RACF

TABLE OF CONTENTS

TABLE OF CONTENTS
(Continued)

1. INTRODUCTION

As computer systems become more sophisticated, it is impractical, if not impossible, for users to exercise sufficient manual procedures to control the processing of data. For this reason, the internal controls operating within a computer installation become even more important.

The purpose of access control software packages, such as RACF, ACF2 and TOP SECRET, is to assist management in providing an adequate level of internal controls in a computer installation to provide protection against the unauthorized disclosure, modification, or destruction of data.

The Coopers & Lybrand Audit Approach includes evaluation of internal controls in computer systems. A subset of the internal controls is the application controls and the programmed procedures, which are defined to include:

- Controls over the completeness, accuracy and validity of the data being input, processed, and maintained on file normally consist of edit tests, accumulation of totals, reconciliations and the identification and reporting of incorrect, exceptional, or missing data. These functions are normally effective only if combined with related manual procedures. For example, the identification and reporting of exceptional data will be ineffective unless there is a subsequent manual investigation of the exceptions.

- Calculation, summarization, and categorization procedures applied to the data are significant in that the results will not normally be checked to the extent required in a non-computer system. This is because these procedures will function consistently without error, provided the relevant programmed procedures are properly implemented and controls exist to prevent their unauthorized alteration and ensure their proper use.

Controls over the design, implementation, security and use of computer programs and the security of data files are collectively known as integrity controls. These controls, performed mainly within the EDP function, are a combination of manual controls and system software. In general, the same integrity controls are applied to all systems being developed or processed at a computer installation. Integrity controls are designed to ensure that:

- Appropriate procedures are effectively included in the program, both when the system originally becomes operational and when changes are subsequently made. These are defined as implementation controls.

- Unauthorized changes cannot be made to computer programs. These are defined as program security controls.

- Procedures in computer programs are consistently applied. These are defined as computer operations controls.

- Unauthorized changes cannot be made to data files. These are defined as data file security controls.

- System software is properly selected and implemented, and unauthorized changes cannot be made. These are defined as system software controls.

This Audit Guide is one of a series covering a range of system software. This range includes MVS, CICS, RACF, ACF2 and TOP SECRET. These Audit Guides, each of which have two volumes (Technical Description and Audit Program), are designed to assist the auditor in gaining an understanding of the concepts and features of the individual piece of system software as well as providing a generic audit program which requires tailoring for the particular engagement. The appropriate selection of guides should be made in the early stages of the audit in order to reflect the combination of system software being used by the client.

2. RISK ASSESSMENT AND THE FILES-FIRST APPROACH

In planning and conducting an audit, the auditor has always implicitly considered the concepts of audit risk and materiality. In recent years, however, the increase in audit failures and increased pressures from forces outside of the audit client management (e.g. financial statement users, audit committees, the SEC, etc.) to detect errors and irregularities have caused the auditing profession to place a greater emphasis on assessing and controlling audit risk.

The release of SAS No. 47, Audit Risk and Materiality in Conducting an Audit requires that the auditor connsider audit risk and materiality in the planning phase of an audit in determining the nature, timing and extent of auditing procedures to be employed.

Audit Risk

SAS No. 47 defines the overall audit risk as the risk that the auditor may issue an unqualified opinion when the financial statements contain a material misstatement. In assessing risk, SAS 47 notes that the audit risk has two major components:

- the risk (consisting of inherent risk and control risk) that material errors will occur and be introduced into the financial statements; and
- the risk that material errors that have occurred will not be detected by the auditor.

Inherent risk, as defined in SAS 47, is "the susceptibility of an account balance or class of transactions to error that could be material, when aggregated with error in other balances or classes, assuming that there were no related internal accounting controls."

Control risk is "the risk that error could occur in an account balance or class of transactions and that could be material, when aggregated with error in other balances or classes, will not be prevented or detected on a timely basis by the system of internal accounting control."

Detection risk is "the risk that an auditor's procedures will lead him to conclude that error in an account balance or class of transactions that could be material, when aggregated with error in other balances or classes, does not exist when in fact such error does exist."

In considering those three risks, the auditor should understand their inter-relationship and how they affect the audit strategy. Inherent risk and control risk differ from detection risk in that they exist independently of the audit of financial statements. They can be assessed, but not controlled by the auditor. The auditor's consideration of inherent and control risk will lead to a better understanding of those risks but will not change them. The auditor can, however, control detection risk, because he can exercise direct control over the specific audit procedures employed and can change them to respond to different levels of inherent and control risk.

The "Files-First" Approach to Assessing Control Risk

The "files-first" approach is a way of assessing control risk and documenting that assessment in computer environments, including environments with highly sophisticated on-line systems. The approach emphasizes the importance of security in providing assurance that unauthorized transactions are not processed, that programmed procedures operate consistently, and that data files are not changed in an unauthorized manner. It focuses on audit objectives and provides a means for the auditor to make timely judgments about the strength of controls and to assess the efficiency of relying on them.

The files-first approach requires the auditor to obtain information about the characteristics of the accounting system, such as whether it uses batch processing or is on-line, and about the control environment, including whether the system contains features, such as the ability to generate failure statistics, that serve control purposes or can be used by the auditor in the risk assessment process.

The remainder of the files-first approach consists of an investigatory process that includes broad-based, nondetailed compliance testing based primarily on inquiry and observation, and the documentation of that process. While the process is described in a series of steps, in reality the auditor is likely to perform many of those steps simultaneously rather than sequentially. The process entails a group of audit judgments, and documentation of evidence supporting those judgments, that occur before the auditor undertakes detailed compliance tests of controls.

The approach to control assessment and strategy determination in an EDP environment involves the following actions and judgments:

- identifying and documenting key files and data fields
- identifying and documenting file controls over "correctness" (completeness, validity, accuracy, and possibly valuation)
- identifying and documenting file controls over continuity (maintenance)
- determining whether the risk of fraud is insignificant and documenting that determination
- identifying and documenting controls over transactions
- determining whether to rely on transaction controls and documenting that determination
- designing detailed compliance tests, substantive tests, or both to obtain the necessary level of assurance for each specific audit objective
- performing, evaluating, and documenting detailed compliance tests
- performing, evaluating, and documenting substantive tests.

Design, Perform, Evaluate, and Document Detailed Compliance Tests and Design Substantive Tests.

Based on the initial assessment, the auditor may determine that controls are strong enough to make it effective to perform detailed compliance tests as a basis for determining that control risk can be assessed at an even lower level, and that it will be efficient to do so. The auditor may decide to perform detailed compliance tests over file controls, transaction controls, or both. Some testing--either substantive or compliance--must be done at the file level. The strategy chosen should reflect the periods covered by file correctness controls and the effectiveness of those controls in meeting the various objectives. The auditor may choose to test file controls and transaction controls in any combination; the only constraint is that a sufficiently low level of audit risk (the combination of inherent, control, and detection risks) must be achieved for each objective for each material account.

Since detailed compliance testing of controls is not considered as part of the audit strategy until after the initial assessment of control risk has been made, it is unlikely that such testing will produce surprises. Clearly, the auditor should not enter into detailed compliance testing without a high expectation of being able to assess control risk at a very low level, particularly since this approach permits and encourages selective detailed compliance testing.

If file controls exist but do not provide control over the entire period under review, analytical review procedures can be effective ways of providing assurance that audit objectives have been met during the intervening period. Analytical review cannot be used for that purpose, however, if the relevant audit objective is not addressed by a file control. Also, the auditor should consider the effect of year-end adjusting entries on the results of analytical review procedures.

File and transaction controls usually do not address the valuation objective, except for instances involving the use of system-generated data, or the cutoff objective, except that controls over completeness frequently suggest control procedures over cutoff. Substantive tests are always necessary to meet the cutoff and valuation objectives.

A key concept in the files-first approach is selective testing and reliance based on a hierarchy or combination of related controls. For example, the auditor is concerned about controls over transactions only if file controls are not sufficient to permit an assessment of control risk that is consistent with the planned strategy. Similarly, implementation and maintenance integrity controls should be assessed only if programmed procedures are relied on, and even then not in all cases. Furthermore, integrity controls over computer operations should be evaluated only if control totals do not provide the necessary comfort regarding continuity. The approach is designed to prevent global evaluations of any kind of controls, including integrity controls, that serve no further audit purpose.

ACCESS PATHS AND THE ACCESS MODEL

The files-first approach may include the review of the client's security procedures and policies. The review should be limited to those computer files, programs, tables, etc. (herein referred to as computer "resources") on which the auditor intends to rely for audit purposes. In order to determine the adequacy of the security in place over resources, it is necessary to determine the methods by which they can be accessed, who can access them and what they can do to them.

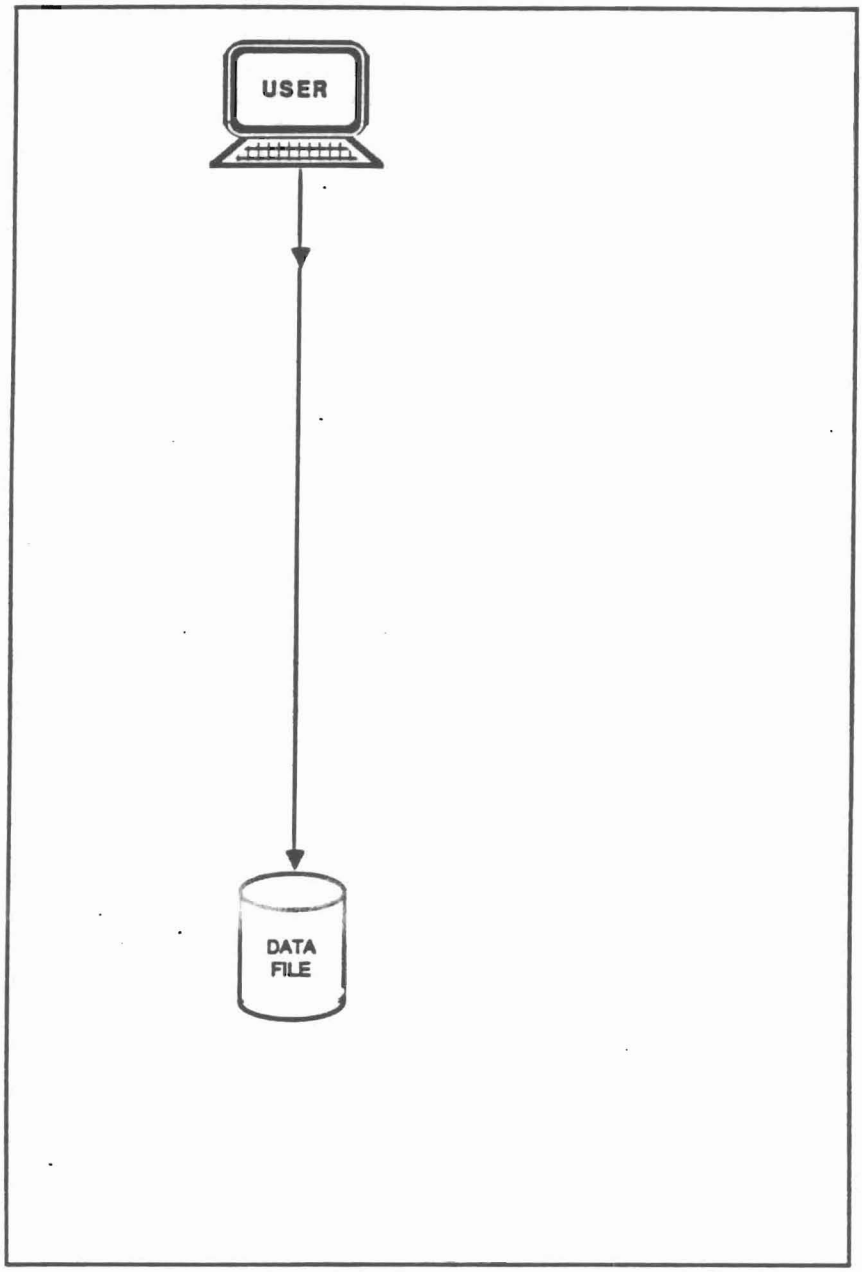
Many files can be accessed by several individuals or jobs. It should be relatively easy to understand, for example, that the General Ledger Master file can be updated by transactions which originate in a number of subordinate systems (i.e., Accounts payable, Accounts Receivable, etc.). It may not be as obvious to the auditor that the G/L Master may be accessible to several application programmers, terminals, the Systems Programmers, Operations personnel, and others. It may be even less apparent that any one (or all) of these individuals may have the capability to modify and/or delete the G/L Master and several other key resources.

The "access paths" by which key files can be modified should be defined by the auditor during the Preliminary Understanding phase of the audit. An access path can be defined as a path or method by which a program can (minimally) read data stored in a given resource. The path can be the batch processing of production jobs, on-line access by user departments, use of utilities by application programmers, etc. As the auditor determines the Access Paths available to the key resources, he should note the controls in place that limit the type(s) of access to the resources available to the various users (e.g., read only, read and write, delete, etc.) The Access Model is the definition of all possible paths to a resource. The controls in place within the Model which limit resource availability and ensure data integrity must be defined and compliance tests developed for those resources on which reliance is to be placed.

Following the definition of the Access Models relating to key resources, the auditor will evaluate the controls in place and determine whether the Models allow for audit reliance. The auditor should only determine Models for those resources on which he wishes to place reliance. There is no need to perform the research necessary to define Models for resources which are not within the scope of the audit. Each Model should be reviewed individually; the lack of the desired controls within one Model should not lead the auditor to conclude that other equally important Models do not contain sufficient controls.

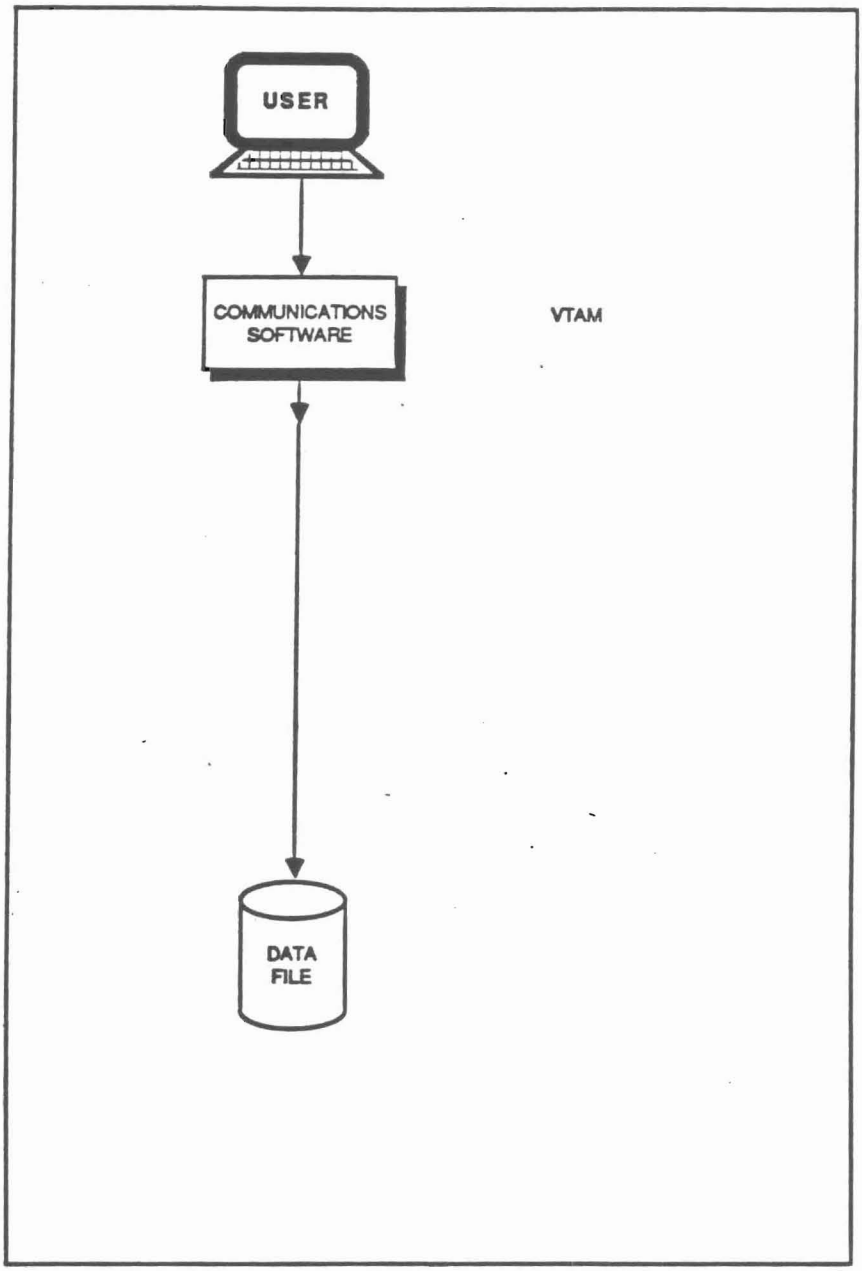
Limiting access to key data files, application programs, and system software files, libraries and tables can be of importance when designing the audit strategy. Generally, these three areas of security must be reviewed individually, however, the strategy developed for an audit must consider them as an integrated whole, each area contributing to the overall control environment.

The following pages describe a typical access path in an on-line environment. In the example there are several "steps" between the user at the terminal and the file. This example is geared to an IBM environment, however, in any computer environment there will be some method of communicating with the files (whether by terminal or through batch processing). Each step along the path is a form of System or application software. The software along the various paths may provide control opportunities which can limit a user from gaining access to the file. It is up to the client to determine which (if any) of the control opportunities he wishes to use. The auditor must be able to recognize the control opportunities, determine the extent to which the client has taken advantage of them, and determine whether thay can be relied on as part of the audit strategy.



Most users access files as shown here. While they know the file exists, they may not realize the "steps" that the computer goes through when accepting data as entered or how the computer "replies" to the terminal.

In a traditional batch installation, restricting access to the computer room provided a great deal of security over programs and data. On-line systems reduced physical security to being a safeguard of the physical asset (hardware), as users can access programs and data at remote sites.



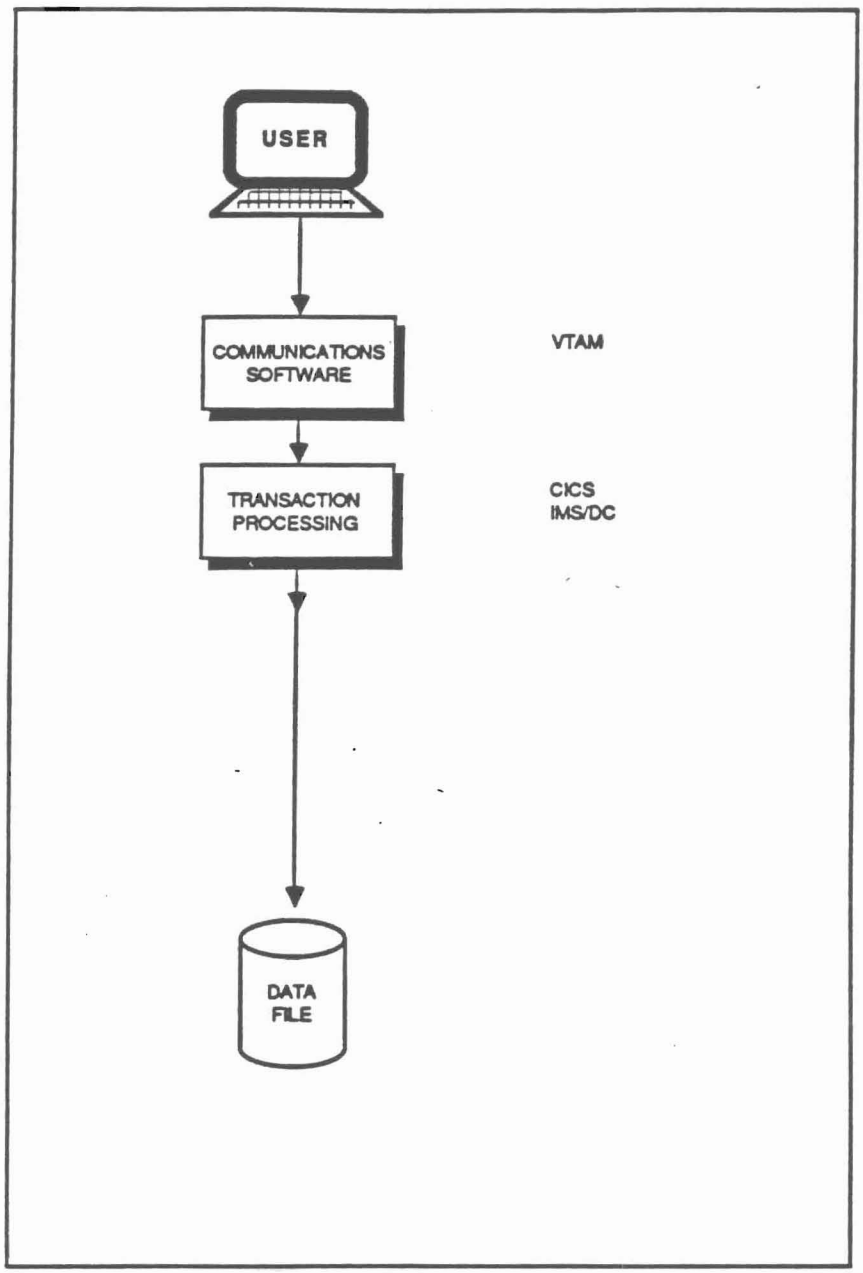
COMMUNICATIONS SOFTWARE

The communications software is the first step of the access model. The computer is continuously checking the network to determine whether a terminal has a request or awaiting a reply.

For the system to accept a message from a terminal, it must be defined to the computer via this software. If a terminalhas not been defined, it cannot access the computer.

At this point, the communications software provides the computer with the message being sent as well as the identification (terminal) from which the request is coming.

The terminal identification is required information–other software will perform further access checking, and the address must be known if the computer is to send a return message.

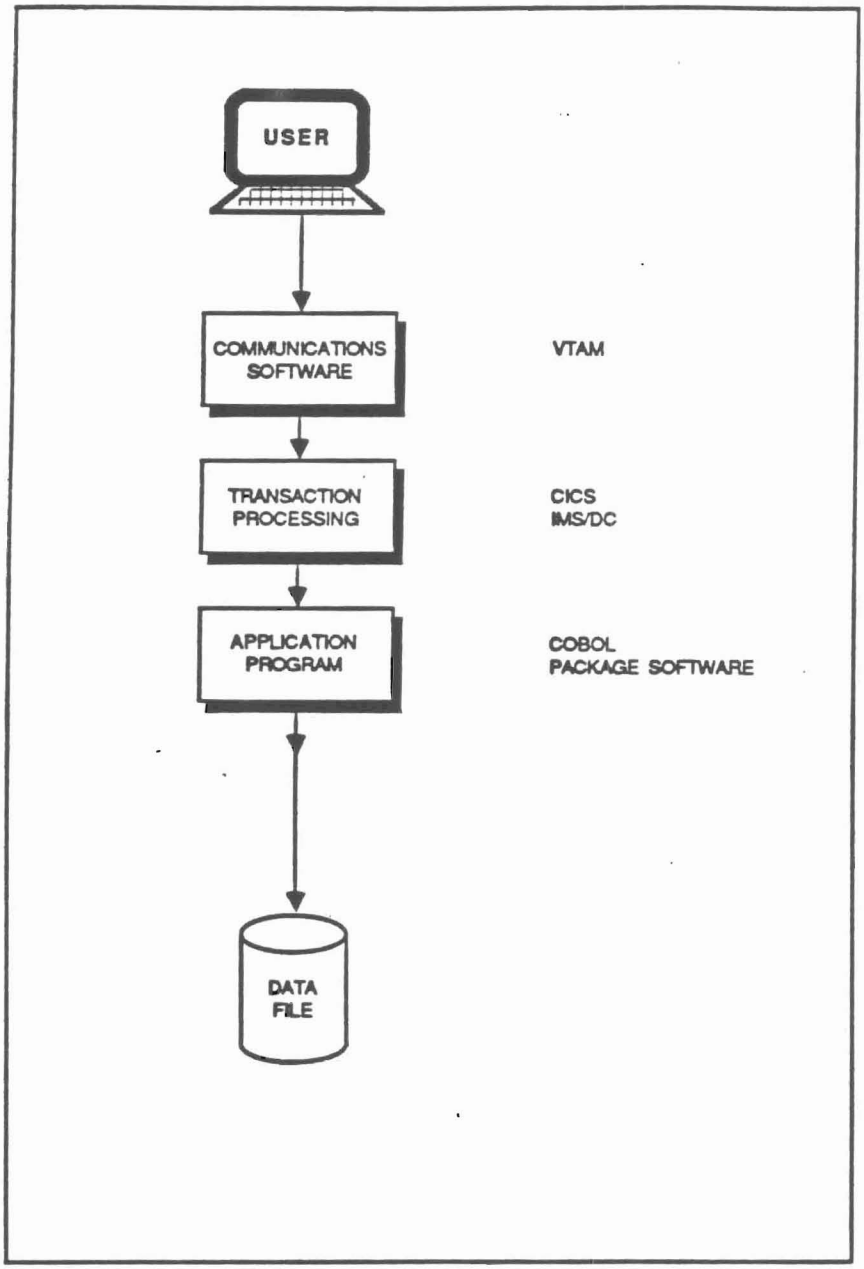


TRANSACTION PROCESSING

Transaction processing software can be used to limit access to the system by matching specific transactions to the terminals and/or users (e.g. payroll tranactions can be limited to the terminals that reside in the payroll area).

Limited password security measures can also be implemented here.

Log files can be produced that can be used for backup/recovery purposes as well as to determine (auditing) system usage.



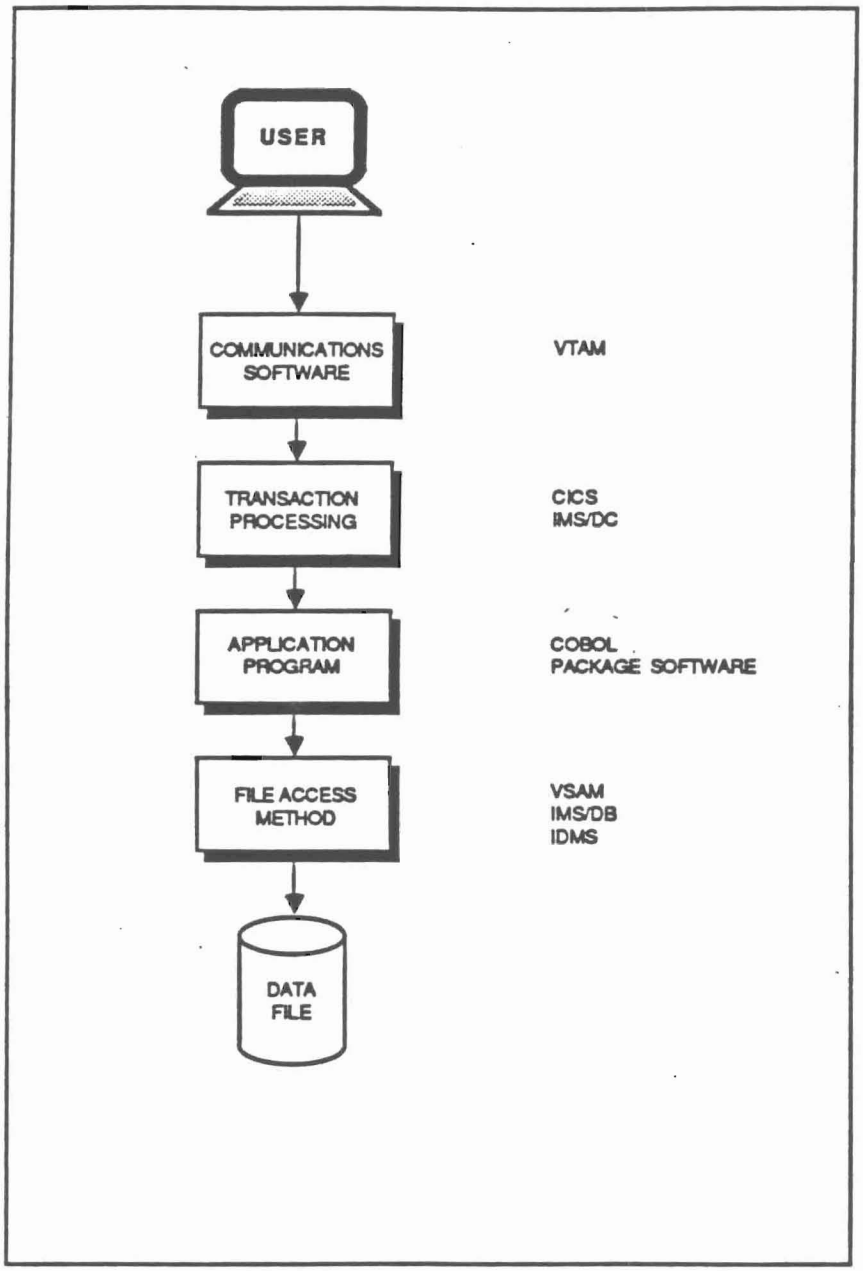
APPLICATION PROGRAM

At this point, the actual computer application programs (developed by the programming department for the user groups) are accessed. The programs analyze (edit, scan, etc.) the data (message) received to determine how the transaction should be processed and recorded, if necessary, on the files.

Editing, such as numeric data checks, reasonableness, etc., can be performed here. In addition, these programs read and write to files, format and send responses (if required) to the requesting terminal, and can perform additional security-related processes.

Many application software packages can be purchased from third-party vendors. In many of these packages, considerable security measures have been implemented. It should be noted that many application packages purchased from third-party vendors include rudimentary security systems. As such, the client may take advantage of the packaged security when designing their access strategy.

In the past, most (if not all) of the security monitoring, edit checking, etc. was built into the application programs. Now, unless batch applications are involved, security concerns can be addressed throughout the access path.



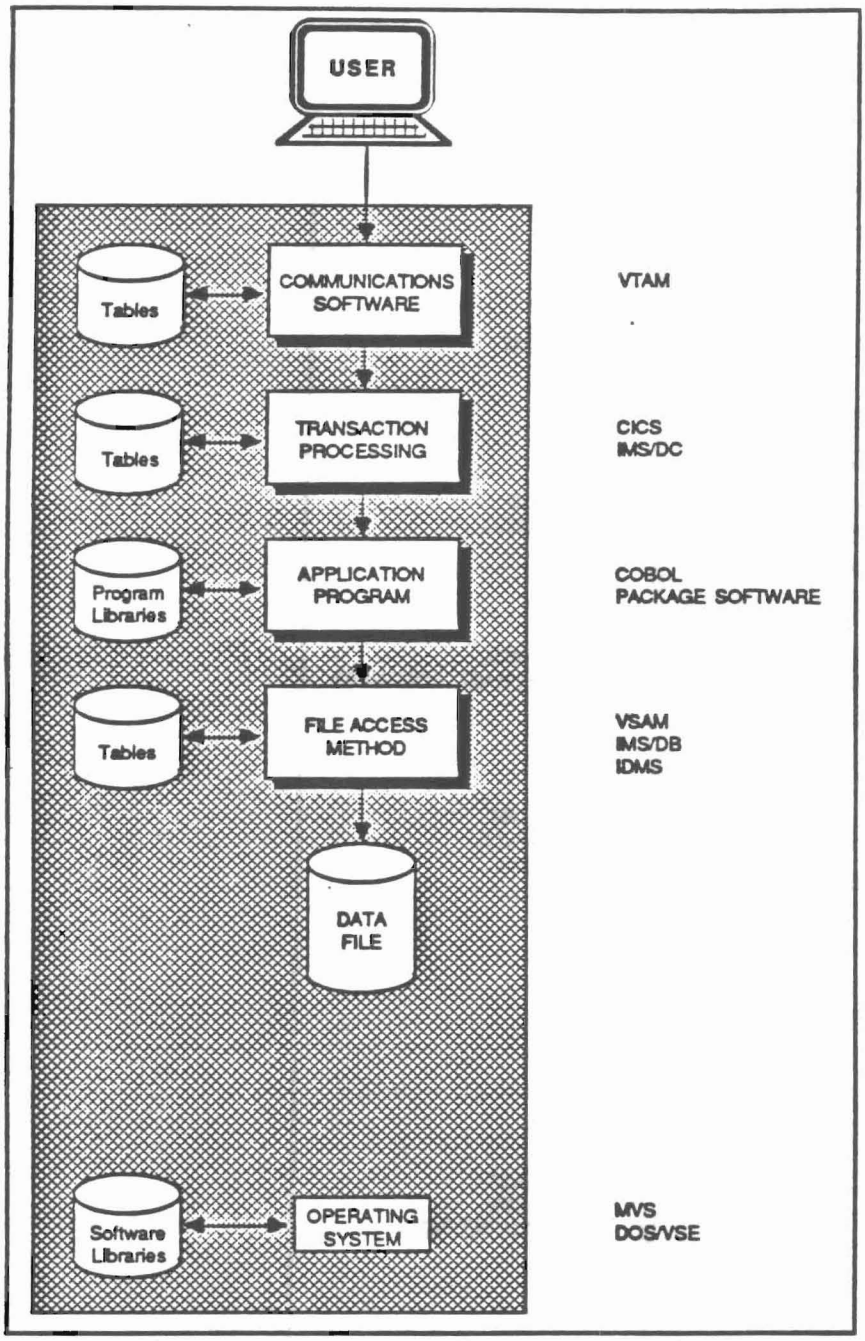
FILE ACCESS METHOD

The method by which files can be accessed is a function of relating the requesting program to the files needed for processing and the method by which the files are read or written to.

Some database software can provide for:

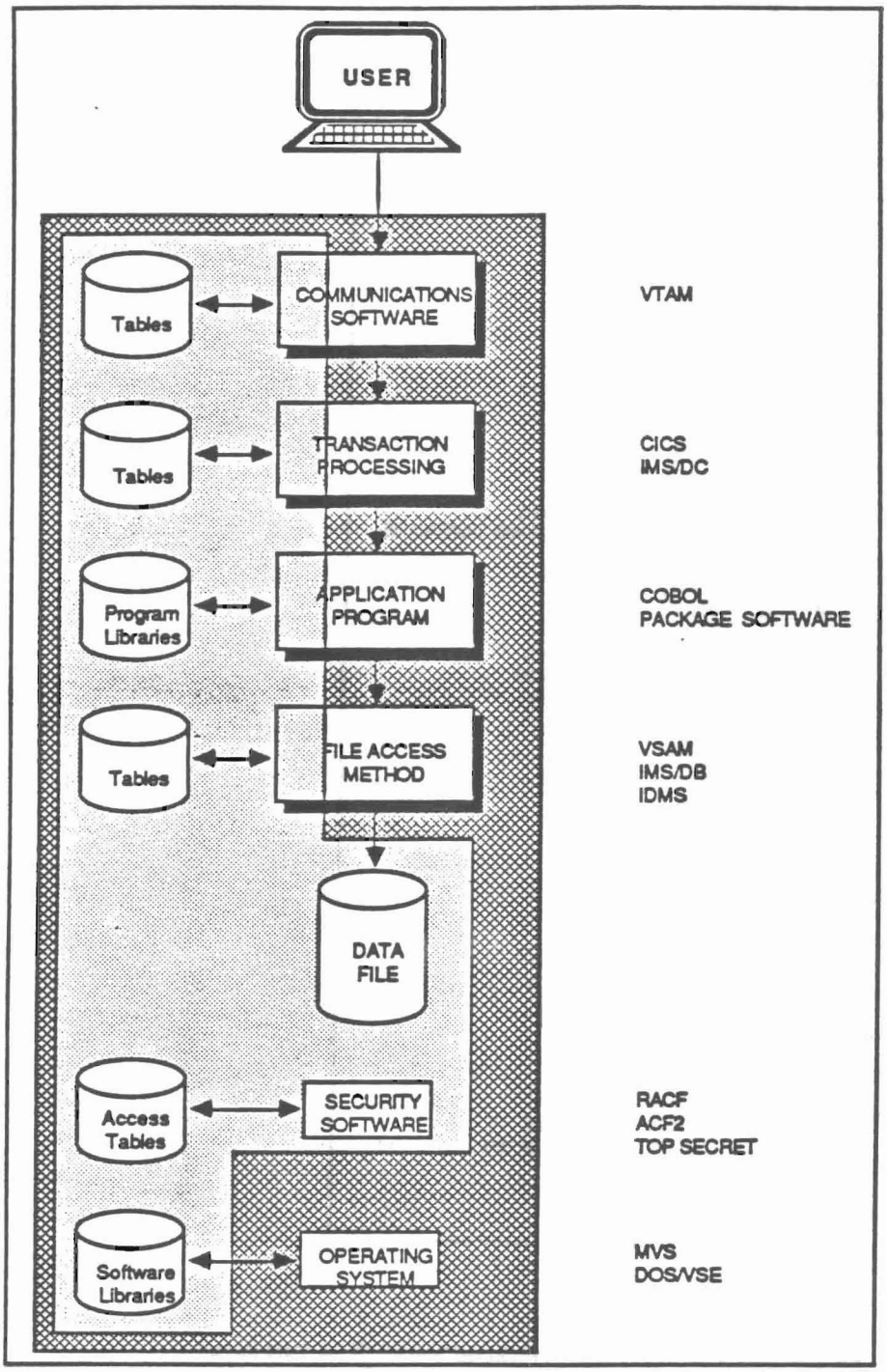
. edit checks (e.g., data field must be numeric).

. security checks which can be used to relate the user and/or the program to the record and data field.



THE OPERATING SYSTEM

The operating system software has control over all the previously mentioned "steps." Since there can be hundreds (or even thousands) of users on the system at any given time, "traffic control" is necessary to give processing time to each request. The operating system schedules all requests (tasks) to ensure that each user is given the appropriate priority and often provides utility programs which can directly access the data file and the table files.

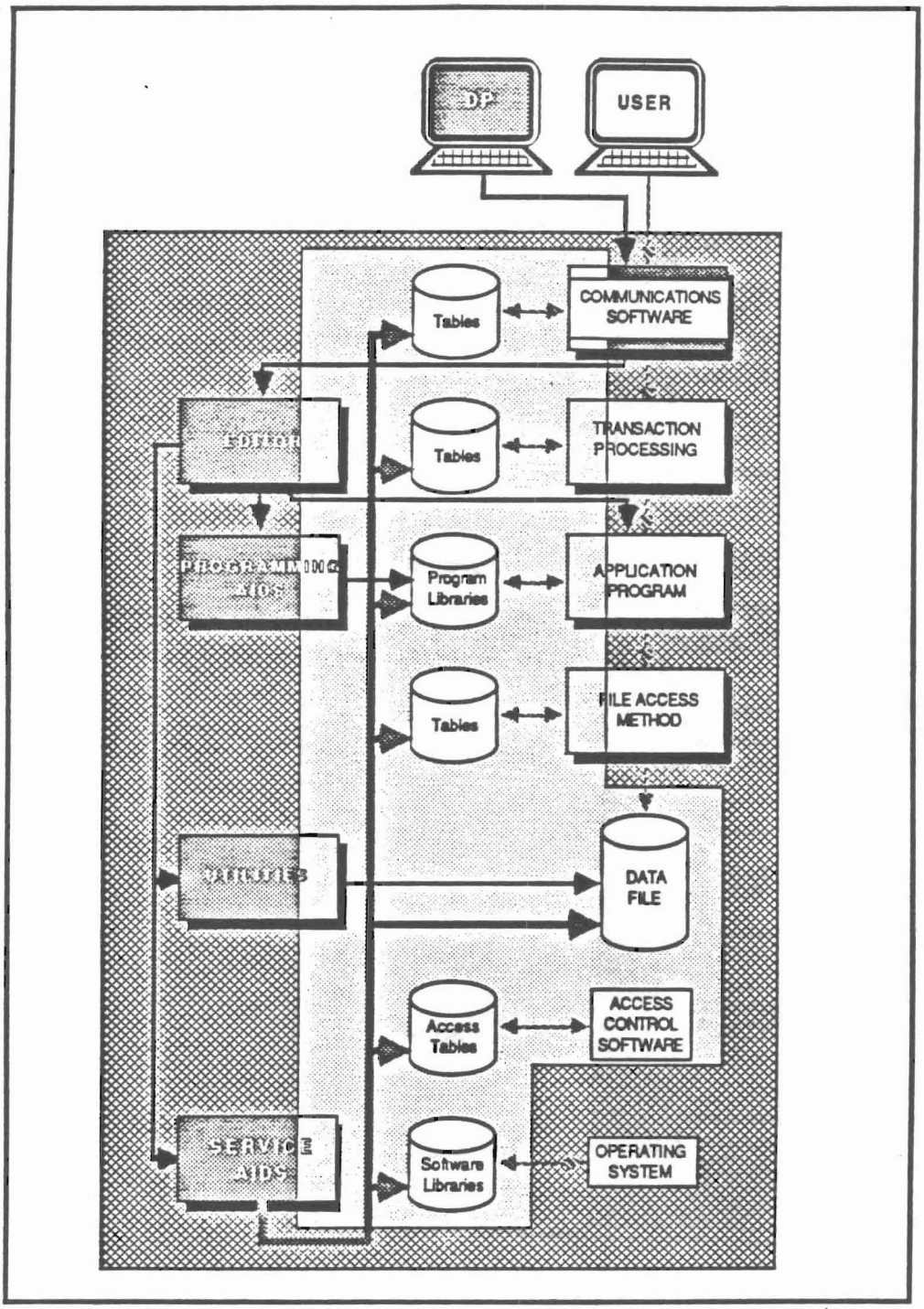


ACCESS CONTROL SOFTWARE

Access control software (security software) is used to limit the access to the files, libraries, and tables held on the computer (see the light grey area). This software and the proper administration of file access can provide a security system.

It is important to note that the proper design, implementation, and subsequent monitoring of this environment is imperative if the overall result is to be a true security system; simply purchasing the software provides no additional security.

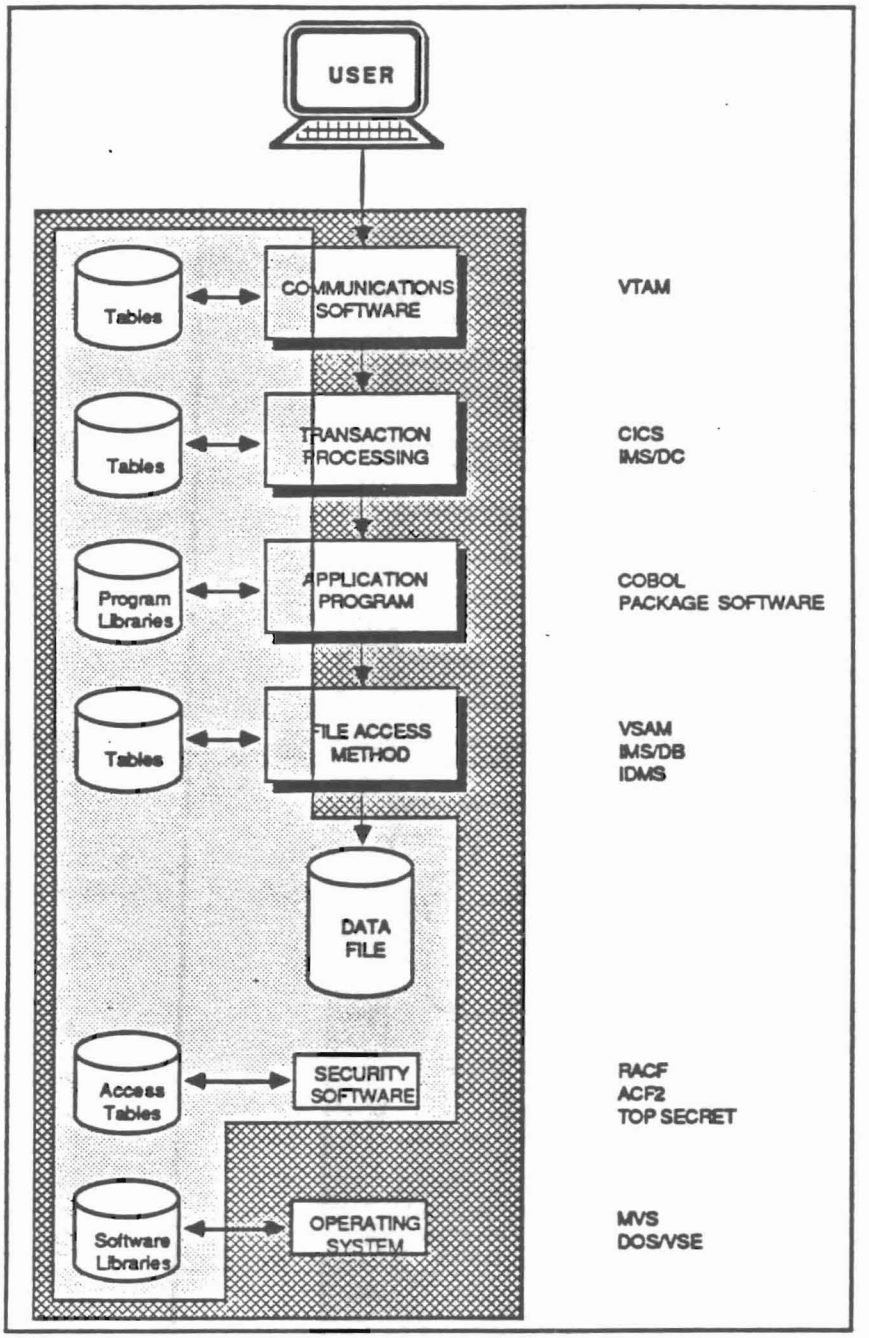
Areas within the light grey area can be protected by the access software. The areas outside the grey indicate that some change in management or administrative control is required to ensure that the proper versions of the software are installed. Not all functions within a program can be controlled.



OTHER ACCESS PATHS

Data Processing personnel will gain access to the system using the same communications software as other users. However, once on the system, Data Processors may have access to the various systems and applications software tables and libraries as well as the data files.

In addition, Data Processing personnel may have access to user transactions in order to "test" the production systems.



A TYPICAL EXAMPLE

Terminals are controlled by VTAM so that only the transaction processing software required by the department can be used: Payroll-CICS Accounts Receivable-IMS/DC Programmers-TSO

CICS transactions are limited to specific terminals by the CICS software. TSO & IMS/DC users have unlimited access (Logon IDs and passwords are required).

Production COBOL and other program libraries can only be updated by two TSO users (this limitation a function of access control software). Source and object libraries are protected by ACF2.

Access to IMS records is limited so that each transaction can only update specific records. Update authorization and control are determined by users and implemented by the Data Base Administration group.

ACF2 protects all files in shaded areas (i.e. VTAM & CICS tables, and critical data files): Payroll master, A/R & Customer master, Program and Operating system software libraries, ACF2 access tables

Security Administrator receives daily ACF2 reportsof attempted access to secured files and has authority to revoke privileges of terminal users when deemed necessary.

3. RACF CONCEPTS

The Resource Access Control Facility (RACF) is an access control system developed by IBM for use on their large mainframes running under the MVS and MVS/XA operating systems. It was first released by IBM in the early 1970s. This guide is current as of RACF Release 1.6.

A particular company's security needs can vary widely. In some companies, "good" security over the payroll and personnel master files is adequate, while in other companies, due to trade secrets, etc., the level of security must be very strict. RACF was designed to accomodate both situations. RACF is built on the concepts of resource ownership and responsibility. Every resource to be RACF-protected must have a RACF user as an owner. The owner of a protected resource will most likely be the individual user or group of users (i.e., department) responsible for the resource. For example, the owner of the payroll master file will most likely be the payroll/personnel department. As described later in this manual in detail, a resource owner can exercise absolute power over an owned resource. Therefore, for example, it would be inappropriate for someone in database administration or in systems programming to be the owner of production datasets.

An access control system is of little value to an organization if accountability and auditability of resource access is not comprehensive. RACF provides a comprehensive logging and reporting facility to meet this need.

When RACF is appropriately implemented, it is difficult to circumvent and provides accountability and auditability. A security system is only as reliable as the operating system of the host computer, the security profiles, implementation options when the system was installed, and the monitoring function subsequent to installation.

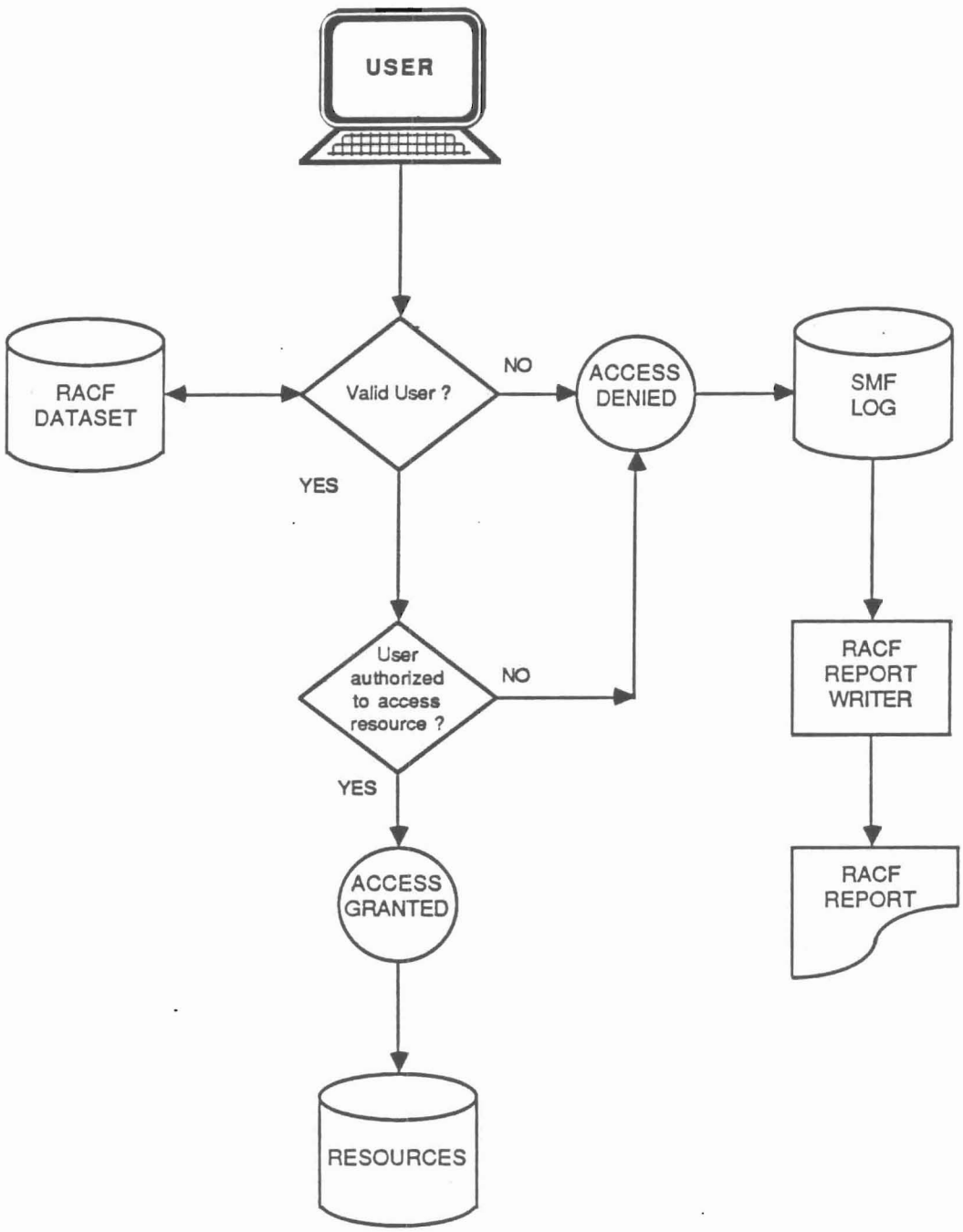
It is these areas that are of concern to auditors. The best software will provide no security if not well designed for a particular site. It is only through the understanding of the functions and selected options of RACF that a decision can be made as to whether we can rely on the controls.

3.1 WHAT IS RACF?

RACF allows the installation to control access to the computer system by controlling

- Users - who can use the system.
- Resources - programs, data and terminals.
- Access Authorities - how each user can access the resources.

A data security administrator creates records called "profiles" which are referenced by RACF to determine who can use what resource. These profiles are maintained in the RACF dataset. RACF uses these profiles to identify the user during logon and to grant or deny authority when a user wishes to



OVERVIEW OF THE RACF ACCESS MODEL

Figure 1.

access a resource or update the RACF dataset. Resources defined to RACF are referred to as "RACF-protected resources." Resources not defined to RACF are not "protected" by RACF. Also, RACF will not issue a warning that the resource is not protected.

Whether access to a particular resource is allowed depends on the RACF "profile" for both the accessing user and the resource to which access is requested. If either the user profile or the resource profile indicates that access is not to be allowed, access will not be allowed. The quality of protection afforded by RACF depends directly upon the quality of the security profiles established by the installation.

RACF provides for accountability of the use of RACF-protected resources through its logging and reporting features. RACF writes records to SMF (System Management Facilities) files for authorized and unauthorized accesses to the system and RACF-protected resources. Also, SMF logging can occur when the RACF profiles are changed. RACF has a parameter-driven report writer (RACFRW) which allows the security adminstrator or auditor to extract selected data from SMF logs to produce reports on system and resource usage and violations.

3.2 ORGANIZATION CONSIDERATIONS

Proper implementation of RACF requires three functions for proper execution and monitoring. These organizational functions are:

- Security Administrator.
- System Software Specialist.
- Auditor.

Security Administrator

The Security Administrator controls the day-to-day functioning of RACF including addition, modification, and deletion of RACF security profiles. His specification as Security Administrator gives him the ability to issue any RACF command.

System Software Specialist

The System Software Specialist is responsible for the technical maintenance of RACF and his duties may include performance tuning of RACF through placement of the RACF dataset(s), coding and implementation of the RACF installation exits, and placement of certain RACF-protected resources. The designation of System Software Specialist allows him full access to any RACF-protected resource.

Auditor

The RACF Auditor is responsible for monitoring accesses to sensitive protected resources, and activity of certain users, such as the Security Administrator and System Software Specialist. The assignment of Auditor also allows him to log and report resource accesses and user activity and violations.

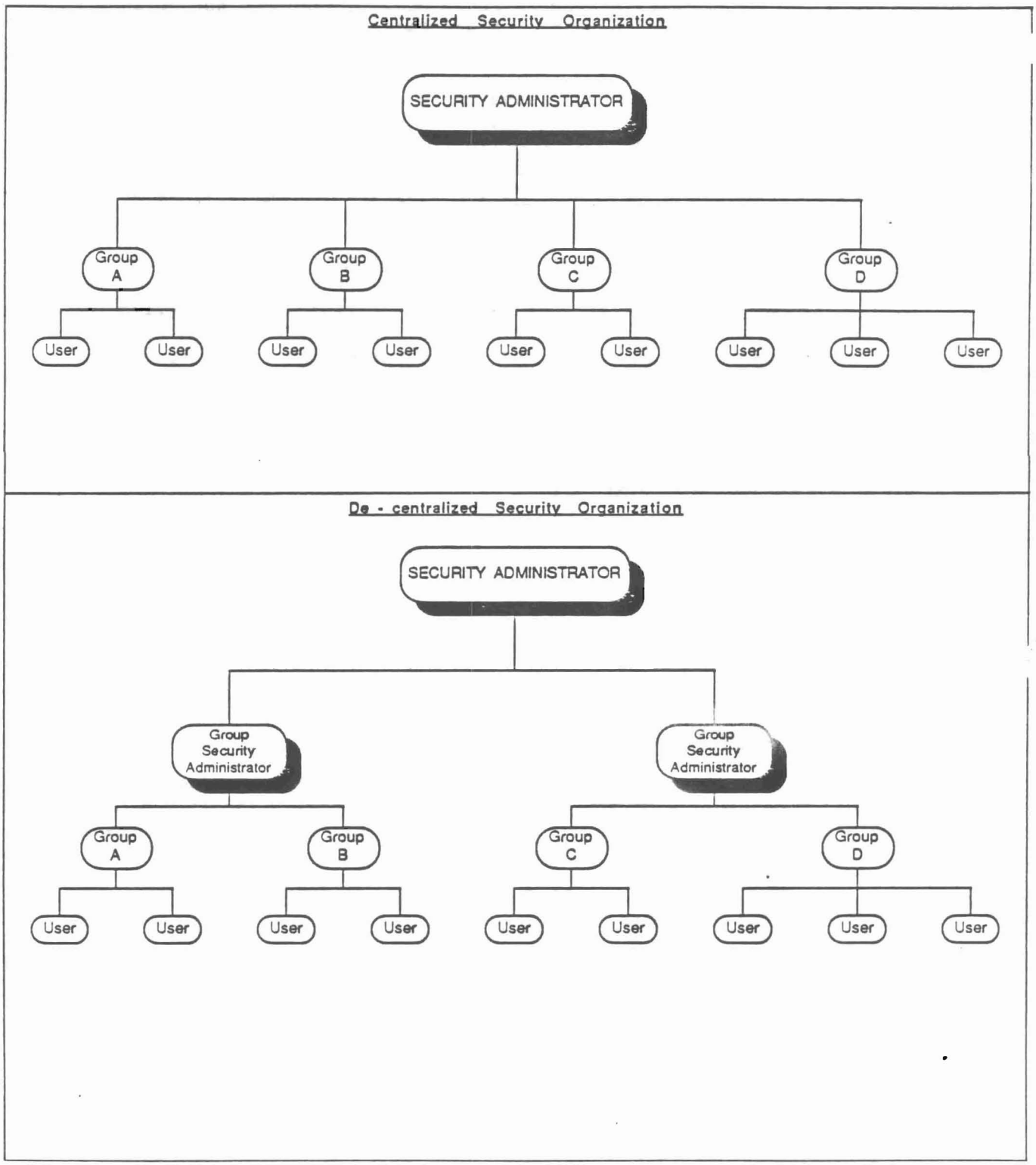

Centralized Security Organization
SECURITY ADMINISTRATOR
Group A
Group B
Group C
Group D
User
User
User
User
User
User
User
User
User
De - centralized Security Organization
SECURITY ADMINISTRATOR
Group Security Administrator
Group Security Administrator
Group A
Group B
Group C
Group D
User
User
User
User
User
User
User
User
User

Figure 2.

Centralized or decentralized security organizations can be supported by RACF. A centralized security organization is usually composed of a single Security Administrator, two or three Backup Security Administrators, two or three System Software Specialists, and an Auditor. Their scope of responsibility includes all users and protected resources. In contrast to the above, a decentralized security organization is marked by the delegation of some security administration duties to the group level. A group is a collection of users that have common responsibilities and access needs to the computer. Group Security Administrators take on the day-to-day duties of security administration for group resources. In addition, there may be a need for a Group System Software Specialist, and a Group Auditor. Their scope of responsibility is restricted to their group.

Figure 2 depicts the centralized and decentralized security organizations.

3.3 CONTROL OVER ACCESS

In any computerized environment, an access control system should be able to adequately control access to resources defined to it. RACF controls access to defined resources using a resource "profile." The resource profile defines both general and specific rules governing access to that resource. The user or group profile and resource profile are used to determine whether access is to be allowed to the resource. If requested, RACF will also perform logging and statistic gathering for later reporting.

However, just controlling access to the system is not sufficient to provide an adequate level of control. The following aspects must be considered in conjunction with limiting access:

- Individual Accountability. A security system must be able to positively associate a job or transaction with the person (or department if a production job) initiating the activity. RACF provides for a unique identifier (user-id) for all users that access the system. This enables the tracking of attempted and unauthorized access to a particular individual in order that appropriate follow-up action may be taken. However, the auditor should be aware that a user could be assigned more than one user-id, and that they may have different attributes.

- Auditability. Regular audit trails and reports of who accessed what resource should be produced. Specific reports regarding maintenance of the security system can be produced using the RACF report writer. In addition, the RACF report writer can be used to report on resource access attempts whether successful or not. Exactly what data is available to be reported on is a function of the options specified when RACF was installed. Unless the appropriate logging and statistic options are active, the information needed for an adequate audit trail will not be available. These logging and statistic options can be activated at any time without re-installing RACF.

4. RACF Environment

4.1 Installation Defined Options

RACF allows the installation to specify certain processing options that apply to all RACF operations. These options determine how RACF operates and therefore must be examined to determine their audit impact. The RACF Security Administrator will be responsible for maintaining this environment, and for documenting any changes to it. To obtain information about the RACF environment, it is useful to print the "SETROPTS LIST" report. This report can be obtained by entering the RACF command SETROPTS LIST.

4.1.1 Resource Class Protection

RACF groups all protected options into "resource classes." These classes are made up of resources sharing similar characteristics. For instance, all disk resident (DASD) datasets are members of the resource class DATASET. All resources that the installation desires to protect must be a member of appropriate resource class. The following resource classes are pre-defined to RACF:

- DASD Datasets (DATASET)
- DASD Volumes (DASDVOL)
- Tape Volumes (TAPEVOL)
- TSO Terminals (TERMINAL)
- CICS Transactions (TCICSTRN) and Groups (GCICSTRN)
- CICS Program Specification Blocks (PCICSPSB) and Groups (QCICSPSB)
- IMS Transactions (TIMS), Groups (GIMS) and Applications (AIMS)
- Global Access Checking Groups (GLOBAL) and Members (GMBR)
- DB2 (DSNR)
- Applications (APPL)

The installation is not obligated to use all of the above resource classes and may establish their own resource classes for specialized resources. In view of this, a determination must be made of which resource classes are going to be active. The data security administrator can select the active resource classes by using the SETROPTS CLASSACT command. Resource classes named in the command will be eligible for RACF protection. However, specific resources within the classes will not be protected unless a profile is created for each resource to receive protection.

4.1.2 Command Usage Logging

Successful or unsuccessful attempts to issue RACF commands can be logged for later reporting. Logging of RACF commands is important since, for example, they can be used to change the security profiles of users.

The data security administrator can initiate command usage logging by issuing the SETROPTS command with the following optional parameters:

AUDIT — Specifies that logging is to be performed for commands that add, change, or delete profiles within the specified resource class(es).

SAUDIT — Causes all commands issued by a user with the SPECIAL attribute to be logged.

CMDVIOL — Causes all unsuccessful attempts to issue RACF commands to be logged.

The following commands are never logged by RACF because their only function is to search for and/or list RACF profiles:

- LISTDSD/LISTGRP/LISTUSER/RLIST/SEARCH

Their usage is restricted to the owners of the profiles and users with the user attributes of "Special" or "Auditor."

4.1.3 User Id and Password Processing

RACF provides features which enhance the effectiveness of using user-ids and passwords as control mechanisms.

User-ids can be disabled after a specified period of inactivity. The specified period (1-255 days) is usually determined by the data security administrator, and will vary depending upon the characteristics of the processing environment. This feature of RACF is active if the data security administrator has issued the SETROPTS INACTIVE command. In order to use this feature, the system active statistics option INITSTATS must be active. To determine if this feature of RACF is active at the installation under review, use the SETR LIST to see that the INITSTATS and INACTIVE options are listed. The INITSTATS option causes logon statistics to be recorded in the user profile.

There are several features of RACF that define criteria for valid passwords. The data security administrator can optionally specify that certain rules over password maintenance be adhered to by all users. The SETROPTS LIST command may be issued to list the following subparameters (see Appendix A for a complete list).

HISTORY — A specified number of previously-used passwords may be kept as history. When a user changes his password, the new password may not match any of the entries in the password history list. This information is stored in each user's RACF profile. In order to use this feature, the system access statistics option INITSTATS must be active.

RULEn — A RACF installation may specify up to eight different password syntax rules. These rules determine up to eight possible valid compositions for passwords, and include specifications of a minimum and maximum password length, and type of characters (vowel, consonant, numeric, alphanumeric, etc.) allowed for each character position of the password. When a user changes his password, the new password must match at least one of the defined password syntax rules.

Example:

```
RULE1(LENGTH(8) CONSONANT(1,3,5:8) NUMERIC(2,4))
```

Syntax Rule 1 applies to passwords 8 characters in length with consonants in positions 1,3,5,6,7, and 8 and numbers in positions 2 and 4.

INTERVAL — This subparameter specifies the maximum number of days (1-254) that a user's password is considered valid by RACF. If a user attempts to enter the system with a password which has expired, he will be required to change his password subject to password history and syntax rules. The INITSTATS option must be active.

REVOKE — A limit on the number of consecutive invalid passwords entered during system access (LOGON, /SIGN ON, etc.) may be specified using this subparameter. If a user exceeds this limit, his user-id is revoked. Before that user can enter the system, the user-id must be restored by a user with the SPECIAL attribute. The INITSTATS option must be active.

In addition to the optional features, above, RACF always provides the facility for every user to change his own password whenever he chooses, provided the user has gained access to the system by entering a valid user-id and password.

4.1.4 Global Access Checking

Global access checking is a feature of RACF that can increase the efficiency of the RACF software by decreasing the time required to check the resource security. A table can be stored in memory which defines the minimum level of access for the resource. If a user requests a greater level of access than is allowed by the global access checking table, normal RACF access checking and logging is performed. For example, if a dataset profile for a dataset called PAY.DATA is created with a universal access of "READ" but the user access list for PAY.DATA contains one or more users with access of "NONE" then PAY.DATA will have an access level of "NONE" in the global access checking table. Subsequently, every user who attempts to read PAY.DATA will go through normal RACF access checking and logging. Global access checking is most commonly used for frequently

accessed data files where the minimum level of access is the most common level of access by users. For example, global access checking might be used to perform access checking for "READ" accesses to SYS1.LINKLIB because of its frequent READ access requirements.

For the auditor, global access checking presents two areas of concern:

1) Global access checking will not log or gather statistics for successful accesses. This would affect the auditor's testing of successful accesses.

2) It is possible that creative systems programmers could change the contents of the in-storage global access checking table and then alter global access checking without detection.

The RLIST GLOBAL * RACF command can be used to list all resources protected using global access checking.

If generic user profiles are created or modified, the in-storage table will not be updated unless the REFRESH option is specified on the SETROPTS listing. If REFRESH is not specified, the in-storage table will not be updated until the next IPL. This may be an audit concern if REFRESH is not active and IPLs are not performed regularly.

4.1.5 Terminal Universal Access Checking

RACF allows terminals to be defined as a resource class. Contrary to other resource classes, universal access to terminals is defined at the resource class level and will apply to all terminals within the class whether they are defined in a specific terminal resource profile or not. Access to terminals by a user can either be "READ" or "NONE."

- READ - allows user to access the terminal.

- NONE - denies user access to the terminal.

For terminals which are not specifically defined in a terminal resource profile, access by a user will default to the universal access authority for the terminal resource class. RACF is initially set up with a terminal universal access authority of "READ". This will allow all valid users to access all terminals unless a specific terminal resource profile contains an access authority of "NONE." The RACF security administrator could change terminal universal access authority to NONE by using the SETROPTS TERMINAL command. If terminal universal access authority is "NONE," all terminals not specifically defined in a resource profile could not be used by any user. If proper naming conventions are used, terminal access could relate groups of users to groups of terminals, thereby decreasing the administrative effort required to set up and maintain terminal resource security. Universal terminal access checking of "NONE" can be used to control access to networks via dial-up lines, since the terminal used by any dial-up user would be denied access unless there is resource profile for the specific terminal.

If the company is using universal access of "NONE," then RACF checks the user authority to use the terminal at logon time during recent RACINIT processing (see New Access to System, page 5-1). For TSO and CICS, RACINIT processing is optional. If RACINIT is not in force for TSO or CICS, terminal access would not be checked even if the proper terminal security is set up.

4.1.6 Automatic Dataset Protection (ADSP)

RACF allows users with the ADSP user attribute (see RACF Users) to have all permanent user datasets automatically RACF protected. The security administrator can allow or disallow this capability using the SETROPTS ADSP or NOADSP parameters. Consideration for having ADSP the primary reason for using the option is that all RACF datasets created by the user are automatically protected removing the responsibility from the user to individual protect critical datasets. The installation may choose not to use ADSP because of disk (DASD) maintenance consideration. This could have an effect on production datasets security if they are created by production batch job and generic profiling is not adequate.

4.2 Installation Exits

Installation exits provide the installation with the means to customize RACF to fit their particular operating environment. An installation exit is a point in processing where the normal program processing may be exited and installation specific processing performed. Usually, control returns to the RACF calling program. While the points in processing where an exit may be given control is fixed by IBM, the processing performed by the exit itself is left up to the installation. Since the RACF installation exits will execute as an integral part of RACF, they can be used to provide additional security checks or used to bypass RACF security checking entirely.

Special attention should be paid to the active RACF installation exits by the auditor. As auditors, we should ensure that installation exits are appropriate by making sure that:

- The function of the exit is valid.
- The assembler source code has been tested and reviewed by a responsible official.
- The libraries in which the exit source and object modules reside are protected.
- Amendments to exits can only take place in a controlled manner.

While the use of installation exits may perform valid system checks or provide accounting information to the installation, they can be used to circumvent RACF security. Weak control in this area can seriously degrade the security afforded by RACF.

Appendix D provides details about each of the RACF installation exits. A complete list of the RACF exits used at the installation can be obtained by reviewing the Data Security Monitor (DSMON) RACF Exit Report. (Refer to Appendix C for information on the DSMON Reports.)

4.3 Started Task Security

A "started task" is one which is executed by the issuance of a "START" command by the system operator. Either user-supplied programs or IBM programs can be run in this way. The JCL for started tasks reside in the system library SYS1.PROCLIB. An example of a common started task is JES2 or JES3 (Job Entry Subsystem).

Once the started task begins, it has the same status as any other task in the system, i.e., it is subject to the same authorization, security, performance, and resource utilization controls. RACF provides a method to allow the started task to access protected resources by assigning a userid or groupname to a started task. This allows RACF to control the started task access authority and log access attempts. Therefore, there are no special considerations of concern to the auditor when dealing with RACF security as related to started tasks.

5. RACF ACCESS CONTROLS

RACF uses the concepts of AUTHORIZED USERS and PROTECTED RESOURCES to control access to the computer system, data files, tables, and libraries.

USERS are defined in RACF by USER PROFILES. User profiles are created by the Data Security Administrator for every user needing access to the system. GROUP PROFILES and CONNECT PROFILES are additional types of user profiles that can be associated with one or more users which make up a group.

RESOURCES are separated into two categories for definition purposes in RACF: DASD dataset category, and other system resources category.

- DASD Datasets consist of all data files, program libraries, and system libraries, residing on DASD volumes. DASD datsets are defined to RACF using DATA SET PROFILES.

- Other System Resources consist of all resources (i.e., DASD volumes, Tape volumes, terminals, CICS transactions, IMS transactions, etc.). Other system resources are defined to RACF using RESOURCE PROFILES.

Based upon the collective contents of the user profiles, dataset profiles, and resource profiles, RACF can be configured to grant or deny access requested by a user to a system resource. RACF can also restrict certain users to certain terminals.

5.1 User Access to System

5.1.1 Online Access. A user attempting to access to the computer system (TSO, IMS, etc.) via a VTAM or TCAM terminal through RACF must first be identified by RACF. The identification process is a two-step procedure. First, the user must supply a valid RACF user-id. After the user-id is validated by matching to a valid user profile, the user's identity must be verified. Two methods are available through RACF to accomplish this. The most common method is the use of a password which is matched to the user's password in his user profile. The usage of passwords is governed by the current installation-wide password rules (see User-Id and Password Processing). Another method of verifying the user's identity is the use of an operator id card (OID). This card is similar to those used in bank automated teller machines in that a magnetic strip of information is on the card which provides information to the computer system about the user. A combination may also be used with a user-id, password, and OID being required for system access. The process of validating a user's authority to obtain access to a system is called RACINIT processing.

Further restrictions may be placed on system access through terminals by defining the terminal itself to RACF as a resource. This would allow only certain users and/or groups of users to access certain terminals. For instance, access to terminals in the order entry department of a manufacturing company could be restricted to members of that department (group). See RACF Terminal Access Control for more detail.

5.1.2 Batch Access. User access to the computer through background access processing can also be restricted by RACF. Batch jobs submitted through the card reader present a special control problem since it is difficult to positively associate a particular job with a user. Without positive identification and validation of the associated user-id, an unauthorized user can submit jobs and access RACF-protected resources (if universal access authority for the resource is sufficient) and these accesses will not be traceable to the submitting user. To control user access via background processing, RACF can require the use of the USER= and PASSWORD= keywords on the JOB card. To implement this access control, the Data Security Administrator uses the SETROPTS JES command with the BATCHALLRACF or XBMALLRACF parameters. When this option is active, RACF will identify and validate the user-id and password. Any users not successfully identified will not be allowed access to the computer system. If NOBATCHALLRACF is specified, batch jobs can be submitted without user-id and password. However, RACF will only allow access based upon the universal access (UACC) specified for the RACF protected resources. If unauthorized access attempts are made to the RACF protected resources, RACF will record the violation on the SMF log, but the user-id will be undefined. Tracing the violation to the user will not be possible.

A User-id and password is required in all JOB cards, whether BATCHALLRACF or NOBATCHALLRACF is used, if the resources are RACF protected and the access level requested is greater than universal access allows. If a JES exit is not installed that appends the user-id and password to the JOB card of TSO submitted jobs, the user-id and password must be hard coded in the JCL. If so, TSO users must be sure that the universal access to their libraries is "NONE." Otherwise, other users could browse their libraries and learn their passwords. Also, any production JCL or PROC libraries that have passwords hard coded in the JCL should not allow unauthorized users to read the libraries.

5.1.3 User Access to TSO

Access to TSO requires, in addition to being defined to RACF, that the user be defined to TSO with a User Attribute Data Set (UADS) entry. Included in the UADS entry are a user id (which may or may not be the same as the user's RACF id) and a password. The TSO password is not used while RACF is active since RACF has alternative password datasets. After RACF identifies and verifies the user, control is passed to TSO. After that, RACF will only be involved when resource access is attempted. If RACF is subsequently disabled via the RVARY command, the user will be required to log on to TSO using the UADS id and password.

5.1.4 Access Checking Methods

When access to a RACF-protected resource is requested, RACF will look up the resource profile and allow or prevent the requested access based on the access rules contained within the profile. RACF provides two basic methods of looking up the resource profile:

RACHECK — This is the default RACF access checking mechanism. When access is requested to a protected resource, RACF will fetch the resource profile from the RACF dataset, allow or disallow the requested access, and perform logging and statistic gathering if required by the resource profile. Because of the input-output processing required, this method has the highest system overhead. From an audit standpoint, this is the most desirable access checking mechanism because of its logging and statistics recording abilities.

FRACHECK — Stands for Fast Path Resource Access Checking. This access checking mechanism is more efficient than RACHECK because no input-output processing is performed on the RACF dataset. All profiles looked up by FRACHECK must be made resident in computer memory by the RACLIST SVC. From an auditing standpoint, this is the least desirable access checking mechanism because it performs no logging or statistics gathering. Use of this access checking mechanism should be restricted to resources that provide an alternate logging facility, such as IMS.

It should be noted that the choice of which access checking mechanism to use for the "standard" resource classes has been made by IBM. Installation defined resource classes may use either mode.

5.1.5 Defining RACF Users

All users requesting access to RACF-protected resources must be positively identified and verified by RACF, therefore all users must be defined to RACF by a user profile. Each user profile is owned by another RACF user profile. The owner can modify and delete the user profiles he owns and can also disable user-ids. Normally, the Security Administrator will define each user to RACF using the ADDUSER command. RACF users may be assigned certain user attributes that confer special abilities within RACF. The user attributes should be assigned to enhance the segregation of duties. The user attributes are listed on the user profile listings.

NONE — Defines the user as having no special authority to override the access level specified in the resource profiles. This means that unless permission for access to a given protected resource is explicitly or implicitly given by definition in the resource profile, the user will not be able to access that resource.

AUDITOR — A user with the AUDITOR attribute has the authority to request logging to the SMF file as follows:

1) Log all uses of certain RACF commands which can change RACF security. The commands which can be monitored are ALTDSD, ALTUSER, RALTER, and SETROPTS. Refer to Appendix A for a detailed explanation of the commands.

2) Log all accesses or selected accesses to specified datasets.

3) Log RACF commands issued by selected users.

The AUDITOR attribute gives the user the authority to monitor successful and/or unsuccessful attempts, to list the RACF dataset and/or RACF protected resources by using the RLIST, LISTDSD, and LISTUSER commands. The auditor can also change the AUDIT/NOAUDIT parameter.

OPERATIONS — Allows a user to copy, rename, catalog, reorganize, and scratch datasets which are protected by RACF.

SPECIAL — Allows a user to issue all RACF commands. This gives the user full control over all RACF profiles in the RACF dataset. This attribute should be limited to RACF security administrators and their activities should be monitored by the RACF Auditor.

GRPACC — A user with GRPACC authority automatically authorizes all users in his group to have UPDATE access authority to any group datasets he defines to RACF. This authority is a control concern since the user with GRPACC authority could allow unauthorized groups of users to update datasets.

REVOKE — Prevents a user from logging on to the system even though the user profile is still defined. This can provide control by disabling a user-id for a user has left the installation. Note: If a user is the "owner" of resources, the user profile cannot be deleted until the resources are assigned to another "owner."

ADSP — ADSP stands for "Automatic Data Set Protection." All permanent datasets created by this user will be protected by RACF. This is accomplished by creating a dataset profile in the RACF dataset with a universal access of "NONE."

CLAUTH — Allows a user to define profiles in one or more of the RACF resource classes. This is known as "class authorization." This capability is useful when certain users are responsible for maintaining RACF profiles in a restricted number of resource classes. For example, data resource management personnel frequently need to be able to manipulate RACF DASD and tape volume profiles. In this case, these users would be assigned class authorization to the DASDVOL and TAPEVOL classes, rather than the SPECIAL user attribute.

When reviewing user profiles, the auditor should review assignment of user attributes and class authorizations to ensure that their assignment is reasonable and proper. User profiles may be listed by a user with the AUDITOR attribute using the RACF command LIST USER (see Appendix A). An example of a user profile follows:

```
LISTUSER IBMUSER

USER=IBMUSER  NAME=I.B.GODD                    OWNER=IBMUSER   CREATED=79.151
 DEFAULT-GROUP=SYS1      PASSDATE=00.000  PASS-INTERVAL= 30
 ATTRIBUTES=SPECIAL OPERATIONS REVOKED
 LAST-ACCESS=83.334/08:32:06
 CLASS AUTHORIZATIONS=NONE
 INSTALLATION-DATA=D1CBKD     IBM SPECIAL USERID
 NO-MODEL-NAME
  GROUP=SYS1       AUTH=CREATE   CONNECT-OWNER=IBMUSER   CONNECT-DATE=79.151
    CONNECTS=     17  UACC=READ     LAST-CONNECT=79.173/08:32:06
    CONNECT ATTRIBUTES=NONE
  GROUP=VSAMDSET   AUTH=CREATE   CONNECT-OWNER=IBMUSER   CONNECT-DATE=79.151
    CONNECTS=     00  UACC=READ     LAST-CONNECT=UNKNOWN
    CONNECT ATTRIBUTES=NONE
  GROUP=SYSCTLG    AUTH=CREATE   CONNECT-OWNER=IBMUSER   CONNECT-DATE=79.151
    CONNECTS=     00  UACC=READ     LAST-CONNECT=UNKNOWN
    CONNECT ATTRIBUTES=NONE
```

5.1.6 RACF User Groups

Each RACF user is a member of at least one RACF group. RACF Group-ids may be listed as user profile owners and entered in resource profile user access lists instead of user ids. Users belonging to the group will automatically have access to all resources where the group-id is listed in the resource profile user access list. Users may belong to more than one group (thereby expanding their scope of potential access ability), however, a user may only be an active member of one group during a given session. When a user is an active member of the group, he is considered "connected to" the group. At system access (LOGON, etc.) time, a determination is made as to which group the user will be connected for that logon session. If the user does not specify a group, he will be connected to his default group, otherwise, the user will be connected to the group specified at system access time, if he is a member of the specified group.

The concept of grouping allows resource profiles to be "owned" by the group in a logical manner. For example, the payroll dataset profiles can be "owned" (and therefore controlled) by the payroll department.

Two concepts of RACF groups should be understood to effectively evaluate access control:

- ownership of RACF groups.
- group authorities.

- Ownership of RACF Groups. For each group defined to RACF via the group profile there must be a RACF-defined user who is assigned ownership of the group. Ownership is assigned to a user via the ADDGROUP or ALTGROUP command. The owner of a group can make the following modifications to the RACF dataset:

  .. Define new users within the group (if the owner has class authorization).

  .. Connect existing users to the group and delete users from the group.

.. Assign and/or change group authorities and set the default universal access authority for all members in the group. If universal access authority for a user is changed to UPDATE or ALTER then anyone in the group can UPDATE or ALTER group datasets created by the user.

.. Maintain the group profile.

.. Maintain subgroups under the group.

.. Restrict users in a group to specific terminals.

Although the ownership of a group can control the population of users within the group, the owner does not necessarily have to be a member of the group. Of course, since the owner can connect existing users to a group, he can connect himself to the group and therefore will have all the same access authority as the group profile. However, the owner of a group cannot assume the access rights of users within his group who have a higher level of access to data than the group profile.

Group Authorities. Since it may not be desirable for all members of a RACF group to have equal capability as regards to group resources, RACF provides levels of "group authority" which can be assigned to each member of a RACF group. When "connected to" the group, the user is restricted by the group authority attributes assigned to him. These "group authority" attributes are listed for each user in the user profile listing.

USE — Assumes all access rights of the group user profile and also allows a user to create and RACF-protect user datasets.

CREATE — A user with the CREATE group authority includes all the privileges of USE and additionally allows the user to RACF-protect group datasets.

CONNECT — A user with the CONNECT group authority includes all the privileges of CREATE and can add existing users to the group. He can also assign the group attributes of USE, CREATE, and CONNECT to the members of the group.

JOIN — A user with the JOIN authority includes all the privileges of CONNECT and can define users and groups to RACF (provided he has class authority (CLAUTH) for the USER class). The new groups become subgroups of the group in which the user has JOIN authority. The new users may belong to the subgroup or group, and may be assigned any level of group authority (including JOIN).

The CONNECT and JOIN group authorities should only be assigned to personnel responsible for maintaining a RACF group.

Members of RACF groups may also be assigned user attributes that only apply within the scope of the group. The SPECIAL, OPERATIONS, GRPACC, ADSP, and REVOKE attributes may be assigned at the group level. This allows delegation of security administration duties to the group level and supports the

decentralized security organization concept. If a user has the group SPECIAL user attribute (as a Group Security Administrator will), he can manipulate the user, subgroup, and resource profiles that belong to the group. These capabilities are effective only when the user is actually connected to the group.

Group profiles may be listed by a user with the AUDITOR attribute using the RACF command LISTGRP (see Appendix A). An example of a group profile follows:

```
LISTGRP SYS1

INFORMATION FOR GROUP SYS1
    SUPERIOR GROUP=NONE              OWNER=L351DSA
    NO INSTALLATION DATA
    NO MODEL DATA SET
    TERMUACC
    SUBGROUP(S)= SYSCTLG  LINEUSER STAFUSER DATABASE TSOUSER  DIVEST
    USER(S)=       ACCESS=       ACCESS COUNT=       UNIVERSAL ACCESS=
      L351DSA        JOIN            004748                NONE
        CONNECT ATTRIBUTES=NONE
      L351UCC         USE            001618                NONE
        CONNECT ATTRIBUTES=NONE
      RAC1LVL         USE            000000                NONE
        CONNECT ATTRIBUTES=NONE
```

5.1.7 RACF Group Terminal Access Option

A group terminal option (specified as NOTERMUACC) can be used to restrict users in a group to specific terminals. If this option is specified in the ADDGROUP or ALTGROUP command, then it overrides the universal terminal access authority for the terminal resource class which is specified in SETR LIST. Refer to the RACF environment section for more information about universal terminal access authority. If NOTERMUACC is specified, users in the group would be restricted to using terminals to which they are specifically authorized access by the PERMIT command.

5.2 User Access to Resources

5.2.1 Dataset Access Control

RACF provides access control for DASD datasets only. As of RACF release 1.6, Datasets held on tape cannot be RACF protected by data set name, although the tape volumes themselves can be protected (see Tape Volume Access Control). All RACF protected DASD datasets are members of the DATASET resource class,

and are protected by discrete or generic "data set profiles." The dataset profile contains an access list which defines user profiles, or group profiles who are allowed to access the dataset, and specifies the level of access granted to each. Two concepts of dataset access controls are important to understand to evaluate the adequacy of RACF protection.

- disk (DASD) dataset ownership.

- access authorities for disk (DASD) data sets.

- DASD Dataset Ownership

  Every disk (DASD) dataset defined to RACF by a dataset profile requires a RACF defined user to be assigned as the owner of the discrete dataset profile. The owner has complete control over the access list for the dataset, and thus can grant or deny all levels of access to other users. The owner grants access by using the PERMIT command. The auditor should evaluate whether financially significant datasets and the RACF dataset are owned by the proper users.

- Access Authorities to Datasets

  Access to a RACF-defined dataset is granted to users and user groups based upon the access authority specifically assigned to each user and user group listed on the discrete dataset profile's access list. If the user or group requesting access is not found on the access list, the access granted defaults to whatever is defined as the "Universal Access Authority" for the dataset. RACF will not provide access control to disk (DASD) datasets which are not defined to RACF with a discrete dataset profile. Disk (DASD) dataset profiles are defined, altered, and deleted using the ADDSD, ALTDSD, and DELDSD commands.

  RACF allows five levels of access to RACF protected disk (DASD) datasets. The level of access is associated with specific users and groups via the access list on the dataset profile. The default access level for all other users or groups is contained in the universal access authority field on the discrete disk (DASD) data set profile. The levels of access allowed to RACF-defined disk (DASD) data sets are:

  NONE — Allows no access to the disk (DASD) data set. This is appropriate as the universal access authority for sensitive datasets that should not be viewed by anyone except the dataset owner.

  READ — Allows the user to read but not write to the disk (DASD) dataset. Note that in order to execute software the user must have read access to the program and system libraries and/or transactions. RACF does not distinguish between READ authority and EXECUTE authority.

UPDATE — Allows the user to read and write to the resource.

CONTROL — Used in the context of a VSAM dataset only, it allows CONTROL level password access. If specified for a non-VSAM dataset, it has the same effect as UPDATE.

ALTER — Allows the user to fully control the resource, including scratching and renaming. This level of access should only be assigned to those users with absolute authority as to the disposition of the resource.

Dataset protection may be defined in the dataset profile in one or both of the following ways:

.. Universal Access Authority

.. Entry in Access List

.. Universal access authority is a specific level of access that is to be allowed to all users. This level of access is stored permanently in the resource profile. For example, most users will require access to a particular program library in order to execute programs contained therein (SYS1.LINKLIB is a likely example since it contains most language compilers and other programming tools). Since execution of these programs only requires READ access, it makes sense to assign this library a universal access authority of READ.

.. More specific protection can be implemented by making entries in the dataset's profile access list. Under this scheme, an entry is made in the dataset profile access list for each specific user or group with the allowed level of access. In most cases the universal access authority provides an adequate level of access for most users, and the access list will contain only a few entries.

It should be noted that an entry in the dataset profile access list overrides the universal access authority for that dataset. For example, if a user requests UPDATE access to a data set that has a universal access authority of UPDATE, but an entry in that dataset profile access list specifies that the requesting user has a lesser level of access (NONE, or READ), the requested access will be denied. In the absence of an entry in the dataset profile access list for the requesting user or group, the universal access authority will specify the allowed level of access.

Discrete Dataset Profiles vs. Generic Dataset Profiles

All RACF protected disk (DASD) data sets are described by a dataset profile in the RACF data set. This profile may be either a discrete profile or a generic profile. A discrete profile applies to datasets with similar names. For example, all datasets with a high level qualifier of SYS1 can be RACF protected with one profile. When setting up the environment, the Security Administrator can use the SETROPTS GENERIC command to specify the resource classes for which generic profile checking is to be performed.

Access Statistics

When access to a protected disk (DASD) dataset is granted by RACF, certain information regarding resource access can be recorded in the data set profiles. The SETROPTS command with the STATISTICS parameter causes the following information to be recorded in the dataset profile:

.. Date of last access.

.. Date of last update.

.. Number of times accessed by access authority.

.. Number of times that each user or group in the profile access list has accessed the dataset.

If the installation is using FRACHECK rather than RACHECK no statistics will be recorded. (Refer to RACF logging for more detail on FRACHECK and RACHECK.)

Data set profiles may be listed using the LISTDSD command (see Appendix A). Two examples of RACF dataset profiles follow:

Example 1 - A discrete dataset profile:

```
LISTDSD DATASET('SYS1.VTAMLIB') ALL

 INFORMATION FOR DATASET SYS1.VTAMLIB

 LEVEL  OWNER     UNIVERSAL ACCESS   WARNING
 -----  --------  -----------------  -------
  00    L322SUP         UPDATE          NO

 AUDITING
 --------
 FAILURES(READ)

 YOUR ACCESS  CREATION GROUP  DATASET TYPE
 -----------  --------------  ------------
 NONE GIVEN       L322            NON-VSAM

 GLOBALAUDIT
 -----------
 NONE

 VOLUMES ON WHICH DATASET RESIDES  UNIT
 --------------------------------  ----
 OLDRES                            3380

 NO INSTALLATION DATA

 CREATION DATE  LAST REFERENCE DATE  LAST CHANGE DATE
 (DAY) (YEAR)       (DAY) (YEAR)      (DAY) (YEAR)
 -------------  ------------------  ----------------
  107    85          107    85          107    85

 ALTER COUNT  CONTROL COUNT  UPDATE COUNT  READ COUNT
 -----------  -------------  ------------  ----------
   00000          00000         00000        00000

   USER     ACCESS   ACCESS COUNT
 --------  -------  ------------
 L322        ALTER      00000
 L321       UPDATE      00000
```

Example 2 - A generic dataset profile:

```
LISTDSD DATASET('SYS1.*') ALL

 INFORMATION FOR DATASET SYS1.* (G)

 LEVEL  OWNER    UNIVERSAL ACCESS   WARNING
 -----  -------- ----------------   -------
  00    L322SUP         READ          NO

 AUDITING
 --------
 FAILURES(READ)

 YOUR ACCESS  CREATION GROUP  DATASET TYPE
 -----------  --------------  ------------
 NONE GIVEN       L322            NON-VSAM

 GLOBALAUDIT
 -----------
 NONE

 NO INSTALLATION DATA

 CREATION DATE  LAST REFERENCE DATE  LAST CHANGE DATE
 (DAY) (YEAR)       (DAY) (YEAR)       (DAY) (YEAR)
 -------------  ------------------  ----------------
  107    85          107    85          107    85

 ALTER COUNT  CONTROL COUNT  UPDATE COUNT  READ COUNT
 -----------  -------------  ------------  ----------
   00000          00000         00000        00000

   USER     ACCESS   ACCESS COUNT
 --------   -------  ------------
 L322        ALTER       00000
```

5.2.2 Other System Resources - Access Control

RACF will provide access control for resources other than disk (DASD) datasets. These resources are known as "system resources" and may include disk (DASD) volumes, tape volumes, VTAM or TCAM terminals, and IMS or CICS transactions. Each system resource profile is similar to the disk (DASD) dataset profile in that a universal access authority may be specified, and entries may be made to the resource profile access list.

- DASD Volume Access Controls

  RACF protected disk (DASD) volumes are members of the DASDVOL class. Disk (DASD) volume protection restricts access to the disk (DASD) volume VTOC (volume table of contents) and other operations performed on a disk (DASD) volume-wide basis. These activites might include initializing the volume, or performing a dump to tape.

- Tape Volume Access Controls

  Many installations keep the majority of their protection data files on tape. RACF can be configured to protect a tape volume. When system-wide tape volume protection is active, RACF will perform authorization checking every time that a tape volume with a standard IBM or ANSI tape label is accessed whether or not the tape volume is defined to RACF. There are significant audit concerns about the quality of RACF protection of tape volumes:

  .. Bypass label processing will bypass RACF protection of the tape volume. This is because the volume serial number is contained in the tape volume label.

  .. RACF only protects the tape volume, therefore dataset level protection is not available on tape.

- Terminal Access Controls

  All VTAM or TCAM terminals are candidates for RACF protection. Terminals can be defined to RACF and accessibility is checked at system access time. Since all terminals may not be defined to RACF, the universal access authority of the undefined terminals may be set to NONE or READ via the SETROPTS TERMINAL command. The RACF profile for terminals can specify a universal access authority and access list for the terminal. This level of protection is valuable when the installation desires to restrict the usage of certain terminals to certain users or groups.

6. ADDITIONAL CONTROL CONSIDERATIONS[1]

6.1 RACF STARTUP AT IPL

RACF is started during IPL and remains unchanged for the life of the IPL except when overridden by the RACF command "RVARY." RVARY can be used to bring down RACF or to bring up the backup dataset in an emergency.

RACF modules and exits are contained in the SYS1.LPALIB or in the SYS1.LINKLIB. They are generally easy to identify because all RACF modules and exits begin with the prefix "ICH." These modules and exits are loaded during IPL to the pageable link pack area (PLPA) or to the fixed link pack area (LPA), based on the names contained in the IEALPA and the IEAFIX members of SYS1.PARMLIB. This load is the result of specifying the CLPA (Create Link Pack Area) parameter in the IEASYS member selected during IPL which initializes the system with RACF.

IEALPA contains the names of the modules that NIP (Nucleus Initialization Program) will load from LINKLIB and LPALIB as a temporary extension to the existing PLPA. Modules in the IEALPA replace the modules in the PLPA for the life of the IPL.

IEAFIX contains the names of the modules that are loaded to the fixed LPA during IPL. If RACF uses IMS, certain RACF modules must be placed in the fixed LPA.

During IPL, if the RACF dataset cannot be found, the operator will be prompted for a RACF dataset name. The operator can respond with the correct name or with "none." If "none" is specified then RACF does not become active for IPL.

A SMF record (type 81) is recorded on the SMF dataset to indicate the completion of the RACF initialization at IPL.

6.2 LOGGING RACF EVENTS

RACF events can be logged to the SMF log provided the SMF record types 80 and 81 are included in the SMFPRM member in SYS1.PARMLIB. All logging by RACF is optional, and the logging can be changed by users with authority to do so. The auditor should review the logging before attempting any RACF testing using the RACF Report Writer, since the integrity of the tests will depend upon the appropriateness of the logging features.

6.2.1 Resource Access Logging

Owners of resources and users with authority to change resource profiles can specify that certain types of access (READ, UPDATE, CONTROL, or ALTER) are to be logged. The logging options are set in the AUDITING operand on the resource file.

---

[1]The auditor may wish to review the MVS Audit Guide for additional information discussed in this section.

Any user with the AUDITOR attribute can also set logging options for resources. The options set by the user AUDITOR can be different than those contained in the AUDITING operand. These AUDITOR's logging options are contained in the GLOBALAUDIT operand. The user AUDITOR may desire to log accesses to a specific resource to use a source of data for audit testing. By using the ALTDSD command (for datasets) or the RALTER command (for other resources) the AUDITOR can initiate logging without assistance from the Data Security Administrator or System Software Specialist.

Different logging criteria can be specified for the access levels requested, and the results of the access check. The logging options which can be specified in both the AUDITING operand and the GLOBAL AUDIT operands are:

. ALL - logs both successful and unsuccessful accesses.

. SUCCESS - logs successful accesses.

. FAILURES - logs unsuccessful attempts.

. NONE - no logging (this would not be appropriate).

The access levels which can be logged are:

. READ.

. UPDATE.

. CONTROL.

. ALTER.

The default value for the auditing parameter is FAILURES(READ). This would normally be appropriate. At a minimum, Auditing should be set to FAILURES(UPDATE). The use of SUCCESS would not be appropriate since the reports produced would be too voluminous. The default value for the GLOBALAUDIT parameter is none.

6.2.2 Logging Activities of Users

Any user with the AUDITOR attribute can specify the RACF events of a specific user to be logged. The events which are logged include all accesses to resources, and all uses of RACF commands (except SEARCH, LISTDSD, LISTGRP, LISTUSER, and RLIST). The user logging is specified by the UAUDIT or NOUAUDIT operand on the user profile. When the user profile is created, NOUAUDIT is the default value placed in the user profile. Only the user AUDITOR can specify UAUDIT.

The auditor could use UAUDIT to monitor the activity of the users with RACF control capabilities, such as the Data Security Administrator. Due to the volume of data logged, consideration should be given to the duration of the UAUDIT logging.

In addition to the ability to audit the activity of specified users, there is a system-wide RACF resource option that will allow logging of all uses of RACF

commands (except SEARCH, LISTDSD, LISTGRP, LISTUSER, and RLIST) for all users. For more detail refer to the SETROPTS CMDVIOL option in the RACF Environment section.

LOGON and LOGOFF activity is logged by MVS, not RACF. The LOGON and LOGOFF activity is recorded as SMF if record types 20 and/or 30 are being recorded on the SMF log.

6.2.3 Logging IMS and CICS Transactions

Since FRACHECK is used to bypass logging for IMS and CICS transactions, the installation should utilize the logging features of IMS and CICS to monitor IMS and CICS access violations.

6.3 PROGRAM PROPERTIES TABLE

If a program is specified in the Program Properties Table (PPT) and bypass password protection is specified (bit 6 is set on), RACF will not perform authorization checking for resources accessed by that program. A complete list of all programs in the PPT can be obtained by reviewing the DSMON "Program Properties Table" report. (Refer to Appendix C for information on the DSMON Report and an example report.)

6.4 RACF UTILITIES

The following utilities are provided with RACF to maintain, modify, and monitor the RACF dataset(s):

ICHMIN00 — This program initializes the RACF dataset(s).

ICHUT100 — This program will provide a cross-reference of all occurrences of a given user-id or group name contained in the RACF dataset(s).

ICHUT200 — This program will identify inconsistencies in the internal organization of a RACF dataset and provide information about the size and organization of a RACF dataset. If requested, ICCHUT200 will also create a backup copy of the RACF dataset.

ICHUT300 — This program will correct any inconsistencies found in a RACF dataset by the RACF dataset verification utility (ICHUT200).

ICHUT400 — This program will split, merge, or extend RACF datasets.

Usage of all of the above utilities (except ICHUT100) should be monitored and restricted because of their ability to make changes to the RACF dataset.

6.5 Security Adminstrator Function

In order to properly control the implementation and maintenance of RACF, it is important that a Security Administrator role is established. This person (or

group) should be responsible for the implementation, modification, monitoring, and enforcement of the access strategy that is developed by the client. In the final analysis, the Security Administrator provides the security to the system. Without such a role, the implementation of an access control package may provide a false sense of security; a review of the compliance with security requirements may prove that, although intentions were good when the access controls were established, over time the rules may be bypassed and forgotten.

Operationally, the client should be able to establish and enforce security requirements more easily if the implementation and maintentance of the rules is centralized. From an auditor's point of view (under a compliance audit) the security policy established should be consistently applied and enforced, and the security function should be separated from the rest of the Data Processing organization (there is a tendency to allow the application or systems programmers to design and control security). Allowing the programmers to control the security policy is, of course, a breakdown in the desirable aspect of separation of duties; the user departments who "own" the files and libraries should understand and approve the security plan that is established.

The Security Administrator's role is to act on behalf of the owners of the application and system files and libraries. As such, some of the areas that the Administrator should be responsible for are:

- User-Id
  - .. Granting (implementing) and revoking access to the system for TSO usage, production jobs, etc.
  - .. Allocating and withdrawing special facilities from the system users.
- Access Authorization
  - .. Assigning access rights to resources by appropriate individuals and jobs.
  - .. Controls over changes to the profiles established.
  - .. Ensuring that change in the status of employees is appropriately reflected in the access authorization, e.g., transfer of an employee from one department to another, termination of employees, etc.
- Enforcement:
  - .. Monitoring and following up on apparent attempted unauthorized access (both successful and repeated unsuccessful attempts).
  - .. Revoking privileges when apparent fraudulent or other unauthorized activity appears to be taking place (the Administrator should not have to wait to act until it is proven that unauthorized activity has taken place; he should have the authority to act first and ask questions afterword).

Finally, it is important that the Security Administrator not be allowed to act unless appropriately authorized by the owners of the data. The Administrator

is acting as an agent on behalf of others. Unilateral decisions on his behalf should be strictly forbidden. All activities performed by the Administrator should be subject to the review and approval to the file and library owners.

7. AUDIT GUIDELINES

Prior to the audit testing, the following steps are recommended for planning the review:

- Identify data that has financial statement significance according to the file matrices completed as part of the File-First Approach.

- Identify the need for executing C&L integrity control software to assist in compliance testing

  - PARMLIB Analyzer

  - SLAPS

  - SMF Analyzer (only if it is expected that a breakdown of RACF control will be encountered, and then only for the uncontrolled time period).

7.1 Interview Guide

To assist the auditor in gaining an understanding of the RACF environment included in this manual is a questionnaire which should be completed at the beginning of the audit.

7.2 Audit Program Testing

To assist the auditor in the successful completion of the audit of a computer installation with RACF, included in this manual are suggested testing procedures to provide the auditor with assurance that the various components of RACF have been installed and are operating satisfactorily.

In addition to the areas mentioned in the audit program, the auditor needs to consider the operating system in the context of integrity controls.

Although it is beyond the scope of this manual to provide the auditor with a guide as to how to audit an operating system, certain features must be considered that may affect the operation of RACF. The auditor should consider using the MVS guide as well as the APF and PARMLIB Analyzer. Areas of interest include the review of controls over supervisor state libraries such as:

- Authorized Program Facility (APF) libraries - these programs may be capable of switching to supervisor state and therefore could circumvent any standard RACF protection.

- Program Properties Table (PPT) - the protect key that a program is to run under may be specified in the PPT

- Supervisor Calls (SVC) - in addition to IBM SVCs, it is possible for custom SVCs to be installed in a system

- Channel End Appendages - these routines get control before, during or after usage of the access methods used by the operating system

According to the combination of security features being used by the installation, a decision will have to be made as to whether CICS and/or IMS interfaces need to be tested.

It is important for the auditor to remember that these suggested testing techniques are not designed to be exhaustive, but are merely a set of guidelines. The ultimate design of audit tests for RACF will still have to consider the method of operations and procedures within each computer installation. Additionally, performance of these tests alone will not be sufficient to provide an opinion on data and program security sections of the integrity controls. Custody and physical security of data need also to be addressed as well as the other aspects of integrity controls not covered by RACF.

INDEX

ALLOCATE. To grant a resource to, or reserve it for a job or task.

APF (AUTHORIZED PROGRAM FACILITY). Facility whereby access to restricted system functions is controlled by maintenance of an authorization list that identifies modules that are permitted to use restricted functions.

BYPASS LABEL PROCESSING (BLP). An option used in JCL statements so that volume or dataset label information on a magnetic tape is not checked.

CATALOG. The collection of all dataset indexes maintained by data management.

To include the volume identification of a dataset in the catalog.

CATALOGED. The status attributed to a dataset whose name and location are stored in the system catalog.

CLASS AUTHORITY. An authority that allows a user to define entities to RACF in the classes defined in the class descriptor table.

DATASET PROFILE. A description of a RACF-defined DASD dataset including dataset name. volume serial number, universal access, owner.

DISCRETE PROFILE. A description of a single RACF-defined resource that belongs either to the DATASET class or to one of the general resource classes.

GENERIC PROFILE. A description of one or more RACF-protected resources that belong either to the DATASET class or to one of the general resource classes and have similar names and similar access-authorization requirements.

JES2 (JOB ENTRY SUBSYSTEM) - The primary job entry subsystem is Multiple Virtual Storage (MVS) that provides:

- an input/output spooling function job class scheduling
- remote job entry capability

JOB CONTROL LANGUAGE (JCL). Any one of the control statements in the input job stream that identifies a job or defines its requirements.

MACRO INSTRUCTION. A general term used to collectively describe a macro instruction statement, the corresponding macro instruction definition, the resulting assembler language statements, the machine language instructions, and other data produced from the assembler language statements. Representations of a sequence of machine language instructions.

OPERATOR IDENTIFICATION CARD (OID). This card is similar to those used in bank automated teller machines in that a magnetic strip of information is maintained on the card which provides information to the computer system about the user.

PDS - Partitioned Dataset. Independent groups of sequentially organized datasets (called members), each identified by a name in the directory.

PROFILE. A description of the characteristics of a RACF-defined entity. A profile resides on the RACF dataset.

STARTED TASK (STC). A "started task" is one which is executed by the issuance of a "START" command by the system operator. Either user-supplied programs or IBM programs can be run in this way. The JCL for started tasks reside in SYS1.PROCLIB. An example of a common started task is JES2 or JES3.

STEPLIB. A data definition statement in JCL in which a private library (where a program resides) is specified.

SUPERVISOR - As applied to the operating system, a routine executed in response to a requirement for altering or interrupting the flow of operations through the CPU, or for performance of input/output operations. The medium through which the use of resources is coordinated and the flow of operations through the CPU is maintained.

SVC ROUTINE. A control program routine that performs or initiates a control program service specified by a supervisor call.

SYSOUT. An indicator used in data definition statements to signify that a dataset is to be written to a system output unit.

SYSTEM MANAGEMENT FACILITIES (SMF). A control program feature that provides the means for gathering and recording information that can be used to evaluate system usage.

SYSTEM MODIFICATION PROGRAM (SMP). An IBM service aid for controlling modifications to an operating system.

UNIVERSAL ACCESS (UACC). The default access authority that applies to a resource if the user or group is not specifically permitted access to the resource. Universal access can be any of the access authorities.

VSAM (VIRTUAL STORAGE ACCESS METHOD). A data access method used with direct access storage devices.

ZAP. A generic name given to a series of vendor-supplied programs. These programs can alter data and other programs (in any form). Because of this capability, ZAP programs must be secure from indiscriminate use.

APPENDICES

A - RACF Commands

B - RACF Report Writer

C - Data Security Monitor (DSMON)

D - Installation Exits

E - RACF/IMS Interface

F - RACF/CICS Interface

G - List of RACF and MVS System Files Requiring Protection

H - IBM/RACF Documentation

RACF COMMANDS

The RACF commands allow appropriately authorized users to maintain profiles in the RACF dataset and to list their contents. Whether a user is authorized to issue a command depends on the user's profile, the command and any operands issued with it, and the resource/profile to which the command refers. In general, a user can maintain and/or list profiles for resources for which he is the owner or the high-level qualifier of the dataset name is the same as the user's user-id. Below is a listing of the RACF commands and their general functions:

ADDGROUP - Adds a new group profile.
ADDSD - Adds a new DASD dataset profile.
ADDUSER - Adds a new user profile.
ALTDSD - Modifies an existing DASD dataset profile.
ALTGROUP - Modifies an existing group profile.
ALTUSER - Modifies an existing user profile.
CONNECT - Establishes a "connection" between a RACF user and a RACF group.
DELDSD - Deletes an existing DASD dataset profile.
DELGROUP - Deletes an existing group profile.
DELUSER - Deletes an existing user profile.
LISTDSD - Lists the contents of a DASD dataset profile.
LISTGRP - Lists the contents of a group profile.
LISTUSER - Lists the contents of a user profile.
PASSWORD - Allows maintenance to a user's password.
PERMIT - Allows or prevents a specific user or group access to a specific file.
RALTER - Modifies an existing general resource profile.
RDEFINE - Adds a new general resource.
RDELETE - Deletes an existing general resource profile.
REMOVE - Removes a "connection" between a RACF user and a RACF group.
RLIST - Lists the contents of a general resource profile.
RVARY - Switches active RACF datasets or deactivates RACF.
SEARCH - Searches the RACF dataset for specific entries.
SETROPTS - Sets system-wide RACF options.

All of the above commands with the exceptions of LISTDSD, LISTUSER, LISTGRP, RLIST, and SEARCH are audit sensitive. During the review, the auditor should be alert for users of these commands. Appropriate documentation and authorization should exist for all usages of the audit sensitive RACF commands.

RACF Commands Used by Auditor

The "SPECIAL" attribute is needed to use most of the commands listed above. However, several commands are made available to users with the "AUDITOR" attribute to provide a means of auditing or monitoring the RACF-protected resources. These commands are:

ALTDSD	Alter Dataset Profile.
ALTUSER	Alter User Profile.
LITDSD	List Dataset Profile.
LITGRP	List Group Profile.
LITUUSER	List User Profile.
RALTER	Alter Resource Profile.
RLIST	List Resource Profile.
SEARCH	Search profiles, users, or groups.
SETROPTS	Set Resource Options.

The ALTDSD, ALTUSER, and RALTER commands can be used by the auditor to change the GLOBALAUDIT parameter of a dataset or resource profile or the AUDIT/NOAUDIT parameter of a user, but it is recommended that the auditor ask the Security Administrator to perform such commands.

The commands can be used in native TSO to display the profile on the terminal or to obtain hard copy printouts of the profiles so they can be included in the auditor's workpapers.

Follow the JCL submitted in batch mode. Execute the RACF program to create the profile listings.

```
//"JOB CARD"
//STEP EXEC PGM=IKJEFT01,DYNAMNBR=20
//SYSTPRT DD SYSOUT=*
//SYSTSIN DD *
*** RACF COMMAND HERE ***
/*
//
```

HELP

To obtain detailed syntax on the RACF commands, HELP listing of the commands can be obtained by using the following JCL:

```
//"JOB CARD"
//STEP EXEC PRM=IKJEFT01,DYNAMNBR=20
//SYSTPRT DD SYSOUT=*
HELP SETROPTS
HELP LISTDSD
/*
//
```

Example of part of the HELP STROPTS listing:

```
HELP SETROPTS

FUNCTION
      THE SETROPTS COMMAND ALLOWS AN INSTALLATION TO DYNAMICALLY CHANGE
      SYSTEM WIDE RACF OPTIONS CONCERNING CLASS PROTECTION, STATISTICS
      UPDATING, AUDITING CONTROLS, PASSWORD CHANGE INTERVAL, PASSWORD
      HISTORY GENERATIONS, PASSWORD REVOKE LIMIT, PASSWORD SYNTAX RULES
      FOR INSTALLATION, TERMINAL VERIFICATION, DATA SET MODELLING,
      AUTOMATIC DATA SET PROTECTION, SINGLE-LEVEL DATA SET NAME
      PROTECTION, AND GENERIC ACCESS CHECKING.  THE CURRENT SET OF
      OPTIONS CAN ALSO BE LISTED.

      TO PROCESS THE AUDITING RELATED OPTIONS (CMDVIOL,AUDIT,SAUDIT),
      THE USER MUST HAVE THE AUDITOR ATTRIBUTE. PROCESSING OF ALL
      OTHER OPTIONS REQUIRES THE SPECIAL ATTRIBUTE.


SYNTAX

      SETROPTS STATISTICS(*/'CLASS-NAME'...)/
                 NOSTATISTICS(*/'CLASS-NAME'...)
               CLASSACT(*/'CLASS-NAME'...)/
                 NOCLASSACT(*/'CLASS-NAME'...)
               AUDIT(*/'CLASS-NAME'...)/
                 NOAUDIT(*/'CLASS-NAME'...)
               GENERIC(*/'CLASS-NAME'...)/
                 NOGENERIC(*/'CLASS-NAME'...)
               GENCMD(*/'CLASS-NAME'...)/
                 NOGENCMD(*/'CLASS-NAME'...)
               GLOBAL(*/'CLASS-NAME'...)/
                 NOGLOBAL(*/'CLASS-NAME'...)
               INITSTATS/NOINITSTATS
               SAUDIT/NOSAUDIT
               CMDVIOL/NOCMDVIOL
               TERMINAL(READ/NONE)
               MODEL(GDG/NOGDG
                     USER/NOUSER
                     GROUP/NOGROUP)/
                 NOMODEL
               INACTIVE(NN)/NOINACTIVE
               GRPLIST/NOGRPLIST
               ADSP/NOADSP
               PREFIX('USERID-OR-GROUP-NAME')/NOPREFIX
               PASSWORD(INTERVAL('CHANGE-INTERVAL')
                        HISTORY('PSWD GENERATIONS')/NOHISTORY
                        REVOKE('REVOKE-COUNT')/NOREVOKE
                        WARNING('PSWD EXPIRATION PERIOD')/NOWARNING
                        NORULES/
                         RULE1(LENGTH('PSWD LENGTH') CONTENT-KEYWORDS)/
                           NORULE1

                         RULE2(LENGTH('PSWD LENGTH') CONTENT-KEYWORDS)/
                           NORULE2
                         RULE3(LENGTH('PSWD LENGTH') CONTENT-KEYWORDS)/
                           NORULE3
                         RULE4(LENGTH('PSWD LENGTH') CONTENT-KEYWORDS)/
                           NORULE4
                         RULE5(LENGTH('PSWD LENGTH') CONTENT-KEYWORDS)/
                           NORULE5
                         RULE6(LENGTH('PSWD LENGTH') CONTENT-KEYWORDS)/
                           NORULE6
                         RULE7(LENGTH('PSWD LENGTH') CONTENT-KEYWORDS)/
                           NORULE7
                         RULE8(LENGTH('PSWD LENGTH') CONTENT-KEYWORDS)/
                           NORULE8
                       )
               LIST

   THE 'CONTENT-KEYWORDS' MAY BE ONE OR MORE OF THE FOLLOWING:
        ALPHA('POSITION-LIST OR RANGE')
        ALPHANUM('POSITION-LIST OR RANGE')
        VOWEL('POSITION-LIST OR RANGE')
        NOVOWEL('POSITION-LIST OR RANGE')
        CONSONANT('POSITION-LIST OR RANGE')
        NUMERIC('POSITION-LIST OR RANGE')
   FOR EACH RULE KEYWORD ALL OF THE ABOVE 'CONTENT' KEYWORDS
   MAY BE SPECIFIED, BUT THE POSITION-LISTS MAY NOT OVERLAP.

   THE 'POSITION-LIST OR RANGE' MAY BE THE FOLLOWING:
       1  OR 1,2,3  OR 1:3,5  FOR EXAMPLE

   REQUIRED - NONE
   DEFAULTS - NONE
   ALIAS    - SETR


OPERANDS

  STATISTICS(*/'CLASS-NAME'...) - SPECIFIES THOSE CLASSES WHICH WILL
      HAVE STATISTICS GATHERING DONE ON THEIR BEHALF.  THE VALID CLASS
      NAMES ARE DATASET AND THOSE CLASSES DESCRIBED IN THE CLASS
      DESCRIPTOR TABLE.  ANY CLASS NAMES SPECIFIED WILL BE ADDED TO THE
      CURRENT SET OF CLASSES FOR WHICH STATISTICS ARE BEING GATHERED. A
      ASTERISK IS USED TO INDICATE ALL APPLICABLE CLASSES.
  NOSTATISTICS(*/'CLASS-NAME'...) - SPECIFIES THOSE CLASSES WHICH ARE
      NOT TO HAVE STATISTICS GATHERING DONE ON THEIR BEHALF. THE VALID
      CLASS NAMES ARE DATASET AND THOSE CLASSES DESCRIBED IN THE CLASS
      DESCRIPTOR TABLE. ANY CLASS NAMES SPECIFIED WILL BE DELETED FROM
      THE CURRENT SET OF CL SSES FOR WHICH STATISTICS ARE BEING
      GATHERED. AN ASTERISK IS USED TO INDICATE ALL APPLICABLE CLASSES.
  CLASSACT(*/'CLASS-NAME'...) - SPECIFIES THOSE CLASSES WHICH ARE TO BE
      MADE ACTIVE. THE VALID CLASS NAMES ARE THOSE DESCRIBED IN THE
      CLASS DESCRIPTOR TABLE. AN ASTERISK MAY BE USED TO REPRESENT ALL
      VALID CLASSES.
  NOCLASSACT(*/'CLASS-NAME'...) - SPECIFIES THOSE CLASSES WHICH ARE TO
      BE MADE INACTIVE. THE VALID CLASS NAMES ARE THOSE DESCRIBED IN TH
      CLASS DESCRIPTOR TABLE. AN ASTERISK MAY BE USED TO REPRESENT ALL ...
```

Syntax of the LIST Command Usable by the Auditor

. LISTDSD Command

Lists details of DASD dataset profiles.

.. Syntax:

```
LISTDSD    DATASET(profile-name...)
           ID(name...)
           PREFIX(char.)
           GENERIC/NOGENERIC
           AUTHUSER
           ALL
```

DATASET	Specifies the names of one or more discrete or generic profile.
ID	Specifies one or more user-ids and/or group names. Details will be listed for all dataset names that have the specified user-ids or group names as the first-level qualifier name.
PREFIX	Details will be be listed for all profiles whose names begin with the specified character strings. The character string may contain one or more levels specified as *.
GENERIC/NOGENERIC	Specifies whether only generic profiles are to be selected. If neither operant is specified, both profile types are selected.
AUTHUSER	List the access for each profile: - all users and groups authorized to access the dataset. - the level of authority for each user and group. - the number of times each user has accessed the dataset.
ALL	All of the above as well as statistics and historic information.

.. Examples:

1. LISTDSD DATASET('SYS1. VTAMLIB') ALL (discrete profile)

```
LISTDSD DATASET('SYS1.VTAMLIB') ALL

 INFORMATION FOR DATASET SYS1.VTAMLIB

 LEVEL  OWNER    UNIVERSAL ACCESS   WARNING
 -----  -------- ----------------   -------
  00    L322SUP        UPDATE         NO

 AUDITING
 --------
 FAILURES(READ)

 YOUR ACCESS  CREATION GROUP  DATASET TYPE
 -----------  --------------  ------------
 NONE GIVEN       L322            NON-VSAM

 GLOBALAUDIT
 -----------
 NONE

 VOLUMES ON WHICH DATASET RESIDES  UNIT
 --------------------------------  ----
 OLDRES                            3380

 NO INSTALLATION DATA

 CREATION DATE  LAST REFERENCE DATE  LAST CHANGE DATE
 (DAY) (YEAR)       (DAY) (YEAR)      (DAY) (YEAR)
 -------------  ------------------  ----------------
  107    85           107    85          107    85

 ALTER COUNT  CONTROL COUNT  UPDATE COUNT  READ COUNT
 -----------  -------------  ------------  ----------
   00000          00000          00000       00000

   USER     ACCESS   ACCESS COUNT
 --------   -------  ------------
 L322        ALTER      00000
 L321       UPDATE      00000
```

2. LISTDSD DATASET('SYS1.*') ALL (generic profile)

```
LISTDSD DATASET('SYS1.*') ALL

 INFORMATION FOR DATASET SYS1.* (G)

 LEVEL  OWNER    UNIVERSAL ACCESS   WARNING
 -----  -------- ----------------   -------
  00    L322SUP        READ           NO

 AUDITING
 --------
 FAILURES(READ)

 YOUR ACCESS  CREATION GROUP  DATASET TYPE
 -----------  --------------  ------------
 NONE GIVEN       L322          NON-VSAM

 GLOBALAUDIT
 -----------
 NONE

 NO INSTALLATION DATA

 CREATION DATE  LAST REFERENCE DATE   LAST CHANGE DATE
 (DAY) (YEAR)       (DAY) (YEAR)       (DAY) (YEAR)
 -------------  ------------------   ----------------
  107    85          107    85           107    85

 ALTER COUNT  CONTROL COUNT  UPDATE COUNT  READ COUNT
 -----------  -------------  ------------  ----------
   00000          00000         00000        00000

   USER     ACCESS   ACCESS COUNT
 --------   -------  ------------
 L322        ALTER       00000
```

- LISTGRP Command

  Lists details of specific RACF group profiles. General information is given as well as information for each user connected to the group.

  .. Syntax:

  LISTGRP GROUPNAME/*

GROUPNAME	Specifies the name of one or more RACF-defined groups.
*	List details of all RACF-defined groups.

  Note: By default your current connect group is listed.

  .. Example:

```
LISTGRP SYS1

INFORMATION FOR GROUP SYS1
    SUPERIOR GROUP=NONE          OWNER=L351DSA
    NO INSTALLATION DATA
    NO MODEL DATA SET
    TERMUACC
    SUBGROUP(S)= SYSCTLG  LINEUSER STAFUSER DATABASE TSOUSER  DIVEST
    USER(S)=       ACCESS=       ACCESS COUNT=       UNIVERSAL ACCESS=
      L351DSA        JOIN          004748                NONE
        CONNECT ATTRIBUTES=NONE
      L351UCC         USE          001618                NONE
        CONNECT ATTRIBUTES=NONE
      RAC1LVL         USE          000000                NONE
        CONNECT ATTRIBUTES=NONE
```

LISTUSER Command

Lists details of specific RACF user profiles. Information is given for the user as well as for each group the user is connected to.

.. Syntax:

LISTUSER USERID/*

USERID	Specifies one or more RACF-defined users.
*	List details of all RACF-defined users.

Note: By default your user-id is listed.

.. Example:

```
LISTUSER IBMUSER

USER=IBMUSER  NAME=I.B.GODD              OWNER=IBMUSER   CREATED=79.151
 DEFAULT-GROUP=SYS1      PASSDATE=00.000  PASS-INTERVAL= 30
 ATTRIBUTES=SPECIAL OPERATIONS REVOKED
 LAST-ACCESS=83.334/08:32:06
 CLASS AUTHORIZATIONS=NONE
 INSTALLATION-DATA=D1CBKD     IBM SPECIAL USERID
 NO-MODEL-NAME
  GROUP=SYS1       AUTH=CREATE   CONNECT-OWNER=IBMUSER   CONNECT-DATE=79.151
    CONNECTS=     17  UACC=READ     LAST-CONNECT=79.173/08:32:06
    CONNECT ATTRIBUTES=NONE
  GROUP=VSAMDSET   AUTH=CREATE   CONNECT-OWNER=IBMUSER   CONNECT-DATE=79.151
    CONNECTS=     00  UACC=READ     LAST-CONNECT=UNKNOWN
    CONNECT ATTRIBUTES=NONE
  GROUP=SYSCTLG    AUTH=CREATE   CONNECT-OWNER=IBMUSER   CONNECT-DATE=79.151
    CONNECTS=     00  UACC=READ     LAST-CONNECT=UNKNOWN
    CONNECT ATTRIBUTES=NONE
```

. RLIST

Lists information of an existing profile for a resource.

.. Syntax:

```
RLIST class-name
      PROFILE-name/*
      GENERIC/NOGENERIC
      AUTHUSER
      ALL
```

CLASS-name	Specifies the name of the class to which the resource belongs.
PROFILE-name	Specifies the name of one or more existing discrete or generic profile to be listed.
*	List information for all resources defined to the specified class.
GENERIC/NOGENERIC	Specifies whether only generic profiles or no generic profiles are to be listed. Default lists both.
AUTHUSER	List the access list for each resource.
ALL	Specifies that you want all information for each resource (this includes statistics and history information).

.. Example

```
RLIST GIMS BCSC018 ALL

CLASS       NAME
-----       ----
GIMS        BCSC018

MEMBER CLASS NAME
------ ----- ----
TIMS

RESOURCES IN GROUP
--------- -- -----
CSC0300B

LEVEL  OWNER      UNIVERSAL ACCESS  YOUR ACCESS  WARNING
-----  --------   ----------------  -----------  -------
 00    L113CJT          NONE        NONE GIVEN     NO

INSTALLATION DATA
-----------------
NONE

APPLICATION DATA
----------------
NONE

AUDITING
--------
FAILURES(READ)

GLOBALAUDIT
-----------
NONE

CREATION DATE  LAST REFERENCE DATE  LAST CHANGE DATE
 (DAY) (YEAR)      (DAY) (YEAR)      (DAY) (YEAR)
-------------  ------------------  ----------------
  352    84          352    84          352    84

ALTER COUNT   CONTROL COUNT   UPDATE COUNT   READ COUNT
-----------   -------------   ------------   ----------
  000000         000000         000000        000000

USER       ACCESS   ACCESS COUNT
----       ------   ------------
L113CJT    ALTER       000000
BCSC18     READ        000000
NYUSER     READ        000000
```

- SETROPTS Command

The SETROPTS command is used to dynamically set systemwide RACF options related to resource protection. But for the auditor it will be specifically useful to list the current options in use.

The SPECIAL attribute is required to be able to list all options while the AUDITOR attribute only allows to list the auditor's option. It is recommended to ask the Security Administrator to list the contents of the SETROPTS.

.. Example:

```
SETROPTS LIST

ATTRIBUTES = INITSTATS SAUDIT CMDVIOL
STATISTICS = NONE
AUDIT CLASSES = DATASET USER GROUP DASDVOL TAPEVOL APPL TIMS GIMS AIMS
                TCICSTRN GCICSTRN PCICSPSB QCICSPSB TTRG GTRG TPRD GPRD
                TDEV GDEV
ACTIVE CLASSES = DATASET USER GROUP DASDVOL TAPEVOL APPL TIMS GIMS AIMS
                 TCICSTRN GCICSTRN PCICSPSB QCICSPSB GMBR GLOBAL TTRG
                 GTRG ATRG TPRD GPRD APRD TDEV GDEV ADEV
GENERIC PROFILE CLASSES =  DATASET
GENERIC COMMAND CLASSES =  DATASET TIMS AIMS TTRG TPRD TDEV
GLOBAL CHECKING CLASSES =  DATASET
AUTOMATIC DATASET PROTECTION IS NOT IN EFFECT
REAL DATA SET NAMES OPTION IS INACTIVE
JES-BATCHALLRACF OPTION IS INACTIVE
JES-XBMALLRACF OPTION IS INACTIVE
JES-EARLYVERIFY OPTION IS INACTIVE
SINGLE LEVEL NAME PREFIX IS RAC1LVL
LIST OF GROUPS ACCESS CHECKING IS ACTIVE.
INACTIVE USERIDS ARE BEING AUTOMATICALLY REVOKED AFTER  60 DAYS.
DATA SET MODELLING NOT BEING DONE FOR GDGS.
USER DATA SET MODELLING IS BEING DONE.
GROUP DATA SET MODELLING IS BEING DONE.
PASSWORD PROCESSING OPTIONS:
  PASSWORD CHANGE INTERVAL IS  30 DAYS.
  10 GENERATIONS OF PREVIOUS PASSWORDS BEING MAINTAINED.
  AFTER   5 CONSECUTIVE UNSUCCESSFUL PASSWORD ATTEMPTS,
      A USERID WILL BE REVOKED.
  PASSWORD EXPIRATION WARNING LEVEL IS  10 DAYS.
  INSTALLATION PASSWORD SYNTAX RULES:
    RULE 1  LENGTH(4:8)   LLLLLLLL
    RULE 2  LENGTH(4:8)   AAAAAAAA
    RULE 3  LENGTH(4:8)   NNNNNNNN
   LEGEND:
    A-ALPHA C-CONSONANT L-ALPHANUM N-NUMERIC V-VOWEL W-NOVOWEL *-ANYTHING
```

THE RACF REPORT WRITER

The RACF REPORT WRITER IS SUPPLIED WITH RACF and is capable of reporting the contents of the RACF SMF record types. The report writer is command driven and may be invoked in batch by executing the terminal monitor program IKJEFT01. The command syntax provides for selection and sub-selection of RACF SMF records. In addition, report formats can be specified. Summary reports of logged events are a standard part of RACF.

The RACF report writer uses as input SMF record types 20, 30, 80, and 81. SMF type 81 records are known as "status" records and SMF types 20, 30, and 80 are known as "process" records. Status records are generated by usage of the RVARY and SETROPTS commands, and contain information relating to the "status" of RACF after issuance of those commands. Process records are generated during normal system processing and contain information relating to resource and profile access.

SMF type 80 records are written during normal RACF processing for the following detected events:

- Unauthorized attempts to enter the system - these events are always logged when RACF detects the unauthorized attempt.

- Authorized accesses or unauthorized attempts to access RACF-protected resources - these events are only logged if the appropriate logging option for the resource in question is active.

- Authorized or unauthorized attempts to modify profiles on a RACF dataset - these events are only logged if a user with the AUDITOR attribute has issued the SETROPTS command with the AUDIT, SAUDIT, or CMDVIOL options, or the ALTUSER command with the UAUDIT option.

SMF type 81 records are written at the completion of RACF initialization. The following information is recorded:

- Date and time of RACF initialization.

- System identification.

- Dataset and volume identification of the RACF dataset for this IPL.

- Active RACF options.

- Maximum password change interval.

The RACF report writer can be run in batch mode using the following Job Control Language:

```
//JOBNAME    JOB Installation Defined JOB Card Goes Here
//STEP01    EXEC PGM=IKJEFT01,DYNAMNBR=30
//SORTLIB     DD DSN=SYS1,SORTLIB,DISP=SHR
//RSMFIN      DD DSN=Name of SMF Dump Dataset Goes Here
//SORTIN      DD UNIT=SYSDA,DISP=(,DELETE),SPACE=(CYL,(5,1,),RLSE)
//SORTWK01    DD UNIT=SYSDA,DISP=(,DELETE),SPACE=(CYL,(5,1,),RLSE)
//SORTWK02    DD UNIT=SYSDA,DISP=(,DELETE),SPACE=(CYL,(5,1,),RLSE)
//SORTWK03    DD UNIT=SYSDA,DISP=(,DELETE),SPACE=(CYL,(5,1,),RLSE)
//SYSPRINT    DD SYSOUT=*
//SYSTSPRT    DD SYSOUT=*
//SYSTSIN     DD *
***** PUT RACF REPORT WRITER COMMAND STATEMENTS HERE - SEE NOTE
/*
//
```

Note: Since the input SMF datasets are allocated on the RSMFIN DD card, neither the DSNAME nor the DATASET parameters on the RACFRW command should be used. If they are entered, the RACF report writer will ignore the dataset(s) entered on the RSMFIN DD card.

Detail of RACF Report Writer (RACFRW)

The command syntax of the report writer has the following structure:

```
RACFRW options
  SELECT options
  EVENT options
  LIST options
  SUMMARY options
END
```

The format, syntax, and meaning of the above commands follows.

RACFRW Options

The RACF command invokes the RACF report writer. The following options can be specified on the command line:

TITLE('string') — Specifies a default title.

DATA('string') — Specifies a string of data to be passed to the ICHRSMFE installation exit.

FORMAT — During processing, RACF will reformat the SMF records to facilitate sorting. This parameter indicates to the RACF report writer that the SMF records used as input have not been previously formatted and saved. If neither the FORMAT nor the NOFORMAT parameters are specified on the command line, then FORMAT processing will occur as the default.

NOFORMAT — This parameter indicates that the input SMF records have been previously formatted by the RACF report writer and have been saved for further processing.

DSNAME('dsname-1, dsname-2, . . .') or
DATASET('dsname-1, dsname-2, . . .')

If either the DSNAME or the DATASET parameters are specified on the command line, then the datasets specified within the quotes are used as the source of the input SMF records. If neither parameter is specified, the RACF report writer will use the dataset pre-allocated to the RSMFIN ddname. There is no functional difference between the DSNAME and DATASET parameters.

SAVE('dsname') — This parameter indicates to the RACF report writer that the formatted SMF records are to be saved for further processing in the dataset specified within the quotes.

GENSUM/NOGENSUM — Indicates a "general summary" report is to be printed. This report lists information relating to the population of input SMF records and the group of SMF records selected. Statistics such as total number of SMF records input and selected, total job/logon attempts, successes, and failures, and total resource access attempts, successes, and failures are provided. If this parameter is not specified, no general summary report will be printed.

An example of a RACFRW command line follows:

```
RACFRW DSNAME('SYS1.SMFLOG1') GENSUM TITLE('SAMPLE REPORT')
```

The above command indicates that the SMF records used as input will come from the dataset SYS1.SMFLOG1 and that a "general summary" report is desired. Since the FORMAT and LINECNT parameters were excluded, NOFORMAT processing are asumed as the defaults. Also, since the SAVE parameter was excluded, the reformatted SMF records will be discarded.

SELECT Options

The SELECT command allows the user to specify which SMF records should be included in further processing. The SELECT command is usually used in conjunction with the EVENT command (see below). The parameters used with the SELECT command are as follows:

DATE(begin-date:end-date) or
(date-1, date-2, ...)

Specifies a range of dates (in Julian format) or a list of dates that determine whether a specific SMF record is included in further processing. If not specified, all records will be included in further processing.

TIME(begin-time:end-time) or
(time-1, time-2, ...)

Specifies a range of times (in HHMMSS format).

VIOLATIONS — Indicates that only SMF records showing security violations are to be included.

SUCCESSES — Indicates that only SMF records showing successful access attempts are included.

USER(name-1, name-2, ...) Specifies a list of user-ids that are included.

NOUSER — Indicates that records containing user-ids are not to be included in further processing. If USER and NONUSER parameters are not specified, all records containing user-ids will be selected for further processing.

JOB(job-name-1, job-name-2, ...) Specifies a list of job names.

NOJOB — Indicates that records containing job names are to be excluded. If the JOB and NOJOB parameters are not specified, all jobs will be included in further processing. If NOUSER and NOJOB operands are specified, both operands will be ignored.

GROUP(group-name-1, group-name-2, ...) Specifies a list of group names.

STEP(step-name-1, step-name-2, ...) Specifies a list of job step names.

STATUS — Indicates that only SMF record type 80 records will be selected. These record types are generated by the SETROPTS or RVARY command.

PROCESS — Specifies that only RACF process SMF record types will be included. RACF process SMF records are types 20, 30, and 80.

SYSID(sytem-id-1, system-id-2, ...) Specifies a list of system ids.

AUTHORITY(authority-1, authority-2, ...)

Specifies a list of authorities from the following list for which records will be included if the user was allowed access because he had the given level of authority:

SPECIAL	User had the SPECIAL attribute.
OPERATIONS	User had the OPERATIONS attribute.
EXIT	Action by an installation exit.

NORMAL — The user had sufficient access authority without the influence of the above authorities.

REASON(reason-1, reason-2, ...)

Specifies a list of reasons why the event was logged for further processing.

- CLASS - Resource class logging was in effect.
- USER - USER logging was in effect.
- SPECIAL - SPECIAL logging was in effect.
- RESOURCE - RESOURCE logging was in effect.
- RACINIT - RACINIT SVC.
- COMMAND - Command that is always logged (SETROPTS or RVARY).
- CMDVIOL - Command violation logging was in effect.
- AUDITOR - GLOBALAUDIT auditing was in effect.

TERMINAL(terminal-id-1, terminal-id-2, ...)

Specifies a list of terminal ids.

An example of a SELECT command line follows:

```
SELECT USER(JONES,SMITH) AUTHORITY(OPERATIONS) DATE(84001:84182)
```

Select only users Jones and Smith for further processing only if they had RACF activity between January 1, 1984 and June 30, 1984, and if the only reason that resource access was granted was because they had the OPERATIONS attribute.

Event Options

The EVENT command must be used in conjunction with the SELECT command (even if the SELECT command had no parameters) and it provides a second level of SMF record selection.

EVENT NAME

- LOGON - TSO or batch job initiation.
- ACCESS - Access to a protected resource.
- ADDVIOL - Addition of a volume to a multi-volume dataset or tape volume.
- RENAME - Renaming of a dataset.
- DELETE - Deletion of a dataset or tape volume.
- DELVIOL - Deletion of a volume from a multi-volume dataset or tape volume.
- DEFINE - Definition of a dataset or tape volume.
- ALLSVC - Any of the above events (ACCESS, ADDVOL, RENAME, DELETE, DELVOL, and DEFINE).
- ADDSD - Adding a dataset profile.
- ADDGROUP - Adding a group profile.
- ADDUSER - Adding a user profile.

ALTDSD - Modification of a dataset profile.
ALTGROUP - Modification of a group profile.
ALTUSER - Modification of a user profile.
CONNECT - Connecting a user to a group.
DELDSD - Deletion of a dataset profile.
DELGROUP - Deletion of a group profile.
DELUSER - Deletion of a user profile.
PASSWORD - Any issuance of the PASSWORD command.
PERMIT - Addition of a user or group to the access list of a resource profile.
RALTER - Modification of a general resource profile.
RDEFINE - Addition of a general resource profile.
RDELETE - Deletion of a general resource profile.
REMOVE - Removal of a user/group connection (established with the CONNECT command).
RVARY - Switches active RACF datasets and/or turns RACF off.
SETROPTS - Sets global processing options.
ALLCOMMAND - Issuance of any of the above commands.

EVQUAL(event-qualifier-1, event-qualifier-2, ...)

Event	Qualifier	Description
TSO or job initiation	0	Successful initiation
	1	Invalid password
	2	Invalid group
	3	Invalid OID card
	4	Invalid terminal
	5	Invalid application
	6	Invalid user-id
	7	Invalid automatically revoked
Resource access	0	Successful access
	1	Insufficient authority
	2	Profile not found
ADDVOL	0	Successful processing
	1	Insufficient authority
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
Delete resource	0	Successful deletion
	1	Resource not found
	2	Invalid volume
DELVOL	0	Successful deletion

Event	Qualifier	Description
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
RVARY	0	Successful completion
	1	Insufficient authority
	2	Keyword violation

CLASS(class-name-1, class-name-2, ...) Specifies a list of class-names.

NAME(name-1, name-2, ...) Specifies a list of resource names.

DSQUAL(ds-qualifier-1, ds-qualifier-2, ...)

Specifies a list of high-level dataset name qualifiers.

INTENT(access level list)

Specifies a list of intended access levels for which records showing attempted resource accesses will be selected.

. READ . UPDATE . CONTROL . ALTER

ALLOWED(access level list)

Specifies a list of allowed access levels for which records showing attempted resource accesses will be selected.

. READ . UPDATE . CONTROL . ALTER

NEWNAME(name-1, name-2, ...)

Specifies a list of new dataset names (RENAME event).

NEWDSQUAL(qualifier-1, ..)

Specifies a list of new dataset name high level qualifiers (RENAME event).

LEVEL(begin-level:end-level) or (level-1, level-2, ...)

Specifies a range or list of resource levels.

An example of the EVENT command line follows:

```
EVENT ACCESS ALLOWED(ALTER,UPDATE)
```

LIST Options

The LIST command allows to specify the order of a printed RACF report.

SORT(sort-field-1, sort-field-2, ...)
(DATE/TIME/SYSID/USER/GROUP/EVENT/EVQUAL/TYPE/NAME/CLASS/TERMINAL/JOBID)

This parameter specifies a list of sort fields from the following:

DATE	- SMF record date in Julian format
TIME	- SMF record time in HHMMSS format
SYSID	- System identifier
USER	- User-id
GROUP	- Group name
EVENT	- Event code
EVQUAL	- Event qualifier
TYPE	- Event types
	1 = JOB/LOGON events
	2 = SVC events
	3 = Command events
NAME	- Resource name
CLASS	- Resource class
TERMINAL	- Terminal identifier
JOBID	- JOB identifier

An example of the LIST command follows:

```
LIST SORT(USER,DATE,TIME) NEWPAGE
```

List all selected records sorted by user, date of record, and time of record. A page break will occur every time the user-id changes during the reporting process. Since neither the ASCEND nor the DESCEND parameter was specified, sorting will proceed in ascending order.

SUMMARY Option

The SUMMARY command allows to specify that a report summarizing the information selected by the SELECT and EVENT commands should be printed.

name-1	Determines the major field on which the information is to be summarized (GROUP, USER, RESOURCE, EVENT, and COMMAND).
VIOLATIONS	This parameter specifies that only violations are to be included in the summary report.
SUCCESSES	This parameter specifies that only successes are to be included in the summary report.

An example:

```
SUMMARY COMMAND BY(USER)
```

Print the summary report summarizing by user within command.

The END command terminates the selection process, and begins the processing phase of the RACF report writer.

Sample RACF report writer commands follow:

```
RACFRW DSNAME('SYS.SMFLOG1') GENSUM
  SELECT USER(SMITH,JONES) AUTHORITY(SPECIAL,OPERATIONS)
  EVENT ALLCOMMAND
  LIST SORT(USER,DATE,TIME) ASCEND
  SUMMARY COMMAND BY(USER) NEWPAGE
END
```

The above command list will cause the RACF report writer to obtain the input SMF records from SYS1.SMFLOG1 and select records for users Smith and Jones only when a RACF command was issued and when the command was allowed because they had the SPECIAL or OPERATIONS attribute(s). The report will be sorted by user-id, date, and time in ascending order. A summary report will be printed summarizing command issuance by user-id. A page break will occur in the summary report when the command changes. A general summary report will also be printed.

Example of RACFRW Reports

The following JCL will create the sample reports included:

```
//STEP01  EXEC PGM=IKJEFT01,DYNAMNBR=20
//RSMFIN    DD DSN=SYS1.MAN1,DISP=SHR
//SORTIN    DD UNIT=SYSDA,SPACE=(CYL,(5,1),RLSE)
//SORTWK01  DD UNIT=SYSDA,SPACE=(4096,(150,25),RLSE)
//SORTWK02  DD UNIT=SYSDA,SPACE=(4096,(150,25),RLSE)
//SORTWK03  DD UNIT=SYSDA,SPACE=(4096,(150,25),RLSE)
//SYSTSPRT  DD DSN=D312RLE.RACF,DISP=(,CATLG,DELETE),
//             UNIT=3380,SPACE=(CYL,(1,1),RLSE)
//SORTMSG   DD SYSOUT=*
//SYSOUT    DD SYSOUT=*
//SYSPRINT  DD SYSOUT=*
//SYSTSIN   DD *
RACFRW TITLE('CNL COMPANY, INC - ANALYSIS OF USE OF SPECIAL AUTHORITY')
SELECT PROCESS AUTHORITY(SPECIAL)
EVENT ALLCOMMAND
LIST SORT(USER EVENT DATE TIME) NEWPAGE
SUMMARY COMMAND BY(USER)
END
RACFRW TITLE('CNL COMPANY, INC - ANALYSIS OF USE OF OPERATIONS AUTHORITY')
SELECT PROCESS AUTHORITY(OPERATIONS)
EVENT ALLSVC
LIST SORT(USER EVENT DATE TIME) NEWPAGE
SUMMARY COMMAND BY(USER)
END
.
.
.
/*
```

Following reports included are:

- Use of SPECIAL Authority
- Use of OPERATION Authority
- Use of EXIT Authority
- Use of SETROPTS nad RVARY Commands
- Resource access violations
- Violation resulting in REVOKE

Use of SPECIAL Authority

```
RACFRW TITLE('CNL COMPANY, INC - ANALYSIS OF USE OF SPECIAL AUTHORITY')
SELECT PROCESS AUTHORITY(SPECIAL)
EVENT ALLCOMMAND
LIST SORT(USER EVENT DATE TIME) NEWPAGE
SUMMARY COMMAND BY(USER)
END
```

```
85.228 17:57:00                         RACF REPORT - LISTING OF PROCESS RECORDS                                 PAGE   3
                                 CNL COMPANY, INC - ANALYSIS OF USE OF SPECIAL AUTHORITY
                                                       E
                                                       V  Q
                                                       E  U
                        *JOB/     *STEP/   --TERMINAL-- N  A
  DATE     TIME   SYSID  USER      GROUP      ID     LVL T  L
85.227 15:56:09 CJAX   L113CRS   DSA                  0 13  0  JOBID=(L113CRSC 85.227 15:53:13),USERDATA=(C ),OWNER=L351DSA
                                                               AUTH=(SPECIAL),REASON=(CLASS,SPECIAL)
                                                                 ALTUSER L112DMM RESUME
85.227 16:42:47 CJAX   L113CRS   DSA                  0 17  0  JOBID=(L113CRSC 85.227 16:42:14),USERDATA=(C ),OWNER=L351DSA
                                                               AUTH=(SPECIAL),REASON=(CLASS,SPECIAL)
                                                                 DELUSER D133NRD
85.227 17:00:53 CJAX   L113CRS   DSA                  0 17  0  JOBID=(L113CRSC 85.227 16:56:38),USERDATA=(C ),OWNER=L351DSA
                                                               AUTH=(SPECIAL),REASON=(CLASS,SPECIAL)
                                                                 DELUSER L311JPW
85.227 17:06:03 CJAX   L113CRS   DSA                  0 17  0  JOBID=(L113CRSC 85.227 17:03:41),USERDATA=(C ),OWNER=L351DSA
                                                               AUTH=(SPECIAL),REASON=(CLASS,SPECIAL)
                                                                 DELUSER D310JRK
                                                               AUTH=(SPECIAL),REASON=(CLASS,SPECIAL)
                                                                 DELUSER D211TMH
85.227 15:56:14 CJAX   L113CRS   DSA                  0 18  0  JOBID=(L113CRSC 85.227 15:53:13),USERDATA=(C ),OWNER=L351DSA
                                                               AUTH=(SPECIAL),REASON=(CLASS,SPECIAL)
                                                                 PASSWORD USER(L112DMM)
85.227 15:56:16 CJAX   L113CRS   DSA                  0 18  0  JOBID=(L113CRSC 85.227 15:53:13),USERDATA=(C ),OWNER=L351DSA
                                                               AUTH=(SPECIAL),REASON=(CLASS,SPECIAL)
                                                                 PASSWORD USER(L112DMM)
```

```
85.228 17:57:00                         RACF REPORT - COMMAND BY USER SUMMARY                                    PAGE   8
                                 CNL COMPANY, INC - ANALYSIS OF USE OF SPECIAL AUTHORITY
                       QUALIFIER                  OCCURRENCES    USER
EVENT = 13 - ALTUSER COMMAND
              0 - NO VIOLATIONS DETECTED
                                                         1       L113CRS
                                                         1       L113RLC
                   ACCUMULATED TOTALS -                  2
              ACCUMULATED TOTALS -                       2
EVENT = 17 - DELUSER COMMAND
              0 - NO VIOLATIONS DETECTED
                                                         6       L113CRS
                                                         3       L113RLC
                   ACCUMULATED TOTALS -                  9
              ACCUMULATED TOTALS -                       9
EVENT = 18 - PASSWORD COMMAND
              0 - NO VIOLATIONS DETECTED
                                                         2       L113CRS
                                                        13       L311BDF
                                                         1       L311JTA
                   ACCUMULATED TOTALS -                 16
              ACCUMULATED TOTALS -                      16
```

Use of OPERATION Authority

```
RACFRW TITLE('CNL COMPANY, INC - ANALYSIS OF USE OF OPERATIONS AUTHORITY')
SELECT PROCESS AUTHORITY(OPERATIONS)
EVENT ALLSVC
LIST SORT(USER EVENT DATE TIME) NEWPAGE
SUMMARY COMMAND BY(USER)
END
```

```
85.231 12:53:21                    RACF REPORT - LISTING OF PROCESS RECORDS                    PAGE    3
                        CNL COMPANY, INC - ANALYSIS OF USE OF OPERATIONS AUTHORITY

                                                                  EVENT  QUAL
DATE     TIME     SYSID  *JOB/USER   *STEP/GROUP  --TERMINAL-- ID  LVL

85.229 19:55:40 CJAX   L322SUP    L322         T12A02R      0    7    0   JOBID=(L322SUP 85.229 19:43:45),USERDATA=(),OWNER=L322SUP
                                                                          AUTH=(OPERATIONS),REASON=(CLASS)
                                                                          DATASET=POPS.DLSCJOB,LEVEL=00

85.229 19:56:14 CJAX   L322SUP    L322         T12A02R      0    7    0   JOBID=(L322SUP 85.229 19:43:45),USERDATA=(),OWNER=L322SUP
                                                                          AUTH=(OPERATIONS),REASON=(CLASS)
                                                                          DATASET=POPS.SAMPFOR,LEVEL=00

85.229 23:45:52 CJAX   L322SUP    L322         T12A03D      0    2    0   JOBID=(L322SUP 85.229 23:45:14),USERDATA=(),OWNER=L322
                                                                          AUTH=(OPERATIONS),REASON=(USER)
                                                                          DATASET=POPS.SAMPFOR,VOLUME=PFIN02,LEVEL=00,INTENT=READ
                                                                          ALLOWED=NONE,APPL=
```

```
85.231 12:53:21                    RACF REPORT - COMMAND BY USER SUMMARY                       PAGE    6
                        CNL COMPANY, INC - ANALYSIS OF USE OF OPERATIONS AUTHORITY

                    QUALIFIER                    OCCURRENCES      USER

EVENT = 2 - RESOURCE ACCESS
        0 - NO VIOLATIONS DETECTED
                                                      10          L322SUP
                                                       2          L327SUP
            ACCUMULATED TOTALS -                      12
        ACCUMULATED TOTALS -                          12
EVENT = 7 - DEFINE RESOURCE
        0 - NO VIOLATIONS DETECTED
                                                       1          L322SUP
                                                       1          L327SUP
            ACCUMULATED TOTALS -                       2
        ACCUMULATED TOTALS -                           2
```

Use of EXIT Authority

```
RACFRW TITLE('CNL COMPANY, INC - ANALYSIS OF USE OF EXIT AUTHORITY')
SELECT PROCESS AUTHORITY(EXIT)
EVENT ALLCOMMAND
EVENT ALLSVC
LIST SORT(USER EVENT DATE TIME) NEWPAGE
SUMMARY COMMAND BY(USER)
END
```

```
85.231 12:53:21                    RACF REPORT - LISTING OF PROCESS RECORDS                    PAGE    3
                                CNL COMPANY, INC - ANALYSIS OF USE OF EXIT AUTHORITY

                                                                  E  Q
                                                                  V  U
                                *JOB/      *STEP/     --TERMINAL--  E  A
DATE      TIME      SYSID       USER       GROUP        ID      LVL  N  L
85.229 19:55:40 CJAX  L322SUP    L322       T12A02R      0    7   0  JOBID=(L322SUP 85.229 19:43:45),USERDATA=(),OWNER=L322SUP
                                                                    AUTH=(EXIT),REASON=(CLASS)
                                                                    DATASET=POPS.DESCJOB,LEVEL=00

85.229 19:56:14 CJAX  L322SUP    L322       T12A02R      0    7   0  JOBID=(L322SUP 85.229 19:43:45),USERDATA=(),OWNER=L322SUP
                                                                    AUTH=(EXIT),REASON=(CLASS)
                                                                    DATASET=POPS.SAMPFOR,LEVEL=00

85.229 23:45:52 CJAX  L322SUP    L322       T12A03D      0    2   0  JOBID=(L322SUP 85.229 23:45:14),USERDATA=(),OWNER=L322
                                                                    AUTH=(EXIT),REASON=(USER)
                                                                    DATASET=POPS.SAMPFOR,VOLUME=PFIN02,LEVEL=00,INTENT=READ
                                                                    ALLOWEW=NONE,APPL=
```

```
85.231 12:53:21                    RACF REPORT - COMMAND BY USER SUMMARY                       PAGE    6
                                CNL COMPANY, INC - ANALYSIS OF USE OF EXIT AUTHORITY

                    QUALIFIER                    OCCURRENCES      USER
EVENT = 2 - RESOURCE ACCESS
          0 - NO VIOLATIONS DETECTED
                                                      10          L322SUP
                                                       2          L327SUP
              ACCUMULATED TOTALS -                    12
          ACCUMULATED TOTALS -                        12
EVENT = 7 - DEFINE RESOURCE
          0 - NO VIOLATIONS DETECTED
                                                       1          L322SUP
                                                       1          L327SUP
              ACCUMULATED TOTALS -                    2
          ACCUMULATED TOTALS -                        2
```

Use of SETROPTS and RVARY Commands

```
RACFRW TITLE('CNL COMPANY, INC - ANALYSIS OF USE OF SETROPTS AND RVARY')
SELECT
EVENT RVARY
EVENT SETROPTS
LIST SORT(USER EVENT DATE TIME) NEWPAGE
END
```

```
85.228 15:19:21                    RACF REPORT - LISTING OF STATUS RECORDS                    PAGE   3

                          CNL COMPANY, INC - ANALYSIS OF USE OF SETROPTS AND RVARY

                                    ACTIVE
DATE    TIME     SYSID MISC. OPTIONS      EXITS    CLASS     PROT STAT AUD GEN GCMD GLBL
85.227 05:59:38 CJAX  ORIGIN:    IPL      ICHRIX01 DATASET   YES  NO   YES YES YES  YES
                      TERMUACC:  READ     ICHRIX02 USER                YES
                      CMNDVIOL:  YES      ICHRCX01 GROUP               YES
                      LOGSPEC:   YES      ICHRDX01 DASDVOL   YES  NO   YES
                      RACINIT:   STATS             TAPEVOL   YES  NO   YES
                      ADSP:      ACTIVE            TERMINAL  NO   NO   NO
                      REALDSN:   NO                APPL      YES  NO   YES
                      JES:                         TIMS      YES  NO   YES      YES
                        NOBATCHALLRACF             GIMS      YES  NO   YES
                        NOXBMALLRACF               AIMS      YES  NO   YES      YES
                        NOEARLYVERIFY              TCICSTRN  YES  NO   YES
                      DUPDS:     YES               GCICSTRN  YES  NO   YES
                                                   PCICSPSB  YES  NO   YES
                                                   QCICSPSB  YES  NO   YES
                                                   GMBR      YES  NO   NO
                                                   GLOBAL    YES  NO   NO
                                                   DSNR      NO   NO   NO
                                                   TTRG      YES  NO   YES      YES
                                                   GTRG      YES  NO   YES
                                                   ATRG      YES  NO   NO
                                                   TPRD      YES  NO   YES      YES
                                                   GPRD      YES  NO   YES
                                                   APRD      YES  NO   NO
                                                   TDEV      YES  NO   YES      YES
                                                   GDEV      YES  NO   YES
                                                   ADEV      YES  NO   NO

                                    TYPE     STATUS   SEQ  UNIT VOLUME DATASET NAME

                                    UADS                       SLIBR2 SYS1.UADS
                                    PRIMARY  ACTIVE     1  236  SRACF3 SYS1.RACF
                                    BACKUP   INACTIVE   1  176  SRACF1 SYS1.BKUP.RACF

                                    OTHER OPTIONS -

                                      USER MODELLING IS ACTIVE

                                      GROUP MODELLING IS ACTIVE

                                      'LIST-OF-GROUPS' ACCESS CHECKING IS ACTIVE

                                      SINGLE LEVEL NAME PREFIX IS RAC1LVL

                                      INTERVAL:    30 DAYS
                                      HISTORY:     10 GENERATIONS
                                      REVOKE:       5 TRIES
                                      WARNING:     10 DAYS
                                      INACTIVE:    60 DAYS

                                      RULE  1   LENGTH(4:8)   LLLLLLLL
                                      RULE  2   LENGTH(4:8)   AAAAAAAA
                                      RULE  3   LENGTH(4:8)   NNNNNNNN
```

Resource Access Violations

```
RACFRW TITLE('CNL COMPANY, INC - ANALYSIS OF RESOURCE ACCESS VIOLATIONS')
SELECT VIOLATIONS
EVENT ALLSVC
EVENT SETROPTS
LIST SORT(EVENT USER DATE TIME) NEWPAGE
END
```

```
85.228 11:06:42                  RACF REPORT - LISTING OF PROCESS RECORDS                                 PAGE   6
                           CNL COMPANY, INC - ANALYSIS OF RESOURCE ACCESS VIOLATIONS
                                                            E
                                                            V  Q
                                                            E  U
                           *JOB/     *STEP/    --TERMINAL-- N  A
 DATE    TIME    SYSID     USER      GROUP      ID     LVL  T  L

85.228 00:38:35 CJAX  *DR3800BM *DR38020                0   2  1  JOBID=(DR3800BM 85.228 00:38:25),USERDATA=(   -2 ),OWNER=L327SUP
                                                                  AUTH=(NORMAL),REASON=(ENTITY OR FAILSOFT PROCESSING)
                                                                  DATASET=PIMS2R.RECON1,GENPROF=PIMS2R.*,VOLUME=PIMSB1,LEVEL=00,
                                                                  INTENT=CONTROL,ALLOWED=READ,APPL=

85.228 00:38:35 CJAX  *DR3800BM *DR38020                0   2  1  JOBID=(DR3800BM 85.228 00:38:25),USERDATA=(   -2 ),OWNER=L327SUP
                                                                  AUTH=(NORMAL),REASON=(ENTITY OR FAILSOFT PROCESSING)
                                                                  DATASET=PIMS2R.RECON2,GENPROF=PIMS2R.*,VOLUME=PIMSB1,LEVEL=00,
                                                                  INTENT=CONTROL,ALLOWED=READ,APPL=

85.227 10:42:55 CJAX  *D210CSTA *STEP02                 0   2  1  JOBID=(D210CSTA 85.227 10:41:50),USERDATA=(   )= ),OWNER=L327SUP
                                                                  AUTH=(NORMAL),REASON=(ENTITY OR FAILSOFT PROCESSING)
                                                                  DATASET=PNSRD.EA.EABUSOP1,GENPROF=PNSRD.*,VOLUME=PDBY01,LEVEL=00,
                                                                  INTENT=READ,ALLOWED=NONE,APPL=

85.227 07:45:28 CJAX  *D320DJGS *LIBGET                 0   2  1  JOBID=(D320DJGS 85.227 07:45:23),USERDATA=(C )> ),OWNER=L322SUP
                                                                  AUTH=(NORMAL),REASON=(ENTITY OR FAILSOFT PROCESSING)
                                                                  DATASET=SYS1.ICFCAT.TDVST1,GENPROF=SYS1.ICFCAT.*,VOLUME=TDVST1,
                                                                  LEVEL=00,INTENT=CONTROL,ALLOWED=UPDATE,APPL=

85.227 16:49:31 CJAX   D451SWE   D451     T12A023       0   2  1  JOBTD=(D451SWE 85.227 12:28:00),USERDATA=(),OWNER=L322SUP
                                                                  AUTH=(NORMAL),REASON=(ENTITY OR FAILSOFT PROCESSING)
                                                                  DATASET=L322.IOGEN.CNTL,GENPROF=L322.*,VOLUME=SMVS01,LEVEL=00,
                                                                  INTENT=READ,ALLOWED=NONE,APPL=

85.227 04:44:45 CJAX   L222TSR   L222     T12A021       0   2  1  JOBID=(L222TSR 85.227 03:10:42),USERDATA=(),OWNER=L327SUP
                                                                  AUTH=(NORMAL),REASON=(ENTITY OR FAILSOFT PROCESSING)
                                                                  DATASET=L113.LIB.MOVE.IMS,VOLUME=POPER1,LEVEL=00,INTENT=READ,
                                                                  ALLOWED=NONE,APPL=

85.227 01:36:24 CJAX   L311ESP   CR6                    0   2  1  JOBID=(AI0100BU 85.227 00:57:49),USERDATA=(   ),OWNER=L327SUP
                                                                  AUTH=(NORMAL),REASON=(ENTITY OR FAILSOFT PROCESSING)
                                                                  DATASET=PIMS3R.RECON1,GENPROF=PIMS3R.*,VOLUME=PIMSC1,LEVEL=00,
                                                                  INTENT=CONTROL,ALLOWED=READ,APPL=

85.227 01:36:24 CJAX   L311ESP   CR6                    0   2  1  JOBID=(AI0100BU 85.227 00:57:49),USERDATA=(   ),OWNER=L327SUP
                                                                  AUTH=(NORMAL),REASON=(ENTITY OR FAILSOFT PROCESSING)
                                                                  DATASET=PIMS3R.RECON2,GENPROF=PIMS3R.*,VOLUME=PIMSC1,LEVEL=00,
                                                                  INTENT=CONTROL,ALLOWED=READ,APPL=

85.227 01:36:25 CJAX   L311ESP   CR6                    0   2  1  JOBID=(AI0100BU 85.227 00:57:49),USERDATA=(   ),OWNER=L327SUP
                                                                  AUTH=(NORMAL),REASON=(ENTITY OR FAILSOFT PROCESSING)
                                                                  DATASET=PIMS3R.RECON3,GENPROF=PIMS3R.*,VOLUME=PIMSC1,LEVEL=00,
                                                                  INTENT=CONTROL,ALLOWED=READ,APPL=

85.227 01:39:11 CJAX   L311ESP   CR6                    0   2  1  JOBID=(EABUSFIX 85.227 00:54:12),USERDATA=(   ),OWNER=L327SUP
                                                                  AUTH=(NORMAL),REASON=(ENTITY OR FAILSOFT PROCESSING)
                                                                  DATASET=PNSRD.EA.EABUSOP1,GENPROF=PNSRD.*,VOLUME=PDBY01,LEVEL=00,
                                                                  INTENT=CONTROL,ALLOWED=NONE,APPL=
```

Violations Resulting in Revoke

```
RACFRW TITLE('CNL COMPANY, INC - LOGON VIOLATIONS RESULTING IN REVOKE')
SELECT VIOLATIONS
EVENT LOGON EVQUAL(7)
EVENT SETROPTS
LIST SORT(USER DATE TIME)
END
```

```
85.228 10:59:20                    RACF REPORT - LISTING OF PROCESS RECORDS                    PAGE   6
                                CNL COMPANY, INC - LOGON VIOLATIONS RESULTING IN REVOKE

                                                                    E  Q
                                                                    V  U
                                                                    E  A
                          *JOB/      *STEP/     --TERMINAL--      N  L
 DATE     TIME    SYSID   USER       GROUP        ID      LVL     T
85.227 13:44:57 CJAX    L311MDK    CR1        T11D0AB      0      1  7   JOBID=( 00.000 00:00:00),USERDATA=(),OWNER=
                                                                         AUTH=(NONE),REASON=(RACINIT FAILURE)
```

THE DATA SECURITY MONITOR

The Data Security Monitor (DSMON) is a program (ICHDSM00) supplied by IBM with RACF which prints seven reports concerning the status of RACF. No control cards are needed to run DSMON. The user executing DSMON must have the system Auditor attribute.

The JCL needed to run DSMON is as follows:

```
//JOBNAME1  JOB Installation Defined JOB Card Goes Here ...
//STEP01   EXEC PGM=ICHDSM00
//SYSUT1     DD DSN=SYS1.PARMLIB,DISP=SHR
//SYSUT2     DD SYSOUT=*
//SYSPRINT   DD SYSOUT=*
/*
//
```

Examples of the DSMON reports follow:

1 - System Report
2 - Program Properties Table
3 - RACF Authorized Caller Table Report
4 - RACF Exits Reports
5 - Selected User Attribute Report
6 - Selected User Attribute Summary Report
7 - Selected Datasets Report

1. SYSTEM REPORT

```
RACF DATA SECURITY MONITOR                                   DATE: 08/13/85     TIME: 10:24:16     PAGE:    1

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

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

CPU-ID                              123456
CPU MODEL                           3081
OPERATING SYSTEM/LEVEL              MVS/ 3.8   SP2.1.2 JBB2125
SYSTEM RESIDENCE VOLUME             SIPLJC
SMF-ID                              SYS4
RACF VERSION 1 RELEASE 6 IS ACTIVE
```

The system report lists information concerning the computer system on which RACF is executing.

2. PROGRAM PROPERTIES TABLE

RACF DATA SECURITY MONITOR DATE: 08/13/85 TIME: 10:24:16 PAGE: 2

PROGRAM PROPERTIES TABLE REPORT

PROGRAM NAME	BYPASS PASSWORD PROTECTION	SYSTEM KEY
IEDQTCAM	NO	YES
ISTINM01	YES	YES
IKTCAS00	NO	YES
AHLGTF	NO	YES
HHLGTF	NO	YES
IHLGTF	NO	YES
IEFIIC	NO	YES
IEEMB860	YES	YES
IEEVMNT2	NO	YES
IASXWR00	NO	YES
CSVVFCRE	NO	YES
HASJES20	YES	YES
DFSMVRC0	NO	YES
IATINTK	YES	YES

Lists all programs contained in the program properties table and whther or not access checking will occur for resources accessed by these programs.

BYPASS PASSWORD PROTECTION — This column indicates whether or not RACF protection is effective for resources accessed by the propram.

SYSTEM KEY — This column indicates whether or not the program is authorized to execute in a system key and is thus able to bypass MVS system integrity controls.

3. RACF AUTHORIZED CALLER TABLE REPORT

RACF DATA SECURITY MONITOR DATE: 08/13/85 TIME: 10:24:16 PAGE: 3

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 NAME	RACINIT AUTHORIZED	RACLIST AUTHORIZED
DS10STXX	YES	NO
DS10ST01	NO	YES

Lists all programs in the RACF authorized caller table. These pograms are auhtorized to issue hte RACINIT and RACLIST SVCs.

RACINIT AUTHORIZED — Indicates whether or not the program is authorized to issue the RACINIT SVC.

RACLIST AUTHORIZED — Indicates whether or not the program is authorized to issue the RACLIST SVC.

4. RACF EXITS REPORT

RACF DATA SECURITY MONITOR DATE: 08/13/85 TIME: 10:24:16 PAGE: 4

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

EXIT MODULE NAME	MODULE LENGTH
ICHDEX01	224
ICHRCX01	296
ICHRDX01	592
ICHRIX02	112
ICHRIX01	168

Lists the names of the active RACF exits.

5. SELECTED USER ATTRIBUTE REPORT

RACF DATA SECURITY MONITOR DATE: 08/13/85 TIME: 10:24:16 PAGE: 5

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
A314ABC	SYSTEM	SYSTEM		
A323CAB			SYSTEM	
A332BCA	GROUP			
B111MDD		GROUP		SYSTEM
B111RLE	GROUP			
B112ME2			GROUP	
IBMUSER	SYSTEM	SYSTEM	SYSTEM	SYSTEM

Lists the user-ids of all users with group or system SPECIAL, OPERATIONS, AUDITOR, or REVOKE attributes.

6. SELECTED USER ATTRIBUTE SUMMARY REPORT

RACF DATA SECURITY MONITOR DATE: 08/13/85 TIME: 10:24:16 PAGE: 6

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: 1,150

TOTAL SELECTED ATTRIBUTE USERS:

ATTRIBUTE BASIS	SPECIAL	OPERATIONS	AUDITOR	REVOKE
SYSTEM	2	2	2	2
GROUP	2	1	1	0

Lists totals for the users listed on the Selected User Attribute Report.

TOTAL DEFINED USERS — The total number of RACF users defined by the installation.

TOTAL SELECTED ATTRIBUTE USERS — The total number of users selected for each of the selected user attributes at both the system and group level.

7. SELECTED DATASETS REPORT

RACF DATA SECURITY MONITOR DATE: 08/13/85 TIME: 10:24:16 PAGE: 7

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
IMSPERF.EM240.01.LOAD	SYSB01	APF	NO	NO	
IMSPERF.EM240112.01.LOAD	SMIX01	APF	NO	NO	
IMSPERF.MZ.AUTHLIB2	SMIX01	APF	NO	NO	
IMSPERF.OMAUTH.LOAD	SLIBR2	APF	NO	NO	
IMSPERF.OMEGAEM.LOAD	SLIBR2	APF	NO	NO	
INFOSYS1.LINKLIB	SCOST1	APF	NO	NO	
INFOSYS1.LINKLIB	SMVS01	APF	N.F.		
IPO1.LINKLIB	IPORES	APF	N.F.		
IPO1.LINKLIB	OLDRES	APF	N.M.		
IPO1.LINKLIB	SIPLJA	APF	NO	NO	
IPO1.LINKLIB	SIPLJB	APF	NO	NO	
IPO1.LINKLIB	SIPLJC	APF	NO	NO	
IPO1.LINKLIB	SXARES	APF	NO	NO	
IPO1.LINKLIB	IPODLB	LNKLST	NO	NO	
L322.LOAD	SDUMP1	APF	YES	YES	READ
NSS.$210130.NCPLIB	TNSS01	APF	N.F.		
NSS.$210130.SSPLIB	TNSS01	APF	NO	NO	
NSS.$210200.NCPLIB	TNSS01	APF	NO	NO	
NSS.$210200.SSPLIB	TNSS01	APF	NO	NO	
NSS.V3R0.NCPLIB	TNSS01	APF	NO	NO	
NSS.V3R0.SSPLIB	TNSS01	APF	NO	NO	
PCICS.LOADLIB1	PCICS1	APF	N.M.		
PCICS.LOADLIB1	PIMSC2	APF	NO	NO	
PIMS.MATRIX	PIMSA1	APF	N.F.	YES	READ

SELECTION CRITERIA Indicates why the dataset was selected.

- LNKLST Included in the link list concatenation at IPL.
- APF Included in the Authorized Program Facility list.
- MASTER CATALOG MVS master catalog.
- RACF PRIMARY Primary RACF dataset.
- RACF BACKUP Backup RACF dataset.
- SYSTEM One of the following datasets:
  - SYS1.CMDLIB
  - SYS1.LINKLIB
  - SYS1.LPALIB
  - SYS1.NUCLEUS
  - SYS1.PARMLIB
  - SYS1.PROCLIB
  - SYS1.SVCLIB
  - SYS1.UADS

RACF INDICATED (YES/NO/NC/NM/NF)	Indicates whether the RACF bit is on in the volume table of contents for the DASD volume on which the dataset resides.
. NC	(Dataset is not cataloged.)
. NM	(Volume not mounted.)
. NF	(Not found on the DASD volume indicated by the catalog.)
RACF PROTECTED	Indicates whether or not the dataset has a RACF profile in the RACF dataset.
UACC	Indicates the dataset's universal access authority.

INSTALLATION EXITS

There are three groups of installation exits that may affect RACF and RACF report writer effectiveness.

. RACF processing installation exits:

RACDEF SVC — SVC used to define, modify, and delete discrete and/or generic DASD dataset profiles, or profiles for any resource defined by classes in the class descriptor table.

Pre-processing exit: ICHRDX01 Post-processing exit: ICHRDX02

RACHECK SVC — SVC used to determine if a user is authorized to obtain use of a resource (DASD dataset, or any resource defined by classes in the class descriptor table) protected by RACF. When a user requests access to a RACF-protected resource, acceptance of the the request is based upon the identity of the user and whether user has been permitted sufficient access to the resource.

Pre-processing exit: ICHRCX01 Post-processing exit: ICHRCX02

RACINIT SVC — SVC used to determine if a user-id is defined to RACF and if the user has supplied a valid password and group name. If requested, RACF will provide further validation of operator identification cards during TSO logon procedures.

Pre-processing exit: ICHRIX01 Post-processing exit: ICHRIX02

RACLIST SVC — SVC is used to build "in-storage" resident security profiles for later use by RACHECK an FRACHECK SVCs (described below). The RACLIST pre-/post-processing exit is entered before an in-storage profile is built and again after it is built. The RACLIST selection exit can make specific decisions as to resolution of multiple profile opinions.

Pre-processing exit: ICHRLX01 Post-processing exit: ICHRLX02

FRACHECK — This routine is not a SVC. It is used only to check authorizations to resources protected by RACLIST-created profiles.

Pre-processing exit: ICHRFX01 Post-processing exit: ICHRFX02

RACF provides two command exits, ICHCNX00 and ICHCCX00, a password encryption exit, ICHDEX01 , and a new password exit, ICHPWX01. The command exits, together with the RACDEF and RACHECK pre-processing exits, allow an installation to maintain a DASD dataset naming convention other than the standard RACF naming convention. The major difference between the two command exits are the commands to which they have jurisdiction. For instance, exit ICHCNX00 receives control after command syntax checking and before command processing for the ADDSD, ALTDSD, DELDSD, LISTDSD, PERMIT, and SEARCH commands. ICHCCX00, however, will receive control at the same point in processing for the DELGROUP, DELUSER, and REMOVE commands. The password encryption exit ICHDEX01 can be used to replace the password-masking algorithm with an installation-developed routine. The new password exit is invoked by the RACINIT SVC and by the ALTUSER and PASSWORD TSO commands. This exit can examine the intended new

password and the new password change interval (if invoked from the PASSWORD command). In the case of new password processing, the exit gains control if the following conditions are true:

.. New password is not a duplicate of the current password.

.. New password is not a duplicate of a previous password if the password history option is active.

.. New password does not fail any one of the installation syntax rules.

. SMF Installation Exits

The second group of installation exits are the SMF installation exits. Since RACF records logged events to the SMF dataset(s), their use can affect the recording of the audit trail. The Coopers & Lybrand SMF Analyzer Technical Guide should be referred to for a discussion of the SMF installation exits.

. RACF Report Writer Exits

The third group of installation exits consists of the RACF report writer ICHRSMFE. This exit gains control each time the RACF report writer reads a record from the input SMF dataset. The exit can inspect and/or modify the record. Before returning to the RACF report writer, a return code can be set to indicate whether normal processing should occur (as if the exit had never been taken), or whether the record should be unconditionally accepted or rejected regardless of the selection criteria in the RACF report writer statements. The installation can use this exit to apply additional selection criteria or to suppress selection of this record from further processing.

RACF/IMS INTERFACE

RACF-IMS/VS Control Capabilities

RACF can be used in conjunction with IMS/VS to provide security in the following ways:

- Using an application resource profile for the IMS/VS application RACF can restrict only authorized users to the IMS/VS system, users not on the IMS/VS application resource profile access list will be denie access as long as the application universal access authority is "NONE." If universal access authority is other than "NONE" then users not defined to RACF may still have access to IMS/VS. This checking is not necessary if you ahve specified that IMS is to use RACF during IMS SYSGEN. If RACF is specified, then a valid RACF user-id is required to gain access to IMS/VS.

- Using terminal resource profiles, users can be restricted to signing on to IMS/VS at certain terminals.

- Using transaction resource profiles, users can be restricted to executing only authorized transactions.

When IMS/VS communications software is used with RACF, datasets cannot be protected from IMS users by restricting access via dataset profiles. The concept of relating users to datasets does not exist within IMS/VS. Users are related to transactions. Users are granted or denied authority to execute transactions based upon the contents of the transaction profiles access lists and universal access authorities. The transaction then has authority to access the database by virtue that the transaction operates within the IMS/DC batch program.

Even though the access to the datasets is controlled by transaction authorization when IMS/DC is running, the datasets can be accessed by non-IMS users if the STARTUP JCL for IMS/DC does not specify the datasets as owned. Also, when the IMS/DC job is terminated, the datasets can be accessed by non-IMS users. Thus, RACF dataset protection should still be used as a method of protecting the datasets when they are not under the control of IMS/DC.

If the IMS/VS sysgen option specifies that RACF checking will be used, a bit is turned on in an MVS load module.

When IMS is started, the bit is checked, and if it is not on, a warning will be sent to the console operator notifying him the RACF checking will not occur. If the IMS/VS sysgen option specifies that RACF checking will be used then IMS/VS builds a profile in the IMS control region for each IMS transaction defined to RACF. IMS/VS builds the resident profiles when the START and RESTART IMS commands are entered by the operator. All IMS transaction authorization will refer to the resident profiles for authorization checking.

RACF-IMS/VS

The sequence of RACF checking within IMS/VS[1] follows:

- RACF provides IMS user verification using RACINIT
  - .. checks user password.
  - .. checks group authority.
  - .. checks authorization to IMS/VS[1] application--checks APPL resources.
  - .. checks authorization to physical terminal id--checks TERMINAL resources.
- RACF provides IMS transaction authorization using RACHECK
  - .. checks transaction profile for user or groups authority to "execute" the transaction. Transaction authorization by RACHECK occurs before IMS/VS performs its own security checking. Transactions authority checked by RACHECK include:
    - transactions requested by an IMS/VS user.
    - transactions initiated by an IMS/VS transaction through a DL/1 CHNG call.
- RACF provides IMS user reverification for IMS/VS transactions
  - .. requires user to resubmit the user's password with the transaction.
  - .. RACF compares the password to the original password entered at signon.

RACF AND CICS/VS INTERFACE

CICS (Customer Information Comtrol System) provides an interface to an external security manager. The section described the interface of CICS and RACF. It assumes an understanding of RACF and CICS. Refer to the RACF Technical Guide and the CICS Technical Guide for a detailed understanding of RACF and CICS.

RACF security over CICS can be configured to:

- Control access to the CICS system libraries.
- Control access to the CICS program libraries.
- Control access to the CICS regions.
- Control access to CICS terminal.
- Protect CICS PSBs and Transactions.

However, it should be noted that the normal RACF logging is bypassed for system monitoring and the installation must rely on the CICS logging facility (i.e., the "transient data destination CICS") to monitor violations.

The CICS/RACF interface is the result of coding the CICS resource management modules to use RACF as the external security manager. These modules include:

- DFHSG
- DFHSIT
- DFHSNT
- DFHPCT

DFHSG (System Generation)

DFHSG PROGRAM=CSS needs to be included in the system generation. This parameter causes the signon, CICS security, and RACF interface programs to be loaded into the system.

DFHSIT

The following should be included in the DFHSIT TYPE=CSECT macro:

```
DFHSIT TYPE=CSECT,
     EXTSEC=YES,        ** RACF SUPPORT
     XPSE=CICSPSS,      RACF CICS PSB
     XSP=YES,           RACF CICS SUPPORT
     XTRAN=CICSTRN      RACF CICS TRANS ID
```

EXTSEC=YES - causes checking by RACF.

XSP=YES - indicates that the CICS security program is to be used for resource access control.

XTRAN=CICSTRN - is the default CICS class name for CICS transactions. A prefix of "T" and "G" will be used for RACf CICS transaction and group CICS transaction class names. The CICS class names must agree with RACF's class description table (CDT) or RACF will not provide transaction protection.

XPSB=CICSPSB - is the same as XTRAN except for PSBs. Prefixes are "P" for the PBS class and "Q" for the group PBS class.

By properly setting these parameters, RACF will protect all CICS transactions and PSBs defined to it via RACF resource profiles.

RACF Class Descriptor Table (ICHRRCDE)

```
ICHERCDE    CLASS=TCICSTRN,
            GROUP=GCICSTRN,
            ID=128,
            MAXLNTH=13,
            FIRST=ALPHANUM,
            OTHER=ANY,
            POSIT=6,
            OPER=NO,
            DFTUACC=NONE

ICHERCDE    CLASS=GCICSTRN,
            MEMBER=TCICSTRN,
            ID=129,
            MAXLNTH=13,
            FIRST=ALPHANUM,
            OTHER=ANY,
            POSIT=7,
            OPER=NO,
            DFTUACC=NONE

ICHERCDE    CLASS=PCICSPSB,
            GROUP=QCICSPSB,
            ID=131,
            MAXLNTH=17,
            FIRST=ALPHANUM,
            OTHER=ANY,
            POSIT=6,
            OPER=NO,
            DFTUACC=NONE

ICHERCDE    CLASS=QCICSPSB,
            MEMBER=PCICSPSB,
            ID=130,
            MAXLNTH=17,
            FIRST=ALPHANUM,
            OTHER=ANY,
            POSIT=7,
            OPER=NO,
            DFTUACC=NONE
```

DFHSNT Sign-On Table

CICS provides some native security in the form of security keys and passwords. This security is defined in the Sign-On Table (SNT). Each CICS operator with security level requirement of greater than 1 is defined in the SNT when only native security is used.

For example:

```
OPNAME="JOHNDOE",
EXTSEC=NO,
PASSWORD=JOHNNY,
SCTKEY=(1,4,7),
RSLKEY=(3,5)
```

The installation can choose one to use RACF to control access to the system for all CICS users or it can use RACF to control access for selected CICS users and native CICS security for others.

If the CICS sign-on table is not used, only one entry is required.

```
DFHSNT TYPE=(ENTRY,DEFAULT),
EXTSEC=YES
```

(For EXTSEC the default is no.)

This DFHSNT specification creates one entry in the SNT with a blank operator. The EXTSEC=YES indicates that external security is to be used for operators not found in the sign-on table. if this is the only entry in the sign-on table, all users will be checked by RACF. To retain selected CICS security functions, individual entries are made in the SNT. The following is an example of the SNT with an operator retaining CICS security:

```
SNTCL     TITLE 'DFHSNTCL CICS CLAC SIGN-ON TABLE'
SNTCL     DFHSNT TYPE=INITIAL,
                 EXTSEC=YES

DFHSNT TYPE=ENTRY,
      OPNAME="STEVE SIGMUND",
      PASSWRD=PASS,
      OPIDENT=SDS,
      SCTYKEY=(1,2,3,4,5
     OPPRTY=255,
     EXTSEC=NO
DFHSNT TYPE=(ENTRY,DEFAULT),
      OPIDENT=CLA
DFHSNT TYPE=FINAL
```

The entry:

```
DFHSNT TYPE=INITIAL
     EXTSEC=YES
```

requests checking by RACF.

The operator entry DFHSNT TYPE=ENTRY coding of EXTSEC=NO overrides the EXTSEC=YES on the DFHSNT TYPE=INITIAL macro.

Having DFHSNT TYPE=(ENTRY,DEFAULT) is the final entry in the SNTY cause RACF checking for all users not found in the SNT.

By using RACF, the better password control processing of RACF can be utilized. Users can maintain their own passwords rather than maintaining them on the sign-on table. Note: if a CICS user is not defined to RACF, or is not defined in the sign-on table, he can only access CICS transactions with security level of 1 and RACF-defined CICS transactions and PSBs can not be used by these users.

DFHPCT Program Control Table

The Program Control Table (PCT) indicates to CICS which transactions require RACF protection. Like the sign-on table, external security (EXTSEC=YES) can be specified at the DHFPCT TYPE=INITIAL macro level, and the indicated TYPE=ENTRY can override the external security cxheck with EXTSEC=NO.

Example of PCT JCL:

```
PCTCL     TITLE  'DFHPCTCL
SNTCL     DFHPCT TYPE=INITIAL,
               SUFFIX=CL,
               EXTSEC=YES,              RACF SECURITY
                INDEX=YES
       /* DFHPCT TYPE=ENTRY
EDF       DFHPCT TYPE=GROUP
               FN=EDF,EXTSEC=NO         NO RACF SECURITY
       /* DFHPCT TYPE=GROUP
 STANDARD DFHPCT TYPE=GROUP,
               FN=STANDARD
       /*DFHPCT TYPE=GROUP
         DFHPCT TYPE=FINAL
```

The CSSN and 8888 transactions will not be secured because users would not be allowed to sign on to CICS is they were.

Other Security Considerations

Because the CICS system libraries and datasets control how CICS functions, the libraries need to be properly restriced from unauthorized access. For example, the sign-on table (SNT) should have a universal access of "NONE". For CICS to run as a job it must be provided with a user-id and the password in its JOB statement. Read access to the dataset containing the JOB statement must be restricted.

Controlling Access to CICS Regions

To prevent a RACF-defined user from signing on to CICS, RACF can be configured to allow only authorized users to sign on to a CICS region (i.e., Test or Production). This is done by activating the RACF APPL Class, defining the CICS regions, and adding the appropriate user to the access list.

LIST OF RACF AND MVS SYSTEM FILES REQUIRING PROTECTION

This list gives the name and description of RACF and MVS system datasets which should be protected. This list should not be regarded as all-inclusive, and will vary among installations.

1. RACF Datasets

As shown on the DSMON report.

- Primary datasets
- Backup datasets

2. RACF Support Files

SYS1.LPALIB	Contains modules which will be loaded into LPA. These include access methods, SVCs, Logon mode tables, some TSO modules, and various other system routines.
SYS1.PARMLIB	A PDS containing IBM-supplied and installation-created lists of system parameter values.
SYS1.LINKLIB	A PDS containing system routines, utilities, and service aids. LINKLIB is searched for programs to be executed in the absence of STEPLIB or JOBLIB cards.
SYS1.PROCLIB	Contains catalogued procedures (JCL) which can be invoked by operator or by programmer.

3. MVS System Files

SYS1.SVCLIB	Contains OLTEP and appendage modules.
SYS1.DUMPXX	(XX=00 through 09) Datatsets containing system dumps.
SYS1.UADS	TSO user descriptions and authorities.
SYS1.BRODCAST	Messages sent to TSO users.
SYS1.IMAGELIB	Contains character sets and parameters for various printers.
SYS1.MACLIB	Contains IBM macro definitions.
SYS1.MAN	Default SMF reporting datasets.

SYS1.SAMPLIB	Contains utilities, IPL text, and sample SMF exits.
SYS1.STGINDEX	Contains storage management records for VIO datasets (VIO=virtual I/O).
SYS1.TELCMLIB	Subroutines used by BTAM or TCAM.
SYS1.VTAMLIB	VTAM load modules, user exits, authorization and accounting exit routines.
SYS1.VTAMLST	Source tables for VTAM definitions.
SYS1.LOGON	TSO logon procedures
SYS1.CMDLIB	TSO command processors and utilities.
SYS1.DCMLIB	PFK (Program Function Key) definitions.
SYS1.NUCLEUS	Resident portion of control program, nucleus initialization modules, pointer to master catalog.
SYS1.HELP	Descriptions of what each TSO command does.
SYS1.LOGREC	Statistical information about machine failures, records for software error recording, missing interrupts, and dynamic device reconfiguration.
SYS1.TCOMMAC	TCAM macros.

JES3

JESPACE	Spooling datasets for JES3.
JES3CKPT	JES3 checkpoint information.
JES3JCT	JES3 job control table dataset.
JES3LIB	All JES3 load modules except those residing in LPALIB.

JES2

HASPACE	Spooling datasets for JES2.
HASPCKPT	JES2 checkpoint records.
HASPOBJ	Object form of source in HASPSRC.
HASPSRC	JES2 program source.

IBM/RACF Documentation

Other publications are available that may be helpful if further explanations are required:

- RACF General Information Manual - GC28-0722
- System Programming Library: RACF - SC28-1343
- RACF Command Language Reference Manual - SC28-0733
- RACF Security Administrator's Guide - SC28-1340
- RACF Auditor's Guide - SC28-1342

Note: This Guide is current as of RACF release 1.6