# IBM: Implementing RACF Security for CICS/ESA and CICS/TS (ES84G)

Course ID #: 0375-301-00-W
Hours: 36

## Course Content

### Course Description:

This course teaches you how to implement security for your CICS systems using RACF as the external security manager. The lecture material will first explain the implementation tasks for a single-region CICS system and then extend the scope to MRO- or ISC-connected multiregion CICS systems. In the classroom you will learn both the CICS and RACF definitions necessary to establish effective security controls for CICS. You will learn how to: Protect CICS system resources so that CICS itself has access but other users, such as TSO users or batch jobs, are denied access. Define CICS terminal users to RACF and restrict the CICS regions to which these users will be allowed to sign on. Control access to individual CICS transactions. Control access to CICS application resources accessed by these transactions. Control execution of CICS system programmer interface (SPI) commands used within transactions. Control access to installation-defined resources used to support application-specific security requirements. Control access to CICS transactions and resources when two or more CICS address spaces are connected to enable use of the CICS transaction routing and function-shipping mechanisms. You will learn about the wide variety of mechanisms that can be used to initiate transactions within CICS and the techniques for imposing security controls on each of these mechanisms. These mechanisms include the connections to CICS using Advanced Program-to-Program Communication (APPC) either from CICS client or server products on other platforms or from other products that support APPC. You will also explore the security interface between CICS, RACF, and DB2 and learn how RACF can be used to secure CICSplex System Manager, one of the elements provided with CICS Transaction Server for z/OS.

### Course Objectives:

Identify the tasks that must be done in RACF and CICS to implement security Develop a step-by-step plan to implement RACF security on your CICS systems Implement RACF-based security for CICS systems in single-system and CICS intercommunication (MRO and ISC) environments Make the definitions in RACF and CICS to protect transactions, CICS resources, and SPI commands Protect CICS system resources so that CICS itself has access but others, such as TSO users or batch jobs, are denied access Define CICS terminal users to RACF and restrict the CICS regions to which these users are allowed to sign on Control access to individual CICS transactions, CICS application resources accessed by these transactions, CICS SPI commands used within transactions, and installation-defined resources used to support application-specific security requirements Use RACF to secure access to CICS from other platforms through Advanced Program-to-Program Communication (APPC) connections Identify the key areas to secure for CICSPlex System Manager

### Target Audience:

This course is for security personnel and CICS support personnel responsible for designing, implementing, or administering RACF security for CICS Transaction Server systems.

# IBM: Implementing RACF Security for CICS/ESA and CICS/TS (ES84G)

Course ID #: 0375-301-00-W

Hours: 36

## Prerequisites:

You should be familiar either with: RACF (perhaps as a security administrator) or with CICS (perhaps as a member of your CICS technical support staff). It is not assumed or necessary that you already be familiar with both RACF and CICS.

## Topics:

### Day 1

- Welcome, course introduction, and administration
- Unit 1 – CICS overview
- Exercise 1 – CICS familiarization
- Unit 2 – RACF overview
- Exercise 2 – RACF familiarization

### Day 2

- Unit 2 lab review
- Unit 3 – Protecting the CICS region
- Exercise 3 – Protecting the CICS region
- Unit 4 – Sign-on security
- Exercise 4 – Sign-on security

### Day 3

- Unit 5 – Transaction security
- Exercise 5 – Transaction security
- Unit 6 – CICS resource and SPI command security
- Exercise 6 – CICS resource security and SPI command security

### Day 4

- Unit 7 – CICS intercommunication bind and link security
- Unit 8 – CICS intercommunication conversation security

### Day 5

- Lab Review
- Unit 9 – Securing CICSPlex SM
- Unit 10 – Planning for implementation
- Unit 11 – CICS and DB2 security
- Unit 12 – CICS Web Services security