

## ROLE BASED ACCESS CONTROL & RACF

**PURPOSE:** The purpose of this document is to describe Role Based Access Control (RBAC) and discuss its implementation in a RACF protected mainframe system.

**INTRODUCTION TO RBAC:** In its earliest origins, the administration of computer security was based on the principle of "least necessary privilege" such that each user was only to be given as much access authority as he or she individually required. This mode of administration required manually tailoring access permissions for each user and proved to be very time consuming and prone to error. It was especially cumbersome and complex in large organizations with many thousands of users.

The concept of Role Based Access Control, or "RBAC" as it is now known, emerged in 1992 as a way to improve the efficiency and accuracy of security administration. To quote directly from the National Institute of Standards and Technology: "With RBAC, security is managed at a level that corresponds closely to the organization's structure. Each user is assigned one or more roles, and each role is assigned one or more privileges that are permitted to users in that role. Security administration with RBAC consists of determining the operations that must be executed by persons in particular jobs, and assigning employees to the proper roles." (See <http://csrc.nist.gov/rbac/> for more information.)

In truth, RBAC concepts were employed by many information security practitioners prior to 1992. Their efforts simply lacked this formal label. Nonetheless, RBAC has become the predominant model for administering access controls today.

**RBAC AND RACF:** RBAC can easily be implemented in RACF through the use of RACF groups. In its simplest form, a RACF group is just a collection of users with similar access needs. In essence, a group is a role. RACF groups offer considerable flexibility in designing an RBAC structure and can be created to correspond to organizational components, organizational positions, job functions, and even specific tasks.

RACF also provides a mechanism for combining multiple CICS, IMS, and DB2 resources into grouping profiles to governing their access collectively. This feature can be used to organize transactions and resources into inter-related sets corresponding to particular tasks or roles. RBAC group design and resource grouping profile design often go hand in hand.

Implementing RBAC effectively in a RACF system requires careful thought and planning to prevent the creation of a complex, confusing mess of groups whose purpose can be difficult to decipher and administer. Characteristics of a well-designed and executed RBAC implementation include:

- A strict naming convention and hierarchical structure is defined clearly delineating RBAC groups from groups used for other purposes (e.g., resource owning and administrative structure).
- Each group can be traced to a role, and ideally, each role should be comprised of a relatively small number of groups and perhaps just one group.
- Different types of users - e.g., batch processes, system started tasks, and end users - are segregated into their own separate sets of groups. Each of them typically has very different access needs that ordinarily should not be granted to and shared via a common group.
- End users are predominantly granted access through groups and not through access granted to their individual IDs.
- An interface between the Human Resources (HR) system and RACF is established such that user and access administration are at least partially automated. This greatly improves administrative efficiency and accuracy.
- Non-employee users (vendors, consultants, temps, auditors, etc.) are identified using groups denoting their status and the department they serve.

Along with improving administrative effectiveness, a well-designed and implemented RBAC structure often boosts RACF processing performance by reducing the number of groups a user is connected to and the number of entries in access lists.

**RBAC ASSISTANCE:** For assistance with designing and implementing RBAC-based access in your RACF protected environment, contact RSH Consulting, Inc. at [info@rshconsulting.com](mailto:info@rshconsulting.com) or at 617-969-9050.