RSH CONSULTING

RACF - Level III Administration, Audit, and Compliance

Course Description

This course is designed for seasoned RACF administrators, technicians, auditors, and compliance monitors seeking to improve RACF protections for critical system resources. This technically-rich course will show attendees how to implement, remediate, and review complex controls for CICS transactions and resources, TSO authorities, data storage management functions, programs, and VTAM application entry. Attendees will learn the details and interrelationships of controls for system operator commands, JES2 functions, and SDSF authorities. Tips and "best practices" will be presented in each topic. As in all RSH training, attendees will examine reports from their own system to understand how their RACF is uniquely configured and identify opportunities for improvement.

Duration

5 Half-Day Online Sessions (20 hours)

Who Should Attend

- **RACF Administrators and Technicians** looking to enhance RACF protections for system resource
- **IT Auditors and Compliance Monitors** seeking to perform more technically detailed control reviews

What You Will Learn

- Essential program protection
- CICS SIT parameters governing all security options
- Controlling CICS internal IDs using SURROGAT profiles
- Comparing installation-defined CICS classes to prefixing
- Protecting critical system operator commands
- Controlling batch job execution and output
- Inbound and outbound NJE transmission controls
- Protecting SDSF functions using RACF
- SDSF Destination Operator authority and control
- Data storage administration without OPERATIONS
- Controlling sensitive TSO authorities

Prerequisites

Completion of either RSH's RACF Level II Administration or RSH's RACF Audit and Compliance Roadmap plus one year of RACF administration or auditing experience.

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 Overview and Refresher
   a. Access authorization process and logic
   b. General resource protection
   c. Grouping profiles and RACLIST merge process
2. Program Protection
   a. PROGRAM class profiles
   b. Maintaining a 'clean' program environment
   c. Definitions required for z/OS Unix
   d. Program conditional access permissions
   e. Enhanced program protection
3. CICS
   a. Systems Initialization Table (SIT) parameters
   b. XUSER parameter and SURROGAT profiles
   c. CICS Default User
   d. Resource classes and SECPRFX profile prefixing
   e. XTRAN classes and transaction security
   f. X-parameters and resource protection
   g. XCMD classes and SPI command security
   h. Transaction and function routing
   i. Bind, link, and attach security
4. Operator Command Controls
   a. PARMLIB console configuration
   b. Console and OPERPARM authorities
   c. CONSOLE class profiles
   d. Console logon for emergency RACF fixes
   e. OPERCMDS class profiles
   f. Privileged operator commands and controls
5. Job Entry Subsystem 2 (JES2) Controls
   a. Submitter, job, and resource tokens
   b. Batch ID assignment and controls
   c. SURROGAT and PROPCNTL profiles
   d. JESINPUT job entry controls
   e. JESJOBS job name and job modify controls
   f. JESSPOOL output access controls
   g. WRITER print and routing controls
   h. NJE NODES profiles and RACFVARS &RACLNDE
6. System Display and Search Facility (SDSF) Controls
   a. ISFPARMS
   b. SDSF and GSDSF class profiles
   c. Use of WHEN(CONSOLE(SDSF)) permissions
   d. Destination operator authority and controls
7. Data Storage Administration Controls
   a. OPERATIONS authority
   b. DASDVOL profiles
   c. FACILITY STGADMIN profiles
   d. ISMF program protection
   e. DFSMS/hsm control considerations
8. TSO Configuration and Controls
   a. PARMLIB IKJTSOxx parameters
   b. TSOAUTH authorities and related commands
9. APPL and VTAMAPPL protection

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