E-SRF

EKC Security
Access Analysis Facility

Release 2.1

Introduction

E-SRF V2R1 – **GENERAL AVAILABILITY**

EKC Inc.

E-SRF™ is a proprietary product
developed and maintained by

EKC Inc.
10400 West Higgins Road
Rosemont, Illinois 60018
USA

(847) 296-8010

Technical Support:
(847) 296-8035

EKC, Inc. provides only software program products, which fully comply with, and maintain MVS integrity.

The vendor hereby warrants that:

1) E-SRF™ ("Software") performs only those functions which are described in the published specifications;

2) there are no methods for gaining access to the Software or other computer resources or data of Licensee (such as a master access key, ID, password, or trap door) other than set forth in the published specifications;

3) the Software does not introduce any MVS integrity exposures. The program code, with the exception of one utility, runs totally in non-authorized, problem state. The one utility, EKCRXCAT, requires APF-authorization to read the MVS System Catalogs. A non-APF authorized utility, EKCRGCAT, is supplied to perform the same function, but at a considerably slower speed.

4) the software shall be year 2000 compliant, and shall function correctly in the next century according to published specifications as long as regular software maintenance is applied.

Version 2, Release 1 April, 2005 (Revised for: LE00450)

Printed in USA

E-SRF Publications

Name	Contents
Installation Guide	E-SRF installation including: installation and maintenance steps, startup and shutdown considerations, and backup and recovery procedures.
Change Summary Guide	Contains all new features and system function changes.
General Overview	An overview of E-SRF and its components.
Resource Grouping Facility Guide	Brief overview of the Resource Grouping Facility, its relationship to E-SRF, language command syntax, TSO commands and JCL.
Access Analysis Reports Guide for ACF2 *Access Analysis Reports Guide for RACF*	Brief overview of Access Analysis reports, explanation of the DataOwner and Userid/LogonidOwner reports, command syntax, utilities necessary for creating input to reports, and JCL.
Event Reporting User Guide	A “How To” guide for users of E-SRF Event Reporting.
Event Reporting Facility - Command Reference	Explains the Event Reporting Facility command processor, command syntax, and JCL.
Event Reporting Facility - Masterfile and Data Dictionary Reference	Explains the structure of the E-SRF Masterfile and describes all Masterfile fields.
Event Reporting Facility - Messages and Codes	Lists Event Reporting Facility messages and codes.
Event Reporting Facility - Report Overlays Guide	An overview of the report overlays provided with the Event Reporting Facility.

Introduction

The Reporting "Wish List"

There are many resources within your security environment that require protection from misuse or destruction. Security administrators spend a great deal of time evaluating this protection. For example, access must be controlled when a dataset is initially created and again if a change is required. There are many other resources besides datasets contained in a typical system, including CICS or IMS transactions, terminals, DASD volumes, tape volumes, TSO commands, etc. Who should have access to these resources and to what extent? What reporting mechanism identifies activity on these resources? These are the questions to which security administrators need answers.

Have you ever wanted to know which users can access resources?

In order to protect the integrity of their data, it is critical for resource owners to know who has access to their resources. They need to know how and when access is granted, and what kind of access is allowed.

Have you ever needed to know what resources a specific user or groups of users have access to?

The vast amount of complicated security data, including RACF group accesses and long ACF2 nextkey rule chains, makes it very difficult to determine an individual's resource access. An automated tool that quickly produces this information is a valuable time-saver.

Have you ever wanted a better reporting facility to alert security administrators, the "owners" of resources, and any other interested parties of security violations or other security loggings?

EKC offers a reporting facility that can interpret security event data, be customized to make these reports meaningful for an installation, and alert owners to an inappropriate access or an attempted access violation to their resource. In addition, these reports can be automatically distributed.

These items are on the *"wish list"* of many security professionals. The security systems today have little, if any, means by which you can associate a "*true*" owner with a resource. They may provide the ability to assign an owner to a resource profile or within a security rule, but not to the resource itself. In addition, significant and succinct event reporting is not easily obtained. The E-SRF product provides all of this and more.

Presenting: E-SRF

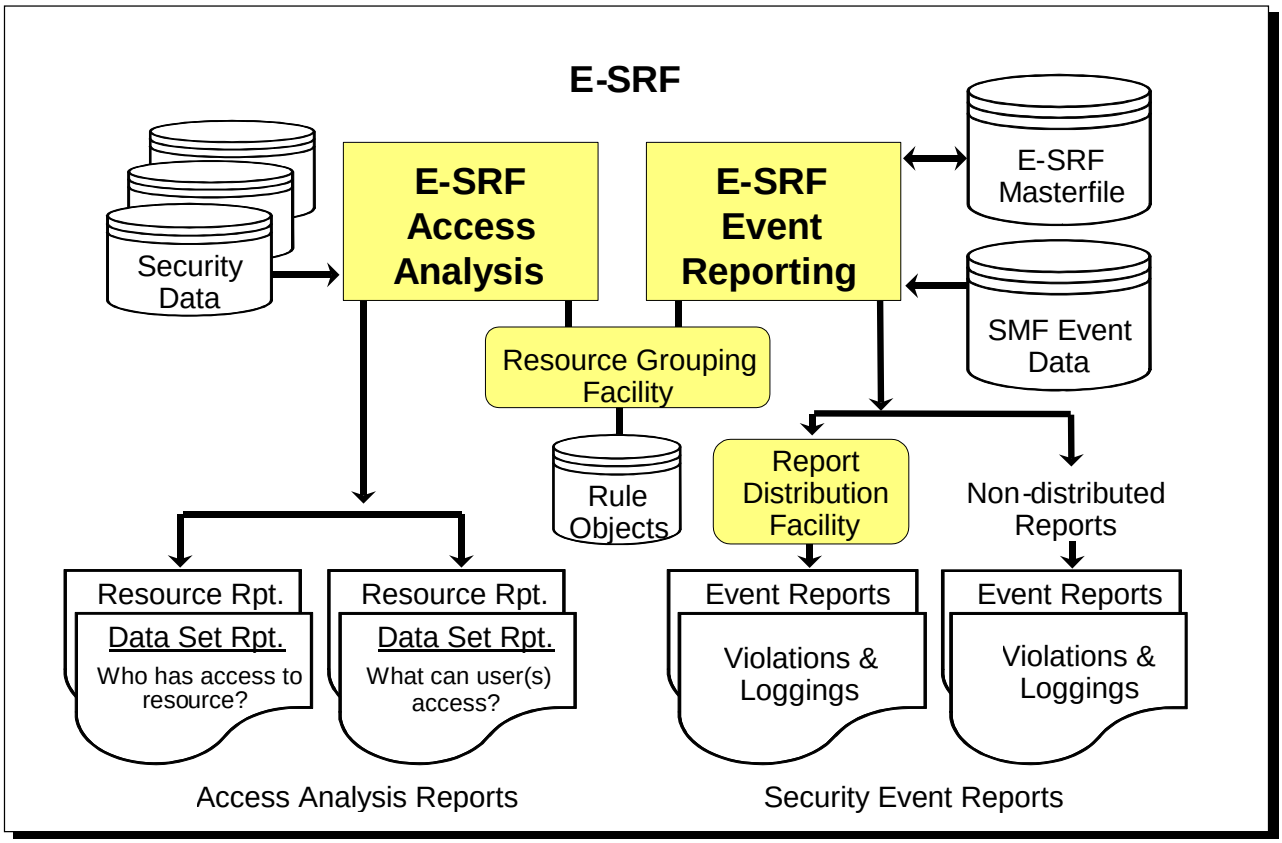
Resident security systems (RSS) currently on the market secure your system but are lacking in administration tools, accountability of resources, reporting, and report distribution. The **EKC Security Reporting Facility** focuses on these areas.

Major Functions

E-SRF security reports provide the comprehensive information needed by the security administrator to respond to system events. They are organized in a manner that allows for quick and easy interpretation. Once it is determined which reports best meet an installation's needs, they can be scheduled to run at regular intervals (daily, weekly, etc.). This eases administrative burden while still providing timely access to the reports.

Rather than only providing for formatted reports, E-SRF produces "intelligent" reporting. That is, E-SRF reporting decisions are based on the relevance of the data contained within the report.

The E-SRF product is an essential tool for the security administrator, auditor, and manager in order to assess the effectiveness of their security systems. In addition, E-SRF enables a proactive approach to adjusting access as changes in that system occur in order to maintain its integrity.



The EKC Security Reporting Facility (E-SRF) major components are:

The **Access Analysis Reporting Facility** is a robust reporting facility that can report against your security system's access information from several perspectives. These reports answer the questions: "Who can access a resource/dataset?" and "What resources/datasets can a specific user or users access?" In addition, the Access Analysis Reports include information about how access is granted and what kind of access is allowed. This is an invaluable tool for resource "owners."

The **Event Reporting Facility** has three major functions. First, it is a powerful mechanism that can report on security events and loggings in a comprehensive yet concise manner. Second, it allows you to define owners to resources. Finally, it automates distribution of these reports to the owners of resources, security personnel, or any other interested party.

The **Resource Grouping Facility** provides the ability to associate a group name to a single resource or group of resources. Resource types include datasets, CICS and IMS transactions, terminals, tapes, DASD volumes, and many more. Users may also be classified as a resource type.

A summary of E-SRF's components and their major functions follows.

E-SRF Components

This section highlights the components of E-SRF.

- EKC Integrated Grouping Facility provides you with the option to group resources and datasets for reporting.
- Event Reports provide summarized reports containing actual security events.
- Access Analysis Reports answer key questions about who has access to critical business data and resources.

What is a "resource"?

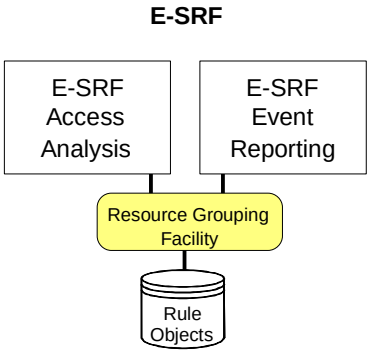
By definition, a "resource" is a name of any item for which your resident security system is providing protection and accountability.

Normally, a typical data processing center has two main types of resources: datasets (files that contain data) and non-dataset resources (such as CICS and IMS transactions and other "labels" placed on computer resources). Most security systems, as well as E-SRF Access Analysis, make a distinction between dataset and non-dataset resources.

However, E-SRF Event System does not make a distinction between the two. All resources will be assigned to their respective classes (e.g., dataset resources will be in the DATASET class). As far as grouping is concerned, even a USERID is considered to be a "resource"; the "classname" might be designated as USER, and the "resource name" would be the User's identification.

Resource Grouping Facility

The EKC Integrated Resource Grouping Facility is a common utility component that is bundled into E-SRF along with the other two separate components, Access Analysis and Event Reporting. It is used to *dynamically* associate a group name to one or more resources on demand. This is a key component of the system. It provides input selection for Access Analysis and for automatically distributing Event Reports. Access Analysis and Event Reporting share this facility. .



Utilizing this grouping facility is optional by one or both reporting components, especially in the early stages of product implementation. *This means you do not have to have any type of grouping established to initially use E-SRF until you so desire to incorporate this facility.* New users to Event Reporting are recommended NOT to attempt grouping until after they have run reports and are familiar with the basic reporting components of the E-SRF system. As product usage matures, the use of grouping will especially enhance Event Reporting. It can provide the means for Automated Report Distribution to various data Owners within your organization.

The Resource Grouping Facility uses "*Grouping Rules*" to associate a group name to a resource(s) for reporting purposes. These grouping rules are not to be confused with any type of *rules* or *groups* that you may already have in place for your Resident Security System.

"Rules" are written and stored on a separate file in order to maintain multiple grouping schemes within a single organization. The EKC Integrated Resource Grouping Facility provides a mechanism for grouping both dataset and non-dataset resources using separate schemes. Resources of differing types can be grouped together under a single group name.

These group names are retained in the Rule Object file for subsequent analysis and reporting. The group name associated with a resource(s) is retrieved from the Resource Grouping Facility and is supplied to the requesting E-SRF component.

A "*resource*" is a dataset or other entity, such as a transaction, command, terminal, or userid that you have protected. To help determine what resources may need to be grouped, Access Analysis utilities may be used to identify your dataset and resource names. It accomplishes this by either reporting the dataset name information obtained from your system catalogs or by reporting on the security definitions, which exist in your Resident Security System.

For example, if you want to create a report for the Payroll Manager to review, you can group all payroll datasets and other resources into a group called PAYROLL. By specifying to E-SRF that you want a report for the PAYROLL group, it will evaluate only those dataset and other resource security definitions or events that fall within the PAYROLL group.

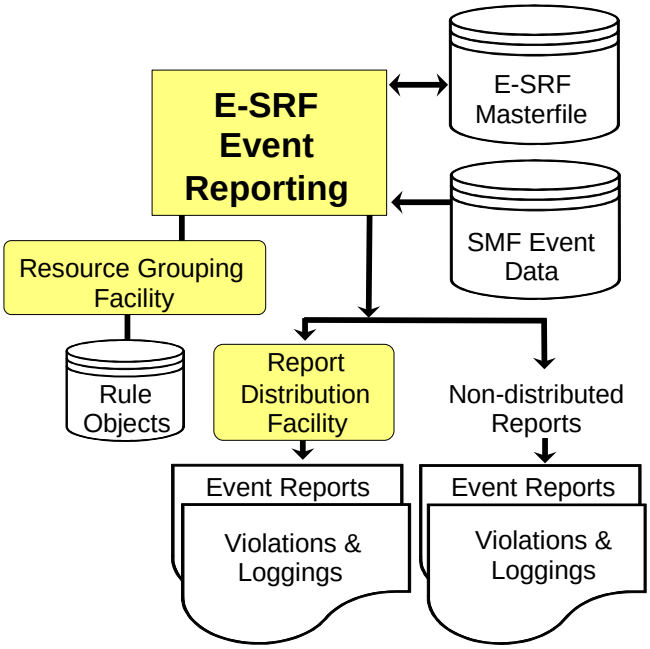
The Resource Grouping Facility allows "grouping" of various resource types within a single group name. As an example, datasets PROD.TECH1, PROD.TECH2 and CICS transaction resources TR01, TR02, and TR03 can all be grouped under group name "MVSTECH". In addition, grouping is dynamic and can be changed whenever the installation makes the determination that the associated group names are no longer appropriate.

More information on why to group, how to group, and the benefits of grouping are covered throughout this publication. The *Resource Grouping Facility Guide* provides detailed information on how to set up E-SRF grouping in your installation.

E-SRF Event Reporting

Event Reporting assists security administrators, auditors, managers, and owners of resources in evaluating the events that have occurred in their system. These events are recorded by the Resident Security System (RSS) as a result of access activity and access logging specifications.

While Resident Security Systems provide security event reporting capabilities, the information is presented in a manner that can be very difficult to understand, evaluate, and distribute to appropriate personnel. Event Reporting provides reports that are clear and concise and summarize the important information for easy evaluation.



Security Event Reports

The E-SRF Event Reporting Facility evaluates data provided by the RSS, updates its Masterfile, and can produce a wide variety of security reports based upon this data. Event reports may contain either detailed event information and/or summary data and include the necessary information to determine who is accessing key resources and if the level of security is appropriate.

Some of these Event Reports are customizable, while others cannot be modified. Fixed-format reports provide a consistent and reliable form for reporting event data. Customizable reports provide flexibility in both the information and the format in which it will be presented to best suit the needs of the installation.

Event Reporting optionally uses the Resource Grouping Facility for input selection, sorting, and report distribution. (More about the Grouping Rules is explained in the E-SRF *Resource Grouping Facility Guide*.) Historical security event journalized information, information from the RSS (Resident Security System), and additional information about users and data in your environment are consolidated and normalized into a relational-style database called the E-SRF Event System Masterfile (normally referred to as "the Masterfile").

Event reporting contains an "engine" that is used to maintain the Masterfile data from any *supported* Resident Security System (RSS). As of release 1.6, the supported RSS systems are CA-ACF2 and IBM RACF. The journalized data is read by "update overlays" and normalized into common event related data. This data is stored on the Masterfile. Reporting is accomplished by executing the Command Processor and requesting one or more "Report Overlays".

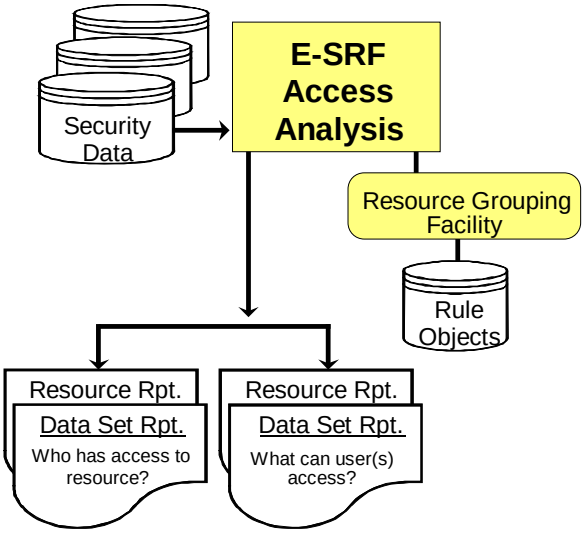
Reporting is done in a normalized fashion, providing reports in as close to "*English*" as possible. A single report may contain security events from multiple systems and multiple RSS systems.

The goal of Event Reporting is an enterprise-wide reporting facility, where the audience does not have to know anything about the security system being executed or the computer systems being reported.

The information about E-SRF Event Reporting Facility provided in this publication is just an introduction to its features. To learn more about E-SRF Event Reporting, please refer to the *E-SRF Event Reporting Facility User Guide*.

E-SRF Access Analysis

The Access Analysis Reporting Facility provides several reports that will analyze and summarize access to resources. Security Professionals need these reports to identify the current levels of security controls: who has access and to what extent.



Access Analysis Reports

For detailed information about Access Analysis, please refer to the particular Access Analysis sections in this User Guide that relate to the security system you wish to report on.

- The reports include sections covering all aspects of access to data and resources including the accesses granted, the security data itself (rules and permits) that provide the accesses, and the users with the ability to change the security data.

- Access Analysis includes utilities to generate the names of datasets and resources in the installation.

- Access Analysis includes utilities and reports that compare security environments. This is particularly useful during system conversions and departmental changes that require mass security changes.

Access Analysis reports were designed in direct response to requests from security administrators and auditors in the world today. With most major security systems, there is no easy way to find out who has access to a particular resource. Auditors found the existing security reports cumbersome and technical. They wanted something that auditors could read and understand and discuss with business managers when a review of who has (and more importantly who should have) access to corporate resources was discussed.

E-SRF Access Analysis reports provide easy-to-read reports identifying the access capabilities of users. Reports are structured to identify who has access to a set of resources, or what are the capabilities of a set of users. The format of the reports is non-technical and simple to read so people not familiar with the security system could easily use the reports. A goal of the reports is to enable business unit managers to be truly responsible for the business data they "own". This is accomplished because they now can see who has access and what they can do. Can they just read the information or update and delete it? Auditors like the format because it provides the information they need without the technical jargon and programmer terminology.

The first set of reports identifies resource or dataset access and identifies who has access to a specific resource/dataset. These reports answer the question, "Who can access and change my data?" The second set of reports identifies user access, specifically presenting the resources a particular user or groups of users can access. These reports answer the question, "What critical business information are my employees able to gain access to and at what level of access (i.e. read/update)?" They are very helpful to both security administrators and resource owners, who will also be alerted to any access changes made.

The Access Analysis Facility of E-SRF evaluates the security controls in place for a set of users or a set of resources. This is accomplished by reviewing the actual security definitions, evaluating and comparing information, and presenting a matrix of the data, users, and types of accesses allowed.

Important Note:

Access analysis reporting was designed for specific security systems and reporting is done on demand. No data is stored beyond the execution of the desired Access Analysis report.

The E-SRF Event Reporting Masterfile is **NOT** used for E-SRF Access Analysis and therefore does not have to be available (or even exist) in order to produce Access Analysis reports.

What are Access Analysis Reports?

The Access Analysis Reports answer two basic types of questions. The LogonidOwner reports (ACF2) and UseridOwner reports (RACF) help identify "What resources can my staff access?" and the DataOwner reports answer the question "Who can access my department's resources?" These are powerful reports that can be used by security personnel, data owners or managers, and auditors.

All Access Analysis reports provide a great deal of information such as what the security definitions are, which users bypassed the security definitions, and who can change the security definitions.

Because the ACF2 and RACF Access Analysis Reports are customized towards their respective audiences, the Access Analysis User Guide contains separate sections covering the input, output, and descriptions for each different Security System. For detailed information on your Resident Security System, refer to *Access Analysis Reports Guide for ACF2* or the *Access Analysis Reports Guide for RACF*.

Personnel	Uses for Access Analysis Reports
Security Administrators	Use reports to identify what access a particular job function has. Can be proactive and periodically check to see what type of access randomly chosen users have. For ACF2, determine how a set of rule modifications will affect user access to resources. For ACF2, determine what changes have been made to the Security Database over a specified period of time. For RACF, determine what RACF groups can be combined and which users have a slightly different access than their colleagues.
Managers or Data Owners	Ensure that users do not have too much access to owned resources. Ensure that users do not have more access than they need.
Auditors	Determine ownership of resources they are investigating - identify who to talk to. Quickly identify areas of focus for evaluation (i.e., who can change system libraries).

The following sections provide an overview of the Access Analysis reports and the utilities used to create input information for the reports.

DataOwner Reports

DataOwner reports answer the question, “Who has the ability to read or update my data or resources?”

E-SRF evaluates the security access definitions, compares them to the users defined to the security system, and determines who has access.

The DataOwner reports can be run for datasets or other defined secured resources. Data owners benefit from these reports because they aid in evaluating any exposures to “their” data by users with the currently defined access controls.

Group, High Level Qualifier, Resource Class, or a list of datasets can be specified when requesting a DataOwner Report. These reports are especially useful to managers and auditors in investigating security breaches. Which users have the capability to see, update, or delete the data and resources anywhere on your system may be quickly and easily determined.

LogonidOwner (ACF2) or UseridOwner (RACF) Reports

LogonidOwner and UseridOwner reports answer the question, "What can my users do?"

These reports provide a different perspective. For ACF2 reports, a group of users is specified based on their Logonid attributes. For RACF reports, a group of users is specified based on their User Profile attributes or RACF Groups to which they are connected.

E-SRF evaluates all of the security rules either for datasets or other resources and determines what accesses those users have. The LogonidOwner and UseridOwner reports allow you to make quick evaluations (e.g., a user with too much access or users who are able to change information beyond their normal day-to-day requirements).

In cases where auditors or others are investigating a security breach, the LogonidOwner reports may conversely assist in eliminating possible suspects since it becomes readily apparent what access users have (or don't have).

ACF2 Specific Reports

For ACF2, E-SRF also provides the Proposed Rule Processor and the System Differences Reports. The combination of these two reports allows the Security Administrator to determine what different access users will have after a set of *proposed* ACF2 Access and Resource Rules are implemented. This eliminates much guesswork and manual analysis.

Additionally for ACF2, E-SRF provides a Database Differences Report. This report shows the changes made to the ACF2 Security Database between two points in time. This might be between yesterday and today, or between last week and now, or between last month and now. The Database Differences Report provides Security Administrators a needed tool to simply audit changes in Logonid definitions or access control rules and definitions.

These reports answer the questions:

- "What are the differences in access for two different databases?"
- "If I make a change to the rules, how can I be sure that the different access allowed will be what I expected?"
- "What portions of the database changed between yesterday (or last week) and today?"
- "What logonid record fields, rule lines, and information storage records are different between two separate databases?"

RACF Specific Reports

E-SRF also provides additional reports for RACF. The Userid Differences Report analyzes the different accesses users have and groups them. The differences between the access for each group are detailed if they are within a certain set of limits specified by the Security Administrator. This provides the Security Administrator the ability to combine RACF groups or to highlight a user who has a slightly different access than his or her colleagues.

Additionally for RACF, E-SRF provides a DataOwner Open Edition Report supporting the OS/390 UNIX System Services portion of the Operating System.

The Access Analysis reports *do not* reference the E-SRF Masterfile.

Reporting Guidelines

Because the Access Analysis Reports require access to the backup copies of the ACF2 databases or the unloaded copy of the RACF database, they should be restricted for use by Auditors or Security Officers. The Security Officers could run the reports and deliver the output to the various data owners or managers for review.

Processing time for the reports will vary with the number of combinations of Logonids/Userids and Resources to be processed.

There are two ways to create the input needed for the dataset reports. The EKCRXCAT utility reads the system catalogs and produces a record for each dataset. In some installations, the number of datasets may exceed one million. This generates a great deal of comparison and evaluation, particularly in the LogonidOwner/UseridOwner Report.

However, much of the same information can be obtained using the EKCRDMSK (for ACF2) or the EKCRRPSD (for RACF) utility. These utilities produce one record for each unique dataset mask in the ACF2 rules or Generic Profile in the RACF database instead of listing every dataset. The number of records is installation dependent, but will be considerably less than all the records produced from the catalogs. If problem areas are identified, the LogonidOwner/UseridOwner Report can be re-run using a specific list of dataset names for further analysis. Similarly, the EKCRRMSK (for ACF2) and the EKCRRPSD (for RACF) utilities create resource names from resource rules or generalized resource profiles for input to the resource reports.

For more information, see the *Access Analysis Reports Guide* for your Resident Security System.