

Flexible Design for Authorizations

Sheila McNeil
Security Team Lead, SAP Project
University of Tennessee

Abstract

The University of Tennessee has implemented the SAP R/3 system to manage financial and human resource processes. SAP R/3 replaces the University's legacy systems, most of which were built in-house. While these systems served the University well for many years, they relied largely on paper-based documents with centralized entry and processing. With the implementation of R/3, the University distributed the entry and processing of information to the academic and administrative departments in order to increase efficiency and decrease paper flow. The decentralization resulted in approximately 2000 users in both end-user departments and central offices, who needed to access the system in diverse ways. The University's implementation of SAP R/3 was set up to provide appropriate authorizations in a flexible manner using standard SAP-delivered security tools, while minimizing the staff needed to maintain the authorizations scheme. While the techniques described within this document are specific to SAP, a similar design could be applied to any system that offers similar tools or to custom applications that are built to use a similar strategy.

Introduction to The University of Tennessee

President: Joseph E. Johnson

Executive Vice President: Emerson H. Fly

Vice President for Administration and Finance: Sylvia S. Davis

Vice President and Treasurer: Charles M. Peccolo

Associate Treasurer: Neal Wormsley

The University of Tennessee (UT) is a statewide higher education system that includes the campuses in Knoxville, Chattanooga, Martin, the Health Science Center at Memphis, a research campus in Tullahoma, and the institutes of agriculture and public service, which serve every county in Tennessee. The University of Tennessee is the state's flagship and land-grant institution. The University is the oldest and largest public higher education institution in Tennessee, tracing its beginnings to the founding of Blount College in Knoxville in 1794 - two years before Tennessee became a state.

The statewide university system has about 42,000 students and approximately 25,000 employees. By 2010, the institution's goal is to be recognized as a premier, internationally recognized flagship university system. New performance goals for the system include a renewed vision, increased research productivity linked to economic development, a heightened emphasis on accountability and private support, a strengthened commitment to equity and diversity, and enhanced relations with faculty, staff, students, alumni, government officials, and others. Each entity has established new

standards of accountability exemplified by public scorecards that show progress toward important quality indicators.

The university system is governed by a board of trustees appointed by the governor of Tennessee. A UT student and faculty member serve one-year terms on the board. The positions rotate annually among the institutions within the UT system. Ex-officio members of the board, in addition to the governor, are the commissioners of education and agriculture, the executive director of the Tennessee Higher Education Commission, and the president of the university.

Source: The Tennessee Blue Book published by the office of the Tennessee Secretary of State <http://www.state.tn.us/sos/bluebook/online/bbonline.htm>

Statement of the problem/initiative

The University of Tennessee implemented SAP R/3 in April 2001 to manage both the human resource and financial processes for the University. In order to increase efficiency and reduce paper flow, the implementation plan called for many processes that had previously been held centrally to be distributed to the academic and administrative departments. The key to distributing processes to the departments lay in the authorizations and security structure, which would be necessary to provide central offices and academic departments only those components of the system necessary for their individual jobs and to support the workflow system which would route documents through the University to obtain required approvals.

Before implementing SAP R/3, the University's centralized processes were managed by separate legacy systems. Because these systems had been developed in-house at the University, the security scheme was customized to UT's organizational structure and the design was simple. The security modules/systems were designed and programmed by the University's technical staff, but the security data was entered and managed within functional offices. Because the authorizations responsibility was spread out among different offices and employees, authorizations support was a "hidden" cost to the University.

When the SAP R/3 implementation began, the University developed an SAP project team, pulling individuals from the financial and human resource offices. The traditional technical roles of systems administration and programming support remained in the information technology division of the University. It soon became clear that the authorizations were much more complex than in the legacy systems, and needed to be an integral part of the configuration. The question remained as to who should be responsible for authorizations and user administration - the SAP project team or information technology?

Once the responsibility for SAP authorizations were assigned, these persons would need to become familiar with a different concept of implementing authorizations and propose a design that would enable the University to manage the authorization component. Since this had been a hidden cost in the legacy system, the design needed to be flexible to

address the needs of the University but able to be addressed efficiently, with limited staffing.

Design

While the details of the design put forth below are specific to an SAP system, the techniques could be employed in many different types of administrative systems.

The key to laying a successful framework for the authorizations system lay in the structure of the support organization. In many organizations, the implementation of R/3 authorizations are treated as a technical issue only and handled by the systems administrators. Although the actual maintenance of the authorizations is a technical component, the University recognized that to be effective, the authorizations should be driven by the business processes. To effectively provide technical skills with business analysis, the University chose to have a separate team for R/3 security/authorizations team that was assigned to the project team rather than the information technology organization, where the system administration function was assigned. The project director then chose to staff the security team with persons who had both technical backgrounds and a broad understanding of business processes at the University.

Once the team was in place, the next challenge was to design and implement the underlying authorizations component of the SAP R/3 system. R/3 is designed to provide role-based authorizations. This means that different functionality can be built into one package, called a role, which can be assigned to multiple users. This technique is effective in that any change, such as authorizations for new functionality, can be added to

the role and will then be inherited to all holders of the role. This is much more efficient than assigning new functionality to all users individually. UT embraced this concept with a goal of maximizing flexibility while minimizing system maintenance requirements. The solution was to build a modular approach with the ability to combine security components to support the required functionality.

The direction of the project's steering committee, comprised of high-level administrators, was also a key enabler to the streamlined authorizations scheme. The steering committee had determined at the offset of the project that each R/3 function should be designed as one process to be implemented at all units. The authorizations plan followed this same strategy. The authorizations were designed to apply to all campuses instead of having a different design for each campus.

Implementation

The security team took the concept of role-based authorizations and applied it to the University's processes by examining the functionality required at various levels of the University and relating the transactions that support the functionality. Financial and Human Resources team members who were familiar with the business processes determined the business requirements for authorizations.

Based on the feedback from the functional teams, the security team then created small units or "building blocks" of authorizations that could mix and match to provide the needed authorization. These building blocks were combined through the SAP technique

of “composite roles” to bundle the individual roles into one unit that was assigned to a particular type of employee.

For example, there is a simple role (EVERY_USER) that has general authorizations and is literally assigned to every user of the system, one role for basic financial authorization (FI_BASIC), one role for basic human resources authorization (HR_BASIC), as well as individual components for the departmental entry staff for accounts payable (DEPT_AP), general ledger (DEPT_GL), human resources (DEPT_HR), purchasing (DEPT_MM), etc. All of these individual roles would be combined into a composite role for a departmental entry person (DEPT_CMP). DEPT_CMP is the only assignment that needs to be made to the departmental end user to receive all of this functionality.

Authorizations for other areas of the University were also provided by composites that combined these existing roles with other specialist roles. Someone in the accounts payable office would have an A/P composite role (AP_CMP) that contains FI_BASIC, DEPT_AP, and additional functionality needed for the accounts payable office (AP_SPEC), but does not include DEPT_GL, DEPT_HR, or DEPT_MM. Again, the only assignment made to the A/P staff member would be AP_CMP. Similar processes would result in composite roles containing different roles/building blocks to provide an appropriate level of access to the payroll office, accounting office, etc.

This strategy resulted in an efficient manner of rolling out new functionality. If a new report were to be designed that was appropriate for all financial users, the report would be added to FI_BASIC, and by that one assignment, it would become available to the departmental users (DEPT_CMP), the A/P office (AP_CMP), and other financial roles, but would not be available to the human resource users. A function that is specific for accounts payable processes might be added to DEPT_AP and become available to both the departments (DEPT_CMP) and the A/P office (AP_CMP), but not be available to the accounting office or the payroll office.

The decision to separate the functional authorizations (what people do) from the data-level roles (those areas of the organization for which they perform their jobs) also affected the overall efficiency of the authorizations design. This was important at UT because of the multiple campuses and units which make up the University of Tennessee. Based on the business decision of adopting common procedures at all campuses, the roles were built so that a departmental entry person would have the same functionality at each of the units. This was true for the central offices as well; campus business offices, campus payroll offices, etc. would have the same functionality, regardless of campus. However, users would need to have access to different sections (departments, campuses, etc.) of the organization.

To accommodate the differences in the data but streamline the maintenance of the operational assignments, three types of roles were developed: functional/transactional roles, campus data roles, and departmental data roles. Functional/transactional roles are

the types of roles that were described above and are packaged into composite roles. They define the processes performed and include roles such as departmental specialist (DEPT_CMP), campus payroll specialist (PAYROLL_CMP), campus business office (CBO_CMP). Campus data roles define campus-specific authorizations, such as campus code and purchasing office. There would be a multiple campus data roles for each functional role with a naming convention such as xx_DEPT_DATA or, xx_PAYROLL_DATA, where the “xx” indicates the campus (CH for Chattanooga, MA for Martin, etc.). Departmental roles indicate the specific department code to be assigned for the departmental users.

Using the design outlined above, departmental users in Memphis and Knoxville would both be assigned DEPT_CMP, which would allow the users to perform functions such as enter timesheets, enter requisitions, pay invoices, etc. The Memphis user would be assigned ME_DEPT_DATA and the appropriate departmental role to limit his actions to only his department in Memphis. The Knoxville user would be assigned DEPT_CMP, KN_DEPT_DATA, and the specific Knoxville department code. But, if new functionality had to be provided to the departments, a change within the DEPT_CMP role would provide the new transaction to all departmental specialists at all campuses (around 1300 users). Likewise, campus payroll office personnel at Chattanooga and Martin would all be assigned the PAYROLL_CMP role, but would be limited to access only their campus personnel by the data-level role assigned, CH_PAYROLL_DATA or MA_PAYROLL_DATA.

Benefits

The beneficiaries of this streamlined approach to authorizations are the end-users of the R/3 system, the project team, and the University as a whole. Being able to make an assignment to a minimal number of roles and provide access to hundreds of people makes it easier and faster to roll out new functionality, results in fewer authorization deficiencies for the end users, and minimizes the amount of authorization testing that must be performed by the project team. Also, once the authorization structure was in place, it has been able to be maintained with minimal staff. The R/3 security staff has averaged 2.5 persons over the implementation and life of the project to support authorizations and user maintenance.

Retrospect

SAP R/3 has been implemented for 2 ½ years at the University of Tennessee, and the authorization concept has worked well. Shortly after go-live, there were some additional roles that needed to be defined in a short timeframe, as the functionality of the system was more far-reaching than the project team originally recognized. Some of these needs would have been more evident with more research and outreach on the part of the project team. However, as with many projects, resources and deadlines determine the initial scope of the implementation. The initial goal and scope of the University's R/3 implementation was to support the departmental offices that would be doing bulk of the entry for the first time and the central offices that had previously been responsible for entry and were now responsible for monitoring and quality control, as well as final processing. In addition, additional functional roles have been developed as new

processes have been defined or as other specialized units (parking services, development office, etc) have requested specialized access to the system. With the modular approach to authorizations, these needs were addressed in a timely manner.