

Moving Your Company towards Role-Based Access Security Controls

By Cary Haggard, Protiviti and Brian Smith, Black & Decker

In January 2008, the French bank Société Générale stunned the financial world when it announced it lost \$7.2 billion due to the unauthorized trading transactions of a single mid-level rogue trader, Jérôme Kerviel. In unraveling the fraud, it was discovered that Kerviel used his inside knowledge of the bank's back-room procedures to subvert the bank's control systems for more than a year. Some of his tactics included: stealing computer passwords from colleagues to conduct trades, fabricating emails to confirm fake trades, and misappropriating IT access codes to hide transactions.

This incident is a wake-up call for organizations to reevaluate their access security controls. Maintaining strong access security controls helps prevent both unauthorized and excessive access to the data from those seeking to compromise data integrity or perform unauthorized transactions. But, as the Société Générale case suggests, securing data involves more than preventing people *outside* the company from accessing data. It must also ensure that its people on the *inside* perform only the activities necessary to discharge their job responsibilities.

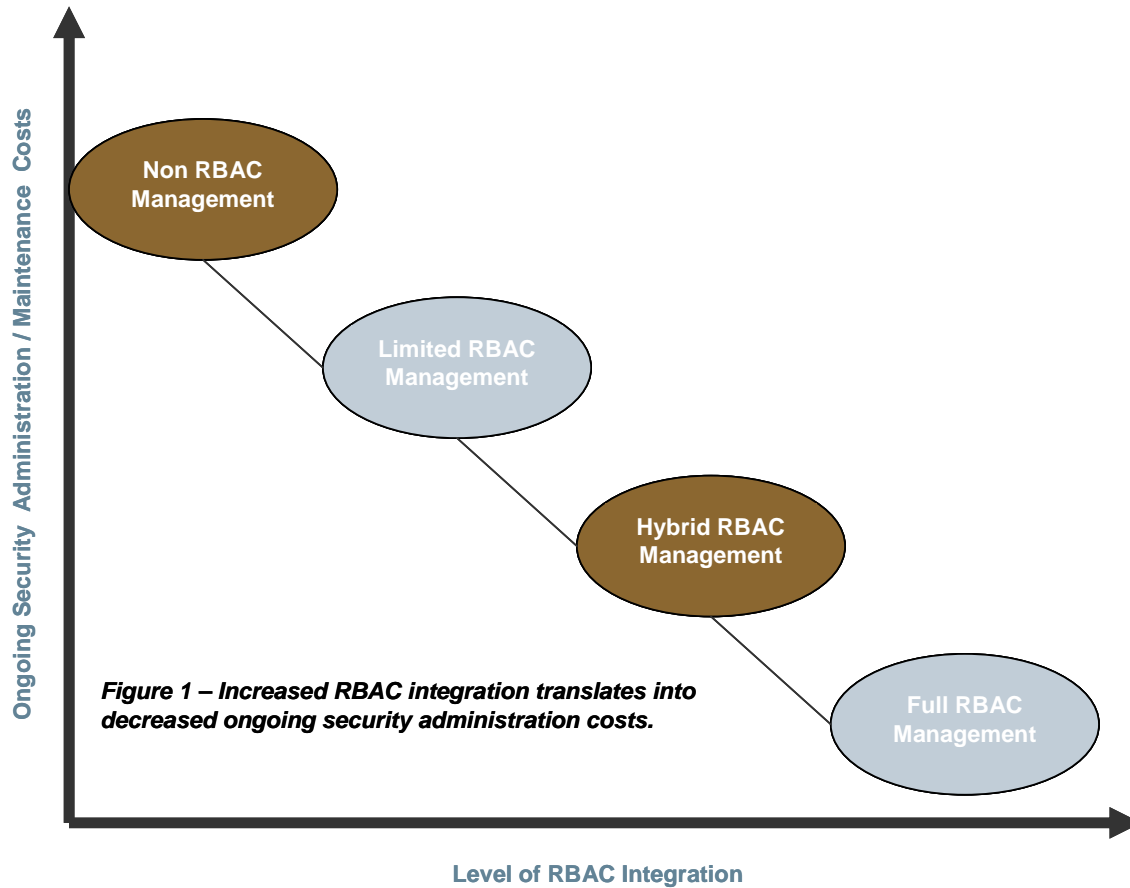
RBAC: A Stronger Model for Access Security

Today's best security practices for managing access to computer systems suggests that companies adopt a role-based access control (RBAC) model. Instead of determining exactly which rights are needed by each and every individual, and adjusting those rights as circumstances and job responsibilities change, privilege and access levels are assigned to specifically named roles, for example accounts payable clerk. Those roles are then assigned to users based on their job responsibility and the organizational model of the company.

The RBAC operational model is especially critical in complex system environments, where an increase in the number and types of users and business applications also increases the risk of unauthorized access and breaches in the segregation of duties. A common error made in granting access rights occurs in organizations that employ an ERP solution (such as SAP or Oracle) for their general ledger, but complement it with a financial consolidation solution (such as OutlookSoft or Hyperion) for financial reporting. While authorization and data access structures within the ERP application may ensure proper restrictions, users can still freely access equivalent data in the consolidation application, thereby circumventing the intended security restrictions. Under an RBAC system, enterprise roles determine access rights rather than users, thus preventing unintended conflicts, while standardizing user access across the organization.

One advantage to implementing an RBAC model is the removal of continuous manual intervention when granting access rights. In many organizations, authorized system administrators in the IT department are responsible for access rights pertaining to business users. Therefore, there are risks when such employees are responsible for interpreting business user requests for increased rights or changes in system rights. Under an RBAC system, specific rules about segregation of duties and limited access to sensitive functions can be defined and regimented in such a way that provisioning procedures* and/or automated governance risk and compliance (GRC) and identity management tools can be used with little human intervention to determine, authorize, assign, change or remove a user's system rights.

Figure 1 illustrates the benefits of RBAC in organizations as they move through four stages of evolution in their applications, users, and access rights.



Three RBAC Models

Given that companies differ in their size and needs, RBAC can be implemented under three models, as follows:

- *Limited RBAC Management* – Users are mapped to roles, although in most cases, users are mapped to specific applications and associated rights when the application does not use the role concept of grouping system rights.
- *Hybrid RBAC Management* – Users are mapped to an enterprise role that applies to most applications, but for specialized systems, users may be mapped directly to the application on a limited basis. For example, an enterprise role is mapped to Applications 1-Oracle and 2-Hyperion, but Application 3-Invoice is mapped directly to the user.
- *Full RBAC Management* – Users are mapped to enterprise role(s) for all applications.

Steps to Implementing an RBAC Model

Although RBAC implementations should be formulated according to the needs of each organization, Protiviti has established a standard four-phase methodology that can be used as a guideline, as shown in the table below.

Project Phases	I. Plan →	II. Design →	III. Build →	IV. Deploy →
Key Activities	Determine engagement plan Develop project roles and responsibilities Develop project strategy Develop an Enterprise Risk Framework for Security Collect data	Perform “as-is” role assessment (including a user and system universe analysis) Map “as-is” roles to “to-be” roles Design enterprise roles Translate roles into technical system specifications	Build enterprise roles and technical system access rights Integrate enterprise roles into user administration procedures Develop testing plan and perform functional as well as compliance (for example, segregation of duties testing)	Assign users to enterprise roles and related system access rights in system production environments Integrate RBAC into documentation (operational, change control, and configuration, help desk procedures and system documentation) Design and construct end user training materials

The Key: Planning and Design

The planning and design phases are perhaps the most critical in the RBAC implementation process, in which roles are researched, defined and determined. The planning phase requires extensive data collection and analysis, including the following:

- HR listing of organizational positions and employee job functions
- All relevant HR and security policies and procedures
- List of all systems in scope
- System access listings by user, job title/department and function
- Security administration account maintenance procedures

Planning can often be completed in four to six weeks. However, in many companies, the information needed may not be available, given that many organizations do not have a centralized, comprehensive listing of all applications and their administrators, or they may have outdated listings. Therefore, budgeting extra time may need to accommodate building this knowledge. Identifying *all* systems is especially critical at this stage. As alluded to before, systems may include ERPs, consolidation tools, worksheets, spreadsheets, user-database programs, active directory/shared drives and Web-based programs. Additionally, the planning

phase must take into account issues such as: naming conventions for each role; authorization to request and approve roles; and monitoring the roles.

The design phase can take from three to six months to ensure the proper design of each role. For example, enterprise roles must be implemented such that no role is translated into a system with excessive rights. Because individuals are normally assigned multiple enterprise roles, the sum total of rights across an individual's roles must also be evaluated to ensure proper segregation of duties.

When similar or conflicting rights exist, it is important to resolve all incompatibilities. In some cases, enterprise roles or user system rights must be reengineered to achieve a more effective and efficient security administration. Many companies find that reengineering user access provides a better return on investment than trying to fix user rights that currently exist within a system.

Unfortunately, the complexity of many applications, especially ERP systems, has often exceeded the ability of IT to implement appropriately robust segregation of duties controls. While most of today's systems support RBAC, they vary in their granularity. Few, if any, provide proactive modeling of segregation of duties violations before assigned or rights are implemented. For this reason, many organizations also turn to add-on software products that provide automated assistance with role analysis, definition, testing and provisioning and holistic identity management. However, it is critical to keep in mind that RBAC implementations require the development of access rights within systems but do not contain excessive sensitive access or segregation of duty exposures.

A Sound Basis

Implementing RBAC provides a sound basis for efficiently managing user security across systems. It provides employees with common and standard enterprise-wide roles to access systems. Moreover, in companies where employees may hold several positions during their career within an organization such as Jerome Kerviel within Société Générale, RBAC provides management and system administrators transparency into an employee's job function through his or her rights within IT systems. This can help reduce the risk of fraud and ensure that the organization's personnel perform only the activities necessary to fulfill their job responsibilities.

Understanding the risks associated with user access is the first step in recognizing the need for an RBAC solution. The next step is identifying and developing a structured plan for the organization to leverage when building a scalable security solution. The design of this solution must be all-inclusive to the applications, technology and solutions already utilized by the organization. The development and deployment of a successful RBAC solution is dependent upon an organization's ability to appropriately define, scope, and communicate the solution across the enterprise. Ultimately, the most successful RBAC solutions are the ones embraced throughout an organization.

This article serves as a companion document to the Protiviti publication “Guide to the Sarbanes-Oxley Act: Managing Application Risks and Controls.”

** See Protiviti’s KnowledgeLeader article “Segregation of Duties Establishing a policy and framework for ongoing success.”*

About the authors

Cary Haggard, MBA, CPA is a director in Enterprise Applications Solutions at Protiviti and may be reached at cary.haggard@protiviti.com.

Brian Smith, CISA, is a director of compliance at Black & Decker. He may be reached at brian.smith2@bdk.com.

Article from Protiviti KnowledgeLeader – www.knowledgeleader.com.

KnowledgeLeader is a subscription-based website that provides audit programs, checklists, tools, resources and best practices to help internal auditors and risk management professionals save time, manage risk, and add value. Free 30-day trials available.

Protiviti (www.protiviti.com) is a global consulting and internal audit firm composed of experts specializing in risk and advisory services. The firm helps clients solve problems in finance, operations, technology, litigation and GRC. Protiviti’s highly trained, results-oriented professionals serve clients in the Americas, Asia-Pacific, Europe and the Middle East and provide a unique perspective on a wide range of critical business issues.

Protiviti has more than 60 locations worldwide and is a wholly owned subsidiary of Robert Half International Inc. (NYSE symbol: RHI). Founded in 1948, Robert Half International is a member of the S&P 500 index.

Protiviti is not licensed or registered as a public accounting firm and does not issue opinions on financial statements or offer attestation services.

© 2008 Protiviti Inc. An Equal Opportunity Employer