SC28-1342-1
File No. S370-40

Program Product

Resource Access Control Facility (RACF) Auditor's Guide

Program Number 5740-XXH
Version 1, Release 6

Second Edition (May 1984)

This is a major revision of, and obsoletes, SC28-1342-0. See the Summary of Amendments following the Contents for a summary of the changes made to this manual.

This edition applies to Version 1 Release 6 with the data security monitor of the program product RACF (Resource Access Control Facility - Program Number 5740-XXH), and to all subsequent releases and modifications until otherwise indicated in new editions or Technical Newsletters. Changes are made periodically to the information herein; before using this publication in connection with the operation of IBM systems, consult the latest *IBM System/370 Bibliography*, GC20-0001, for the editions that are applicable and current.

References in this publication to IBM products, programs, or services do not imply that IBM intends to make these available in all countries in which IBM operates. Any reference to an IBM program product in this publication is not intended to state or imply that only IBM's program product may be used. Any functionally equivalent program may be used instead.

Publications are not stocked at the address given below. Requests for IBM publications should be made to your IBM representative or to the IBM branch office serving your locality.

A form for readers' comments is provided at the back of this publication. If the form has been removed, comments may be addressed to IBM Corporation, Information Development, Department D58, Building 920-2, PO Box 390, Poughkeepsie, N.Y., 12602. IBM may use or distribute whatever information you supply in any way it believes appropriate without incurring any obligation to you.

Preface

This book contains information for Version 1 Release 6, with the data security monitor, of the Resource Access Control Facility program product, RACF (Program Number 5740-XXH). The book is intended for those individuals defined as RACF auditors (persons who have the AUDITOR or group-AUDITOR user attribute). This book explains the RACF auditing facilities and includes detailed information about using the RACF report writer and the data security monitor. The reader of this book should be familiar with both RACF and MVS.

This book has three chapters:

- Chapter 1. The RACF Auditor -- describes the role of the RACF auditor and explains how to use the auditing tools that RACF provides. These tools include logging, audit controls that affect the information that RACF logs, and the RACF report writer, which generates reports on the information that RACF logs. Chapter 1 also includes a section on asking the right questions, designed to make the auditor aware of the potential scope of auditing the security of an MVS/RACF installation.

- Chapter 2. The RACF Report Writer -- describes the RACF report writer, a function of RACF that lists RACF SMF records and produces reports on system and resource use from information found in RACF SMF records. This chapter includes samples of all the reports the RACF report writer can produce. Chapter 2 is not tailored specifically to the auditor; it addresses the needs of any user of the RACF report writer.

- Chapter 3. The Data Security Monitor (DSMON) -- describes the data security monitor, a batch program that generates reports that provide the auditor with information about the basic system security environment of an installation. This chapter includes samples of the reports that the data security monitor produces.

Other books containing information about RACF that might be useful to the auditor are:

- *RACF General Information Manual*, GC28-0722, which presents introductory and overview information about RACF

- *RACF Command Language Reference*, GC28-0733, which describes the commands and ISPF panels you use to communicate with RACF

- *System Programming Library: RACF*, SC28-1343, which contains detailed information about optional changes or additions that might be required to audit your installation

- *RACF Security Administrator's Guide*, SC28-1340, which explains RACF concepts and the user attributes

For information about SMF (system management facilities), see one of the following publications:

- In MVS/370 environments, see *OS/VS2 System Programming Library: System Management Facilities (SMF)*, GC28-1030.

- In MVS/XA environments, see *MVS/Extended Architecture System Programming Library: System Management Facilities (SMF)*, GC28-1153.

For overview information about the MVS products and features that are available to support the implementation of a security program, see *MVS Security*, GC28-1400.

Contents

Figures

Summary of Amendments

Summary of Amendments
for SC28-1342-1
RACF Version 1, Release 6 with DSMON

Additions and changes have been made throughout this publication to describe the data security monitor (DSMON). Chapter 3, "The Data Security Monitor (DSMON)," contains most of the new information.

In addition, minor technical and editorial changes have been made.

Chapter 1. The RACF Auditor

RACF is a flexible security tool; it allows an installation to set its own security objectives and use RACF to help achieve those objectives in a way that best meets the installation's needs.

While installations might have slightly different security needs, there are certain RACF user roles or tasks that are common to all. And, at any installation, different users have different levels of responsibility for security or different needs to access resources. Some people might have extensive responsibility for security, while others might have little or none; some users might require almost unlimited access to resources, while others might need only limited access, and some might be barred from entering the system at all.

The primary means of defining a user's responsibility for security is the RACF *user attribute*. A user attribute is, simply, a part of the RACF definition of what an installation allows a particular user to do. The SPECIAL attribute, for example, is normally assigned to the RACF security administrator; a SPECIAL user can execute any RACF command except those reserved for a user with the AUDITOR attribute.

This separation of powers is necessary because it is the security administrator's job to establish RACF controls; it is the auditor's job to test the adequacy and effectiveness of these controls. In this sense, your job as the auditor is very similar to the job of a financial auditor in a bank. Other people do the work; the auditor checks the work.

Once a SPECIAL user assigns the AUDITOR user attribute to you, your responsibility is to verify that RACF is meeting your installation's security goals. As a RACF auditor, your job is essentially the same, regardless of whether you have the AUDITOR attribute (with responsibility for checking RACF controls on a user, or system-wide, level) or the group-AUDITOR attribute (with responsibility for checking RACF controls for a group and its subgroups). While a user with the group-AUDITOR attribute can only monitor the users and resources owned by a specific group and its subgroups, the responsibility is so much like that of a user with the AUDITOR attribute that this book applies to both and notes any specific differences.

As the auditor, you are responsible for checking that the use of RACF at an installation is meeting that installation's needs for access control and accountability. Access control means that you can trace, or audit, user accesses to resources and verify that the accesses allowed are appropriate to the particular resource. For example, you might question why a tape librarian had access to a payroll data set. Accountability means that you can trace activities of users on the protected system to a particular person. Normally, several people should not share a userid. When userids are shared, the installation should enforce additional security measures.

The auditor needs to verify that an installation has a way to maintain this accountability.

To help you to audit access control and accountability, RACF provides:

- Logging routines that record the information you require
- Audit control functions that enable you to specify the information RACF is to record (or log)
- The RACF report writer, which generates user-tailored reports based on the information you have directed RACF to log
- The data security monitor, which generates reports containing information about the security environment at an installation

To specify the audit control functions, you use either the RACF ISPF panels or the RACF commands to direct RACF to log any events that might be inconsistent with your installation's data security program. You invoke the RACF report writer to print out the data RACF has logged, then use the reports to identify possible security violations or weaknesses in the security mechanism.

Note: To use the ISPF panels, your system must include the Interactive System Productivity Facility (ISPF), Program Number 5668-960, and TSO/E Release 2, Program Number 5665-285.

A user with the AUDITOR attribute can run the data security monitor (DSMON) program to generate a set of reports. You can use the reports to audit the current status of your installation's data security environment by comparing the actual system characteristics and resource protection levels with the installation's requirements.

Logging

Logging -- the recording of data about specific events -- is the key to auditing the use of RACF at your installation. You must ensure that RACF logs the information you need. RACF uses the system management facilities (SMF) to log data about various RACF events in RACF SMF records.

RACF **always** logs information about certain events because knowing about these events is essential to an effective data security mechanism. The events that RACF always logs are:

- Every use of the RVARY or SETROPTS command
- Every time the RACINIT SVC, which identifies and verifies users, fails to verify a user because the user supplied an invalid group, password, or OIDCARD, or tried to use an unauthorized terminal
- Every time the console operator grants access to a resource as part of the failsoft processing performed when RACF is inactive

RACF **never** logs some events, however, because knowing about these events is not essential to effective data security. The events RACF never logs are any use of the following RACF commands: LISTDSD, LISTGRP, LISTUSER, RLIST, and SEARCH.

In addition to the events that RACF always logs and never logs, there are other events that RACF can **optionally** log, under the control of either a resource owner or the auditor.

Owner-Controlled Logging

Owners of resources can specify, in the resource profile, what types of accesses to log (success and/or failure) and what level of access to log (read, update, control, or alter). Owners can also specify that no logging is to occur for an access that is a success and/or failure. Owner-controlled logging is not directly under your control, but you should verify that resource owners request a level of logging that is consistent with the sensitivity of the resource. There are, however, two methods that your installation can use to **override** the logging the owner specifies in the resource profile.

Your installation can override a resource owner's logging specification by using the RACHECK postprocessing exit routine. This exit routine can, for certain accesses, specify unconditional logging or unconditionally suppress logging. For example, you might use the exit routine to specify unconditional logging for accesses to a resource that the routine can identify as so highly classified that logging is always required. Or, you might suppress logging when the exit routine recognizes READ access to common system resources, such as SYS1.MACLIB. You should be aware of any such exit routine specifications. For more information on using exit routines, see *SPL: RACF*.

You can also cause additional logging that supersedes the owner's logging specification for a specific resource by **adding** audit controls to the resource profile. Note that you cannot **change** the owner's logging specifications. Using these controls is described later in this chapter under "Data Set Controls" and "General Resource Controls."

Auditor-Controlled Logging

You, the auditor, can direct RACF to log additional events. These events are:

- All changes to any RACF profiles that are the result of RACF commands or the RACDEF SVC
- All RACF commands that a SPECIAL or group-SPECIAL user issues
- All RACF command violations
- All RACF-related activities of specific users
- All or some of the accesses to specific data sets
- All or some of the accesses to specific general resources

You can identify which of these events apply to your installation's security goals and use audit controls to direct RACF to log the events you require.

Setting Audit Controls

Audit controls are special RACF functions that RACF allows only the auditor to perform. To preserve the checks and balances so necessary to an effective security mechanism, not even the security administrator with the SPECIAL attribute can execute auditor functions. Therefore, you should ensure that SPECIAL users do not also have the AUDITOR attribute.

As the auditor, you execute these functions, either through the RACF ISPF panels or as operands on RACF commands. If you have a choice of using either the panels or the commands, note that using the panels creates an additional summary record in the ISPF log of the work that you do; the RACF commands do not create such a record. Both approaches are described in detail in the *RACF Command Language Reference*.

Whichever method you choose to enter your audit controls -- to specify to RACF what information you want it to log -- the controls themselves are either general or specific. General audit controls apply to the system-wide operation of RACF; specific audit controls apply to a single user or resource.

General Audit Controls

You specify general (system-wide) audit controls on either the SETROPTS command or the "Set Audit Options" ISPF panels. General audit controls direct RACF to log (or not to log) changes to profiles, the activities of SPECIAL or group-SPECIAL users, and command violations.

To specify the general audit controls, you must have the AUDITOR attribute; if you have the group-AUDITOR attribute, you can only issue the REFRESH GENERIC command and list the general controls (you cannot change them). After you have initially established your controls or modified existing controls, it is a good practice to list the current options to verify that the controls are correct.

If you have the AUDITOR attribute, you can specify these SETROPTS operands or request the corresponding function on the RACF "Set Audit Options" ISPF panel:

AUDIT/NOAUDIT
SAUDIT/NOSAUDIT
CMDVIOL/NOCMDVIOL
REFRESH GENERIC
LIST

If you are a group-AUDITOR, you can use only the LIST operand.

Figure 1-1 summarizes the auditor operands on the SETROPTS command. Figure 1-2 shows the RACF panels you would use to perform the same functions. Either method allows you to audit changes to profiles, the activities of SPECIAL or group-SPECIAL users, and command violations.

Note: In all of the panels in this chapter, the panel name is shown as if you had issued the PANELID command.

Operand	Effect
AUDIT	Logs modifications to profiles in the specified class(es)
NOAUDIT	No logging of profile modifications in the specified class(es)
SAUDIT	Logs all commands of SPECIAL and group-SPECIAL users
NOSAUDIT	No logging of SPECIAL and group-SPECIAL user commands
CMDVIOL	Logs all command violations
NOCMDVIOL	No logging of command violations
REFRESH GENERIC	Replaces the in-storage generic profiles with a new copy from the RACF data set
LIST	Lists logging options in effect. No log options changed

Figure 1-1. Summary of SETROPTS Operands for Auditors

```
ICHP52                                RACF - SET AUDIT OPTIONS
COMMAND ===>

TO ACTIVATE OPTIONS, ENTER YES; TO DEACTIVATE OPTIONS, ENTER NO:

    COMMAND VIOLATIONS ===>       Log violations in RACF command usage
    SPECIAL USER       ===>       Log command usage by SPECIAL users
    AUDIT CLASS        ===>       Log profile creation and changes for classes

ENTER CLASSES FOR THE AUDIT CLASS OPTION:

    ===>          ===>          ===>          ===>          ===>
    ===>          ===>          ===>          ===>          ===>
    ===>          ===>          ===>          ===>          ===>
    ===>          ===>          ===>          ===>          ===>
    ===>          ===>          ===>          ===>          ===>
    ===>          ===>          ===>          ===>          ===>
    ===>          ===>          ===>          ===>          ===>
    ===>          ===>          ===>          ===>          ===>
    ===>          ===>          ===>          ===>          ===>
    ===>          ===>          ===>          ===>          ===>
    ===>          ===>          ===>          ===>          ===>
    ===>          ===>          ===>          ===>          ===>
```

Figure 1-2. System-Wide Audit Control Panel

Changes to Profiles

The AUDIT/NOAUDIT operand on the SETROPTS command allows you to specify the extent of the logging RACF is to perform for changes that users, and system routines that issue the RACDEF SVC, make to the RACF profiles:

- If you specify AUDIT with one or more class names, RACF logs all changes to all profiles in the classes that you name. If you specify AUDIT(*), RACF logs all changes to all profiles in all classes.

- If you specify NOAUDIT with one or more class names, RACF does not log any changes to any profiles in the classes that you name. If you specify NOAUDIT(*), RACF does not log any change to any profile in any class.

NOAUDIT(*) is in effect when RACF is first initialized.

SPECIAL User Actions

Specifying the SAUDIT operand directs RACF to log all the RACF commands issued by users with the SPECIAL or group-SPECIAL attribute (except LISTDSD, LISTGRP, LISTUSER, RLIST, and SEARCH). The SAUDIT operand thus gives you the ability to audit the RACF-related activities of the SPECIAL and group-SPECIAL users, who have the ability to change the RACF profiles. You can, once RACF logs their activities, use the RACF report writer to produce a report of these activities.

If you specify NOSAUDIT, then RACF does not log the RACF-related activities of these users. If you are concerned only with how SPECIAL users change profiles, there is no need to specify SAUDIT when AUDIT(*) is in effect.

SAUDIT is in effect when RACF is first initialized.

Command Violations

RACF command processors verify the authority of a user to issue a command before performing the requested action. If a user does not have the required authority, RACF recognizes a command violation and does not perform the requested action.

Specifying CMDVIOL causes RACF to log all the command violations that it detects. You can then use the RACF report writer to produce a printed audit trail of command violations. You can determine how many command violations are occurring and which users are causing the violations. A significant number of command violations, especially when RACF is first installed, might indicate the need for more user education. The report can also help you to identify any specific users who are persistently trying to alter profiles without the proper authority.

If you specify NOCMDVIOL, RACF does not log the command violations that it detects.

CMDVIOL is in effect when RACF is first initialized.

Refreshing of Generic Profiles

REFRESH GENERIC causes all the in-storage generic profiles (except those in the global access checking table) to be replaced with a new copy from the RACF data set. You might want to use REFRESH GENERIC after changing the logging options in a generic profile protecting a specific data set, as described in the next section, "Specific Audit Controls."

Examples

The following examples show how to set system-wide audit controls. The examples use the SETROPTS command; Figure 1-3 shows how to do the same things with the panel.

Example 1: To log any changes to the profiles in the USER, GROUP, DATASET, and DASDVOL classes, enter:

```
SETR AUDIT(USER,GROUP,DATASET,DASDVOL)
SETR LIST
```

or:

```
SETR AUDIT(USER,GROUP,DATASET,DASDVOL) LIST
```

Example 2: To log all commands issued by SPECIAL and group-SPECIAL users, enter:

```
SETR SAUDIT
SETR LIST
```

or:

```
SETR SAUDIT LIST
```

Example 3: To log all command violations that RACF detects, enter:

```
SETR CMDVIOL
SETR LIST
```

or:

```
SETR CMDVIOL LIST
```

Example 4: To refresh the in-storage generic profiles, enter:

```
SETR REFRESH GENERIC(DATASET)
SETR LIST
```

or:

```
SETR REFRESH GENERIC(DATASET) LIST
```

Note: You could combine these four examples into a single SETROPTS command by entering:

```
SETR AUDIT(USER,GROUP,DATASET,DASDVOL) SAUDIT CMDVIOL
REFRESH GENERIC(DATASET) LIST
```

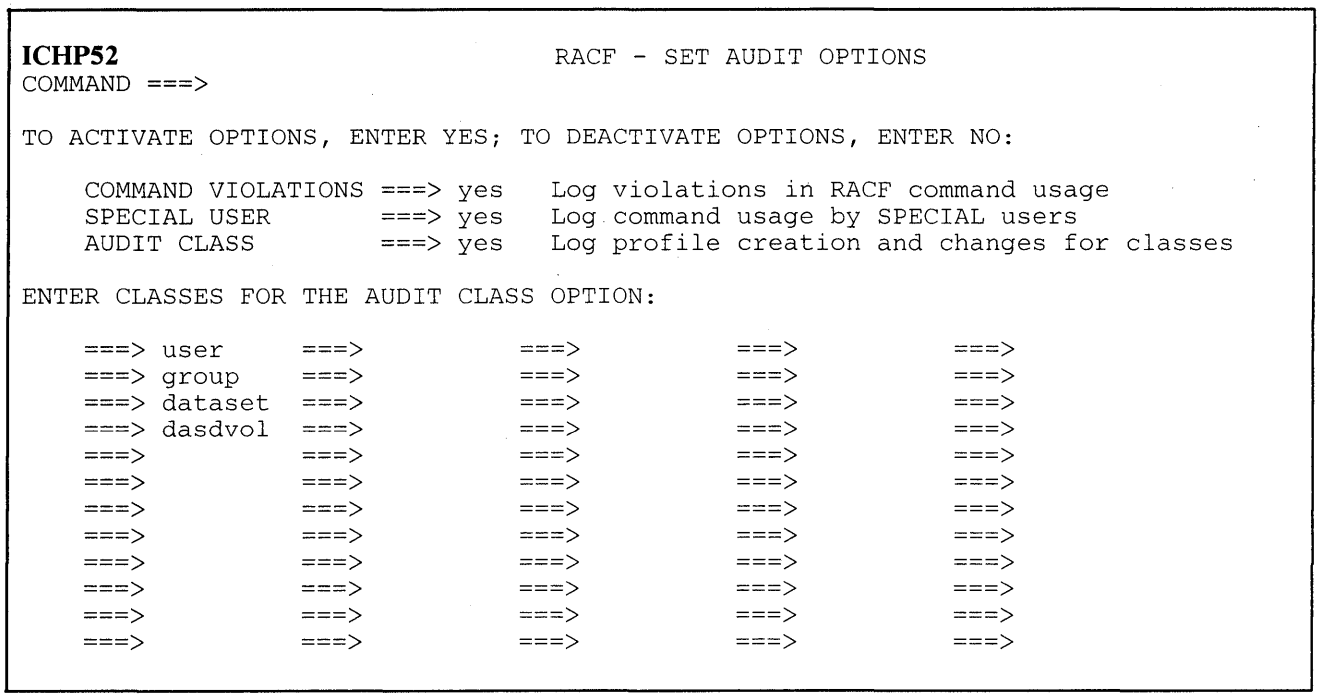


Figure 1-3. Sample Audit Control Panel

Specific Audit Controls

Specific audit controls enable you to log the following:

- All RACF-related activities for specific users
- Attempts to access specific DASD data sets
- Attempts to access specific general resources

You can also list the complete contents of all profiles, including the owner-specified and auditor-specified logging options for resources.

If you have the AUDITOR attribute, you can set specific controls for any user, data set, or general resource, and list the contents of any profile. If you have the group-AUDITOR attribute, you can set controls and list profile contents only for those users, data sets, and general resources owned by the group in which you have the attribute, and any subgroup of that group.

User Controls

You can direct RACF, using either the UAUDIT/NOUAUDIT operand on the ALTUSER command or the "Audit User" panel, to log all RACF-related activities for a specific user. When you set this control, RACF logs the following events:

- All RACF commands that the user issues
- All additions, changes, or deletions that the user makes to the RACF profiles
- All attempts that the user makes, regardless of authorization, to access RACF-protected resources

In general, you would probably not request user audit logging as a matter of course. Rather, it is useful in special situations. For example, you can specify user audit logging in a situation where you suspect, based on other indicators such as command violations, that a particular user might be misusing the system or persistently trying to access or delete resources outside the user's control. Examples of the type of event that might indicate misuse of the system are either unauthorized attempts to access a critical system resource (like SYS1.PARMLIB) or a highly classified user resource (like a payroll or business planning data set) or attempts to perform unauthorized disk pack restore operations.

Example: To use the UAUDIT operand on the ALTUSER command to audit the person whose userid is J08563, enter:

```
ALU J08563 UAUDIT
```

Figure 1-4 shows the sequence of panels you would use to do the same thing.

```
ICHP00                          RACF - SERVICES OPTION MENU
OPTION ===> 4

SELECT ONE OF THE FOLLOWING:

   1 DATA SET              ADD, CHANGE, DELETE, or DISPLAY the profile
                           for a DASD data set.

   2 GENERAL RESOURCE      ADD, CHANGE, DELETE, or DISPLAY the profile
                           for a general resource.

   3 GROUP                 ADD, CHANGE, DELETE, or DISPLAY a group profile.
                           CONNECT or REMOVE users.

   4 USER                  ADD, CHANGE, DELETE, or DISPLAY a user profile.
                           Change a user's password.

   5 SYSTEM OPTIONS        DISPLAY or SET the system wide security options.
                           REFRESH in-storage profile lists.

   T TUTORIAL              View a general description of RACF.
```

```
ICHP40                                RACF - USER SERVICES
OPTION ===> 5

SELECT ONE OF THE FOLLOWING:

   1 ADD          Add a user profile      D DISPLAY     Display profile contents
   2 CHANGE       Change a user profile   S SEARCH      Search RACF data set for
   3 DELETE       Delete a user profile                 profiles
   4 PASSWORD     Change your own password
   5 AUDIT        Monitor users activity
                  (for auditors only)

ENTER USER INFORMATION:

    USER ID   ===> j08563
```

```
ICHP45                          RACF - AUDIT USER - J08563
COMMAND ===>

TO AUDIT USER'S ACTIVITY, ENTER YES:
TO END AUDIT OF USER'S ACTIVITY, ENTER NO:

    AUDIT USER===> yes


Note: Only users with the AUDITOR attribute can use this panel.
```

Figure 1-4. Setting User Audit Control

Data Set Controls

In addition to owner-controlled logging, you can direct RACF, using either the GLOBALAUDIT operand on the ALTDSD command or the "Audit Data Set Access" ISPF panel, to log user accesses to data sets. The GLOBALAUDIT level that you specify can be used when the owner-controlled logging specification does not generate sufficient records for your needs. Thus, RACF provides you, the auditor, with a separate control to specify which types and to what access levels to log, in conjunction with the owner-specified values, at resource access time.

Figure 1-5 shows the various valid combinations of what to log and when to log it.

WHAT TO LOG	WHEN TO LOG
NONE	-
ALL	READ, UPDATE, CONTROL, or ALTER
FAILURES	READ, UPDATE, CONTROL, or ALTER
SUCCESS	READ, UPDATE, CONTROL, or ALTER
FAILURES SUCCESS	READ, UPDATE, CONTROL, or ALTER READ, UPDATE, CONTROL, or ALTER

Figure 1-5. GLOBALAUDIT Settings

As with the other specific controls, you would not audit accesses to most data sets as a general rule. Thus, GLOBALAUDIT(NONE) is the default for the operand. After you have completed your audit of the data set, it is good practice to restore the default. When GLOBALAUDIT(NONE) is in effect, RACF logs accesses to the data set only as specified by the resource owner.

Example 1: To use the GLOBALAUDIT operand of the ALTDSD command to direct RACF to log all accesses to data set BELDING.MEMO.TEXT, enter:

```
ALTDSD 'BELDING.MEMO.TEXT' GLOBALAUDIT( ALL(READ) )
```

Figure 1-6 shows how to use the RACF panel to do the same thing.

```
ICHP15                          RACF - AUDIT DATA SET ACCESS
COMMAND ===>

    PROFILE NAME: 'belding.memo.text'

ENTER DATA SET AUDITING INFORMATION:

    AUDIT SUCCESSES===> read         READ, UPDATE, CONTROL, ALTER, or NOAUDIT
    AUDIT FAILURES ===> read         READ, UPDATE, CONTROL, ALTER, or NOAUDIT

Note: Only users with the AUDITOR attribute can use this panel.
```

Figure 1-6. Data Set Controls -- Example 1

Example 2: To use the GLOBALAUDIT operand of the ALTDSD command to direct RACF to log all failed accesses, all successful updates, and any scratch of data set A.B.C, enter:

```
ALTDSD 'A.B.C' GLOBALAUDIT( FAILURES(READ) SUCCESS(UPDATE) )
```

Figure 1-7 shows how to use the RACF panel to do the same thing.

```
ICHP15                          RACF - AUDIT DATA SET ACCESS
COMMAND ===>

    PROFILE NAME: 'a.b.c'

ENTER DATA SET AUDITING INFORMATION:

    AUDIT SUCCESSES===> update       READ, UPDATE, CONTROL, ALTER, or NOAUDIT
    AUDIT FAILURES ===> read         READ, UPDATE, CONTROL, ALTER, or NOAUDIT

Note: Only users with the AUDITOR attribute can use this panel.
```

Figure 1-7. Data Set Controls -- Example 2

General Resource Controls

You can direct RACF, using either the GLOBALAUDIT operand on the RALTER command or the RACF "Audit General Resources Access" ISPF panel, to log user accesses to a specific general resource. Because the audit level that you specify on GLOBALAUDIT overrides the level the data set owner specified in the profile, you would use it when the logging specified in the profile does not produce enough information for your needs.

When you set audit controls for a general resource, you specify what information RACF is to log -- the result of the access attempt -- and when RACF is to log the information -- the level of access. Figure 1-5 on page 1-11 earlier in this chapter shows the various valid combinations of what to log and when to log it.

As with the other specific controls, you would not audit accesses to most general resources as a general rule. Thus, GLOBALAUDIT(NONE) is the default for the operand. After you have completed your audit of the general resource, it is good practice to restore the default. When GLOBALAUDIT(NONE) is in effect, RACF logs accesses to the resource as specified in the profile.

Example: To use the RALTER command to specify auditing all events for a tape volume NR1234, enter:

```
RALTER TAPEVOL NR1234 GLOBALAUDIT(ALL(READ))
```

Figure 1-8 shows the RACF panels you would use to log accesses to a specific general resource.

```
ICHP20                          RACF - GENERAL RESOURCE SERVICES
OPTION ===> 5

SELECT ONE OF THE FOLLOWING:

   1 ADD        Add a profile            D DISPLAY     Display profile contents
   2 CHANGE     Change a profile         S SEARCH      Search RACF data set for
   3 DELETE     Delete a profile                       profiles
   4 ACCESS     Maintain access list
   5 AUDIT      Monitor access attempts
                (for auditors only)

ENTER RESOURCE PROFILE INFORMATION:

    RESOURCE CLASS ===>tapevol

    RESOURCE NAME  ===>nr1234
```

```
ICHP25                          RACF - AUDIT GENERAL RESOURCE ACCESS
COMMAND ===>

    CLASS: tapevol       PROFILE NAME: nr1234

ENTER RESOURCE AUDITING INFORMATION:

    AUDIT SUCCESSES===> read         READ, UPDATE, CONTROL, ALTER, or NOAUDIT
    AUDIT FAILURES ===> read         READ, UPDATE, CONTROL, ALTER, or NOAUDIT

Note: Only users with the AUDITOR attribute can use this panel.
```

Figure 1-8. Setting General Resource Audit Values

Listing Specific Audit Controls

RACF provides commands, and corresponding ISPF panels, that allow RACF users, depending on their authority or attributes, to examine the contents of RACF profiles. You, as auditor, can list the contents of all the RACF profiles (or all the profiles within the scope of your group if you are a group-AUDITOR). You can find a complete description of each of the commands, including sample output, in the *RACF Command Language Reference*. The commands and the functions related to auditing are:

- LISTDSD: lists the contents of data set profiles. If you have the AUDITOR attribute, you can list all profiles; if you have the group-AUDITOR attribute, you can list only those profiles within the scope of your group and/or its subgroups.

- LISTGRP: lists the contents of group profiles. While the output does not contain any information directly related to specific audit controls, it does include information about the group structure and each user's authority within the group, which might be useful to you. If you have the AUDITOR attribute, you can list all group profiles; if you have the group-AUDITOR attribute, you can list only the profiles within the scope of your group and/or its subgroups.

- LISTUSER: lists the contents of user profiles. If you have the AUDITOR attribute, you can list all user profiles; if you have the group-AUDITOR attribute, you can list only those profiles within the scope of your group and/or its subgroups.

- RLIST: lists the contents of general resource profiles. If you have the AUDITOR attribute, you can list all resource profiles; if you have the group-AUDITOR attribute, you can list only those profiles within the scope of your group and/or its subgroups.

Example: To list the complete profile for data set BELDING.MEMO.TEXT, enter:

```
LISTDSD D('BELDING.MEMO.TEXT') ALL
```

Figure 1-9 shows the RACF panel you would use to list a data set profile.

```
ICHP10                              RACF - DATA SET SERVICES
OPTION ===> D

SELECT ONE OF THE FOLLOWING:

   1 ADD         Add a profile              D DISPLAY     Display profile contents
   2 CHANGE      Change a profile           S SEARCH      Search RACF data set for
   3 DELETE      Delete a profile                         profiles
   4 ACCESS      Maintain access list
   5 AUDIT       Monitor access attempts
                 (for auditors only)

ENTER DATA SET PROFILE INFORMATION:

    PROFILE NAME      ===> 'belding.memo.text'
    GENERIC           ===>          YES If the profile name is generic
    VOLUME SERIAL     ===>          If the data set is not cataloged
    UNIT              ===>          If option 1 and VOLUME SERIAL entered
    DATA SET PASSWORD ===>          If the data set is password protected
```

```
ICHP181                  RACF - DISPLAY DATA SET PROFILE
 COMMAND ===>
    PROFILE NAME: 'BELDING.MEMO.TEXT'

 TO SELECT INFORMATION TO BE DISPLAYED, ENTER YES:

    ACCESS LIST ===> YES       Profile access list
    HISTORY     ===>           Profile history
    STATISTICS  ===>           Profile use statistics

 TO LIMIT THE DISPLAY TO PROFILES FOR DATA SETS ON SPECIFIC VOLUMES,
 ENTER VOLUME SERIAL NUMBER(s):

    ===>        ===>        ===>        ===>        ===>
    ===>        ===>        ===>        ===>        ===>
    ===>        ===>        ===>        ===>        ===>
```

Figure 1-9. Display Data Set Profile

Using the RACF Cross-Reference Utility Program (ICHUT100)

If you have the AUDITOR attribute, you can use the ICHUT100 utility to find and list all occurrences of a userid or group name that are in the RACF data set. If you have the group-AUDITOR attribute, you can use the ICHUT100 utility only for a userid or group that is within your scope of authority. For more information on using the ICHUT100 utility, see *SPL: RACF.*

Using the RACF Report Writer

The profile listings that the RACF commands provide can help you to verify the audit controls that exist at any particular time. The RACF report writer, in contrast, enables you to monitor RACF-related activity during system operation. Using it, you can obtain printed reports based on the data your audit controls directed RACF to log. The audit trails these reports contain enable you to monitor RACF-related activities and verify that these activities are consistent with your installation's security goals.

Chapter 2, "The RACF Report Writer," describes in detail the process of issuing the RACFRW command that invokes the RACF report writer. It also describes the SELECT and EVENT subcommands that define the RACF SMF records that the RACF report writer is to use as input, and the LIST and SUMMARY subcommands that define the output that the RACF report writer is to produce. In addition, Chapter 2 includes samples of the available reports.

In considering your use of the RACF report writer as an auditing tool, it is important to note that you can obtain reports only on data that RACF has logged. For example, you cannot obtain a report on the commands issued by SPECIAL and group-SPECIAL users if you have not directed RACF to log all the commands that those users issue. It is also important to ensure that your installation protects both the SMF data sets and the report writer work data sets (which contain reformatted SMF records) against unauthorized use.

Because of variations from one installation to another, it is not possible to identify all of the ways an auditor might use the RACF report writer. The following list, however, identifies some possibilities:

- Monitoring password violation levels
- Monitoring access attempts in WARNING mode
- Monitoring access violations during normal operation of RACF
- Monitoring the use of RACF commands
- Monitoring the RACF activities of selected users
- Monitoring the RACF activities of SPECIAL and group-SPECIAL users
- Monitoring the RACF activities of OPERATIONS and group-OPERATIONS users

The following detailed descriptions of these tasks include brief examples of the report writer command and subcommands needed for each. If you are unfamiliar with the RACF report writer, see Chapter 2 for complete descriptions of each command and subcommand, as well as for samples of each report.

Monitoring Password Violation Levels

Monitoring password violation levels enables you to:

- See how effectively new RACF users are coping with the LOGON process
- See if the number of password violations stabilizes over time
- See where (at which terminals) these password violations are occurring

To obtain a report that describes password violations, issue the following command and subcommands:

```
RACFRW GENSUM...
 SELECT PROCESS
  EVENT LOGON EVQUAL(1)
 LIST ...
END
```

These subcommands create a general summary report and a listing of the selected process records. (See Figure 2-6 and Figure 2-4 for samples of the general summary report and listings of selected process records. See Chapter 2 for a description of process records.)

The total number of job or logon violations in the general summary report includes all types of violations (invalid password, invalid group, invalid OIDCARD, and invalid terminal). Because the EVENT subcommand causes the RACF report writer to select only those process records that describe an invalid password, you can use the number of process records selected to determine the percentage of password violations. If, for example, the number of process records selected was 13 and the total number of job/logon attempts was 393, you could compute the percentage of password violations by dividing 13 by 393. In this particular example, the value is 3.3%.

The violation percentage is a useful number to record and track over time. As users become more familiar with using their userid and password, this percentage should tend to stabilize at a relatively low level.

You can look at the terminal name in the listing of process records to determine where persistent violations are originating.

Monitoring Access Attempts in WARNING Mode

Your installation might choose to use warning mode during the initial implementation of RACF. During this period, resource profiles contain a warning indicator (specified when the owner creates or later changes the profile). When the warning indicator is set, RACF allows all requestors to access the resource, and, if the requestor would not otherwise be allowed access, RACF sends a message to the requestor. If you specify GLOBALAUDIT ALL(READ) in a profile, RACF then logs each access to the resource, and you can use the RACF report writer to provide a list of the accesses RACF allowed only because the warning indicator was set.

Using the warning indicator can help your installation to migrate gradually to RACF. Checking the requestors and resources in the report writer listing can enable you to develop access lists without disrupting authorized work and without the immediate need to write and test a RACF exit routine.

As the auditor, however, you must be aware that using the warning indicator in a resource profile means that any requestor can access the resource. You should verify that the profile for a highly classified resource (such as a payroll or business planning data set) does not contain the warning indicator.

To obtain a report of accesses granted only because the warning indicator was set, issue the following command and subcommands:

```
RACFRW ...
 LIST ...
  SELECT PROCESS WARNINGS
END
```

These subcommands produce a listing of the selected process records. The records selected are those that contain an event code of 2 and a qualifier of 3.

Monitoring Access Violations

Both when warning mode is in effect and during normal operation of RACF, it is essential to your job as an auditor that you be able to monitor access violations. RACF detects and logs an access violation when it denies a user access to a resource because that user is not authorized to access the resource. An access violation is thus a symptom that someone either does not understand his or her role as a RACF user or is trying to bypass RACF protection. You can use a report of access violations to identify such users as well as to help your installation identify when it might need to change access lists and/or universal access codes (UACCs).

You can request the report for data set violations as well as for violations in any of the classes identified in the class descriptor table.

To obtain an access violation report, issue the following command and subcommands:

```
RACFRW ...
 LIST ...
  SELECT PROCESS
   EVENT ACCESS EVQUAL(1) CLASS(DATASET,TAPEVOL,DASDVOL,user-defined)
   EVENT LOGON  EVQUAL(4)
END
```

The subcommands create a listing of all process records that meet the criteria set in the EVENT subcommands. The EVENT ACCESS subcommand selects all access violation process records for the specified classes. The EVENT LOGON subcommand expands the scope of the report to include all user attempts to log on from a terminal the user is not authorized to use.

Monitoring the Use of RACF Commands

In any installation, the security administrator is probably the most frequent user of RACF commands. Occasionally, users without any privileged attributes will execute ADDSD, PERMIT, or another similar command against one of their own TSO data sets. Some users, however, might try to use the whole range of RACF commands. Unless the user is authorized, RACF does not execute the command. Each unauthorized attempt to use a RACF command, however, represents a potential security violation, an event that you should know about. You monitor the use of commands with the command summary report.

To obtain a command summary report, issue the following command and subcommand:

```
RACFRW ...
 SUMMARY COMMAND BY (USER)
END
```

A sample command by user summary report appears in Figure 2-19.

If you detect certain users making persistent unauthorized use of RACF commands, you can extract the details of the commands used and the resources involved. To obtain details of any command violations logged for specific users, issue the following command and subcommands:

```
RACFRW ...
 SELECT VIOLATIONS USER(violator(s) userid(s) ...)
 LIST ...
END
```

Note that RACF does not automatically log the events that these reports describe. To obtain meaningful data, you must direct RACF to log the activities of specific users and/or command violations. The reports are useful only after RACF has logged the events for the time interval that is meaningful to you. See "Monitoring Specific Users" and "Monitoring SPECIAL Users" later in this chapter for related information.

Monitoring Specific Users

If you have directed RACF, either through the UAUDIT operand on the ALTUSER command or the corresponding ISPF panel, to log the RACF-related activities of one or more specific users, you can use the report writer to obtain a listing of the activities of these users.

To obtain a listing of all records RACF has logged because you requested auditing of one or more specific users, issue the following command and subcommands:

```
RACFRW ...
  SELECT PROCESS REASON(USER) ...
  LIST ...
END
```

Monitoring SPECIAL Users

If you have directed RACF, either through the SAUDIT operand on the SETROPTS command or the corresponding ISPF panel, to log the RACF-related activities of SPECIAL or group-SPECIAL users, you can use the report writer to obtain a listing of the activities of these users.

To obtain a listing of all records RACF has logged because you requested auditing of SPECIAL or group-SPECIAL users, issue the following command and subcommands:

```
RACFRW ...
  LIST ...
   SELECT PROCESS REASON(SPECIAL)
   SELECT PROCESS AUTHORITY(SPECIAL)
END
```

Note the difference between REASON and AUTHORITY:

REASON shows why the SMF record was logged. REASON(SPECIAL) causes the report writer to select records logged because the SETROPTS SAUDIT operand was in effect.

AUTHORITY shows why RACF accepted a command as valid. AUTHORITY(SPECIAL) causes the report writer to select records logged because the command required the SPECIAL or group-SPECIAL attribute and the user had the required attribute.

Monitoring OPERATIONS Users

The OPERATIONS and group-OPERATIONS attributes are very powerful. OPERATIONS allows a user to access almost all resources. Group-OPERATIONS allows a user to access almost all resources within the scope of the group and its subgroups. (The only resources not accessible to the OPERATIONS or group-OPERATIONS user are those that have been explicitly barred by placing the OPERATIONS user in the access list of a resource with an access level of NONE at either the userid level or default group level.) Thus, you should carefully monitor the activities of these users, to ensure that all accesses to installation resources were for valid reasons.

To obtain a report of the activities of OPERATIONS and group-OPERATIONS users, issue the following command and subcommand:

```
RACFRW ...
  LIST ...
   SELECT PROCESS AUTHORITY(OPERATIONS)
END
```

Note: RACF automatically logs the activities of users with the OPERATIONS and group-OPERATIONS attributes.

Asking the Right Questions

Asking the right questions is an essential part of any audit, particularly an audit or review of your own MVS/RACF installation or a peer review of another installation. In such a review or audit, your principal review objectives are:

1. To judge the effectiveness of the RACF implementation from a security viewpoint
2. To identify any security exposures
3. To recommend ways to improve the system

To accomplish these objectives, you need to quickly understand the significant features of the installation under review. It is generally useful to interview as few people as possible and to include a senior member of the system support group in the people you interview. If you ask the right questions of the right people, you will often find that the person you are talking with can both supply the information you need and identify any security exposures.

One way to deal with the mass of information available or required for an audit is to divide it into categories: preliminary information, MVS information, and RACF information. The balance of this chapter uses these categories as a structure for identifying blocks of information you need or questions you might ask. You will probably find that not all of the suggestions apply at any one installation, and that a particular installation requires additional investigation. Thus, it is a good idea to treat these suggestions as a starting point, then tailor and expand your audit to fit the conditions that exist.

When you are conducting an audit, you should have current installation reports from the data security monitor (DSMON). These reports are helpful in answering a number of your questions. You can also use the DSMON reports to verify that the **actual** status of various security mechanisms is what you and the installation expect.

Preliminary Information

An * before a question indicates you can answer all or part of the question by using the DSMON reports.

1. * List the processor complexes and their associated system control programs (SCPs), as well as the release and level of RACF for each.

2. For each processor complex, list the subsystems, such as TSO, IMS, CICS and any other subsystems protected by RACF (including the release and level of each).

3. Are processor complexes linked (for example, by NJE, JES2, or JES3)?

4. Is DASD shared between systems? What type of data is shared?

5. Do you have dial-up lines?

6. Explain briefly the classification system.

7. What is the highest classification of data processed and/or transmitted?

MVS Implementation/Integrity

An operating system should have integrity; that is, it should prevent one program from interfering with or modifying the execution of another system or user program unless the interference is authorized. To increase your awareness of potential security problems, see *MVS Security*, GC28-1400. It provides overview information about the MVS products and features that promote security.

Basic MVS System

An * before a question indicates you can answer all or part of the question by using the DSMON reports.

1. * What is the MVS version and release level and PTF level (PUT tape)?
2. How many local modifications have been applied (excluding exit routines)?
3. What are the main areas and/or functions modified?
4. What user SVCs does the system include and what is their purpose?
5. What exit routines are in the system and what is their purpose? Could these exit routines affect RACF protection? (Do not list RACF exit routines here.) Some examples of subsystems or components that can have exit routines are:

   SMF
   TSO
   JES
   Job management

6. Are the MVS systems the same on all processor complexes?

MVS Authorization

An * before a question indicates you can answer all or part of the question by using the DSMON reports.

1. * What are the entries in the program properties table (PPT) that automatically bypass password protection?
2. What are the authorized libraries?

   * In SYS1.PARMLIB (IEAAPFxx)?
   * In SYS1.PARMLIB (LNKLSTxx)?
   In SYS1.PARMLIB (IEALPAxx)?

3. What programs that require authorization, other than standard IBM programs, are in these libraries?
4. What are the commands and programs that can be executed APF-authorized in the foreground (CSECTs IKJEFTE2 and IKJEFTE8 in module IKJEFT03)?
5. * Is the list of authorized programs and commands reasonable and consistent with the installation's security goals?
6. How are changes and additions to the authorized libraries controlled? Who authorizes changes?

MVS System Protection

An * before a question indicates you can answer all or part of the question by using the DSMON reports.

1. How are changes to the MVS system controlled and documented?
2. How are the system libraries (including page data sets, dump data sets, JES spool and checkpoint data sets, and SMP data sets) protected? Who can access these libraries?
3. * What libraries have a universal access of READ?
4. * What libraries have a universal access of UPDATE or higher?
5. Are the DLIB data sets also protected?
6. * Are all the catalogs (VSAM and CVOL) protected?
7. * Are key security items, (such as RACF data sets, SYS1.UADS, password data set, cipher key file, SMF data sets, source and load modules for RACF exit routines, and SMF routines) all identified and protected?
8. If JES3 is installed, is use of DSP controlled (including utilities such as tape to tape and tape to print)?

Miscellaneous

An * before a question indicates you can answer all or part of the question by using the DSMON reports.

1. Can bypass label processing (BLP) be used? If yes, how is it controlled?
2. Is OS password protection used? If yes, why?
3. If dial up terminals are used, how is unauthorized use prevented?
4. Is full SMF recording in use? If not, what is excluded either by options or exit routine code?
5. What is the wait limit that causes a terminal to be logged off?
6. How far back do system backup dumps go?
7. Are all IPLs logged and the reasons reported?
8. Is all time on the system accounted for?
9. * Is it possible to detect if the system has been loaded without RACF?
10. How is the use of TSO commands (such as RVARY) controlled?

RACF Implementation

Installing RACF does not necessarily mean that the RACF security facilities were correctly implemented and are being correctly maintained. (For more information about implementing RACF, see the *RACF Security Administrator's Guide.*)

Protection Plan

An * before a question indicates you can answer all or part of the question by using the DSMON reports.

1. * How many RACF users and groups do you have?
2. Do you have any non-RACF users? If so, why?
3. Which of the following resources are RACF-protected, what proportion of each is protected, and how is it decided which to protect?

   DASD data sets
   Tapes
   Terminals
   IMS
   CICS
   Key resources unique to the installation

4. How does the installation ensure that appropriate protection is maintained? Does it, for example, use ADSP, end user decision, or installation procedures?
5. What protection is available for resources NOT protected by RACF?
6. Is the protection policy reasonable?

Usage

An * before a question indicates you can answer all or part of the question by using the DSMON reports.

1. * Which userids (including started tasks) have any of the following privileged attributes or authorities? Why?

   SPECIAL and group-SPECIAL
   OPERATIONS and group-OPERATIONS
   AUDITOR and group-AUDITOR
   CLAUTH
   JOIN
   CONNECT
   GRPACC

2. How is the granting of these privileges controlled?
3. Is DASDVOL authorization used instead of the OPERATIONS user attribute?
4. Are userids shared? If so, why, and how is accountability maintained?

5. Is the default for UACC always NONE? If not, why?

6. How are password qualities complied with? Do you use, for example, password length, nature (alphabetic, alphanumeric, no vowels), repetition, or change frequency?

7. What RACF information, such as the following, is logged to SMF?

   Command violations
   Changes to profiles
   Accesses to specific resources
   Actions of SPECIAL and group-SPECIAL users
   Actions of OPERATIONS and group-OPERATIONS users

8. Who decides what resource access information is to be collected? On what criteria?

9. What RACF statistics are collected?

10. What are the access rules when RACF is inactive or unavailable, such as stop production, perform repair work only, or allow selected jobs/applications to run?

11. Is WARNING mode active, entirely or partially? Are there non-WARNING mode resources?

12. Do access lists contain groups rather than individuals?

13. How is the authority to run production work handled? Does the job submitter have access to production data?

14. Do you need to delete tape profiles before using them again? If so, how are the profiles deleted?

15. How is RACF protection handled in disaster recovery plans?

16. Describe any operational/usage problems for which the installation cannot currently determine a solution.

Technical

An * before a question indicates you can answer all or part of the question by using the DSMON reports.

1. * What RACF exit routines are used, and what functions do they perform? The following list identifies the exits.

   ICHDEX01 (password encryption)
   ICHRIX01 (RACINIT pre)
   ICHRIX02 (RACINIT post)
   ICHRCX01 (RACHECK pre)
   ICHRCX02 (RACHECK post)
   ICHRDX01 (RACDEF pre)
   ICHRDX02 (RACDEF post)

ICHCCX00 (command pre)
ICHCNX00 (command pre)
ICHRFX01 (FRACHECK pre)
ICHRFX02 (FRACHECK post)
ICHPWX01 (new password)
ICHRLX01 (RACLIST pre/post)
ICHRLX02 (RACLIST selection)
ICHRSMFE (report writer)

2. How are the exit routine functions and changes authorized and controlled?
3. Who is allowed to update exit routine code (both source and load form)?
4. What SETROPTS options are used? Are any important protection and/or monitoring functions set off?
5. Have basic RACF facilities been enhanced, excluding exit routine code?
6. * How many primary RACF data sets are there?
7. * Does each primary data set have a backup on a different volume?
8. What other backup facilities exist for RACF data sets?
9. How is the RACF data set synchronized after a restore?
10. * Are all RACF data sets adequately protected, and who has access to them?
11. How does the installation control the switching and deactivating of the RACF data sets (RVARY command, IPL/data set name table)?
12. What is in the started task table (ICHRIN03), and is the authority of the associated userids appropriate?
13. Are any special checks required on the use of PERMIT?
14. How are passwords protected against disclosure when batch jobs are submitted through internal readers?
15. How are restores of entire volumes handled? How are synchronization problems between volumes and RACF data sets resolved?

Administration Control

An * before a question indicates you can answer all or part of the question by using the DSMON reports.

1. Who is responsible for the administration of RACF?
2. Who is responsible for the technical aspects of RACF?
3. Are data owners identified?
4. Do data owners classify their data?

5. Is the degree of protection provided by the installation based on the owner classification?

6. Are there written and approved procedures for RACF administration?

7. Does the installation maintain written records of requests for changes to RACF protection and the resulting actions taken?

8. How are users and groups administered? How are additions, deletions, changes, connections, and authorities handled?

9. How is the authority to protect resources and grant access checked and handled?

10. How is the granting of temporary authorities handled? Can users issue PERMIT/CONNECT for temporary access, or are there privileged attributes available for emergency use?

11. How is password distribution handled?

12. How are lost passwords handled?

13. Is additional verification required for users with privileged attributes? Are these users restricted to particular terminals?

14. * Is there an emergency userid with the SPECIAL attribute available for use when no other SPECIAL userid can be used? If so, how does the installation protect the userid and its password?

15. * Is the auditor a different person from the RACF security administrator? What are the responsibilities of the auditor?

16. Is there any user education available?

Management Control

1. What reports are available to users, owners, and installation management to ensure that the system is not being misused? Examples are reports that identify violation attempts, unauthorized access attempts, and unauthorized use of commands and privileges.

2. How frequently are reports produced, and who sees them?

3. If a security violation occurs, what follow-up action does the installation take?

4. Is the installation using DSMON reports to monitor the basic system security environment? If not, why isn't it?

Chapter 2. The RACF Report Writer

A successful security mechanism requires that appropriate personnel, particularly the auditor and the security administrator, can assess the implementation of the security mechanism and the use of the resources it protects. The RACF report writer provides a wide range of reports that enable you to monitor and verify the use of the system and resources.

The RACF report writer lists the contents of RACF SMF records in a format that is easy to read. The RACF report writer can also generate reports based on the information in the SMF records. With the RACF report writer, you can obtain:

- Reports that describe attempts to access a particular RACF-protected resource in terms of user identity, number and type of successful accesses, and number and type of attempted security violations.
- Reports that describe user and group activity.
- Reports that summarize system use and resource use.

How the RACF Report Writer Operates

The RACF report writer consists of three phases: (1) command and subcommand processing, (2) record selection, and (3) report generation. See Figure 2-1 for an overview of the RACF report writer. Figure 2-1 also shows the installation-replaceable module for the RACF report writer, ICHRSMFI, and the RACF report writer installation exit, ICHRSMFE.

ICHRSMFI is a non-executable module that contains default values for the RACF report writer sort parameters, dynamic allocation parameters, and processing options. See *SPL: RACF* for a description of the contents of the module and, if necessary, how to modify the module.

ICHRSMFE is an installation exit that the RACF report writer calls during the record selection phase. The exit allows you to add functions, such as the following, to the RACF report writer:

- Create additional selection and/or rejection criteria for records that the RACF report writer processes
- Modify data set naming conventions in records that the RACF report writer processes
- Add other reports to those that the RACF report writer provides

Detailed information about coding the ICHRSMFE exit routine appears in *SPL: RACF*.

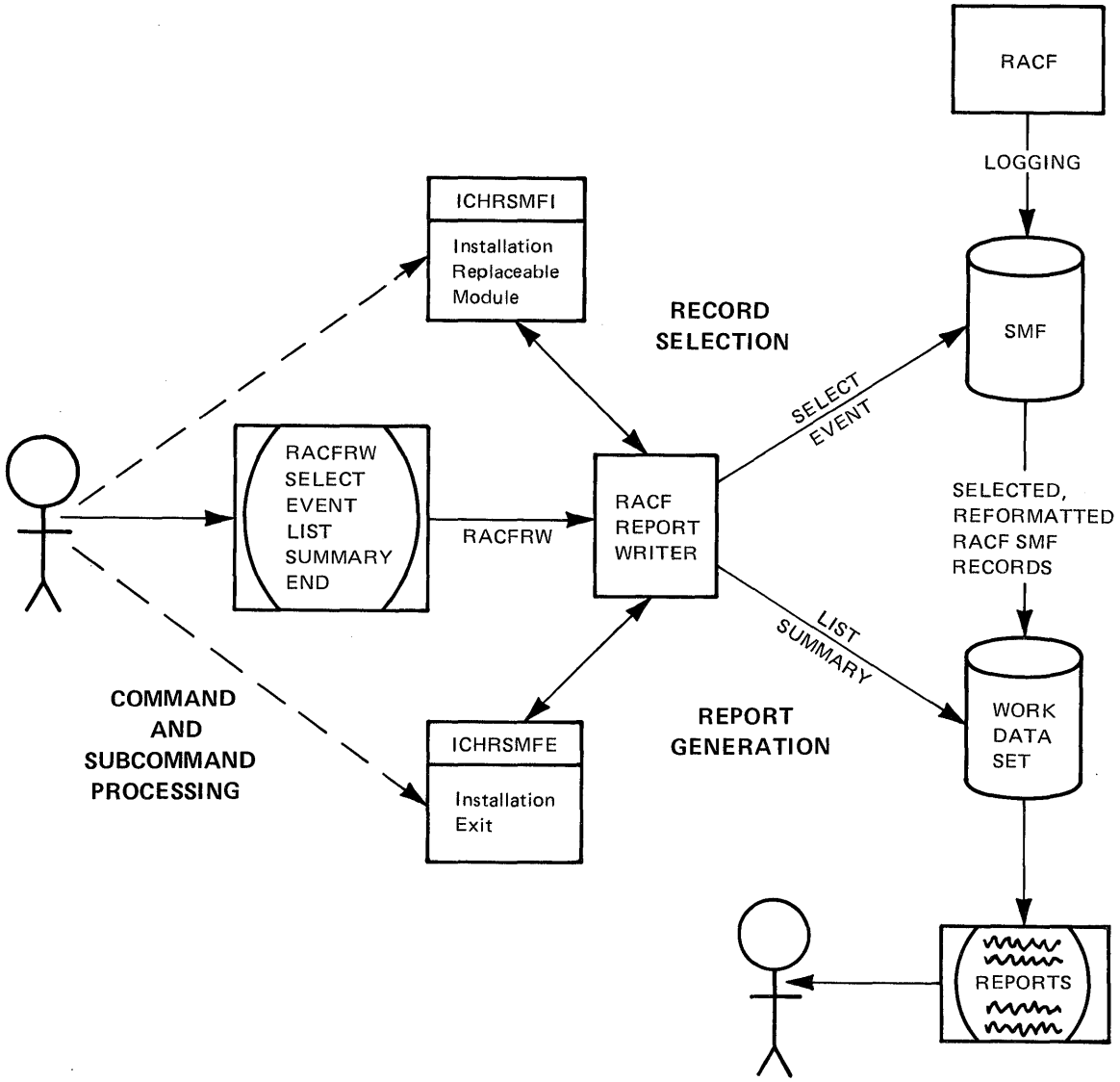


Figure 2-1. RACF Report Writer Overview

The First Phase

The first phase, *command and subcommand processing*, starts when you enter the TSO command RACFRW. RACFRW invokes the RACF report writer through the terminal monitor program (TMP) and places you in subcommand mode. At this time, you can enter the RACF report writer subcommands, which are SELECT, EVENT, LIST, SUMMARY, and END.

Briefly, the SELECT and EVENT subcommands specify which of the input records the RACF report writer is to select and use to generate the reports you request with the LIST and SUMMARY subcommands. After entering all the

subcommands you need, enter the END subcommand. END terminates subcommand mode and the first processing phase. Note that entering ATTENTION at any time during this first phase terminates the RACF report writer immediately and returns control to the TMP.

The Second Phase

During the second phase, *record selection*, the RACF report writer compares each record from the input file -- the SMF records -- against the criteria you specify on the SELECT and EVENT subcommands. The RACF report writer accepts as input only RACF-generated SMF records. These are PROCESS records (SMF type 20, 30, and 80 records) and STATUS records (SMF type 80 records generated by a SETROPTS or RVARY command and SMF type 81 records).

The RACF report writer uses the records that satisfy the selection criteria specified on the SELECT and EVENT subcommands for further processing. If you do not specify any SELECT and EVENT subcommands, the RACF report writer selects all of the records from the input file for further processing.

To sort the records during later processing, the RACF report writer must reformat the SMF records. When the RACF report writer reformats a record, it combines all the record segments into a single record. If the record is larger than the maximum record length that the sort can handle, the RACF report writer truncates the record and marks it as a truncated record. The listing of selected records that the RACF report writer produces identifies any truncated records. The default maximum record length is 1,024. If you want to change the default, located in the WRKLRECL field in ICHRSMFI, see the description of ICHRSMFI in *SPL: RACF*.

The RACF report writer copies the reformatted records to a work data set. You can save this work data set and use the reformatted records as input to a later run of the RACF report writer.

When the input consists of reformatted SMF records, the RACF report writer skips the reformatting step for those records. Thus, you do not need to reformat records each time you run the RACF report writer. Operands on the RACFRW command control whether or not the RACF report writer is to reformat the input records and whether or not the work data set is to be saved for subsequent runs of the RACF report writer.

When the RACF report writer has compared all of the input records against the selection criteria and, if necessary, reformatted the selected records and copied them to a work data set, the second processing phase is complete.

The Third Phase

During the third phase, *report generation*, the RACF report writer generates the reports that you request with the LIST and SUMMARY subcommands. It uses as input only the records from the work data set. The RACF report writer always produces a header page that lists the subcommands that you have entered and describes the meanings of some values that appear in the reports. The other reports depend on operands you have specified, but the RACF report writer always produces the reports you request in the same order.

If you have specified the GENSUM operand on the RACFRW command, the RACF report writer first produces a general summary report, which summarizes overall system activity related to RACF protection. The RACF report writer collects the data for the general summary report during the record selection phase. If you have specified the LIST subcommand, the RACF report writer next lists all the records from the work data set in the sequence that you have specified with the SORT operand on the LIST subcommand. Last, it produces a summary report for each SUMMARY subcommand that you have specified. Samples of all these reports, appear in "Sample Reports" later in this chapter. When it has completed the last report, the RACF report writer terminates and returns control to the TMP.

RACF Report Writer Command and Subcommands

This section lists the function and syntax of the RACF report writer command (RACFRW) and subcommands (SELECT, EVENT, LIST, SUMMARY, and END). The command and subcommands are not listed alphabetically but in the order in which you might typically enter them. This order is: RACFRW, SELECT, EVENT, LIST, SUMMARY, and END.

The following key defines the symbols used in this chapter to define the syntax of the command and subcommands:

Key to Symbols in Command Definitions

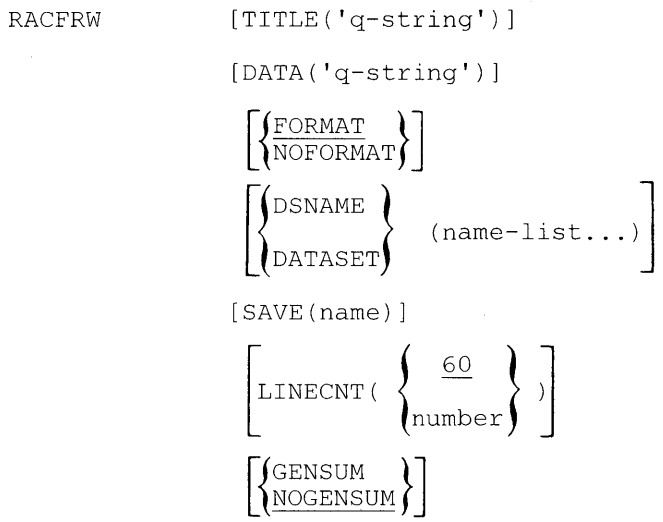
UPPERCASE	must appear as shown
lowercase	the user supplies the information
list...	the item can be listed more than once
{ }	groups alternative items; you can only specify one item
[ ]	optional item that you can specify
KEYWORD	default when no item is specified

RACFRW Command

The TSO command RACFRW invokes the RACF report writer. After you enter the RACFRW command, TSO places you in subcommand mode and prompts you to enter the RACF report writer subcommands until you enter the END subcommand.

On the RACFRW command, you can specify the source and disposition of input records, the data to be passed to the installation exit routine (ICHRSMFE), whether or not the RACF report writer is to reformat the input records, and whether or not the RACF report writer is to print a general summary report. (See *SPL: RACF* for further information about the installation exit ICHRSMFE.)

The syntax of the RACFRW command is:



TITLE('q-string')
specifies a string of up to 132 characters, enclosed insingle quotation marks, to be used as a default heading for the report pages, if the TITLE operand on either the SUMMARY or LIST subcommand does not specify a unique report heading for a requested report.

DATA('q-string')
specifies a string of up to 256characters of data, enclosed in single quotation marks, to be passed to the installation exit routine (ICHRSMFE).

FORMAT
specifies that the RACF SMF records used as input to the RACFreport writer must be reformatted before processing. For additional information about the reformatted records, see *SPL: RACF*. FORMAT implies that the RACF report writer has not previously processed the input records. FORMAT is the default value.

NOFORMAT
specifies that the RACF SMF records used as input to theRACF report writer are already reformatted and suitable for processing. NOFORMAT implies that the input records have been processed previously by the RACF report writer and saved with the SAVE operand.

Note: Specifying FORMAT for a data set that is already reformatted or specifying NOFORMAT for a data set that is not already reformatted can cause unpredictable results.

DSNAME(name-list...) or DATASET(name-list...)
specifies the name ofone or more cataloged data sets to be concatenated and used as input to the RACF report writer. If you omit this operand, the RACF report writer uses as input the data set you have preallocated to the RSMFIN ddname.

SAVE(name)
specifies the name of a sequential data set to be assigned to thework data set that is to contain the selected reformatted RACF SMF records. If this 'name' data set is new, the RACF report writer allocates and catalogs it. If this 'name' data set is old, the RACF report writer replaces the data currently in the data set with the new data and keeps the data set. You can use this saved work data set as input to a later run of the RACF report writer.

If you omit this operand and you have not preallocated a SORTIN ddname, the work data set is deleted at job termination.

LINECNT(number)
specifies the maximum number of lines to be written beforeejecting to a new page. The minimum number that you can specify is 20. If you specify a number less than 20, LINECNT defaults to 20. If you omit this operand, LINECNT defaults to 60.

GENSUM
specifies that a general summary report is to be printed.This report contains various statistics about all the RACF SMF records processed, such as total JOB/LOGON attempts, successes, and violations, total resource accesses, successes, and violations, and a breakdown of JOB/LOGON and resource access violations by hour.

NOGENSUM
specifies that a general summary report is not to be printed.NOGENSUM is the default value.

SELECT Subcommand

The SELECT subcommand allows you to choose specific records from the input file containing the RACF SMF records. The RACF report writer reformats these selected records, if necessary, and copies them to a work data set. While all input records are used for the general summary report, the RACF report writer can list and generate summary reports for only the records that are in the work data set.

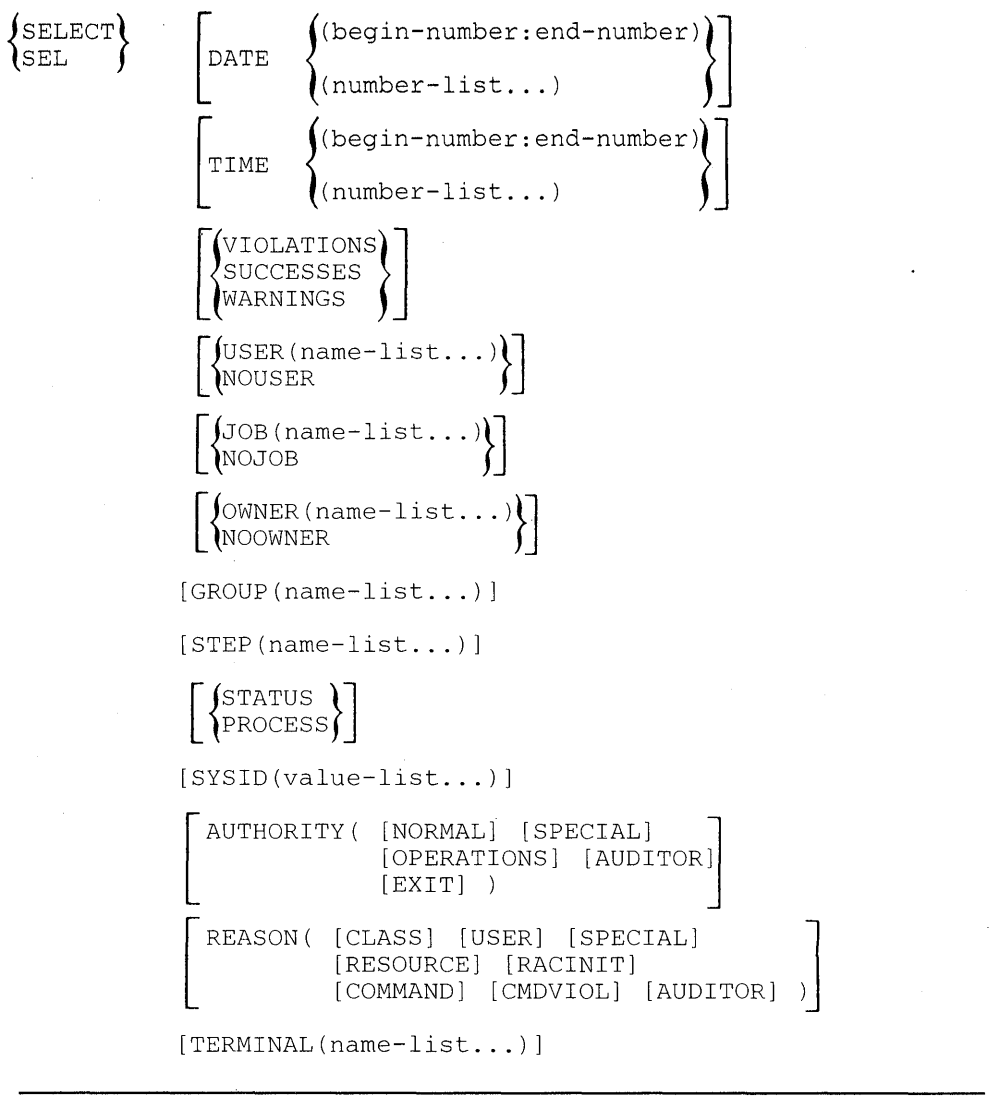
You can issue SELECT subcommands separately or with EVENT subcommands to form what is called a SELECT/EVENT group. A SELECT/EVENT group must begin with a SELECT subcommand, even if it is a SELECT subcommand with no operands. You can then follow this subcommand with up to 49 EVENT subcommands that specify additional selection criteria for that group. See "EVENT Subcommand" later in this chapter.

For the RACF report writer to select an input record for further processing, the record must meet all the criteria specified on (1) a SELECT subcommand and (2) one of a group's EVENT subcommands, if the SELECT subcommand begins a SELECT/EVENT group.

If you specify multiple SELECT subcommands and/or SELECT/EVENT groups, you can specify the groups in any order. The listing and summary reports that you request, however, will reflect *all* the records that have been selected by *all* the groups, not just the records selected by one particular SELECT/EVENT group. If you do not issue any SELECT subcommands or SELECT/EVENT groups, then *all* the RACF SMF records from the input file are selected.

The RACF report writer can process a maximum of 50 SELECT and EVENT subcommands. If you enter more, TSO accepts only the first 50, then prompts you to enter a subcommand other than SELECT or EVENT.

The syntax of the SELECT subcommand is:



DATE(begin-number:end-number) or DATE(number-list...)
specifies a range (in ascending order) or a list of dates in theform YYDDD that are to be selected for further processing.

TIME(begin-number:end-number) or TIME(number-list...)
specifies a range (in ascending order) or a list of times in theform HHMMSS that are to be selected for further processing.

VIOLATIONS
specifies that only records identifying security violations areto be selected for further processing. VIOLATIONS appliés to PROCESS records only.

SUCCESSES
specifies that only records identifying successful access attemptsare to be selected for further processing. SUCCESSES applies to PROCESS records only.

WARNINGS
specifies that only records for which an insufficient accessauthorization warning message was issued are to be selected for further processing. WARNINGS applies to PROCESS records only.

If you do not specify VIOLATIONS, SUCCESSES, or WARNINGS, none of these are used as selection criteria.

USER(name-list...)
specifies a list of userids that are to be selected for furtherprocessing. USER applies to PROCESS records only. If you omit both the USER and NOUSER operands, the RACF report writer selects all records containing userids. (See Note 1.)

NOUSER
specifies that records that contain userids are not to be selectedfor further processing. If you omit both the USER and NOUSER operands, the RACF report writer selects all records containing userids. If you specify both the NOUSER and NOJOB operands, the RACF report writer ignores both operands. (See Note 1.)

JOB(name-list...)
specifies a list of jobnames that are to be selected for furtherprocessing. JOB applies to PROCESS records only. If you omit both the JOB and NOJOB operands, the RACF report writer selects all records containing jobnames. (See Note 1.)

NOJOB
specifies that records that contain jobnames are not to be selectedfor further processing. If you omit both the JOB and NOJOB operands, the RACF report writer selects all records containing jobnames. If you specify both the NOUSER and NOJOB operands, the RACF report writer ignores both operands. (See Note 1.)

OWNER(name-list...)
specifies a list of resource owner names that are to be selectedfor further processing. OWNER applies to PROCESS records only. If you omit both the OWNER and NOOWNER operands, owner will not be a selection criteria.

NOOWNER
specifies that records that containresource owner names are not to be selected for further processing. If you omit both the OWNER and NOOWNER operands, owner will not be a selection criteria.

GROUP(name-list...)
specifies a list of group names that are to be selected for furtherprocessing. GROUP applies to PROCESS records only. (See Note 1.)

STEP(name-list...)
specifies a list of step names that are to be selected for furtherprocessing. STEP applies to PROCESS records only. (See Note 1.)

STATUS
specifies that only STATUS records are to be selected for furtherprocessing. STATUS records are RACF SMF record types 80 (those generated by the SETROPTS or RVARY command) and 81.

PROCESS
specifies that only RACF SMF record types 20, 30, and 80 are to beselected for further processing.

SYSID(value-list...)
specifies a list of system identifiers that are to be selected forfurther processing.

AUTHORITY(type...)
specifies a list of authority types that are to be selectedfor further processing, where type can be any of the following:

SPECIAL -	selects records produced because the user had the SPECIAL or group-SPECIAL attribute.
OPERATIONS -	selects records produced when access was granted because the user had the OPERATIONS or group-OPERATIONS attribute.
AUDITOR -	selects records produced because the user had the AUDITOR or group-AUDITOR attribute.
EXIT -	selects records produced when access was granted by an installation exit routine.
NORMAL -	selects records produced when access was granted for a reason other than those mentioned above (for example, when the user had sufficient access authority).

AUTHORITY applies to PROCESS records only.

REASON(value...)
specifies the reasons for logging the records that are to beselected for further processing, where value can be any of the following:

CLASS -	selects records produced because auditing of profile changes was in effect for a particular class.
USER -	selects records produced because auditing was in effect for the specific user
SPECIAL -	selects records produced because auditing was in effect for SPECIAL or group-SPECIAL users.
RESOURCE -	selects records produced because auditing was in effect for the specific resource or because a RACHECK installation exit routine requested auditing (see Note 2).
RACINIT -	selects records produced by the RACINIT SVC.
COMMAND -	selects records produced by commands that are always logged.
CMDVIOL -	selects records produced because auditing of command violations was in effect.
AUDITOR -	selects records produced because auditing of the specific resource was in effect (see Note 2).

REASON applies to PROCESS records only.

TERMINAL(name-list...)
specifies a list of terminal IDs that are to be selected forfurther processing. TERMINAL applies to PROCESS records only.

Note 1: Users who are not defined to RACF do not have a RACF userid. In addition, they cannot connect to RACF. Thus, the RACF SMF records associated with these users contain the jobname in place of the userid and the stepname in place of the group name.

Note 2: The RACF report writer can select a record because of either RESOURCE or AUDITOR or both RESOURCE and AUDITOR.

EVENT Subcommand

The EVENT subcommand allows you to specify selection criteria related to particular RACF events. For a record to be selected for further processing by the RACF report writer, it must satisfy *all* the selection criteria that you specify on this EVENT subcommand.

You can use the EVENT subcommand only with a SELECT subcommand in a SELECT/EVENT group. With the EVENT subcommand, you can create a subset of the records that have already passed the selection criteria specified on the SELECT subcommand. ("SELECT Subcommand" earlier in this chapter describes SELECT/EVENT groups in more detail.)

The EVENT subcommand applies to PROCESS records only.

The syntax of the EVENT subcommand is:

```
{EVENT}
{EV   }    event-name

           [EVQUAL(value-list...)]

           [CLASS(name-list...)]

           [NAME(name-list...)]

           [DSQUAL(name-list...)]

           [ INTENT( [ALTER] [CONTROL]          ]
           [         [UPDATE] [READ] [NONE] )   ]

           [ ALLOWED( [ALTER] [CONTROL]         ]
           [          [UPDATE] [READ] [NONE] )  ]

           [NEWNAME(name-list...)]

           [NEWDSQUAL(name-list...)]

           [ LEVEL( {begin-number:end-number} ) ]
           [        {number-list...          }   ]
```

event-name

specifies one of the following valid event names:

EVENT NAME	DESCRIPTION
LOGON	TSO logon or batch job initiation
ACCESS	Access to a RACF-protected resource
ADDVOL	Add a volume to a multivolume data set or tape volume set
RENAME	Rename a data set
DELETE	Delete a data set or tape volume
DELVOL	Delete one volume of a multivolume data set or tape volume set
DEFINE	Define a data set or tape volume
ALLSVC	All of the preceding SVC functions (ACCESS, ADDVOL, RENAME, DELETE, DELVOL, and DEFINE)
ADDSD	ADDSD command
ADDGROUP	ADDGROUP command
ADDUSER	ADDUSER command
ALTDSD	ALTDSD command
ALTGROUP	ALTGROUP command
ALTUSER	ALTUSER command
CONNECT	CONNECT command
DELDSD	DELDSD command
DELGROUP	DELGROUP command
DELUSER	DELUSER command
PASSWORD	PASSWORD command
PERMIT	PERMIT command
RALTER	RALTER command
RDEFINE	RDEFINE command
RDELETE	RDELETE command
REMOVE	REMOVE command
RVARY	RVARY command
SETROPTS	SETROPTS command
ALLCOMMAND	All of the preceding RACF commands (ADDSD through SETROPTS)

Not all of the EVENT subcommand operands are valid with certain event names. Use Figure 2-2 to determine which event name and operand combinations are valid.

EVENT NAME	EVENT CODE	EVQUAL EVENT QUALIFIERS								CLASS	NAME	DSQUAL	INTENT	ALLOWED	NEWNAME	NEWDSQUAL	LEVEL
		0	1	2	3	4	5	6	7								
LOGON	1	X	X	X	X	X	X	X	X								
ACCESS	2	X	X	X	X					X	X	X	X	X			X
ADDVOL	3	X	X							X	X	X		X			X
RENAME	4	X	X	X	X	X	X				X	X			X	X	X
DELETE	5	X	X	X						X	X	X					X
DELVOL	6	X								X	X	X					X
DEFINE	7	X	X	X	X	X	X			X	X	X					X
ALLSVC	2-7	X	X	X	X	X	X			X	X	X	X	X	X	X	X
RACF Commands	8-25	X	X	X						X[1]	X	X[2]					
ALL COMMAND	8-25	X	X	X						X	X	X					

Notes:

1. CLASS is valid for the PERMIT, RALTER, RDEFINE, and RDELETE commands only.
2. DSQUAL is not valid for the RDEFINE, RALTER, and RDELETE commands.

Figure 2-2. EVENT Subcommand Operand Combination Table

EVQUAL(value-list...)
specifies a list of event qualifiers to be selected.Figure 2-2 lists the valid event qualifiers for each event name. Figure 2-3, later in this chapter, which shows the contents of the header page, identifies the meaning of each event qualifier.

CLASS(class-name...)
specifies a list of resource class names to be selected.Only the DATASET class and class names found in the class descriptor table are valid. See Figure 2-2 for the event names that are valid with the CLASS operand.

NAME(name-list...)
specifies a list of resource namesor generic names to be selected. To select specific data sets, you must specify fully-qualified data set names in the 'name-list'. Also, if a data set has been renamed and you want to use this operand to select the old data set name, you must specify the fully-qualified old data set name in the 'name-list'. This operand is not valid with the LOGON event name.

DSQUAL(name-list...)
specifies a list of data set qualifiers to be selected.Valid data set qualifiers are any userids or group names used as the high-level qualifier of a data set name or any qualifiers supplied by the ICHRSMFE installation exit routine. If a data set has been renamed and you want to use this operand to select the old data set name, you must specify the qualifier of the old data set name in the 'name-list'.

INTENT
specifies a list of intended access authorities to be selected.An intended access authority is the minimum authority needed by a user to access a particular resource (not the actual authority held by the user). The valid intended access authorities are ALTER, CONTROL, UPDATE, READ, and NONE. The INTENT operand is valid only with the ACCESS event name.

ALLOWED
specifies a list of allowed access authorities to be selected.An allowed access authority is the actual authority held by the user requesting access to a particular resource (not the minimum authority needed by the user to access that resource). The valid allowed access authorities are ALTER, CONTROL, UPDATE, READ, and NONE. The ALLOWED operand is valid only with either the ACCESS or the ADDVOL event names.

NEWNAME(name-list...)
specifies a list of new fully-qualifieddata set names to be selected. This operand is valid only with the RENAME event name.

NEWDSQUAL(name-list...)
specifies a list of qualifiers for new data setor generic names to be selected. Valid qualifiers are any userids or group names used as the high-level qualifier of a data set name or any qualifiers supplied by the ICHRSMFE installation exit routine. This operand is valid only with the RENAME event name.

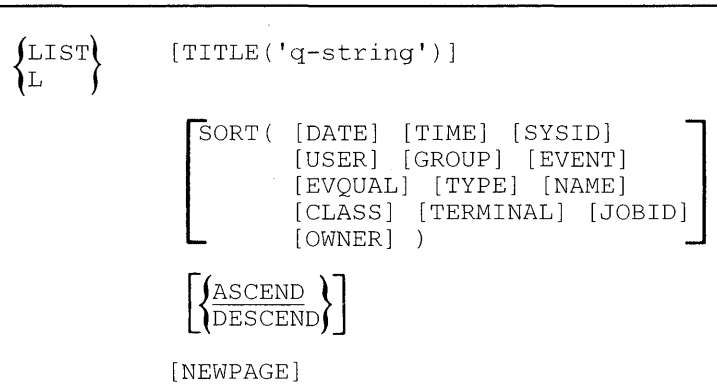
LEVEL(begin-number:end-number) or LEVEL(number-list)
specifies a range (in ascending order) or a list of resource levelsto be selected.

The meaning of the level indicator is set by your installation with the ADDSD command. See the *RACF Command Language Reference* for more information about the LEVEL operand. Figure 2-2 shows the event names that are valid with the LEVEL operand.

LIST Subcommand

The LIST subcommand formats and prints a listing of each individual RACF SMF record that passes the selection criteria specified on the SELECT and EVENT subcommands. On the LIST subcommand, you can specify the title, sort sequence, and format control for the listing. The RACF report writer processes only one LIST subcommand; if you enter more than one, the RACF report writer recognizes only the last LIST subcommand that you have entered. (The RACF report writer does all processing after you enter the END command.)

The syntax of the LIST subcommand is:



TITLE('q-string')
specifies a string of up to 132 characters, enclosed in singlequotation marks, to be used as the heading for each page of this particular listing. If you omit this operand but specify a default heading in the TITLE operand of the RACFRW command, the default heading appears on each page of the listing. If you omit both this operand and the RACFRW TITLE operand, no heading at all appears on the listing.

SORT(field-list)
specifies the fields of the input record (a reformatted RACF SMFrecord) that are to be used for sorting. If you specify the LIST subcommand without specifying the SORT operand, the RACF report writer sorts the records by RCDTYPE, at offset 5(5) in the reformatted SMF record, with STATUS records preceding PROCESS records. If you specify SORT operand values, the records are then further sorted within the STATUS and PROCESS groups by the fields that you specify on the SORT operand.

The sequence in which you specify the SORT operands determines the sequence in which the RACF report writer sorts the records. For example, specifying SORT(OWNER GROUP USER DATE TIME) causes the RACF report writer to sort on the profile owner first, then group name, then user name, and so forth.) If you omit the SORT operand, the order in which the records were written to SMF is not necessarily the order in which the records appear in the output listing, unless you have specified EQUALS in the SORTEQU field of the installation-replaceable module (ICHRSMFI). The following table describes the operands you can use to select a sort sequence.

OPERAND	DESCRIPTION	SORTS ON REFORMATTED RACF SMF RECORD FIELD NAME	OFFSET
DATE	Julian date (YYDDDF)	RCDDATE	16 (10)
TIME	Time of day (HHMMSSTH)	RCDTIME	11 (B)
SYSID	System identifier	RCDSYSID	6 (6)
USER[1]	User (job) names	RCDUSER	29 (1D)
GROUP[1]	Group (step) names	RCDGROUP	37 (25)
EVENT[1]	Security event codes	RCDEVENT	25 (19)
EVQUAL[1]	Security event code qualifiers	RCDQUAL	26 (1A)
TYPE[1]	Event types: 1 = JOB/LOGON events 2 = SVC events 3 = command events	RCDLOGCL	45 (2D)
NAME[1]	Names of resources within event types: USERID for JOB/LOGON events RESOURCE NAME for SVC and command events	RCDNAME	54 (36)
CLASS[1]	Resource class names	RCDCLASS	46 (2E)
TERMINAL[1]	Terminal ID	RCD80TRM	122 (7A)
JOBID[1]	Job ID from SMF job management record	RCDJOBID	98 (62)
OWNER	Owner of the resource	RCDOWNER	131 (83)

ASCEND

specifies that the fields identified by the DATE and TIMEoperands are to be sorted in ascending order. If you omit the DATE and TIME operands, this operand is ignored.

ASCEND is the default value.

DESCEND

specifies that the fields identified by the DATE and TIMEoperands are to be sorted in descending order. If you omit both the DATE and TIME operands, this operand is ignored.

NEWPAGE

specifies that the listing is to start printing on a new pagewhenever the value in the major (first) sort field changes. If you omit the SORT operand, this operand is ignored.

---

[1] Even though these operands apply only to process records, specifying them does not affect the order of status records.

SUMMARY Subcommand

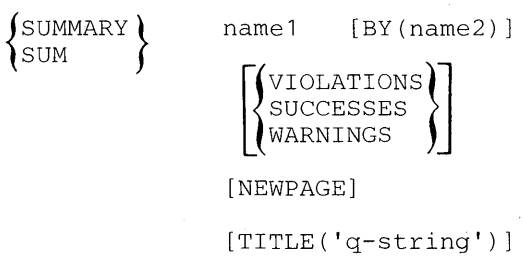
The SUMMARY subcommand causes the RACF report writer to format and print reports that summarize the information in the RACF SMF records that have passed the selection criteria on the SELECT and EVENT subcommands.

Using the SUMMARY subcommand, you can request reports that summarize the following:

- Group activity
- User activity
- Resource activity
- Security event activity
- RACF command activity
- Owner activity
- Group activity broken down by resource
- User activity broken down by resource
- Resource activity broken down by user
- Resource activity broken down by group
- Resource activity broken down by security event
- Security event activity broken down by resource
- RACF command activity broken down by user
- RACF command activity broken down by group
- RACF command activity broken down by resource
- Owner activity broken down by resource

On a SUMMARY subcommand, you can specify only one of the activities mentioned in the preceding list. You can, however, enter as many as sixteen different SUMMARY subcommands for each RACFRW command. You can thus request reports of all possible activities in one run of the RACF report writer. (Note that, if you accidentally enter more than one SUMMARY subcommand for the same type of activity, it does not cause an error; the RACF report writer recognizes only the last one.) The order in which you enter the SUMMARY subcommands is the order in which the summary reports are printed.

The syntax of the SUMMARY subcommand is:



name1
specifies the major field on which information is to be grouped andsummarized. The valid values for name1 are: GROUP, USER, RESOURCE, EVENT, COMMAND, and OWNER.

BY(name2)
specifies a minor field within the major field on which informationis to be grouped and summarized also. The valid values for name2 are: GROUP, USER, RESOURCE, and EVENT.

Note: Only the following name1 [BY(name2)] combinations are valid:

GROUP	RESOURCE BY(USER)
USER	RESOURCE BY(GROUP)
RESOURCE	RESOURCE BY(EVENT)
EVENT	EVENT BY(RESOURCE)
COMMAND	COMMAND BY(USER)
OWNER	COMMAND BY(RESOURCE)
GROUP BY(RESOURCE)	COMMAND BY(GROUP)
USER BY(RESOURCE)	OWNER BY(RESOURCE)

VIOLATIONS
specifies that only information about access violations is tobe included in the summary.

SUCCESSES
specifies that only information about successful accessattempts is to be included in the summary. If you omit VIOLATIONS, SUCCESSES, and WARNING, the summary includes information for both access violations and successful access attempts.

WARNINGS
specifies that only accesses that weresuccessful only because WARNING mode was in effect are to be included in the summary. The information appears under the WARNINGS heading.

If you do not specify VIOLATIONS, SUCCESSES, or WARNINGS, the report summarizes all access attempts.

NEWPAGE
specifies that the summary report is to start printing on a newpage whenever the value in name1 changes. NEWPAGE is valid only when BY(name2) is specified.

TITLE('q-string')
specifies a string of up to 132 characters, enclosed insingle quotation marks, to be used as the heading for each page of this particular summary report. If you omit this operand but specify a default heading in the TITLE operand of the RACFRW command, the default heading appears on each page of the summary report. If you omit both this operand and the RACFRW TITLE operand, no heading at all appears on the summary report.

END Subcommand

The END subcommand terminates subcommand mode. All report generation processing is done after you enter the END subcommand.

The syntax of the END subcommand is:

```
END
```

RACF Report Writer Examples

This section gives some examples of how to use the RACF report writer command and subcommands to produce various reports.

The first four examples show how to obtain single reports. To create all the reports that you require at your installation, you might, however, need to execute the RACF report writer more than once. (An execution of the RACF report writer consists of the RACFRW command, report definition subcommands, and the END subcommand.) Example 5 shows a situation where the reports that the installation needs require two executions of the RACF report writer.

1. To obtain a report of all RACF SMF records, listed in the order read from the input file, and a general summary report, showing overall RACF-related system activity, you enter:

```
RACFRW TITLE('BIG LISTING') GENSUM
LIST
END
```

2. To obtain a report of all jobs, sorted by job name, with only process records included, you enter:

```
RACFRW
SELECT NOUSER PROCESS
LIST TITLE('JOB LIST REPORT') SORT(USER) NEWPAGE
```

   and to obtain a summary of these jobs, you enter:

```
SUMMARY RESOURCE TITLE('JOB SUMMARY REPORT')
END
```

3. To obtain a report of all violations against data sets owned by USERA (USERA is the high-level qualifier of the data set name) in January, 1984, sorted in date and time sequence, you enter:

```
RACFRW TITLE('USERA DATASETS LIST REPORT')
SELECT VIOLATIONS DATE(84001:84031)
EVENT ALLSVC CLASS(DATASET) DSQUAL(USERA)
EVENT ALLCOMMAND CLASS(DATASET) DSQUAL(USERA)
LIST SORT(DATE TIME)
```

and to obtain a summary of this activity, you enter:

```
SUMMARY RESOURCE BY(USER) TITLE('USERA DATA SETS SUMMARY
REPORT')
```

4. To obtain a report on data set activity by (a) jobs A and B on system 158A and (b) users C and D on system 158B, you enter:

```
RACFRW
SELECT JOB(A B) NOUSER SYSID(158A)
EVENT ALLSVC CLASS(DATASET)
EVENT ALLCOMMAND CLASS(DATASET)
SELECT USER(C D) NOJOB SYSID(158B)
EVENT ALLSVC CLASS(DATASET)
EVENT ALLCOMMAND CLASS(DATASET)
LIST TITLE('SELECTED DATA SET ACTIVITY REPORT') SORT(SYSID) END
```

5. Assume that a user needs to produce four separate reports: (1) a detailed listing of all access violations, sorted by user, (2) a resource by user summary report, with totals for access violations only, (3) a listing of all successful accesses, sorted by date and time, and (4) a resource by user summary report, with totals for successful accesses only. It is necessary to produce four *separate* reports because each report is to be distributed to a different individual who, because of the nature that person's job, is entitled to see only the information on that one report. Assume that the user enters:

```
(1)  RACFRW
(2)  SELECT VIOLATIONS
(3)  LIST TITLE('ACCESS VIOLATIONS LIST REPORT') SORT(USER)
(4)  SUMMARY RESOURCE BY(USER) TITLE ('ACCESS VIOLATIONS SUMMARY
     REPORT')
(5)  SELECT SUCCESSES
(6)  LIST TITLE('ACCESS SUCCESS LIST REPORT') SORT(DATE TIME)
(7)  SUMMARY RESOURCE BY(USER) TITLE('ACCESS SUCCESS SUMMARY
     REPORT')
(8)  END
```

Instead of receiving the four desired reports, the user receives two reports: (1) a list report of all violations and successes, sorted by date and time, and (2) a summary report of resources by user with both violations and successful accesses. The reasons for receiving two reports, instead of four, are:

a. Although the user intended to first select, list, and summarize only violations from the input file (statements 2, 3, and 4), then select, list, and summarize only successful accesses (statements 5, 6, and 7), the RACF report writer does not execute in that sequence. It selects records first, based on *all* the SELECT and EVENT subcommands entered. Only after this selection process has completed are any of the requested reports produced. Based on the subcommands that this user entered, the RACF report writer checked each record from the input file to see if it was either an access violation (statement 2) or a successful access (statement 5). Because all the input records passed one of these conditions, the RACF report writer selected all of the records for further processing.

b. The RACF report writer then produced a list report (statement 6). The RACF report writer ignored the LIST subcommand in statement 3 because only one LIST subcommand, the last one entered, is valid for each execution of the RACF report writer. The report that was produced listed

in date and time sequence all the records selected (both access violations and successful accesses).

c. Last, the RACF report writer produced a single summary report (statement 7). The RACF report writer ignored the SUMMARY subcommand in statement 4 because it requested the same type of summary report (resource by user) that statement 7 requested. When a user enters multiple SUMMARY subcommands for the same type of summary reports, the RACF report writer recognizes only the last one entered. Thus, the summary report produced in this example gave totals for all the records selected (both access violations and successful accesses).

To produce the four listings that the user intended, the user should enter:

```
RACFRW
SELECT VIOLATIONS
LIST TITLE('ACCESS VIOLATIONS LIST REPORT') SORT(USER)
SUMMARY RESOURCE BY(USER) TITLE ('ACCESS VIOLATIONS SUMMARY
REPORT')
END
RACFRW
SELECT SUCCESSES
LIST TITLE('ACCESS SUCCESS LIST REPORT') SORT(DATE TIME)
SUMMARY RESOURCE BY(USER) TITLE ('ACCESS SUCCESS SUMMARY
REPORT')
END
```

Planning Considerations

To use the RACF report writer at your installation, you must have:

- OS/VS Sort/Merge Release 4 (IBM Program Product, Program Number 5740-SM1), or equivalent.
- An output device that can handle 133 character lines.

Preallocating Data Sets

If you want to preallocate any of the data sets required by the RACF report writer, you must use the following ddnames:

RSMFIN	The input data set(s). Note, however, that if you enter the DATASET operand on the RACFRW command, the RACF report writer assigns a system-generated ddname to this input data set and ignores RSMFIN. If you neither preallocate the input data set nor specify the DATASET operand, the RACF report writer issues message ICH64305I and terminates immediately.
SYSPRINT	The output data set. If you do not preallocate this output data set, the RACF report writer allocates this data set to a SYSOUT data set (such as the terminal on which you are entering the commands and subcommands).
SORTIN	The work data set. If you enter the SAVE operand on the RACFRW command, the RACF report writer assigns SORTIN to the work data set that you specify in the SAVE operand. If you preallocate the work data set or specify the SAVE operand, the RACF report writer saves this work data set for future use; otherwise, it allocates the work data set to a temporary data set and deletes it at job termination.

SORTLIB	The system library that contains the SORT/MERGE load modules. If you do not preallocate this system library, the RACF report writer allocates it to the sort data set named in SORTDSN in ICHRSMFI. Initially, the name in SORTDSN is SYS1.SORTLIB.
SORTDDNM	The SORT/MERGE messages. The RACF report writer allocates these messages to the data set named in SORTDDNM in ICHRSMFI. If you do not preallocate these messages, they go to the terminal on which you are entering the commands and subcommands because the initial name in SORTDDNM is SYSOUT.
SORTWKxx	The SORT/MERGE work file(s), named SORTWK01 to SORTWKnn. If you do not preallocate these files, dynamic allocation occurs, using the dynamic allocation parameter specified in SORTDYN in ICHRSMFI. Initially, SORTDYN contains 'DYNALLOC=3330'.

Note that any data set that you preallocate remains allocated after the RACF report writer terminates, while any data set allocated by the RACF report writer is deallocated prior to termination.

RACF Report Writer Return Codes

Upon completion, the RACF report writer returns control to the terminal monitor program (TMP), with a return code in register 15. This return code is 0 if the RACF report writer has terminated normally. This return code is 12 if the RACF report writer:

- Was unsuccessful in dynamically allocating any needed data set that was not preallocated by the user
- Was unsuccessful in opening any needed data set
- Received a non-zero return code from a TSO service routine that it has invoked
- Received a non-zero return code from the SORT/MERGE routines

Use Hints

When using the RACF report writer, consider the following:

1. If you have MVS System Product Version 2 installed, you must use the SMF dump program, IFASMFDP, to dump the SMF data set, which is a VSAM data set, into a QSAM data set, which is what the RACF report writer requires. For additional information on IFASMFDP, see *System Management Facilities (SMF).*

2. In an installation using RACF to protect multiple systems, each system writes RACF-generated SMF records to a different data set. You can concatenate all of these data sets into a single data set for input to the RACF report writer. Later, should you have to separate the information based on the identifier of the system that generated it, you could use the SYSID operand on either the LIST or SELECT subcommand.

3. By using the SELECT and EVENT subcommands, you can retrieve individual SMF records of interest for display at a TSO terminal (display screen).

4. If your SMF file is large or resides on multiple tape volumes, you might consider specifying the SAVE operand for the work data set that you create. This action would reduce the amount of time and number of devices you would need, should you have to use this work data set again at a later time to produce additional reports. Note that by using SELECT and EVENT subcommands, you can create and save a subset of a work data set that you saved in a previous run of the RACF report writer.

5. You can use the RACF report writer exit routine, ICHRSMFE, to modify the data set names that exist in the SMF records.

6. The RACF report writer executes as a post-processor of RACF and does not interfere with normal RACF processing.

Sample Reports

This section includes examples of the various reports that you can request the RACF report writer to generate. Review each sample report to determine its usefulness to your particular installation.

The following list summarizes the sample reports and the command or subcommand you issue to request the report:

Figure	Report	Command/Subcommand Issued
2-3	Standard Header Page. Each time that you invoke the RACF report writer, it produces a standard header page that lists the subcommands that you entered and describes the meanings of the event and event qualifier values used in the reports.	
2-4	General Summary	RACFRW GENSUM
2-5	Listing of Status Records	LIST (see Note 1)
2-6	Listing of Process Records	LIST (see Note 1)
2-7	Short User Summary	SUMMARY USER
2-8	Short Group Summary	SUMMARY GROUP
2-9	Short Resource Summary	SUMMARY RESOURCE
2-10	Short Command Summary	SUMMARY COMMAND
2-11	Short Event Summary	SUMMARY EVENT
2-12	Short Owner Summary	SUMMARY OWNER
2-13	User by Resource Summary	SUMMARY USER BY(RESOURCE)
2-14	Group by Resource Summary	SUMMARY GROUP BY(RESOURCE)
2-15	Resource by User Summary	SUMMARY RESOURCE BY(USER)
2-16	Resource by Group Summary	SUMMARY RESOURCE BY(GROUP)
2-17	Resource by Event Summary	SUMMARY RESOURCE BY(EVENT)
2-18	Event by Resource Summary	SUMMARY EVENT BY(RESOURCE)
2-19	Command by User Summary	SUMMARY COMMAND BY(USER)
2-20	Command by Group Summary	SUMMARY COMMAND BY(GROUP)
2-21	Command by Resource Summary	SUMMARY COMMAND BY(RESOURCE)
2-22	Owner by Resource Summary	SUMMARY OWNER BY(RESOURCE)

Note: A single LIST subcommand produces both the listing of status records and the listing of process records.

```
84.062 10:16:44                                    RACF REPORT                                    PAGE   1

COMMAND GROUP ENTERED -
RACFRW DSN('VEND000.RACF14.SMFORMAT') NOFORMAT GENSUM
SUM USER
SUM GROUP
SUM RESOURCE
SUM COMMAND
SUM EVENT
SUM OWNER
SUM USER BY(RESOURCE)
SUM GROUP BY(RESOURCE)
SUM RESOURCE BY(USER)
SUM RESOURCE BY(GROUP)
SUM RESOURCE BY(EVENT)
SUM EVENT BY(RESOURCE)
SUM COMMAND BY(USER)
SUM COMMAND BY(GROUP)
SUM COMMAND BY(RESOURCE
 SUM OWNER BY(RESOURCE)
LIST
END


EVENT/QUALIFIER KEY ------

   EVENT  QUALIFIER  MEANING

     1               JOB INITIATION / TSO LOGON
              0       SUCCESSFUL INITIATION
              1       INVALID PASSWORD
              2       INVALID GROUP
              3       INVALID OIDCARD
              4       INVALID TERMINAL
              5       INVALID APPLICATION
              6       REVOKED USERID ATTEMPTING ACCESS
              7       USERID AUTOMATICALLY REVOKED

     2               RESOURCE ACCESS
              0       SUCCESSFUL ACCESS
              1       INSUFFICIENT AUTHORITY
              2       PROFILE NOT FOUND
              3       ACCESS PERMITTED DUE TO WARNING

     3               ADDVOL/CHGVOL
              0       SUCCESSFUL PROCESSING OF NEW VOLUME
              1       INSUFFICIENT AUTHORITY

     4               RENAME DATASET
              0       SUCCESSFUL RENAME
              1       INVALID GROUP
              2       USER NOT IN GROUP
              3       INSUFFICIENT AUTHORITY
              4       DATASET NAME ALREADY DEFINED
              5       USER NOT DEFINED TO RACF

     5               DELETE RESOURCE
              0       SUCCESSFUL SCRATCH
              1       RESOURCE NOT FOUND
              2       INVALID VOLUME

     6               DELETE ONE VOLUME OF A MULTIVOLUME RESOURCE
              0       SUCCESSFUL DELETION

     7               DEFINE RESOURCE
              0       SUCCESSFUL DEFINITION
              1       GROUP UNDEFINED
              2       USER NOT IN GROUP
              3       INSUFFICIENT AUTHORITY
              4       RESOURCE NAME ALREADY DEFINED
              5       USER NOT DEFINED TO RACF

     8               ADDSD COMMAND
     9               ADDGROUP COMMAND
    10               ADDUSER COMMAND
    11               ALTDSD COMMAND
    12               ALTGROUP COMMAND
    13               ALTUSER COMMAND
    14               CONNECT COMMAND
    15               DELDSD COMMAND
    16               DELGROUP COMMAND
    17               DELUSER COMMAND
    18               PASSWORD COMMAND
    19               PERMIT COMMAND
    20               RALTER COMMAND
    21               RDEFINE COMMAND
    22               RDELETE COMMAND
    23               REMOVE COMMAND
    24               SETROPTS COMMAND
    25               RVARY COMMAND
              0       NO VIOLATIONS DETECTED
              1       INSUFFICIENT AUTHORITY
              2       KEYWORD VIOLATIONS DETECTED


REPORT KEY ------
  .AN '*' PREFIXED TO A USER OR GROUP NAME INDICATES THE NAME IS ACTUALLY A JOB OR STEP NAME, RESPECTIVELY
  .THE PHRASE 'UNDEFINED USER' REFERS TO THOSE TSO LOGONS WHICH SPECIFIED USERIDS THAT WERE NOT DEFINED TO RACF,
   AND TO BATCH JOBS WHICH DID NOT SPECIFY THE 'USER=' OPERAND ON THEIR JOB STATEMENTS
  .A '+' PREFIXED TO A RESOURCE NAME INDICATES THAT A GENERIC PROFILE WAS ACCESSED
  .A '(G)' APPENDED TO A RESOURCE NAME MEANS THAT THE RESOURCE NAME IS GENERIC
```

Figure 2-3. Standard Header Page

```
84.062 10:16:44                    RACF REPORT - GENERAL SUMMARY                    PAGE   3

                                                      READ     SELECTED    %-SELECTED

STATUS RECORDS                                          31           31      100 %
PROCESS RECORDS                                        145          145      100 %
TOTAL PROCESS RECORDS FOR DEFINED USERS                145          145      100 % (OF ALL PROCESS RECORDS)
TOTAL PROCESS RECORDS FOR UNDEFINED USERS                0            0        0 % (OF ALL PROCESS RECORDS)

                                        --- JOB / LOGON  STATISTICS ---

TOTAL JOB/LOGON ATTEMPTS                                 6
TOTAL JOB/LOGON SUCCESSES                                0                      0 % OF TOTAL ATTEMPTS
TOTAL JOB/LOGON VIOLATIONS                               6                    100 % OF TOTAL ATTEMPTS
TOTAL JOB/LOGON ATTEMPTS BY UNDEFINED USERS              0                      0 % OF TOTAL ATTEMPTS
TOTAL JOB/LOGON SUCCESSES BY UNDEFINED USERS             0                      0 % OF TOTAL ATTEMPTS
TOTAL JOB/LOGON VIOLATIONS BY UNDEFINED USERS            0                      0 % OF TOTAL ATTEMPTS
JOB/LOGON VIOLATIONS BY HOUR -

          0-1         1-2         2-3         3-4         4-5         5-6         6-7         7-8
            0           0           0           0           0           0           0           0

          8-9         9-10       10-11       11-12       12-13       13-14       14-15       15-16
            0           6           0           0           0           0           0           0

        16-17       17-18       18-19       19-20       20-21       21-22       22-23       23-24
            0           0           0           0           0           0           0           0

                                        --- RESOURCE  STATISTICS ---

TOTAL RESOURCE ACCESSES (ALL EVENTS)                    59
TOTAL RESOURCE ACCESS SUCCESSES                         58                     98 % OF TOTAL ACCESSES
TOTAL RESOURCE ACCESS WARNINGS                           0                      0 % OF TOTAL ACCESSES
TOTAL RESOURCE ACCESS VIOLATIONS                         1                      2 % OF TOTAL ACCESSES
TOTAL RESOURCE ACCESSES (ALL EVENTS) BY UNDEFINED USERS  0                      0 % OF TOTAL ACCESSES
TOTAL RESOURCE ACCESS SUCCESSES BY UNDEFINED USERS       0                      0 % OF TOTAL ACCESSES
TOTAL RESOURCE ACCESS WARNINGS BY UNDEFINED USERS        0                      0 % OF TOTAL ACCESSES
TOTAL RESOURCE ACCESS VIOLATIONS BY UNDEFINED USERS      0                      0 % OF TOTAL ACCESSES
TOTAL RESOURCE ACCESSES USING GENERIC PROFILE            0                      0 % OF TOTAL ACCESSES
TOTAL RESOURCE ACCESS SUCCESSES USING GENERIC PROFILE    0                      0 % OF TOTAL ACCESSES
TOTAL RESOURCE ACCESS WARNINGS USING GENERIC PROFILE     0                      0 % OF TOTAL ACCESSES
TOTAL RESOURCE ACCESS VIOLATIONS USING GENERIC PROFILE   0                      0 % OF TOTAL ACCESSES
RESOURCE ACCESS VIOLATIONS BY HOUR -

          0-1         1-2         2-3         3-4         4-5         5-6         6-7         7-8
            0           0           0           0           0           0           0           1

          8-9         9-10       10-11       11-12       12-13       13-14       14-15       15-16
            0           0           0           0           0           0           0           0

        16-17       17-18       18-19       19-20       20-21       21-22       22-23       23-24
            0           0           0           0           0           0           0           0
```

Figure 2-4. General Summary Report

```
84.062 10:16:44                          RACF REPORT - LISTING OF STATUS RECORDS                          PAGE    4

                                                ACTIVE
DATE    TIME      SYSID MISC. OPTIONS           EXITS     CLASS    PROT STAT AUD GEN GCMD GLBL

81.251 07:49:25 MVS1  ORIGIN:    SETROPTS                 DATASET  YES  YES  YES
                      TERMUACC:  READ                     USER                YES
                      CMNDVIOL:  YES                      GROUP               YES
                      LOGSPEC:   YES                      DASDVOL  YES  YES  YES
                      RACINIT:   STATS                    TAPEVOL  YES  YES  YES
                      ADSP:      ACTIVE                   TERMINAL YES  YES  YES
                      REALDSN:   NO                       APPL     YES  YES  YES
                      JES:                                TIMS     YES  YES  YES
                        NOBATCHALLRACF                    GIMS     YES  YES  YES
                        NOXBMALLRACF                      AIMS     YES  YES  YES
                        NOEARLYVERIFY                     TCICSTRN YES  YES  YES
                                                          GCICSTRN YES  YES  YES
                                                          PCICSPSB YES  YES  YES
                                                          QCICSPSB YES  YES  YES
                                                          FLDM     YES  YES  YES
                                                          FLDG     YES  YES  YES
                                                          RSCM     YES  YES  YES

                                                ACTIVE
DATE    TIME      SYSID MISC. OPTIONS           EXITS     CLASS    PROT STAT AUD GEN GCMD GLBL

81.251 07:58:28 MVS1  ORIGIN:    IPL            ICHRIX01
                      TERMUACC:  READ           ICHRIX02
                      CMNDVIOL:  YES            ICHRCX01
                      LOGSPEC:   YES            ICHRCX02
                      RACINIT:   STATS          ICHRDX01
                      ADSP:      ACTIVE         ICHCCX00
                      REALDSN:   NO
                      JES:
                        NOBATCHALLRACF
                        NOXBMALLRACF
                        NOEARLYVERIFY
                      DUPDS:     NO

                                                TYPE     STATUS   SEQ  UNIT VOLUME DATASET NAME

                                                UADS                          MVSVM1 SYS1.UADS
                                                PRIMARY  ACTIVE     1  260  MVSVM1 SYSINV.I0
                                                BACKUP   INACTIVE   1  260  MVSVM1 SYSINV.I0BACK
                                                PRIMARY  ACTIVE     2  260  MVSVM1 SYSINV.I1
                                                BACKUP   INACTIVE   2  260  MVSVM1 SYSINV.I1BACK

                                                OTHER OPTIONS -

                                                  USER MODELLING IS ACTIVE

                                                  INTERVAL:   30 DAYS
                                                  HISTORY:  NONE
                                                  REVOKE:      5 TRIES
                                                  WARNING:    40 DAYS
                                                  INACTIVE:  212 DAYS

                                                  RULE  1   LENGTH(4:5)   LLLLL
                                                  RULE  2   LENGTH(5:5)   AAAAA
                                                  RULE  3   LENGTH(6:8)   LLLLLLLL
                                                  RULE  4   LENGTH(6:8)   AAAAAAAA
                                                  RULE  5   LENGTH(6:8)   NNNNNNNN
```

Figure 2-5. Listing of Status Records

```
84.062 10:16:44                           RACF REPORT - LISTING OF PROCESS RECORDS                                        PAGE  16

                                                            E
                                                            V  Q
                                                            E  U
                           *JOB/      *STEP/     --TERMINAL--  N  A
 DATE     TIME    SYSID   USER       GROUP          ID     LVL  T  L

81.251 07:48:01 MVS1    WORLEY     SYSSDEV                  0  9  0  JOBID=(ADDGROUP 81.251 07:47:49),USERDATA=(),OWNER=
                                                                     AUTH=(SPECIAL),REASON=(CLASS,SPECIAL)
                                                                       ADDGROUP TESTGRP SUPGROUP(SYS1) OWNER(WORLEY) TERMUACC

81.251 07:48:04 MVS1    WORLEY     SYSSDEV                  0 16  0  JOBID=(ADDGROUP 81.251 07:47:49),USERDATA=(),OWNER=
                                                                     AUTH=(SPECIAL),REASON=(CLASS,SPECIAL)
                                                                       DELGROUP TESTGRP

81.251 07:48:05 MVS1    WORLEY     SYSSDEV                  0  9  0  JOBID=(ADDGROUP 81.251 07:47:49),USERDATA=(),OWNER=
                                                                     AUTH=(SPECIAL),REASON=(CLASS,SPECIAL)
                                                                       ADDGROUP TESTGRP SUPGROUP(SYS1) OWNER(WORLEY) TERMUACC MODEL()

81.251 07:48:09 MVS1    WORLEY     SYSSDEV                  0 16  0  JOBID=(ADDGROUP 81.251 07:47:49),USERDATA=(),OWNER=
                                                                     AUTH=(SPECIAL),REASON=(CLASS,SPECIAL)
                                                                       DELGROUP TESTGRP

81.251 07:48:44 MVS1    WORLEY     SYS1                     0 10  0  JOBID=(ADDUSER 81.251 07:48:35),USERDATA=(),OWNER=
                                                                     AUTH=(NORMAL),REASON=(CLASS)
                                                                       ADDUSER TESTUSR DFLTGRP(SYS1) PASSWORD(****) NAME('TEST USER')
                                                                       AUTHORITY(USE) NOGRPACC UACC(NONE) NOADSP OWNER(WORLEY) NOSPECIAL
                                                                       NOOPERATIONS NOCLAUTH() NOAUDITOR NOOIDCARD

81.251 07:48:45 MVS1    WORLEY     SYS1                     0 13  0  JOBID=(ADDUSER 81.251 07:48:35),USERDATA=(),OWNER=
                                                                     AUTH=(NORMAL),REASON=(CLASS)
                                                                       ALTUSER TESTUSR MODEL()

81.251 07:48:46 MVS1    WORLEY     SYS1                     0 13  0  JOBID=(ADDUSER 81.251 07:48:35),USERDATA=(),OWNER=
                                                                     AUTH=(NORMAL),REASON=(CLASS)
                                                                       ALTUSER TESTUSR NOMODEL

81.251 07:48:48 MVS1    WORLEY     SYS1                     0 17  0  JOBID=(ADDUSER 81.251 07:48:35),USERDATA=(),OWNER=
                                                                     AUTH=(NORMAL),REASON=(CLASS)
                                                                       DELUSER TESTUSR

81.251 07:48:49 MVS1    WORLEY     SYS1                     0 10  0  JOBID=(ADDUSER 81.251 07:48:35),USERDATA=(),OWNER=
                                                                     AUTH=(NORMAL),REASON=(CLASS)
                                                                       ADDUSER TESTUSR DFLTGRP(SYS1) PASSWORD(****) NAME('TEST USER')
                                                                       AUTHORITY(USE) NOGRPACC UACC(NONE) NOADSP OWNER(WORLEY) NOSPECIAL
                                                                       NOOPERATIONS NOCLAUTH() NOAUDITOR NOOIDCARD

81.251 07:48:50 MVS1    WORLEY     SYS1                     0 13  0  JOBID=(ADDUSER 81.251 07:48:35),USERDATA=(),OWNER=
                                                                     AUTH=(NORMAL),REASON=(CLASS)
                                                                       ALTUSER TESTUSR DATA('')

81.251 07:48:51 MVS1    WORLEY     SYS1                     0 17  0  JOBID=(ADDUSER 81.251 07:48:35),USERDATA=(),OWNER=
                                                                     AUTH=(NORMAL),REASON=(CLASS)
                                                                       DELUSER TESTUSR

81.251 07:48:52 MVS1    WORLEY     SYS1                     0 10  0  JOBID=(ADDUSER 81.251 07:48:35),USERDATA=(),OWNER=
                                                                     AUTH=(NORMAL),REASON=(CLASS)
                                                                       ADDUSER TESTUSR DFLTGRP(SYS1) PASSWORD(****) NAME('TEST USER')
                                                                       AUTHORITY(USE) DATA('1111111111111111111111111111111111111111111111111
```

Figure 2-6. Listing of Process Records

84.062 10:16:44 RACF REPORT - SHORT USER SUMMARY PAGE 29

USER/ *JOB	JOB/LOGON SUCCESS	JOB/LOGON VIOLATION	RESOURCE STATISTICS SUCCESS	WARNING	VIOLATION	INTENTS ALTER	CONTROL	UPDATE	READ	TOTAL
TESTUSR	0	0	2	0	1	1	0	0	1	3
TESTUS1	0	6	16	0	0	8	0	0	0	16
WORLEY	0	0	40	0	0	27	0	0	0	40
ACCUMULATED TOTALS -	0	6	58	0	1	36	0	0	1	59
PERCENTAGE OF TOTAL ACCESSES -			98 %	0 %	2 %	61 %	0 %	0 %	2 %	
UNDEFINED USERS (JOBS) ONLY										
ACCUMULATED TOTALS -	0	0	0	0	0	0	0	0	0	0
PERCENTAGE OF TOTAL ACCESSES -			0 %	0 %	0 %	0 %	0 %	0 %	0 %	

Figure 2-7. Short User Summary Report

84.062 10:16:44 RACF REPORT - SHORT GROUP SUMMARY PAGE 30

GROUP/ *STEP	JOB/LOGON SUCCESS	JOB/LOGON VIOLATION	RESOURCE STATISTICS SUCCESS	WARNING	VIOLATION	INTENTS ALTER	CONTROL	UPDATE	READ	TOTAL
SYSSDEV	0	0	20	0	0	11	0	0	0	20
SYS1	0	6	28	0	0	20	0	0	0	28
TESTGRP	0	0	10	0	0	5	0	0	0	10
TESTGRP1	0	0	0	0	1	0	0	0	1	1
ACCUMULATED TOTALS -	0	6	58	0	1	36	0	0	1	59
PERCENTAGE OF TOTAL ACCESSES -			98 %	0 %	2 %	61 %	0 %	0 %	2 %	
UNDEFINED USERS (JOBS) ONLY										
ACCUMULATED TOTALS -	0	0	0	0	0	0	0	0	0	0
PERCENTAGE OF TOTAL ACCESSES -			0 %	0 %	0 %	0 %	0 %	0 %	0 %	

Figure 2-8. Short Group Summary Report

84.062 10:16:44 RACF REPORT - SHORT RESOURCE SUMMARY PAGE 31

RESOURCE NAME	SUCCESS	WARNING	VIOLATION	INTENTS ALTER	INTENTS CONTROL	INTENTS UPDATE	INTENTS READ	TOTAL
CLASS = DASDVOL								
111111	12	0	0	12	0	0	0	12
CLASS = DATASET								
SYS1.PARMLIB	2	0	0	2	0	0	0	2
TESTGRP.GRPLIST.PROFILE	4	0	1	2	0	0	1	5
TESTGRP.MODEL.PROFILE	9	0	0	6	0	0	0	9
TESTGRP.MODEL.TEST.DS.PROFILE	2	0	0	0	0	0	0	2
TESTUS1.MODEL.PROFILE	6	0	0	4	0	0	0	6
TESTUS1.MODEL.TEST.DS.PROFILE	2	0	0	0	0	0	0	2
WORLEY.EXEC.RACF.CLIST	1	0	0	0	0	0	0	1
WORLEY.LDAD.TEST.DATASET	2	0	0	0	0	0	0	2
WORLEY.SR.MODEL1	4	0	0	2	0	0	0	4
WORLEY.SR.MODEL2	4	0	0	2	0	0	0	4
WORLEY.SR.MODEL3	4	0	0	2	0	0	0	4
WORLEY.TEST.PROFILE	6	0	0	4	0	0	0	6
ACCUMULATED TOTALS -	58	0	1	36	0	0	1	59
PERCENTAGE OF TOTAL ACCESSES -	98 %	0 %	2 %	61 %	0 %	0 %	2 %	
GENERIC PROFILE USED								
ACCUMULATED TOTALS -	0	0	0	0	0	0	0	0
PERCENTAGE OF TOTAL ACCESSES -	0 %	0 %	0 %	0 %	0 %	0 %	0 %	

Figure 2-9. Short Resource Summary Report

```
84.062 10:16:44                    RACF REPORT - SHORT COMMAND SUMMARY                    PAGE  32

                        QUALIFIER                    OCCURRENCES

EVENT = 8 - ADDSD COMMAND
            0 - NO VIOLATIONS DETECTED                      6

            ACCUMULATED TOTALS -                            6

EVENT = 9 - ADDGROUP COMMAND
            0 - NO VIOLATIONS DETECTED                      7

            ACCUMULATED TOTALS -                            7

EVENT = 10 - ADDUSER COMMAND
            0 - NO VIOLATIONS DETECTED                     10

            ACCUMULATED TOTALS -                           10

EVENT = 11 - ALTDSD COMMAND
            0 - NO VIOLATIONS DETECTED                      6

            ACCUMULATED TOTALS -                            6

EVENT = 13 - ALTUSER COMMAND
            0 - NO VIOLATIONS DETECTED                      8

            ACCUMULATED TOTALS -                            8

EVENT = 14 - CONNECT COMMAND
            0 - NO VIOLATIONS DETECTED                      2

            ACCUMULATED TOTALS -                            2

EVENT = 15 - DELDSD COMMAND
            0 - NO VIOLATIONS DETECTED                      7

            ACCUMULATED TOTALS -                            7

EVENT = 16 - DELGROUP COMMAND
            0 - NO VIOLATIONS DETECTED                      8

            ACCUMULATED TOTALS -                            8

EVENT = 17 - DELUSER COMMAND
            0 - NO VIOLATIONS DETECTED                     11

            ACCUMULATED TOTALS -                           11

EVENT = 18 - PASSWORD COMMAND
            0 - NO VIOLATIONS DETECTED                      2
            1 - INSUFFICIENT AUTHORITY                      1

            ACCUMULATED TOTALS -                            3

EVENT = 19 - PERMIT COMMAND
            0 - NO VIOLATIONS DETECTED                      5

            ACCUMULATED TOTALS -                            5
```

Figure 2-10. Short Command Summary Report

```
84.062 10:16:44                    RACF REPORT - SHORT EVENT SUMMARY                    PAGE  34

                          QUALIFIER                OCCURRENCES

EVENT = 1 - JOB INITIATION / TSO LOGON
            1 - INVALID PASSWORD                          6

            ACCUMULATED TOTALS -                          6

EVENT = 2 - RESOURCE ACCESS
            1 - INSUFFICIENT AUTHORITY                    1

            ACCUMULATED TOTALS -                          1

EVENT = 5 - DELETE RESOURCE
            0 - SUCCESSFUL SCRATCH                       12

            ACCUMULATED TOTALS -                         12

EVENT = 7 - DEFINE RESOURCE
            0 - SUCCESSFUL DEFINITION                    10

            ACCUMULATED TOTALS -                         10

EVENT = 8 - ADDSD COMMAND
            0 - NO VIOLATIONS DETECTED                    6

            ACCUMULATED TOTALS -                          6

EVENT = 9 - ADDGROUP COMMAND
            0 - NO VIOLATIONS DETECTED                    7

            ACCUMULATED TOTALS -                          7

EVENT = 10 - ADDUSER COMMAND
            0 - NO VIOLATIONS DETECTED                   10

            ACCUMULATED TOTALS -                         10

EVENT = 20 - RALTER COMMAND
            0 - NO VIOLATIONS DETECTED                    8

            ACCUMULATED TOTALS -                          8

EVENT = 21 - RDEFINE COMMAND
            0 - NO VIOLATIONS DETECTED                    2

            ACCUMULATED TOTALS -                          2

EVENT = 22 - RDELETE COMMAND
            0 - NO VIOLATIONS DETECTED                    2

            ACCUMULATED TOTALS -                          2

EVENT = 23 - REMOVE COMMAND
            0 - NO VIOLATIONS DETECTED                    1

            ACCUMULATED TOTALS -                          1

EVENT = 24 - SETROPTS COMMAND
            0 - NO VIOLATIONS DETECTED                   30

            ACCUMULATED TOTALS -                         30

          ACCUMULATED TOTALS -                          145
```

Figure 2-11. Short Event Summary Report

84.062 10:16:44 RACF REPORT - SHORT OWNER SUMMARY PAGE 36

OWNER	SUCCESS	WARNING	VIOLATION	INTENTS ALTER	CONTROL	UPDATE	READ	TOTAL
	58	0	1	36	0	0	1	59
JONES	12	0	0	8	0	0	0	12
BELDING	8	0	0	4	0	0	0	8
ACCUMULATED TOTALS -	78	0	1	48	0	0	1	79
PERCENTAGE OF TOTAL ACCESSES -	99%	0%	1%	61%	0%	0%	1%	

Figure 2-12. Short Owner Summary Report

RESOURCE NAME	SUCCESS	WARNING	VIOLATION	INTENTS ALTER	INTENTS CONTROL	INTENTS UPDATE	INTENTS READ	TOTAL
USER = TESTUSR								
CLASS = DATASET								
TESTGRP.GRPLIST.PROFILE	2	0	1	1	0	0	1	3
ACCUMULATED TOTALS -	2	0	1	1	0	0	1	3
PERCENTAGE OF TOTAL ACCESSES -	67 %	0 %	33 %	33 %	0 %	0 %	33 %	
GENERIC PROFILE USED								
ACCUMULATED TOTALS -	0	0	0	0	0	0	0	0
PERCENTAGE OF TOTAL ACCESSES -	0 %	0 %	0 %	0 %	0 %	0 %	0 %	
USER = TESTUS1								
CLASS = DATASET								
TESTGRP.MODEL.PROFILE	6	0	0	4	0	0	0	6
TESTGRP.MODEL.TEST.DS.PROFILE	2	0	0	0	0	0	0	2
TESTUS1.MODEL.PROFILE	6	0	0	4	0	0	0	6
TESTUS1.MODEL.TEST.DS.PROFILE	2	0	0	0	0	0	0	2
ACCUMULATED TOTALS -	16	0	0	8	0	0	0	16
PERCENTAGE OF TOTAL ACCESSES -	100 %	0 %	0 %	50 %	0 %	0 %	0 %	
GENERIC PROFILE USED								
ACCUMULATED TOTALS -	0	0	0	0	0	0	0	0
PERCENTAGE OF TOTAL ACCESSES -	0 %	0 %	0 %	0 %	0 %	0 %	0 %	
USER = WORLEY								
CLASS = DASDVOL								
111111	12	0	0	12	0	0	0	12
CLASS = DATASET								
SYS1.PARMLIB	2	0	0	2	0	0	0	2
TESTGRP.GRPLIST.PROFILE	2	0	0	1	0	0	0	2
TESTGRP.MODEL.PROFILE	3	0	0	2	0	0	0	3
WORLEY.EXEC.RACF.CLIST	1	0	0	0	0	0	0	1
WORLEY.LDAD.TEST.DATASET	2	0	0	0	0	0	0	2
WORLEY.SR.MODEL1	4	0	0	2	0	0	0	4
WORLEY.SR.MODEL2	4	0	0	2	0	0	0	4
WORLEY.SR.MODEL3	4	0	0	2	0	0	0	4
WORLEY.TEST.PROFILE	6	0	0	4	0	0	0	6
ACCUMULATED TOTALS -	40	0	0	27	0	0	0	40
PERCENTAGE OF TOTAL ACCESSES -	100 %	0 %	0 %	68 %	0 %	0 %	0 %	
GENERIC PROFILE USED								
ACCUMULATED TOTALS -	0	0	0	0	0	0	0	0
PERCENTAGE OF TOTAL ACCESSES -	0 %	0 %	0 %	0 %	0 %	0 %	0 %	

Figure 2-13. User by Resource Summary Report

84.062 10:16:44 RACF REPORT - GROUP BY RESOURCE SUMMARY PAGE 38

RESOURCE NAME	SUCCESS	WARNING	VIOLATION	INTENTS ALTER	INTENTS CONTROL	INTENTS UPDATE	INTENTS READ	TOTAL
GROUP = SYSSDEV								
CLASS = DATASET								
SYS1.PARMLIB	2	0	0	2	0	0	0	2
TESTGRP.GRPLIST.PROFILE	2	0	0	1	0	0	0	2
TESTGRP.MODEL.PROFILE	3	0	0	2	0	0	0	3
WORLEY.EXEC.RACF.CLIST	1	0	0	0	0	0	0	1
WORLEY.SR.MODEL1	4	0	0	2	0	0	0	4
WORLEY.SR.MODEL2	4	0	0	2	0	0	0	4
WORLEY.SR.MODEL3	4	0	0	2	0	0	0	4
ACCUMULATED TOTALS -	20	0	0	11	0	0	0	20
PERCENTAGE OF TOTAL ACCESSES -	100 %	0 %	0 %	55 %	0 %	0 %	0 %	
GENERIC PROFILE USED								
ACCUMULATED TOTALS -	0	0	0	0	0	0	0	0
PERCENTAGE OF TOTAL ACCESSES -	0 %	0 %	0 %	0 %	0 %	0 %	0 %	
GROUP = SYS1								
CLASS = DASDVOL								
111111	12	0	0	12	0	0	0	12
CLASS = DATASET								
TESTUS1.MODEL.PROFILE	6	0	0	4	0	0	0	6
TESTUS1.MODEL.TEST.DS.PROFILE	2	0	0	0	0	0	0	2
WORLEY.LDAD.TEST.DATASET	2	0	0	0	0	0	0	2
WORLEY.TEST.PROFILE	6	0	0	4	0	0	0	6
ACCUMULATED TOTALS -	28	0	0	20	0	0	0	28
PERCENTAGE OF TOTAL ACCESSES -	100 %	0 %	0 %	71 %	0 %	0 %	0 %	
GENERIC PROFILE USED								
ACCUMULATED TOTALS -	0	0	0	0	0	0	0	0
PERCENTAGE OF TOTAL ACCESSES -	0 %	0 %	0 %	0 %	0 %	0 %	0 %	
GROUP = TESTGRP								
CLASS = DATASET								
TESTGRP.GRPLIST.PROFILE	2	0	0	1	0	0	0	2
TESTGRP.MODEL.PROFILE	6	0	0	4	0	0	0	6
TESTGRP.MODEL.TEST.DS.PROFILE	2	0	0	0	0	0	0	2
ACCUMULATED TOTALS -	10	0	0	5	0	0	0	10
PERCENTAGE OF TOTAL ACCESSES -	100 %	0 %	0 %	50 %	0 %	0 %	0 %	
GENERIC PROFILE USED								
ACCUMULATED TOTALS -	0	0	0	0	0	0	0	0
PERCENTAGE OF TOTAL ACCESSES -	0 %	0 %	0 %	0 %	0 %	0 %	0 %	
GROUP = TESTGRP1								
CLASS = DATASET								
TESTGRP.GRPLIST.PROFILE	0	0	1	0	0	0	1	1
ACCUMULATED TOTALS -	0	0	1	0	0	0	1	1
PERCENTAGE OF TOTAL ACCESSES -	0 %	0 %	100 %	0 %	0 %	0 %	100 %	
GENERIC PROFILE USED								
ACCUMULATED TOTALS -	0	0	0	0	0	0	0	0
PERCENTAGE OF TOTAL ACCESSES -	0 %	0 %	0 %	0 %	0 %	0 %	0 %	

Figure 2-14. Group by Resource Summary Report

84.062 10:16:44 RACF REPORT - RESOURCE BY USER SUMMARY PAGE 40

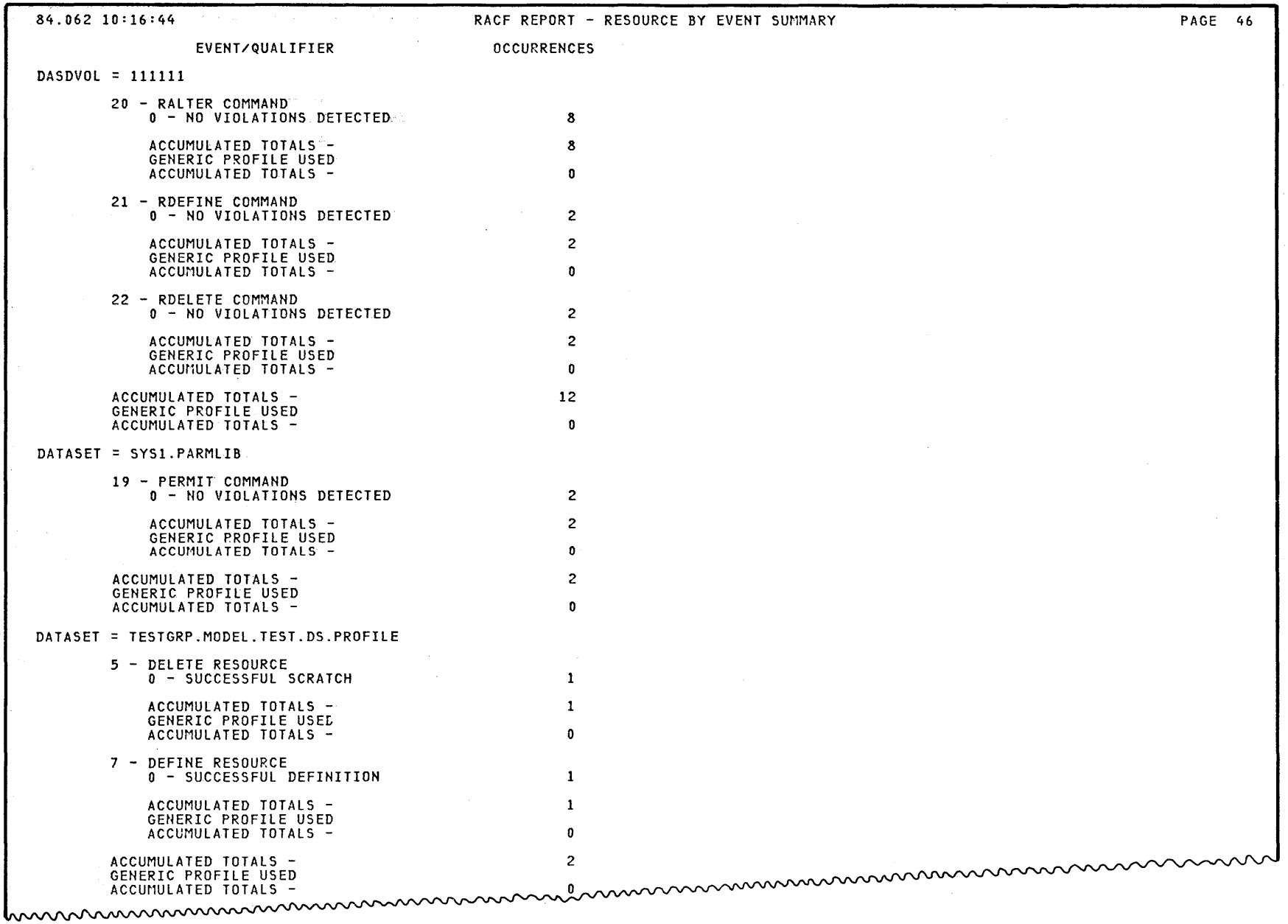
GROUP/ *STEP	SUCCESS	WARNING	VIOLATION	INTENTS ALTER	INTENTS CONTROL	INTENTS UPDATE	INTENTS READ	TOTAL
DASDVOL = 111111								
WORLEY	12	0	0	12	0	0	0	12
ACCUMULATED TOTALS -	12	0	0	12	0	0	0	12
PERCENTAGE OF TOTAL ACCESSES -	100 %	0 %	0 %	100 %	0 %	0 %	0 %	
UNDEFINED USERS (JOBS) ONLY								
ACCUMULATED TOTALS -	0	0	0	0	0	0	0	0
PERCENTAGE OF TOTAL ACCESSES -	0 %	0 %	0 %	0 %	0 %	0 %	0 %	
GENERIC PROFILE USED								
ACCUMULATED TOTALS -	0	0	0	0	0	0	0	0
PERCENTAGE OF TOTAL ACCESSES -	0 %	0 %	0 %	0 %	0 %	0 %	0 %	
DATASET = SYS1.PARMLIB								
WORLEY	2	0	0	2	0	0	0	2
ACCUMULATED TOTALS -	2	0	0	2	0	0	0	2
PERCENTAGE OF TOTAL ACCESSES -	100 %	0 %	0 %	100 %	0 %	0 %	0 %	
UNDEFINED USERS (JOBS) ONLY								
ACCUMULATED TOTALS -	0	0	0	0	0	0	0	0
PERCENTAGE OF TOTAL ACCESSES -	0 %	0 %	0 %	0 %	0 %	0 %	0 %	
GENERIC PROFILE USED								
ACCUMULATED TOTALS -	0	0	0	0	0	0	0	0
PERCENTAGE OF TOTAL ACCESSES -	0 %	0 %	0 %	0 %	0 %	0 %	0 %	
DATASET = TESTGRP.GRPLIST.PROFILE								
TESTUSR	2	0	1	1	0	0	1	3
WORLEY	2	0	0	1	0	0	0	2
ACCUMULATED TOTALS -	4	0	1	2	0	0	1	5
PERCENTAGE OF TOTAL ACCESSES -	80 %	0 %	20 %	40 %	0 %	0 %	20 %	
UNDEFINED USERS (JOBS) ONLY								
ACCUMULATED TOTALS -	0	0	0	0	0	0	0	0
PERCENTAGE OF TOTAL ACCESSES -	0 %	0 %	0 %	0 %	0 %	0 %	0 %	
GENERIC PROFILE USED								
ACCUMULATED TOTALS -	0	0	0	0	0	0	0	0
PERCENTAGE OF TOTAL ACCESSES -	0 %	0 %	0 %	0 %	0 %	0 %	0 %	
DATASET = TESTGRP.MODEL.PROFILE								
TESTUS1	6	0	0	4	0	0	0	6
WORLEY	3	0	0	2	0	0	0	3
ACCUMULATED TOTALS -	9	0	0	6	0	0	0	9
PERCENTAGE OF TOTAL ACCESSES -	100 %	0 %	0 %	67 %	0 %	0 %	0 %	
UNDEFINED USERS (JOBS) ONLY								
ACCUMULATED TOTALS -	0	0	0	0	0	0	0	0
PERCENTAGE OF TOTAL ACCESSES -	0 %	0 %	0 %	0 %	0 %	0 %	0 %	
GENERIC PROFILE USED								
ACCUMULATED TOTALS -	0	0	0	0	0	0	0	0
PERCENTAGE OF TOTAL ACCESSES -	0 %	0 %	0 %	0 %	0 %	0 %	0 %	

Figure 2-15. Resource by User Summary Report

84.062 10:16:44 RACF REPORT - RESOURCE BY GROUP SUMMARY PAGE 43

GROUP/ *STEP	SUCCESS	WARNING	VIOLATION	INTENTS ALTER	INTENTS CONTROL	INTENTS UPDATE	INTENTS READ	TOTAL
DASDVOL = 111111								
SYS1	12	0	0	12	0	0	0	12
ACCUMULATED TOTALS -	12	0	0	12	0	0	0	12
PERCENTAGE OF TOTAL ACCESSES -	100 %	0 %	0 %	100 %	0 %	0 %	0 %	
UNDEFINED USERS (JOBS) ONLY								
ACCUMULATED TOTALS -	0	0	0	0	0	0	0	0
PERCENTAGE OF TOTAL ACCESSES -	0 %	0 %	0 %	0 %	0 %	0 %	0 %	
GENERIC PROFILE USED								
ACCUMULATED TOTALS -	0	0	0	0	0	0	0	0
PERCENTAGE OF TOTAL ACCESSES -	0 %	0 %	0 %	0 %	0 %	0 %	0 %	
DATASET = SYS1.PARMLIB								
SYSSDEV	2	0	0	2	0	0	0	2
ACCUMULATED TOTALS -	2	0	0	2	0	0	0	2
PERCENTAGE OF TOTAL ACCESSES -	100 %	0 %	0 %	100 %	0 %	0 %	0 %	
UNDEFINED USERS (JOBS) ONLY								
ACCUMULATED TOTALS -	0	0	0	0	0	0	0	0
PERCENTAGE OF TOTAL ACCESSES -	0 %	0 %	0 %	0 %	0 %	0 %	0 %	
GENERIC PROFILE USED								
ACCUMULATED TOTALS -	0	0	0	0	0	0	0	0
PERCENTAGE OF TOTAL ACCESSES -	0 %	0 %	0 %	0 %	0 %	0 %	0 %	
DATASET = TESTGRP.GRPLIST.PROFILE								
SYSSDEV	2	0	0	1	0	0	0	2
TESTGRP	2	0	0	1	0	0	0	2
TESTGRP1	0	0	1	0	0	0	1	1
ACCUMULATED TOTALS -	4	0	1	2	0	0	1	5
PERCENTAGE OF TOTAL ACCESSES -	80 %	0 %	20 %	40 %	0 %	0 %	20 %	
UNDEFINED USERS (JOBS) ONLY								
ACCUMULATED TOTALS -	0	0	0	0	0	0	0	0
PERCENTAGE OF TOTAL ACCESSES -	0 %	0 %	0 %	0 %	0 %	0 %	0 %	
GENERIC PROFILE USED								
ACCUMULATED TOTALS -	0	0	0	0	0	0	0	0
PERCENTAGE OF TOTAL ACCESSES -	0 %	0 %	0 %	0 %	0 %	0 %	0 %	
DATASET = TESTGRP.MODEL.PROFILE								
SYSSDEV	3	0	0	2	0	0	0	3
TESTGRP	6	0	0	4	0	0	0	6
ACCUMULATED TOTALS -	9	0	0	6	0	0	0	9
PERCENTAGE OF TOTAL ACCESSES -	100 %	0 %	0 %	67 %	0 %	0 %	0 %	
UNDEFINED USERS (JOBS) ONLY								
ACCUMULATED TOTALS -	0	0	0	0	0	0	0	0
PERCENTAGE OF TOTAL ACCESSES -	0 %	0 %	0 %	0 %	0 %	0 %	0 %	
GENERIC PROFILE USED								
ACCUMULATED TOTALS -	0	0	0	0	0	0	0	0
PERCENTAGE OF TOTAL ACCESSES -	0 %	0 %	0 %	0 %	0 %	0 %	0 %	

Figure 2-16. Resource by Group Summary Report

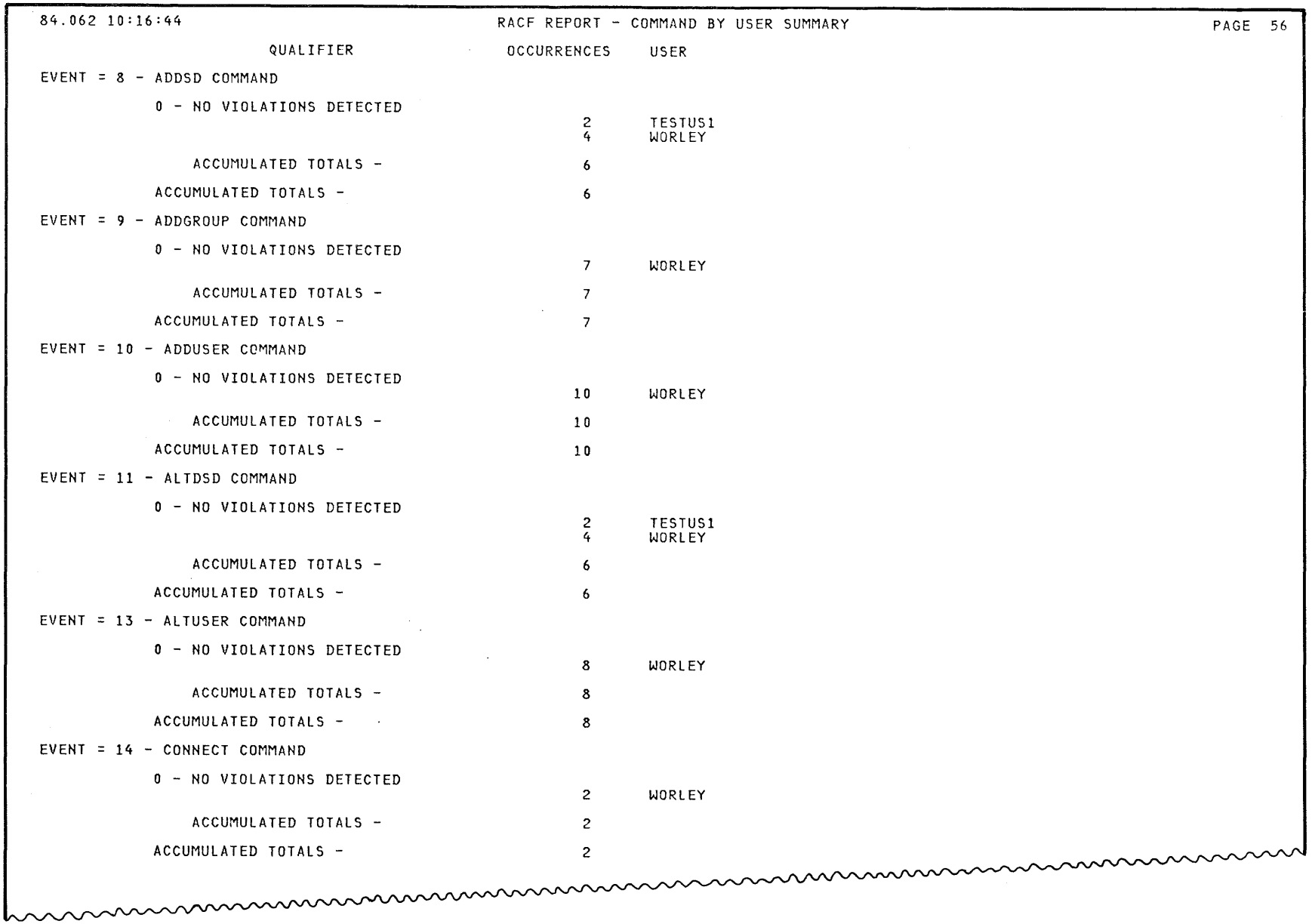


```
84.062 10:16:44                    RACF REPORT - RESOURCE BY EVENT SUMMARY                    PAGE  46

                EVENT/QUALIFIER                  OCCURRENCES

DASDVOL = 111111

        20 - RALTER COMMAND
            0 - NO VIOLATIONS DETECTED                  8

                ACCUMULATED TOTALS -                    8
                GENERIC PROFILE USED
                ACCUMULATED TOTALS -                    0

        21 - RDEFINE COMMAND
            0 - NO VIOLATIONS DETECTED                  2

                ACCUMULATED TOTALS -                    2
                GENERIC PROFILE USED
                ACCUMULATED TOTALS -                    0

        22 - RDELETE COMMAND
            0 - NO VIOLATIONS DETECTED                  2

                ACCUMULATED TOTALS -                    2
                GENERIC PROFILE USED
                ACCUMULATED TOTALS -                    0

        ACCUMULATED TOTALS -                           12
        GENERIC PROFILE USED
        ACCUMULATED TOTALS -                            0

DATASET = SYS1.PARMLIB

        19 - PERMIT COMMAND
            0 - NO VIOLATIONS DETECTED                  2

                ACCUMULATED TOTALS -                    2
                GENERIC PROFILE USED
                ACCUMULATED TOTALS -                    0

        ACCUMULATED TOTALS -                            2
        GENERIC PROFILE USED
        ACCUMULATED TOTALS -                            0

DATASET = TESTGRP.MODEL.TEST.DS.PROFILE

        5 - DELETE RESOURCE
            0 - SUCCESSFUL SCRATCH                      1

                ACCUMULATED TOTALS -                    1
                GENERIC PROFILE USED
                ACCUMULATED TOTALS -                    0

        7 - DEFINE RESOURCE
            0 - SUCCESSFUL DEFINITION                   1

                ACCUMULATED TOTALS -                    1
                GENERIC PROFILE USED
                ACCUMULATED TOTALS -                    0

        ACCUMULATED TOTALS -                            2
        GENERIC PROFILE USED
        ACCUMULATED TOTALS -                            0
```

Figure 2-17. Resource by Event Summary Report

```
84.062 10:16:44                    RACF REPORT - EVENT BY RESOURCE SUMMARY                    PAGE  53

                        QUALIFIER              OCCURRENCES    RESOURCE

EVENT = 2 - RESOURCE ACCESS

            1 - INSUFFICIENT AUTHORITY
                                                         1     DATASET  = TESTGRP.GRPLIST.PROFILE

                ACCUMULATED TOTALS -                     1
                GENERIC PROFILE USED
                ACCUMULATED TOTALS -                     0

            ACCUMULATED TOTALS -                         1
            GENERIC PROFILE USED
            ACCUMULATED TOTALS -                         0

EVENT = 5 - DELETE RESOURCE

            0 - SUCCESSFUL SCRATCH
                                                         1     DATASET  = TESTGRP.GRPLIST.PROFILE
                                                         2     DATASET  = TESTGRP.MODEL.PROFILE
                                                         1     DATASET  = TESTGRP.MODEL.TEST.DS.PROFILE
                                                         1     DATASET  = TESTUS1.MODEL.PROFILE
                                                         1     DATASET  = TESTUS1.MODEL.TEST.DS.PROFILE
                                                         1     DATASET  = WORLEY.EXEC.RACF.CLIST
                                                         1     DATASET  = WORLEY.LDAD.TEST.DATASET
                                                         1     DATASET  = WORLEY.SR.MODEL1
                                                         1     DATASET  = WORLEY.SR.MODEL2
                                                         1     DATASET  = WORLEY.SR.MODEL3
                                                         1     DATASET  = WORLEY.TEST.PROFILE

                ACCUMULATED TOTALS -                    12
                GENERIC PROFILE USED
                ACCUMULATED TOTALS -                     0

            ACCUMULATED TOTALS -                        12
            GENERIC PROFILE USED
            ACCUMULATED TOTALS -                         0

EVENT = 7 - DEFINE RESOURCE

            0 - SUCCESSFUL DEFINITION
                                                         1     DATASET  = TESTGRP.GRPLIST.PROFILE
                                                         1     DATASET  = TESTGRP.MODEL.PROFILE
                                                         1     DATASET  = TESTGRP.MODEL.TEST.DS.PROFILE
                                                         1     DATASET  = TESTUS1.MODEL.PROFILE
                                                         1     DATASET  = TESTUS1.MODEL.TEST.DS.PROFILE
                                                         1     DATASET  = WORLEY.LDAD.TEST.DATASET
                                                         1     DATASET  = WORLEY.SR.MODEL1
                                                         1     DATASET  = WORLEY.SR.MODEL2
                                                         1     DATASET  = WORLEY.SR.MODEL3
                                                         1     DATASET  = WORLEY.TEST.PROFILE

                ACCUMULATED TOTALS -                    10
                GENERIC PROFILE USED
                ACCUMULATED TOTALS -                     0

            ACCUMULATED TOTALS -                        10
            GENERIC PROFILE USED
```

Figure 2-18. Event by Resource Summary Report



```
84.062 10:16:44                    RACF REPORT - COMMAND BY USER SUMMARY                    PAGE  56

                    QUALIFIER                OCCURRENCES     USER

EVENT = 8 - ADDSD COMMAND

          0 - NO VIOLATIONS DETECTED
                                                   2         TESTUS1
                                                   4         WORLEY

              ACCUMULATED TOTALS -                 6

          ACCUMULATED TOTALS -                     6

EVENT = 9 - ADDGROUP COMMAND

          0 - NO VIOLATIONS DETECTED
                                                   7         WORLEY

              ACCUMULATED TOTALS -                 7

          ACCUMULATED TOTALS -                     7

EVENT = 10 - ADDUSER COMMAND

          0 - NO VIOLATIONS DETECTED
                                                  10         WORLEY

              ACCUMULATED TOTALS -                10

          ACCUMULATED TOTALS -                    10

EVENT = 11 - ALTDSD COMMAND

          0 - NO VIOLATIONS DETECTED
                                                   2         TESTUS1
                                                   4         WORLEY

              ACCUMULATED TOTALS -                 6

          ACCUMULATED TOTALS -                     6

EVENT = 13 - ALTUSER COMMAND

          0 - NO VIOLATIONS DETECTED
                                                   8         WORLEY

              ACCUMULATED TOTALS -                 8

          ACCUMULATED TOTALS -                     8

EVENT = 14 - CONNECT COMMAND

          0 - NO VIOLATIONS DETECTED
                                                   2         WORLEY

              ACCUMULATED TOTALS -                 2

          ACCUMULATED TOTALS -                     2
```

Figure 2-19. Command by User Summary Report

```
84.062 10:16:44                RACF REPORT - COMMAND BY GROUP SUMMARY                PAGE  59

                      QUALIFIER              OCCURRENCES    GROUP

EVENT = 8 - ADDSD COMMAND

            0 - NO VIOLATIONS DETECTED
                                                     3      SYSSDEV
                                                     2      SYS1
                                                     1      TESTGRP

                ACCUMULATED TOTALS -                 6

            ACCUMULATED TOTALS -                     6

EVENT = 9 - ADDGROUP COMMAND

            0 - NO VIOLATIONS DETECTED
                                                     7      SYSSDEV

                ACCUMULATED TOTALS -                 7

            ACCUMULATED TOTALS -                     7

EVENT = 10 - ADDUSER COMMAND

            0 - NO VIOLATIONS DETECTED
                                                     6      SYSSDEV
                                                     4      SYS1

                ACCUMULATED TOTALS -                10

            ACCUMULATED TOTALS -                    10

EVENT = 11 - ALTDSD COMMAND

            0 - NO VIOLATIONS DETECTED
                                                     2      SYSSDEV
                                                     3      SYS1
                                                     1      TESTGRP

                ACCUMULATED TOTALS -                 6

            ACCUMULATED TOTALS -                     6

EVENT = 13 - ALTUSER COMMAND

            0 - NO VIOLATIONS DETECTED
                                                     2      SYSSDEV
                                                     6      SYS1

                ACCUMULATED TOTALS -                 8

            ACCUMULATED TOTALS -                     8
```

Figure 2-20. Command by Group Summary Report

```
                    QUALIFIER              OCCURRENCES    RESOURCE

EVENT = 8 - ADDSD COMMAND

          0 - NO VIOLATIONS DETECTED
                                                 1       DATASET  = TESTGRP.MODEL.PROFILE
                                                 1       DATASET  = TESTUS1.MODEL.PROFILE
                                                 1       DATASET  = WORLEY.SR.MODEL1
                                                 1       DATASET  = WORLEY.SR.MODEL2
                                                 1       DATASET  = WORLEY.SR.MODEL3
                                                 1       DATASET  = WORLEY.TEST.PROFILE

              ACCUMULATED TOTALS -               6
              GENERIC PROFILE USED
              ACCUMULATED TOTALS -               0

          ACCUMULATED TOTALS -                   6
          GENERIC PROFILE USED
          ACCUMULATED TOTALS -                   0

EVENT = 11 - ALTDSD COMMAND

          0 - NO VIOLATIONS DETECTED
                                                 1       DATASET  = TESTGRP.GRPLIST.PROFILE
                                                 2       DATASET  = TESTGRP.MODEL.PROFILE
                                                 1       DATASET  = TESTUS1.MODEL.PROFILE
                                                 2       DATASET  = WORLEY.TEST.PROFILE

              ACCUMULATED TOTALS -               6
              GENERIC PROFILE USED
              ACCUMULATED TOTALS -               0

          ACCUMULATED TOTALS -                   6
          GENERIC PROFILE USED
          ACCUMULATED TOTALS -                   0

EVENT = 15 - DELDSD COMMAND

          0 - NO VIOLATIONS DETECTED
                                                 2       DATASET  = TESTGRP.MODEL.PROFILE
                                                 1       DATASET  = TESTUS1.MODEL.PROFILE
                                                 1       DATASET  = WORLEY.SR.MODEL1
                                                 1       DATASET  = WORLEY.SR.MODEL2
                                                 1       DATASET  = WORLEY.SR.MODEL3
                                                 1       DATASET  = WORLEY.TEST.PROFILE

              ACCUMULATED TOTALS -               7
              GENERIC PROFILE USED
              ACCUMULATED TOTALS -               0

          ACCUMULATED TOTALS -                   7
          GENERIC PROFILE USED
          ACCUMULATED TOTALS -                   0
```

Figure 2-21. Command by Resource Summary Report

84.062 10:16:44 RACF REPORT - OWNER BY RESOURCE SUMMARY PAGE 64

RESOURCE NAME	SUCCESS	WARNING	VIOLATION	INTENTS ALTER	INTENTS CONTROL	INTENTS UPDATE	INTENTS READ	TOTAL
OWNER =								
CLASS = DASDVOL								
111111	12	0	0	12	0	0	0	12
CLASS = DATASET								
SYS1.PARMLIB	2	0	0	2	0	0	0	2
TESTGRP.GRPLIST.PROFILE	4	0	1	2	0	0	1	5
TESTGRP.MODEL.PROFILE	9	0	0	6	0	0	0	9
TESTGRP.MODEL.TEST.DS.PROFILE	2	0	0	0	0	0	0	2
TESTUS1.MODEL.PROFILE	6	0	0	4	0	0	0	6
TESTUS1.MODEL.TEST.DS.PROFILE	2	0	0	0	0	0	0	2
WORLEY.EXEC.RACF.CLIST	1	0	0	0	0	0	0	1
WORLEY.LDAD.TEST.DATASET	2	0	0	0	0	0	0	2
WORLEY.SR.MODEL1	4	0	0	2	0	0	0	4
WORLEY.SR.MODEL2	4	0	0	2	0	0	0	4
WORLEY.SR.MODEL3	4	0	0	2	0	0	0	4
WORLEY.TEST.PROFILE	6	0	0	4	0	0	0	6
ACCUMULATED TOTALS -	58	0	1	36	0	0	1	59
PERCENTAGE OF TOTAL ACCESSES -	98 %	0 %	2 %	61 %	0 %	0 %	2 %	
GENERIC PROFILE USED								
ACCUMULATED TOTALS -	0	0	0	0	0	0	0	0
PERCENTAGE OF TOTAL ACCESSES -	0 %	0 %	0 %	0 %	0 %	0 %	0 %	

Figure 2-22. Owner by Resource Summary Report

Chapter 3. The Data Security Monitor (DSMON)

RACF enables you to protect resources, but the protection is only as good as the implementation. You need a way to verify that the security mechanisms actually in effect are the ones intended. DSMON helps provide this information.

DSMON is a program that produces reports on the status of the security environment at your installation and, in particular, on the status of resources that RACF controls. You can use the reports to audit the current status of your installation's system security environment by comparing the actual system characteristics and resource protection levels with the intended characteristics and levels.

DSMON produces the following reports:

- System report
- Program properties table report
- RACF authorized caller table report
- RACF exits report
- Selected user attribute report
- Selected user attribute summary report
- Selected data sets report

The information in these reports answers many of your audit questions. (See "Asking the Right Questions" in Chapter 1.)

How to Run DSMON

To run the data security monitor (DSMON), you must have the RACF AUDITOR user attribute. DSMON is an APF-authorized batch program that normally runs while RACF is active. If you run DSMON while RACF is inactive, DSMON produces only the system report.

The input to DSMON consists of the SYS1.PARMLIB data set; it does not include any user input. The output from DSMON consists of a message data set and an output data set for the reports.

The following example contains JCL (job control language) statements that you could use to invoke DSMON. The words that appear in lower case are parameters that you can change.

```
//stepname EXEC PGM=ICHDSM00
//SYSPRINT DD  sysout=a
//SYSUT1   DD  DSN=SYS1.PARMLIB,DISP=SHR
//SYSUT2   DD  sysout=a
```

SYSPRINT defines the sequential message data set (for example, SYSOUT), for status and error messages. SYSPRINT has a VB (variable blocked) format; block size, if specified, must be 137 (LRECL of 133 plus 4 for the block length) or greater.

SYSUT1 defines the SYS1.PARMLIB data set. Specifying DISP=SHR allows other programs to access SYS1.PARMLIB while DSMON is executing.

SYSUT2 defines the output listing data set (for example, SYSOUT) for the printed reports that DSMON generates. Block size, if specified, must be a multiple of 133.

Functions DSMON Uses

DSMON performs a number of functions to generate the reports. After completing each function (except the functions used to produce the system report), DSMON issues a message to SYSPRINT stating whether the function executed successfully or unsuccessfully.

If the function ended unsuccessfully, DSMON issues an error code that indicates the cause of the failure. In most cases, DSMON continues processing with the next function.

The function(s) used for each report and the information (or checks) each function provides are:

System report:

SYSCPU - identification number of the processor complex (CPU-ID)

SYSMDL - model number of the processor complex

SYSREL - name, version, and release number of the operating system

SYSRES - system residence volume

SYSSID - system identifier used by the system management facilities

SYSRAC - RACF version and release number and whether RACF is active

Program properties table report:

SYSPPT - all information

RACF authorized caller table report:

RACAUT - all information

RACF exits report:

RACEXT - all information

Selected user attribute reports:

RACUSR - all information

Selected data sets report:

SYSAPF - authorized program facility (APF) libraries

SYSLNK - LNKLSTxx data set members of the SYS1.PARMLIB library

SYSMCT - master catalog

RACDST - primary and backup RACF data sets

SYSSDS - the selected system data sets

System Report

The system report contains the identification number and model of the processor complex; the name, version, and release of the operating system; the serial number of the system residence volume; and the system-identifier (SMF-ID) that SMF uses. The report also specifies the RACF version and release number and whether RACF is active. If RACF is inactive, either because it was not activated at IPL or because it has been deactivated by the RVARY command, DSMON prints a message.

You can use the system report to verify that the system has the expected hardware and software. In addition, you can verify the status of RACF.

Note: DSMON always produces the system report. However, if RACF is not installed and active, or if RACF is active but the version and release are a level earlier than Version 1 Release 6, DSMON produces only the system report and terminates.

Column Headings

The report contains the following information:

CPU-ID
the identification number of the processor complex on which the system is running.

CPU MODEL
the model number of the processor complex.

OPERATING SYSTEM/LEVEL
the name and level number of the system control program (SCP). MVS/3.8 is the SCP on which MVS/System Product is built.

If the information is present in the CVT preface, this line also includes the version and release number of the operating system (for example SP1.3.3), the product FMID identifier for the operating system (for example, JBB1329), and the installation's personalized name.

SYSTEM RESIDENCE VOLUME
the serial number of the volume on which the system resides.

SMF-ID
the system identifier that the system management facilities (SMF) uses when creating log records.

Report Messages

The following messages might appear at the end of the report:

RACF VERSION n RELEASE m IS ACTIVE

Explanation: The specified version of RACF is active. In most cases, this is the message that appears on the report.

Note: If the version and release specified is a level of RACF earlier than Version 1 Release 6, DSMON produces a separate error message stating that the version is invalid and the program terminates.

RACF VERSION n RELEASE m IS INACTIVE

Explanation: The specified version of RACF was deactivated during initial program load (IPL).

Note: Under normal circumstances, this message should not appear. If it does, notify your RACF security administrator and/or installation manager.

RACF VERSION n RELEASE m HAS BEEN DEACTIVATED

Explanation: The specified version of RACF has been deactivated by the RVARY command; this situation is normally temporary.

RACF IS NOT INSTALLED

Explanation: DSMON cannot locate the RACF communications vector table (RCVT), indicating that RACF has not been installed.

Note: Under normal circumstances, this message should not appear. If it does, notify your RACF security administrator and/or installation manager.

RACF UNKNOWN VERSION

Explanation: DSMON retrieved a RACF version and release number from the RCVT that identifies a level of RACF that is earlier than RACF Version 1 Release 6.

Note: Under normal circumstances, this message should not appear. If it does, notify your RACF security administrator and/or installation manager.

```
RACF DATA SECURITY MONITOR                                    DATE: 02/22/84     TIME: 16:43:40     PAGE:    1

                                        S Y S T E M    R E P O R T

-------------------------------------------------------------------------------------------------------------------

CPU-ID                              010842
CPU MODEL                           3031
OPERATING SYSTEM/LEVEL              MVS/ 3.8   SP1.3.3 JBB1329
SYSTEM RESIDENCE VOLUME             DRV38X
SMF-ID                              WEE3
RACF VERSION 1 RELEASE 6 IS ACTIVE
```

Figure 3-1. Sample System Report

Program Properties Table Report

The program properties table report lists all the programs in the program properties table (PPT). The report also indicates whether each program is authorized to bypass password protection and whether it runs in a system key.

You can use the program properties table report to verify that only those programs that should be authorized to bypass password protection are, in fact, able to do so. (If a program has bypass password protection, RACF does not perform authorization checking for RACF-protected DASD data sets and tape volumes during system operations such as OPEN.) Such programs are normally communication and data base control programs, or other system control programs. You can also verify that only those programs that need to run in a system key are authorized to do so.

Column Headings

The report contains the following information:

PROGRAM NAME
the name of the program as defined in the PPT.

BYPASS PASSWORD PROTECTION
indicates whether the program is authorized to bypass password protection checking when accessing data sets that have password protection. The value is either YES or NO.

SYSTEM KEY
indicates whether the program is authorized to run in a system key (keys 0-7) and is thus able to bypass system integrity controls. The value is either YES or NO.

Report Messages

The following message might appear below the report column headings:

NO ENTRIES IN PROGRAM PROPERTIES TABLE

Explanation: There are no entries in the program properties table. This message does not indicate an abnormal condition unless you expect the PPT to contain entries.

RACF DATA SECURITY MONITOR DATE: 02/22/84 TIME: 16:43:40 PAGE: 3

PROGRAM PROPERTIES TABLE REPORT

PROGRAM NAME	BYPASS PASSWORD PROTECTION	SYSTEM KEY
MAMIRGSR	NO	YES
SMUTMODN	NO	NO
ITPENTER	YES	YES
AFFPGM01	NO	NO
AFFPGM02	NO	NO
AFFPGM03	NO	NO
AFFPGM04	NO	NO
AFFPGM05	NO	NO
CSVVFCRE	NO	YES
IFDOLT	YES	NO
CBFDISP	NO	NO
APSPPIEP	NO	YES
AKPCSIEP	NO	YES

Figure 3-2. Sample Program Properties Table Report

RACF Authorized Caller Table Report

The RACF authorized caller table report lists the names of all programs in the RACF authorized-caller table. The report also indicates whether each program is authorized to issue the RACINIT SVC (which performs user verification) and the RACLIST SVC (which loads profiles into main storage).

You can use this report to verify that only those programs that need to be authorized to modify an ACEE (access control environment element) are able to issue a RACINIT SVC. This verification is a particularly important security requirement because the ACEE contains a description of the current user. This description includes the userid, the current connect group, the user attributes, and the group authorities. A program that is authorized to issue the RACINIT SVC could alter the ACEE to simulate any userid.

You can also use the report to verify that only those programs that are supposed to be authorized to access any resident profile on the RACF data set are able to issue the RACLIST SVC. Because profiles contain complete descriptions of the characteristics associated with RACF-defined entities, you must carefully control access to them.

Column Headings

The report contains the following information:

MODULE NAME
the name of the program module as it is defined in the RACF authorized caller table.

RACINIT AUTHORIZED
indicates whether the module is authorized to issue a RACINIT SVC. The value is either YES or NO.

RACLIST AUTHORIZED
indicates whether the module is authorized to issue a RACLIST SVC. The value is either YES or NO.

Report Messages

The following message might appear below the report column headings:

NO ENTRIES IN RACF AUTHORIZED CALLER TABLE

Explanation: There are no entries in the RACF authorized-caller table. This message does not indicate an error condition. When RACF is initially installed, for example, the RACF authorized-caller table normally contains no entries.

```
RACF DATA SECURITY MONITOR                                    DATE: 02/22/84     TIME: 16:43:40     PAGE:    4

                          R A C F    A U T H O R I Z E D    C A L L E R    T A B L E    R E P O R T

MODULE                    RACINIT          RACLIST
NAME                      AUTHORIZED       AUTHORIZED
-------------------------------------------------------------------------------------------------------------------

DS1OSTXX                  YES              NO

DS1OST01                  NO               YES
```

Figure 3-3. Sample RACF Authorized Caller Table Report

RACF Exits Report

The RACF exits report lists the names of all the installation-defined RACF exit routines and specifies the size of each exit routine module. DSMON prints an error message if (1) the RACF communications vector table (RCVT), which contains the address of each RACF exit routine module, indicates that an exit routine module should exist but the module cannot be loaded, or (2) the entry address does not correspond with the address specified in the RCVT.

You can use this report to verify that the only active exit routines are those that your installation has defined. The existence of any other exit routines might indicate a system security exposure, because RACF exit routines could be used to bypass RACF security checking. Similarly, if the length of an exit routine module differs from the length of the module your installation defined, the module might have unauthorized modifications.

Column Headings

The report contains the following information:

EXIT MODULE NAME
the name of the RACF exit routine module, as defined by your installation.

MODULE LENGTH
the length of the exit routine module in bytes (decimal).

Report Messages

The following message might appear below the report column headings:

NO RACF EXITS ARE ACTIVE

Explanation: There are no active RACF exit routines. This absence does not indicate an abnormal condition, unless your installation has defined RACF exit routines.

```
RACF DATA SECURITY MONITOR                                    DATE: 02/22/84     TIME: 16:43:40     PAGE:    5

                                        R A C F    E X I T S    R E P O R T

EXIT MODULE NAME          MODULE LENGTH
-------------------------------------------------------------------------------------------------------------------

ICHDEX01                        256

ICHNCV00                        128

ICHRCX01                        512
```

Figure 3-4. Sample RACF Exits Report

Selected User Attribute Report

The selected user attribute report lists all RACF users with the SPECIAL, OPERATIONS, AUDITOR, or REVOKE attribute and indicates whether a user possesses the attribute on a system (user) or group level.

You can use the selected user attribute report to verify that only those users who need to be authorized to perform certain functions have been assigned the corresponding attribute.

Column Headings

The report contains the following information:

USERID
the user's system identifier.

ATTRIBUTE TYPE
identifies each attribute and indicates whether the user has the attribute on a system (user) or group level. SYSTEM indicates the user has that attribute on a system level, or at all times. GROUP indicates user has the attribute only within one or more of the groups to which the user is connected. If neither SYSTEM nor GROUP appears, the user does not possess that attribute on either level.

If a user has one or more attributes on a group level, you can determine the names of the corresponding group or groups via the LISTUSER command or the "User Services" panel.

The report lists the following attribute types:

SPECIAL
gives the user complete control over all the RACF profiles in the RACF data sets, and authority to issue all RACF commands except those reserved for the auditor's use.

OPERATIONS
gives the user authority to perform maintenance operations and provides full authority to access RACF-protected DASD data sets and certain resource classes.

AUDITOR
gives the user complete authority to audit security controls and the use of system resources.

REVOKE
prevents a RACF-defined user from entering the system, on a system or group level.

For more information on each attribute, especially at the group level, see the *RACF Security Administrator's Guide*.

The following message might appear below the report column headings:

NO SELECTED USERS FOUND

Explanation: There are no users with the SPECIAL, OPERATIONS, AUDITOR, or REVOKE attributes on either a system or group level.

Note: Under normal circumstances, this message should not appear. At least one user should have the SPECIAL attribute on a system level, and at least one user should have the AUDITOR attribute on a system level. If this message appears, notify your RACF security administrator and/or installation manager.

RACF DATA SECURITY MONITOR DATE: 02/22/84 TIME: 16:43:40 PAGE: 6

S E L E C T E D U S E R A T T R I B U T E R E P O R T

USERID	ATTRIBUTE TYPE			
	SPECIAL	OPERATIONS	AUDITOR	REVOKE
BELDING			SYSTEM	
CDELONG	GROUP			
DEWING	SYSTEM			
IBMUSER	SYSTEM	SYSTEM		SYSTEM
LESCHER	GROUP			
RGUSKI	SYSTEM			
SEFCIK	GROUP	GROUP	SYSTEM	
BUILD01	GROUP			SYSTEM
BUILD03		GROUP		SYSTEM
BUILD05	GROUP	GROUP	GROUP	
BUILD06	GROUP			
BUILD10	GROUP	GROUP	GROUP	
BUILD12				SYSTEM

Figure 3-5. Selected User Attribute Report

Selected User Attribute Summary Report

The selected user attribute summary report shows totals for installation-defined users and for users with the SPECIAL, OPERATIONS, AUDITOR, and REVOKE attribute, at both the system and group level.

You can use this report to verify that the number of users with each of the selected attributes, on either a system or group level, is the number your installation wants.

Column Headings

The report contains the following information:

TOTAL DEFINED USERS
the number of users defined by your installation.

TOTAL SELECTED ATTRIBUTE USERS
the number of users with each of the four selected attributes (SPECIAL, OPERATIONS, AUDITOR, and REVOKE) at both the system and group level.

Report Messages

No messages appear at the end of this report.

RACF DATA SECURITY MONITOR DATE: 02/22/84 TIME: 16:43:40 PAGE: 7

S E L E C T E D U S E R A T T R I B U T E S U M M A R Y R E P O R T

TOTAL DEFINED USERS: 234

TOTAL SELECTED ATTRIBUTE USERS:

ATTRIBUTE BASIS	SPECIAL	OPERATIONS	AUDITOR	REVOKE
SYSTEM	3	1	2	4
GROUP	7	4	2	1

Figure 3-6. Selected User Attribute Summary Report

Selected Data Sets Report

The selected data sets report lists all the data sets that meet one or more of the selection criteria (for example, being a primary RACF data set) that DSMON uses. For each selected data set, the report specifies the serial number of the volume on which the data set resides, the selection criterion, whether the data set is RACF-indicated and/or RACF-protected, and the universal access authority (UACC) for the data set. If a data set meets more than one selection criterion, there is a separate entry for each criterion.

You can use the selected data sets report to determine which system and RACF data sets are protected by RACF and which are not. You can also check whether the UACC associated with each of the data sets is compatible with the resource access control requirements of your installation.

Column Headings

The report contains the following information:

DATA SET NAME
the name of the data set.

VOLUME SERIAL
the serial number of the direct access volume on which the data set resides. If the data set is not cataloged, this column is blank.

SELECTION CRITERION
the criterion that was used to select the data set for the report.

The following entries might appear:

LNKLST
the data set is a SYS1.LINKLIB concatenation via one or more link list (LNKLSTxx) members of SYS1.PARMLIB.

APF
the data set is in the in-storage APF list.

MASTER CATALOG
the data set is the MVS master catalog.

RACF PRIMARY
the data set is a primary RACF data set, containing RACF access control information. This information includes user, group, connect, DASD data set, and general resource profiles.

RACF BACKUP
the data set is a backup, or recovery, RACF data set.

SYSTEM
the data set is one of the following system data sets:

SYS1.CMDLIB
SYS1.LINKLIB
SYS1.LPALIB
SYS1.NUCLEUS
SYS1.PARMLIB
SYS1.PROCLIB
SYS1.SVCLIB
SYS1.UADS

RACF INDICATED
indicates whether or not the data set is RACF-indicated. The following entries might appear:

YES
the RACF indicator for the data set is on.

NO
the RACF indicator for the data set is off.

N.C.
the data set is not listed (cataloged) in the master catalog.

N.M.
the DASD volume on which the data set resides is not mounted.

N.F.
DSMON cannot find the data set on the specified volume.

RACF PROTECTED
indicates whether or not the data set has a RACF profile. The following entries might appear:

YES
the data set has a discrete or generic profile. If the RACF indicator for the data set is on, the data set is protected by a discrete profile.

NO
no profile exists for the data set. The data set is not protected in any way by RACF.

Note: An error condition exists when the RACF indicator for a data set is on but no profile exists for the data set. The data set is not accessible until the condition is corrected.

This column is blank when the RACF INDICATED contains N.C., N.M., or N.F.

UACC
the data set's universal access authority (UACC), if it is defined. The UACC is the default access authority that specifies how the data set can be accessed by users or groups not in the access list of the data set's RACF profile.

Note: The UACC does not necessarily indicate the actual authority that a user has to access the data set. The global access checking table might contain an entry applicable to the data set, or the user might be on the access list if the data set has a discrete profile.

The following universal access authorities might appear:

ALTER
For a data set that is protected by a discrete profile, ALTER allows all users to read, update, or delete the data set.

CONTROL
For VSAM (virtual storage access method) data sets, CONTROL provides all users with the same authority that is provided with the VSAM CONTROL password; that is, authority to perform control-interval access (access to individual VSAM data blocks), and to retrieve, update, insert, or delete records in the specified data set.

For non-VSAM data sets, CONTROL is equivalent to UPDATE.

UPDATE
Allows all users to read or update the data set. UPDATE does not, however, authorize a user to delete the data set.

READ
Allows all users to access the data set for reading only.

NONE
Does not allow users to access the data set.

Report Messages

The following message might appear below the report column headings:

NO SELECTED DATA SETS FOUND

Explanation: DSMON did not find any data sets meeting the criteria.

Note: Under normal circumstances, this message should not appear. If it does, notify your RACF security administrator and/or installation manager.

RACF DATA SECURITY MONITOR DATE: 02/22/84 TIME: 16:43:40 PAGE: 8

S E L E C T E D D A T A S E T S R E P O R T

DATA SET NAME	VOLUME SERIAL	SELECTION CRITERION	RACF INDICATED	RACF PROTECTED	UACC
ISF.R1M0.ISFLOAD		LNKLST	N.C.		
MATTLIB		LNKLST	N.C.		
NCP.NCPLOAD		LNKLST	N.C.		
NFSJ.LOAD		LNKLST	N.C.		
NUC02.LPALIB		LNKLST	N.C.		
NUC03.LPALIB		LNKLST	N.C.		
OS.COBOL.COBLIB		LNKLST	N.C.		
OS.COBOL.LINKLIB		LNKLST	N.C.		
PAGE38.MASTER.CATALOG	PAGE38	MASTER CATALOG	NO	YES	UPDATE
PP.PPLIB	PAGE38	LNKLST	NO	NO	
PPC1.ISFLOAD	DRV38X	LNKLST	NO	YES	NONE
REG.LOAD		LNKLST	N.C.		
SPP3.ATESTLIB		LNKLST	N.C.		
SPP3.TESTLIB		LNKLST	N.C.		
SYS1.BACKUP	SPOOL1	RACF BACKUP	NO	YES	NONE
SYS1.CMDLIB	DRV38X	LNKLST	NO	YES	READ
SYS1.CMDLIB	DRV38X	SYSTEM	NO	YES	READ
SYS1.COBLIB		LNKLST	N.C.		
SYS1.IMAGELIB	DRV38X	SYSTEM	NO	YES	READ
SYS1.JES2		LNKLST	N.C.		
SYS1.JES3		LNKLST	N.C.		
SYS1.LINKLIB	DRV38X	APF	NO	YES	READ
SYS1.LINKLIB	DRV38X	SYSTEM	NO	YES	READ
SYS1.LPALIB	DRV38X	SYSTEM	NO	YES	READ

Figure 3-7. Sample Selected Data Sets Report

Index

M

N

O

S

Resource Access Control Facility (RACF) Auditor's Guide (File No. S370-34) Printed in U.S.A. SC28-1342-1

SC28-1342-1

Resource Access Control
Facility (RACF) Auditor's Guide

SC28-1342-1

READER'S COMMENT FORM

This manual is part of a library that serves as a reference source for system analysts, programmers, and operators of IBM systems. You may use this form to communicate your comments about this publication, its organization, or subject matter, with the understanding that IBM may use or distribute whatever information you supply in any way it believes appropriate without incurring any obligation to you. Your comments will be sent to the author's department for whatever review and action, if any, are deemed appropriate.

Note: ***Copies of IBM publications are not stocked at the location to which this form is addressed. Please direct any requests for copies of publications, or for assistance in using your IBM system, to your IBM representative or to the IBM branch office serving your locality.***

Possible topics for comment are:

Clarity Accuracy Completeness Organization Coding Retrieval Legibility

If you wish a reply, give your name, company, mailing address, and date:

_____

_____

_____

_____

What is your occupation? _____

How do you use this publication? _____

Number of latest Newsletter associated with this publication: _____

Thank you for your cooperation. No postage stamp necessary if mailed in the U.S.A. (Elsewhere, an IBM office or representative will be happy to forward your comments or you may mail directly to the address in the Edition Notice on the back of the title page.)

Note: Staples can cause problems with automated mail sorting equipment.
Please use pressure sensitive or other gummed tape to seal this form.

Cut or Fold Along Line

Reader's Comment Form

Cut or Fold Along Line

Fold and tape | Please Do Not Staple | Fold and tape

NO POSTAGE NECESSARY IF MAILED IN THE UNITED STATES

BUSINESS REPLY MAIL

FIRST CLASS PERMIT 40 ARMONK, NEW YORK

POSTAGE WILL BE PAID BY ADDRESSEE:

International Business Machines Corporation
Department D58, Building 920-2
PO Box 390
Poughkeepsie, New York 12602

Fold and tape | Please Do Not Staple | Fold and tape

IBM®

Resource Access Control Facility (RACF) Auditor's Guide (File No. S370-34) Printed in U.S.A. SC28-1342-1

Resource Access Control
Facility (RACF) Auditor's Guide

SC28-1342-1

READER'S COMMENT FORM

This manual is part of a library that serves as a reference source for system analysts, programmers, and operators of IBM systems. You may use this form to communicate your comments about this publication, its organization, or subject matter, with the understanding that IBM may use or distribute whatever information you supply in any way it believes appropriate without incurring any obligation to you Your comments will be sent to the author's department for whatever review and action, if any, are deemed appropriate.

Note: ***Copies of IBM publications are not stocked at the location to which this form is addressed. Please direct any requests for copies of publications, or for assistance in using your IBM system, to your IBM representative or to the IBM branch office serving your locality.***

Possible topics for comment are:

Clarity Accuracy Completeness Organization Coding Retrieval Legibility

If you wish a reply, give your name, company, mailing address, and date:

_____

_____

_____

_____

Note: Staples can cause problems with automated mail sorting equipment.
Please use pressure sensitive or other gummed tape to seal this form.

Cut or Fold Along Line

What is your occupation? _____

How do you use this publication? _____

Number of latest Newsletter associated with this publication: _____

Thank you for your cooperation. No postage stamp necessary if mailed in the U.S.A. (Elsewhere, an IBM office or representative will be happy to forward your comments or you may mail directly to the address in the Edition Notice on the back of the title page.)

Reader's Comment Form

Cut or Fold Along Line

Fold and tape | Please Do Not Staple | Fold and tape

NO POSTAGE
NECESSARY
IF MAILED
IN THE
UNITED STATES

BUSINESS REPLY MAIL
FIRST CLASS PERMIT 40 ARMONK, NEW YORK

POSTAGE WILL BE PAID BY ADDRESSEE:

International Business Machines Corporation
Department D58, Building 920-2
PO Box 390
Poughkeepsie, New York 12602

Fold and tape | Please Do Not Staple | Fold and tape

IBM®

Resource Access Control Facility (RACF) Auditor's Guide (File No. S370-34) Printed in U.S.A. SC28-1342-1

Resource Access Control
Facility (RACF) Auditor's Guide

SC28-1342-1

READER'S COMMENT FORM

This manual is part of a library that serves as a reference source for system analysts, programmers, and operators of IBM systems. You may use this form to communicate your comments about this publication, its organization, or subject matter, with the understanding that IBM may use or distribute whatever information you supply in any way it believes appropriate without incurring any obligation to you. Your comments will be sent to the author's department for whatever review and action, if any, are deemed appropriate.

Note: ***Copies of IBM publications are not stocked at the location to which this form is addressed. Please direct any requests for copies of publications, or for assistance in using your IBM system, to your IBM representative or to the IBM branch office serving your locality.***

Possible topics for comment are:

Clarity Accuracy Completeness Organization Coding Retrieval Legibility

If you wish a reply, give your name, company, mailing address, and date:

_____

_____

_____

_____

Note: Staples can cause problems with automated mail sorting equipment. Please use pressure sensitive or other gummed tape to seal this form.

Cut or Fold Along Line

What is your occupation? _____

How do you use this publication? _____

Number of latest Newsletter associated with this publication: _____

Thank you for your cooperation. No postage stamp necessary if mailed in the U.S.A. (Elsewhere, an IBM office or representative will be happy to forward your comments or you may mail directly to the address in the Edition Notice on the back of the title page.)

Reader's Comment Form

Cut or Fold Along Line

Fold and tape | Please Do Not Staple | Fold and tape

NO POSTAGE NECESSARY IF MAILED IN THE UNITED STATES

BUSINESS REPLY MAIL

FIRST CLASS PERMIT 40 ARMONK, NEW YORK

POSTAGE WILL BE PAID BY ADDRESSEE:

International Business Machines Corporation
Department D58, Building 920-2
PO Box 390
Poughkeepsie, New York 12602

Fold and tape | Please Do Not Staple | Fold and tape

Resource Access Control Facility (RACF) Auditor's Guide (File No. S370-34) Printed in U.S.A. SC28-1342-1