RACF - Audit and Compliance Roadmap

Course Description

This course is designed for IT auditors and compliance monitors seeking to identify security vulnerabilities in RACF-protected z/OS mainframe systems and bring the systems into compliance with government and industry mandated security requirements. Much more than just a simple "how to audit" class, this course will show you how to pinpoint and address serious security exposures of the kinds commonly found during RSH's RACF audits. By the end of class, you will have gained a solid understanding of RACF, familiarity with RSH's "best practices" for RACF implementation, and a comprehensive knowledge of the tools and techniques for evaluating the status of RACF protection. Better still, we will review RACF reports from your own system during class and immediately identify control concerns. You are likely to compile a lengthy list of findings just by attending this class.

Duration

3 Days -or- 5 Half-Day WebEx Sessions

Who Should Attend

- **IT Auditors** seeking to perform more effective audits
- **Compliance Monitors** who want to ensure the security staff or outsource service providers have properly implemented RACF

What You Will Learn

- RACF's components, profiles, and functions
- RACF SETROPTS configuration options
- RACF commands for gathering information
- Restricting use of powerful authorities like OPERATIONS
- RACF's access authorization logic
- Identifying and protecting for system dataset
- Assignment of IDs and privileges for Started Tasks
- Ensuring comprehensive event logging and reporting
- RACF administrative authorities
- Interpretation of RACF DSMON reports

Prerequisites

Familiarity with z/OS mainframes, RACF, and using TSO

Instructor - Robert S. Hansel

Mr. Hansel has worked with RACF since 1986 as an administrator, auditor, consultant, and trainer. He is a prominent speaker on RACF audit and technical topics at conferences and user groups throughout the U.S. He has audited over one hundred RACF implementations.

Course Outline

1. RACF Concepts
   a. Introduction to RACF
   b. RACF functions
   c. Profiles and relationships
   d. SETROPTS and DSMON Overview
2. Users
   a. Identification and authentication process
   b. IBMUSER control
   c. Password change and composition controls
   d. Password encryption options
   e. User profile contents and segments
   f. Started Task, Batch, and System/Process IDs
   g. RACF commands and reports for users
3. Groups
   a. Concepts and functional roles
   b. Group hierarchy
   c. Group profile contents and segments
   d. RACF commands and reports for groups
4. Resource Protection
   a. Resource profiles - discrete, generic, grouping
   b. Access permissions and default access
   c. OPERATIONS and privileged access authorities
   d. RESTRICTED users
   e. Access authorization process and logic
5. Datasets
   a. Dataset protection basics
   b. Dataset profile contents
   c. Tape dataset protection
   d. Catalog and system dataset protection
   e. PROTECTALL
   f. z/OS Program Properties Table (PPT)
   g. RACF commands and reports for datasets
6. General Resources
   a. Resource protection basics
   b. Profile classes and resource names
   c. General Resource profile contents
   d. Critical General Resources
   e. RACF commands and reports for resources
7. Logging and Reporting
   a. System Management Facilities (SMF)
   b. SETROPTS and profile monitoring options
   c. Reporting tools
8. Administrative Authorities
   a. System and Group level SPECIAL and AUDITOR
   b. Group connect authorities
   c. Password Reset and segment change authority
9. RACF Configuration
   a. Database backup and maintenance
   b. RACF exits and tables
   c. RACF management practices
10. RACF Audit Plan, Process, and Tools

To register for public courses or find out more about how RSH Consulting can help you better secure your system, call us at 617-969-9050, email us at info@rshconsulting.com, or visit our web site at www.rshconsulting.com.