployed IDM solutions to drive automation and better provisioning and deprovisioning capabilities within IT are now challenged with new requirements. They must leverage the same technology to demonstrate compliance with regulatory standards and enhance the visibility into "who has access to what," "why" and "approved by whom" at a more granular level than the existing IDM solutions were initially designed to provide. An additional layer of governance related to IDM is required to address these needs. These requirements are also related to IT governance and compliance and speak to the needs of business functions being serviced by IT.

The benefits presented by recognizing the need for and managing the governance and access management layers on top of the IDM technology are many, and can be summarized as:

- Automation of the entire entitlement and role review process, in alignment with business needs and requirements as stated by business leaders and managers
- Enterprisewide visibility into all user access privileges. Reviews are easy for business users to understand and can be configured to accommodate unique processes.
- Oversight in the form of dashboards reconciling and centralizing information for immediate insight into the status of the review and certification processes
- Certification and remediation of user entitlements; archived certifications and complete audit trail of historical changes that provide the evidence required by auditors
- Integration with the user provisioning infrastructure to track all entitlement changes; simplified role and access definitions at every stage of the user life cycle
- Change request workflows triggered by a change event or revocation of entitlements or event-driven workflows initiated by a change event requiring an incremental review of a user's access

These benefits cannot be realized by the deployment of IDM technology alone, and in some cases, the enterprise can be oversold on the provisioning technology by a vendor. Without oversight, the technology will not resolve business issues. The access management and governance layers must be in place to ensure that the full value of the investment is realized. This is not always the case.

Enjoying this article?

- Read *Identity Management Audit/Assurance Program*.

http://www.isaca.org/bookstore

- Learn more and collaborate on Identity Management.

http://www.isaca.org/topic-identity-management

THE IMPACT OF IDM GOVERNANCE ON STAKEHOLDERS

Figure 2 shows the positive impacts of governance elements applied to an IDM deployment to varying stakeholders affected by the technology within a typical organization.

CONCLUSION

IDM solutions offer an incredible value proposition for organizations. Like other complex technologies, such as customer relationship management (CRM) and enterprise resource planning (ERP), they touch and influence the way key revenue-generating business processes function. To a higher degree than CRM and ERP, IDM has the potential to affect any business process of an enterprise as roles, identities and access to IS are managed by the solution. And, as the technology becomes more pervasive in the organization, the potential for IDM—properly or poorly deployed—to deliver a positive or negative impact on stakeholders is immense.

The main factor affecting these outcomes is governance. Technology vendors will have a limited ability to understand the business issues driving the acquisition of the IDM solution by an organization, and will not have insight into its business

Figure 2—Impact of Identity and Access Governance on Organizational Functions

Stakeholder	Governance Elements	Impact
Chief information officer (CIO)	• Reduced complexity • Increased productivity • Scalability • Reduced costs • Improved audit readiness	• Service desk—Visibility and control over user and access change, provisioning and termination; reduced incidence of password reset cases • System development life cycle (SDLC)/Software as a Service (SaaS)—Standardized methods for identification and authentication, authorization and access for internal and external clients and partners; code reusage • IT support—Local databases in individual systems eliminated and replaced by a centralized access repository. Fewer cycles and resources are required to maintain and authorize access to applications and systems. • Auditing and compliance—Formalized, repeatable and documented identity and access processes that are ready for validation; reduced costs responding to audits
Chief information security officer (CISO)	• Risks managed to an acceptable level • Implementation and monitoring of controls	• Risk and control assessments—Facilitated by clear rules governing access to sensitive data, enabling the prompt identification of violations
Internal audit	• Faster audit exercises with limited resources • Accurate findings • Improved attestation	• Audit hours—Reduced effort in the validation of controls • Automated and reliable evidence • Comparable audit results—Trend mapping of control gaps, gap ownership and gap remediation
Business lines	• Reduced costs • Increased productivity • Maximized profitability and bottom-line results • Fraud and loss prevention	• Reduced cycles spent on system revisions, troubleshooting and QA related to access reviews • Consistency in business-system access rules • Visibility into who has access to business data at any point in time • Reduced fraud and losses due to improperly configured access rules, which would not be prevented by the IDM technology alone
Chief financial officer (CFO)	• Maximized revenue • Managed costs • Optimized bottom line • Maximized value for shareholders/owners • Compliance, audit and liability sign-offs	• Reduced operational expenditures—Optimized headcount, reduced consulting/contractor expenses • Budgeting—Reduced requests for *ad hoc*/emergency funding due to poor visibility into IT systems and infrastructure • Risk reduction—Enforcement of segregation of duties and due diligence • Expedited audits, reduced audit costs, and accurate and predictable findings

processes or the skill sets required to integrate and adjust its existing systems. The acquiring organization must be prepared to assess its own capabilities and gaps against best practices for managing roles and identities in areas such as access certification, entitlement management, access requisitions, and tracking and reporting, and it must be prepared to prioritize the closure of those gaps accordingly.

At a very high level, the main areas of activity include documenting a program charter (e.g., communications plan, responsibilities); determining which processes are to be considered; and identifying associated roles and IS, applicable policies, and related standards to be performed by selected subject matter experts in the organization and coordinated by a program manager in consultation with the relevant business areas.

Timing can also be a critical factor: If the solution is implemented too soon, it may not be understood by the user community and IT functions; if implemented too late, the investment fails to deliver value within the expected timelines. Technology deployment, process adjustment, learning and knowledge absorption, and oversight and management must be carefully synchronized to ensure a successful IDM implementation.

These elements are not simple to manage; however, when they are included in the planning process and considered during all stages of implementation, identity and access management solutions can deliver immense value to any organization that relies on technology to deliver business value.

ENDNOTES

[1] Kampman, Kevin; "Role Management in the Enterprise: Street Scenes," Burton Group, 23 August 2007, *www.burtongroup.com/Research/PublicDocument.aspx?cid=1126*

[2] Identity Management Forum, The Open Group, *www.opengroup.org/idm*

[3] Cser, Andras; Bill Nagel; Stephanie Balaouras; Nicholas M. Hayes; "Identity and Access Management Adoption in Europe: 2009—Uptake of Individual Technologies Is Low, But Cloud Options Hold Promise," Forrester Research, 14 May 2010, *www.forrester.com/rb/Research/identity_and_access_management_adoption_in_europe/q/id/56811/t/2*

[4] Kampman, Kevin; "Characteristics of an Effective Identity Management Governance Program," Burton Group, 22 January 2010, *www.burtongroup.com/Research/PublicDocument.aspx?cid=1731*

[5] See the keynote addresses and the "IAM Foundations: Assessing the Maturity of Your IAM Program" session from the 2010 Gartner Identity & Access Management Summit, *www.gartner.com/technology/summits/na/identity-access/index.jsp.*

[6] These terms are being defined by the authors for the sake of this article. Different etymology is used in the industry, reflecting the lack of maturity and clarity around identity and access management disciplines.

[7] Stachtchenko, Patrick; "Taking Governance Forward," *ISACA Journal*, vol. 6, 2008, *www.isaca.org/archives*