When is Role-Based Risk Control the Best Security Strategy?

by Thomas Tsan, President, TK Consultants, Inc.

ABSTRACT: Simplify user provisioning by using a role-based risk control strategy and a four-tier architecture model that weighs the importance of different kinds of roles.

KEY CONCEPT: A **role-based access control (RBAC) strategy** operates under the assumption that you should only grant necessary authorization to users for functions that they need to perform for their job. Most companies use the RBAC strategy to architect their SAP access for users. A **role-based risk control (RBRC) strategy** adds the element of risk evaluation, which not only grants access according to jobs, but also allows non-sensitive authorization to be granted generously among a variety of users. RBRC is a design paradigm shift that encourages business owners to share non-sensitive and semi-sensitive access to reduce administration cost while controlling sensitive and segregation of duties access for compliance.

ARTICLE BODY:

Many companies use a role-based access control (RBAC) strategy, and different methods within that strategy, to handle their SAP security. You can avoid the risks of both strategies by using a role-based risk control (RBRC) strategy that allows non-sensitive authorizations to be spread widely among users while maintaining access limits to sensitive data and processes. The RBRC strategy is a combination of sorts of the RBAC strategy and mandatory access control (MAC) principle, which allows you to design flexible and powerful access for end users.

I'll show you the key elements of an RBRC strategy. I'll also discuss a four-tier architecture that lays out different levels of users and what levels of authorizations they can expect. I'll start with an explanation of the RBAC strategy and the methods within it, and then I'll go into the RBRC discussion.

RBAC Strategy

The basic premise of the RBAC strategy is granting only the necessary authorization for a user to perform his or her job. There are several RBAC methods commonly used by security architects to design job roles. One of the most widely used RBAC methods is to define roles by grouping transactions or tasks that are part of a business process or job function. For example, the payment processing business process might contain the following transactions or tasks:

- Post incoming payment
- Payment request
- Void issued check

After all the business process roles (BPRs) are defined, you can assign authorization to users in two ways. One option is to group BPR single roles into composite job roles. For example, the payment processor composite job role might contain the following BPR single roles:

- Invoice processing
- Invoice approval
- Payment processing

Another common authorization assignment option is to assign one or more BPRs directly to the users based on the job functions within an organization. The BPR strategy gives the role owner the flexibility to assign, remove, or control critical access. However, without a clearly defined maintenance strategy, many organizations deviate from the intents of the BPR strategy. One of the major risks of the BPR strategy is that role modification causes a ripple effect to many users with many different jobs. Another risk is that supervisors might resort to user modeling and rubber stamp approvals because the job roles are not clearly defined or there are too many role combinations to review. Because the modeled user might have assumed additional responsibilities, the new user inherits unintended sensitive or segregation of duties (SoD) access. Over time, the user master becomes convoluted and difficult to maintain and review.

The second common RBAC method is defining a job role based on the organization's jobs. A payment processor job role should contain all necessary transactions and authorizations. The benefit of using the job role strategy is that the roles are clearly defined. As a result, a supervisor might be less inclined to resort to user modeling and rubber stamp approval. Finally, there is no ripple effect because role modification only affects the intended group of users with the same job.

The downside of the job role method is that a user might be given the entire job role even though he or she only needs a few transactions or reports. This inflexibility increases sensitive and SoD risks.

Although both methods have benefits and risks, one common issue is that users tend to request access to non-sensitive display and reporting. As users assume greater responsibilities, the high maintenance costs also increase.

RBRC Strategy and Four-Tier Risk Architecture

The principle of the RBRC method states that authorization to perform sensitive activities and SoD are always transparent and controlled while non-sensitive activities, such as display and reporting, are granted generously to all users.

Based on the RBRC principle, you can follow a four-tier risk architecture method to improve controls and Sarbanes-Oxley compliance (**Figure 1**). Because risk plays an important role in the four-tier model, the pyramid shown in **Figure 1** illustrates where a particular authorization resides. The foundation of the pyramid has the least risks while the top of the pyramid assumes the greatest risks.

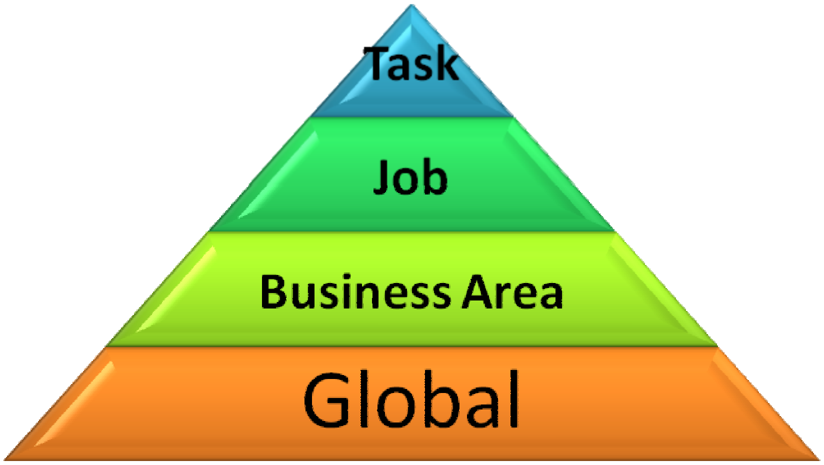


Figure 1 Four-tier risk architecture

As shown in **Figure 2**, the global role represented in tier 1 is the authorization foundation that empowers all employees with only non-sensitive displays and reports across all business units. Regardless of industries, not all data is sensitive. If requirements restrict the display access to non-sensitive data due to regulation with various countries, then it can be accomplished by restricting access to organization data.

Basically, it expands on the the traditional concept of the global role, which is often reserved for basic system activities such as printing, but not business activities. The global role encourages each business unit owner to share all non-sensitive data by creating and owning a display role per business area. After you define the finance, purchasing, and plant maintenance global roles, you can group them into a composite role called global display and reports (**Figure 3**). This global composite role is assigned to every employee that has an SAP User ID.

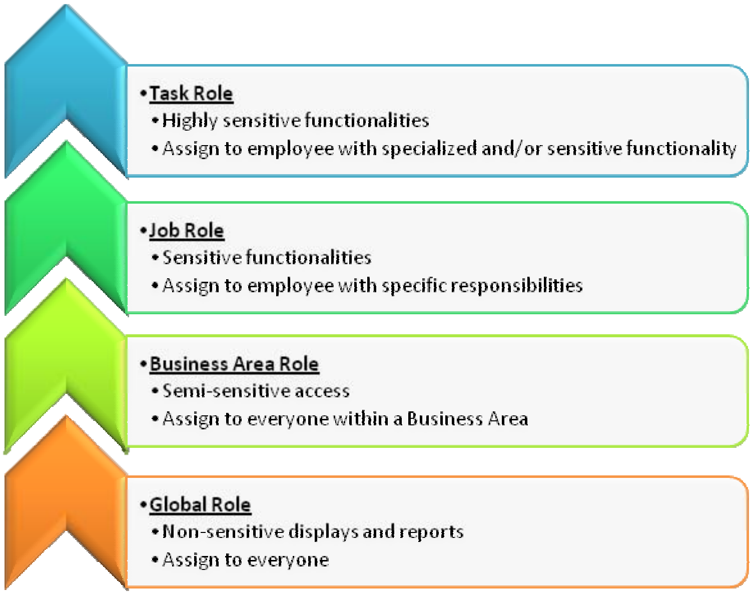

•Task Role
•Highly sensitive functionalities
•Assign to employee with specialized and/or sensitive functionality
•Job Role
•Sensitive functionalities
•Assign to employee with specific responsibilities
•Business Area Role
•Semi-sensitive access
•Assign to everyone within a Business Area
•Global Role
•Non-sensitive displays and reports
•Assign to everyone

Figure 2 Roles in each tier

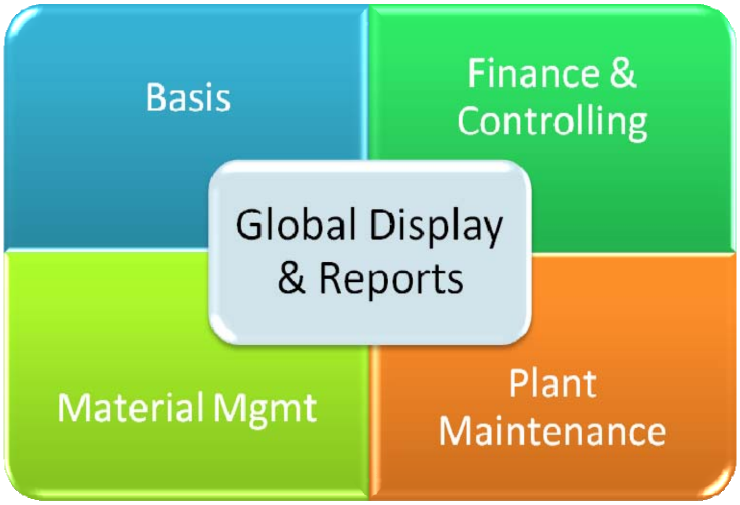
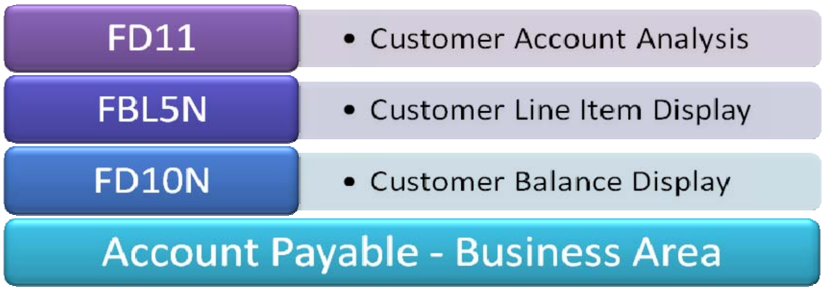


Figure 3 Group roles in a global composite role

The business area role in tier 2 contains semi-sensitive displays and maintenance activities (**Figure 4**). This role is normally shared by everyone within their respective business unit such as finance or purchasing. Similarly to the global role, the business area role empowers users with more non-sensitive or semi-sensitive access. This results in fewer authorization requests and operation maintenance cost. Note that sensitive and SoD access are not allowed within the business area role.



FD11	• Customer Account Analysis
FBL5N	• Customer Line Item Display
FD10N	• Customer Balance Display

Account Payable - Business Area

Figure 4 Contents of the business area role

You should allocate all sensitive access according to jobs using a tier-3 job role such as a PO invoice analyst (**Figure 5**). Regardless of the size of an organization, there are a finite number of jobs to be performed by one or more employees. By allocating all necessary authorization to a job role, SoD is also taken into account. If a job violates SoD and you cannot remediate it due to business requirements, you need to define strong mitigation control to mitigate fraud. For example, the jobs update pay and approve pay changes are SoD threats because an individual might fraudulently change pay without any oversight. However, if an organization is small and you must grant a supervisor access to both, you need to define the mitigation control as, “Before each payroll run, the HR manager must review the pay change report and compare it to a manual pay change approved document to ensure that all pay changes are valid.” In addition, clearly defined jobs and authorizations help an organization to standardize processes, improve efficiency, and minimize maintenance cost.

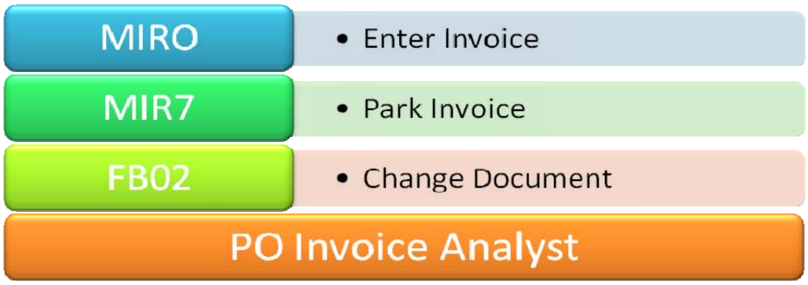


Figure 5 Contents of the job role

Finally, any highly sensitive access such as maintaining vendor master data should be tightly controlled using a tier 4 task role (**Figure 6**). You can selectively assign or remove this access from a user based on his or her job requirement. For example, imagine that you have two people performing the same job, such as accountant, but accountant 1 is granted additional access to maintain vendor master data. Without using the task role, you need to create two accounting roles:

- Accountant job role 1 with vendor master data
- Accountant job role 2 without vendor master data

If you grant additional access to both accountants, you need to double the maintenance efforts by adding the additional authorization to both accountant job roles 1 and 2.

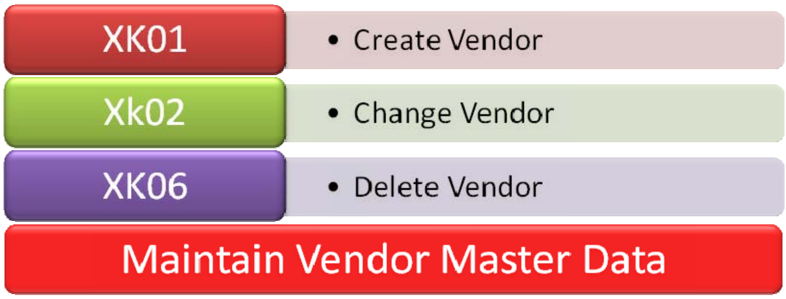


Figure 6 Contents of a task role

The four-tier risk-based approach allows the business to view authorization access in favor of sharing rather than the restrictive view of access-based controls. Because risk is an important element of the four-tier equation, each company and its business owners must clearly identify all sensitive data to be protected and define business actions that create risk. The best approach to evaluate risk is to use the sensitive and SoD matrix that has been defined as an industry best practice, or by the business owner. As a rule of thumb, if the authorization does not create significant risk, role owners are encouraged to share the access. In most companies, the majority of the requests are related to non-sensitive or semi-sensitive display and reporting. If the business shares this access then it minimizes the number of requests and thus reduces maintenance cost. Finally, because the four-tier approach also takes SoD into account, you can easily mitigate or remediate job roles without affecting a large population.

As noted in **Figure 7**, the lower the risk, the more access given to everyone. As the risk increases, the authorizations are granted according to one’s responsibilities.

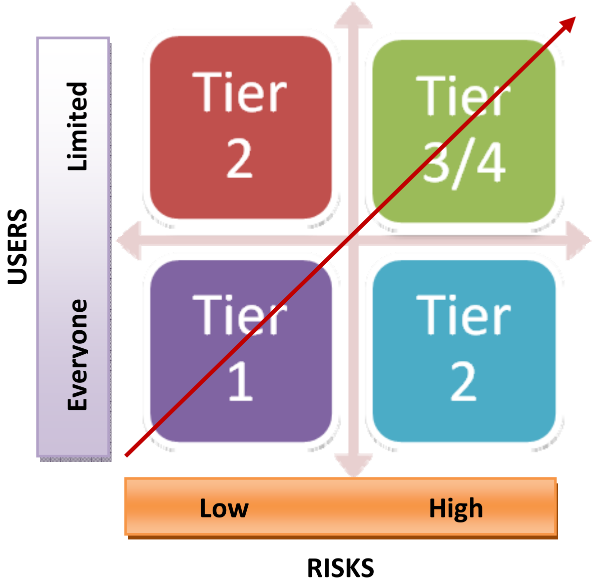


Figure 7 Risk assessments of the four tiers

--

Thomas Tsan, President of TK Consultants, Inc., has more than 12 years of SAP security experience, involving all phases of SAP ERP implementations, upgrades, and redesigns. He has assisted more than 20 companies, ranging from small to Fortune 500 companies in various industries, in securing and streamlining their SAP security processes and manage risk for Sarbanes-Oxley Compliance. In 2005, Marathon named TK Consultants Supplier Diversity Vendor of the Year. You may contact Thomas via email at ttsan@tkconsultants.com or 281-412-6800.