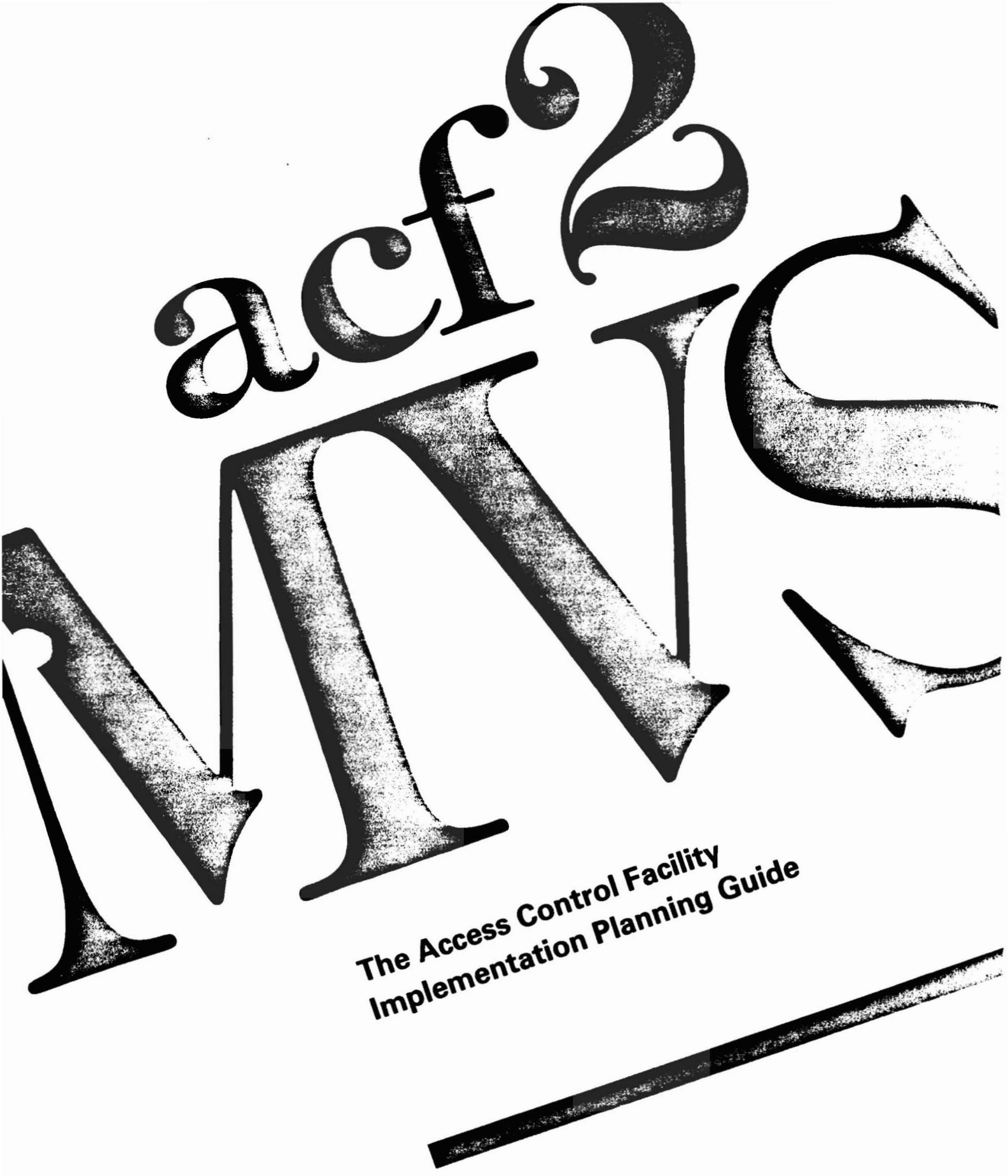
acf2
MVS
The Access Control Facility
Implementation Planning Guide

acf2™

The Access Control Facility

IMPLEMENTATION PLANNING GUIDE

for

acf2/MVS Release 4.0 Installations

Base Manual Dated: January 15, 1985

Doc. Nr. ABP0012-03

Printed in U.S.A.

ACF2 is a proprietary product developed and maintained by:

SKK, Inc.
10400 West Higgins Road
Rosemont, Illinois 60018-9990

Business Office: (312) 635-1040
Product Support: (312) 635-3000
TELEX: 206-186 (SKK ROSM)

A 24 hour answering service on (312) 825-5150 is available for emergency assistance outside of normal business hours.

ACF2 IMPLEMENTATION PLANNING GUIDE

INTRODUCTION

PURPOSE

This manual is primarily intended for sites preparing for the initial installation of ACF2, the Access Control Facility. A number of other ACF2 manuals provide details about various aspects of the system itself and are meant to be used on an ongoing basis. Information contained in these other manuals is not repeated here, but is referenced where appropriate.

The Implementation Planning Guide focuses on how to approach the implementation of access control. Most ideas presented here have been successfully used by many sites. But because circumstances vary significantly from site to site, the actual steps taken will also differ. It is hoped, however, that these suggestions will provide a useful base for the successful implementation of ACF2 at your site.

THE PRODUCT

ACF2 is a systems software product which helps control the use (sharing) of your computer resources including computer usage, data (stored on disks, tapes, etc.), programs, transactions, accounts, and similar resources. In general, ACF2 helps control use of these resources by requiring each user to enter an identifier to gain access to the system, whether through TSO, IMS, CICS, batch, or other subsystems. This identifier is validated against a central ACF2 database in which the installation has previously established one Logonid record for each authorized user. After a user has been allowed to enter the system, ACF2 verifies that each request made for a resource is also authorized. Basically, ACF2 determines whether a request is authorized by checking if either (1) the user "owns" the resource (data) or (2) an ACF2 rule has been set up to allow "sharing". A rule describes the conditions under which data or resources can be shared. Rules are also set up by the installation in a central ACF2 database. If an access request is not authorized, it is rejected and the event is logged by creating a System Management Facility (SMF) record. These records can later be edited and reported by use of one of the report generators provided with ACF2.

A number of options allow ACF2 controls to be tailored to the needs of each installation. An important aspect of preplanning is to decide which options to use initially, and how to migrate your installation from its current level of security to a site with full ACF2 controls in place.

For additional information on the basic features of ACF2 and the facilities it provides, see the ACF2 Overview, the General Information Manual, and the Administrator's Guide.

SYSTEM INTEGRITY

Proper implementation of ACF2 provides a significant enhancement to data and resource security at an installation. ACF2 is designed to protect against unauthorized accesses and similar exposures. Maximum protection and benefit is achieved when ACF2 is utilized as part of an overall approach to DP security. ACF2 interfaces with and supports a number of management controls such as separation of function, individual responsibility and accountability, access to data on a need-to-know (job function) basis, detailed auditing of system resource usage, data access, and internal controls. ACF2's features, options, and audit trails provide valuable assistance to management in implementing these controls. A sensible combination of ACF2 and appropriate management controls should minimize administrative requirements while maximizing the protection levels possible for a given installation and operating system.

The protection provided by ACF2 cannot be more absolute than the integrity of the operating system under which it is running. ACF2 alone cannot prevent or protect against integrity exposures within the operating system. However, ACF2 does not knowingly introduce any exposures, and provides the maximum realistic protection under the given operating system.

PREPLANNING

ORGANIZING FOR SECURITY

The most commonly used organizing approach at ACF2 sites has been to:

1. Appoint an individual as the Installation Security Officer (ISO) whose responsibility is to manage and coordinate the overall information security program for the installation.

2. Establish an ACF2 Implementation Team (IT) to help the ISO plan for, install, and implement ACF2 and any related security practices and procedures.

3. If the installation size and activity warrants, the ISO should have the option to assign additional people to the information security function (full-time or part-time) to work for or with the ISO. These assignments may be on a centralized or decentralized basis in accordance with the organizational structure.

THE INSTALLATION SECURITY OFFICER (ISO)

The ISO should serve as the central coordinator for information security and represents a permanent staff position. The ISO's areas of responsibility encompass all phases of implementing ACF2 (i.e., initial planning, progression towards full security, and ongoing administrative activities). Most of the ACF2-related effort occurs early during the planning and implementation phases (usually the first few months). Once ACF2 controls have been integrated into production systems, a continuing effort must be made to properly enforce security measures. Ongoing administrative functions for ACF2 include: updating the ACF2 databases which contain user Logonids and access rules, reviewing reports on SMF records created by ACF2, and (based on these reports) following up on suspicious events or possible problems.

These administrative functions and their associated responsibilities can be either centralized or decentralized. For example, one way to decentralize the administrative responsibilities might be to authorize numerous people throughout the organization to fill out forms that request user Logonids/access rules be added/changed. The actual validation/updating function could be centralized by requiring such requests to be forwarded to the ISO, who permits the actual update. Whether ACF2 administration is centralized or decentralized (and to what degree) depends on the size, structure, and unique needs of an installation. Many options are available so that an installation can tailor ACF2 administration, both initially and on a continuing basis.

Preplanning considerations also require the determination of scopes of authority various users will have as they apply to writing and updating Logonid records and rules. In a decentralized environment, multiple ISOs may have jurisdiction over limited groups of users, data, or resources. These limitations are imposed by use of the ACF2 scoping features. Refer to the ACF2 Administrator's Guide for details on scope assignments.

The total work load of the ISO after ACF2 implementation will depend on such factors as:

* the actual volume of work in the system (batch jobs and online users)

* centralization/decentralization of ACF2 administrative duties (e.g., how many users have the SECURITY or ACCOUNT attributes)

* centralization/decentralization of responsibilities and authorization functions

* site commitment to data security. This commitment will be reflected in such areas as the detail level of access rules, follow-up actions taken on violation attempts, and whether started task/CICS/IMS/IDMS ACF2 interfaces are being used or only batch and TSO users are controlled.

The person best suited for this job, if that person needs a staff of helpers, and where this position appears in the corporate organizational structure depend upon the activity levels and factors mentioned above. Although an ISO does not need previous experience as a programmer or computer operator, it is useful if the person selected for this position has some technical data processing knowledge. To assist the ISO, the Implementation Team (IT) should contain members who are experts in the following areas:

* use of the online system (such as TSO or ROSCOE)

* setting up JCL and submitting batch jobs

* dataset, user-id, volume, and job naming conventions at the installation

* existing resource security mechanisms already in use, such as OS passwords, date protection, and local SMF exit code

* data center schedules and operations

The ISO normally chairs the IT, scheduling meetings with all or parts of the team as necessary, performing the majority of the coordination functions, and taking an instrumental role in selecting ACF2 options. Once ACF2 is installed, the ISO coordinates the administration of the ACF2 system.

It is preferable that the ISO have a relatively autonomous position in the organizational structure in order to make independent and fair decisions and to sufficiently enforce policies and rules. A low level position inside the data processing department is not independent. Similarly, the ISO's position should not be in the EDP audit area, as the EDP auditors must also be able to independently audit the security system and its implementation and administration. Remember that true management commitment to information security is necessary to achieve any reasonable level of protection and enforcement.

THE IMPLEMENTATION TEAM (IT)

The primary function of the Implementation Team is to properly implement ACF2 and related information security systems and procedures. This is a limited function because most of the work occurs during the planning and implementation phases. In fact, the team may be disbanded after ACF2 has been implemented and is functioning as desired in ABORT mode.

However, many sites retain the team and hold meetings periodically to review the system, reconsider options being used, and evaluate overall security measures at the installation. This team may also be useful as an ongoing "Information Security Committee" to assist the ISO in identifying security policies and in enforcing these policies at various levels. A similar security committee might already exist at your installation and, with or without modifying its membership or its charter, may well serve as the basis for the ACF2 Implementation Team.

The Implementation Team normally consists of the ISO as chairperson, and perhaps 3-8 other people representing areas such as:

1. Systems Maintenance - usually the IT representative will be the system programmer responsible for installing and maintaining ACF2 on the system. This person should be familiar with the operating system, JES, SMP, SYSGENs, and related areas.

2. Data Center Operations - someone from operations who is familiar with current naming conventions, production schedules, and normal operations maintenance activities.

3. User Support Services - normally sites have liaison personnel between data processing and the nontechnical user groups to help run jobs, answer TSO questions, etc. Representatives from this area can help present the user's viewpoint and also help provide communications between the technical and nontechnical personnel.

4. User Groups - representatives from these groups (e.g., accounting department) might be included on the IT where user support services people are not available to represent the user's viewpoint.

5. Data Security Officers - if Database Administrators (DBAs), Physical Security personnel, or other personnel are already active in the data security area, they can often provide valuable input on current usage and future data security needs.

6. EDP Audit - a representative from the EDP audit group can help define audit's concerns for internal controls and their auditability. An auditor can often suggest options to promote acceptable levels of control, accountability, and auditability.

7. Upper Management - rather than have upper management sit in on all the committee meetings, the ISO can represent (and periodically report progress to) upper management. If this arrangement is not adequate, the committee may prepare recommendations to be forwarded to and acted upon by a higher group. This may be preferable when corporate security policies need to be clarified or established. Either arrangement can work smoothly as long as communications channels are defined and open.

The activities in which the Implementation Team will be involved include:

a. establishment of an implementation schedule
b. assignment of responsibilities for each activity
c. reviewing and selecting the ACF2 options to tailor the system in accordance with local policies and requirements.

THE IMPLEMENTATION SCHEDULE

An early function of the IT is to establish a preliminary ACF2 implementation schedule. Initially this may only include the major milestones, such as the test IPL, the production/installation IPL, and migration to full ABORT mode. As the team proceeds through the ACF2 documentation and identifies additional tasks to be performed, these must be added to the schedule. A good implementation schedule should include a relatively detailed list or group of tasks, target completion dates for each, and the name of the person responsible for completing that task. The IT should also monitor progress in each area, resolve conflicts, and periodically update the schedule as necessary.

A sample general implementation schedule is provided below. General time frames are provided for chronological reference. However, specific completion dates should be used where possible. No sample assignments are included in this example, as those would vary significantly from site to site depending on the type and number of personnel available for the project and the size of the task for that installation. Additional detailed tasks should also be added as they are defined. Also note that this is an ACF2 implementation schedule, not an ACF2 installation schedule. The installation of ACF2 is only the activation of the code on your computer. The implementation of a security system includes much more, whether or not the tool being used to help automate the security process is ACF2. This is why the planning process is important and why a team of knowledgeable people should be used, rather than one or two people needed to just install the package.

Sample ACF2 Implementation Schedule

Time Frame	Activity
Week 1	. Appoint an Installation Security Officer. . Establish Implementation Team. . Hold organizational meeting. . Distribute basic ACF2 documentation to team members. . Have key personnel (such as the ISO and the ACF2 system programmer) attend an ACF2 Training Class. (Note: This is recommended but not mandatory.)
Week 2	. Establish general time table and responsibilities. . Further identify existing governmental, corporate, industry, and local security policies, goals, and objectives. (Note: Preliminary research in this area ideally would have been done before product selection.) . Identify local conditions or operating environment, such as naming conventions, etc. . Identify system users and user groups.
Week 3	. Make preliminary option selections. . Refine the schedule and responsibilities. . Perform test install of ACF2 on a target system pack.
Week 4	. Finalize schedule and responsibilities. . Refine option selections. . Perform initial training, if needed (administrators, computer operators, etc.) . Prepare for test IPL of target system - write or tailor any local exits, check option selection, select sample users/jobs/rules, prepare test job streams, etc.
Week 5	. Test IPL (in LOG mode or RULE mode*). . Review results, including report outputs. . Modify option selections, as necessary. . Modify procedures, operator instructions, etc., as necessary. . Test backup/recovery procedures. . Prepare to install ACF2 on production system(s). . Perform additional training and announcements.
Week 6	. Install on production system (LOG mode or RULE mode*). . Establish initial users. . Write/compile/store initial rules. . Closely monitor reports and reactions. . Retest backup/recovery procedures.

* The 'modes' of the ACF2 system (QUIET, LOG, WARN, and ABORT) may be phased in on a rule set basis by means of the MODE field of the OPTS Global System Option (GSO) record. See the chapter of this manual entitled "Conversion to Full Security" for details.

Weeks 7-12
- Readjust system options and/or exits.
- Complete user definitions.
- Complete rules.
- Continue to closely monitor reports.
- Test maintenance (SMP) procedures.
- Migrate system to WARN and ABORT modes.

The above schedule merely provides guidelines for the timing of various implementation activities, which will vary significantly depending on local circumstances at your site. Also, many of these activities can occur concurrently, or proceed independently. For example, the technical installation and IPL of the target system may occur before or after the less technical activities listed in weeks 4-5. Detailed information on some of these topics, such as what should be done to perform the install or during the first IPL, is covered in the "Establishing Initial Logonids" and the "General Installation and Maintenance Planning" sections of this manual.

ACF2 DOCUMENTATION DISTRIBUTION

ACF2-related documentation should be distributed to the Implementation Team and other selected people as early as possible. The documentation provided by SKK is itemized in Appendix A of this manual. It should be apparent from reviewing this list that not all team members require all manuals. Determine which manuals are applicable for each group, and obtain and distribute copies as appropriate. This normally means distributing manuals to various groups as outlined below:

All IT members
: Implementation Planning Guide, Overview, General Information Manual, Utilities Manual, Composite Index, and Administrator's Guide.

System Programming IT representative(s)
: All group 1 manuals (above), plus the Messages Manual and System Programmer's Guide.

EDP Audit IT representative(s)
: All group 1 manuals (above), plus the Auditor's Guide.

Other personnel, such as upper management or special users
: Selected manuals, as appropriate.

During later phases of implementation, additional documentation distribution may be appropriate. For example, operations should be provided with copies of the ACF2 Messages Manual (or those portions of it applicable to your installation) before the first IPL. Users may also be provided with copies of the Administrator's Guide or with a user's manual developed locally. Also, when IMS, IDMS or CICS interfaces are being installed, the IMS, IDMS or CICS Support manuals need to be distributed to the ISO, system programmers, and other IT members. Members of your systems staff may need the ACF2 Other Products Manual for information on other product interfaces to ACF2. Your employee education center may require the ACF2 Customer Education Catalog to explore the need for further ACF2 training of your staff.

Besides the initial distribution of documentation, be sure to establish procedures for the timely and complete distribution of all new and revised documentation. That way all personnel who need current information always have the latest copies; outdated and possibly misleading copies of the documentation should not be left in use.

IDENTIFYING SECURITY POLICIES, GOALS, AND OBJECTIVES

It is important that the IT has some idea of the site's data security goals and objectives before implementing ACF2 or any other product. ACF2 is a tool used to implement security policies, automate policy enforcement, and help the site achieve its goals. If these policies and goals are unknown or undefined, it will be very difficult for the IT to choose appropriate ACF2 options and to proceed quickly through ACF2 implementation. Various factors may influence a site's policies and objectives. These include, but are not limited to, the following areas which should be reviewed for applicability to your site:

Government Regulations

The U.S. government has a number of regulations which may affect data security requirements at your installation. Some of these are the Privacy Act, Foreign Corrupt Practices Act (FCPA), Securities and Exchange Commission (SEC) and other agency regulations, and various other accounting and reporting requirements. There are also similar regulations in other countries, such as national "privacy acts", transborder data flow regulations, and accounting and taxing regulations. Additionally, any state, provincial, or local regulations should be considered. Of course, government regulations for governmental agencies are often even more encompassing.

Legal Requirements

Many of these are tied to government regulations, such as requirements pertaining to controls over Electronic Funds Transfers. Others may be contractual, such as union agreements (employee record accessibility by other than authorized personnel, etc.). If you operate as a service bureau and have contractual agreements with customers about the confidentiality and protection of their data/programs, you may be subject to other legal requirements.

Industry Practices and Agreements

Some industries frequently share certain data, while other highly competitive industries guard much of theirs. In some areas the possibility of industrial espionage may be a factor to contend with. In addition, various practices become common within an industry and can even evolve into recognized "Standards of Due Care" which can have legal ramifications if your site does not implement them. Using access control software and personal passwords for individual identities are becoming standards in the area of data security.

Sabotage, White Collar Crime, and Computer Frauds

The severity of these threats for your installation depends on a number of factors. Threats from both external (activist groups, competition, etc.) and internal (disgruntled employees, opportunists, etc.) forces must be considered. Personnel practices, ease of conversion of assets to cash via computer fraud, and the degree of collusion necessary to perpetrate fraud should all be reviewed.

Good Business Practices

Normal good business practices (the same ones your company has previously been using in non-computerized areas) should also be used in computerized environments. These would include separation of function, clear line of responsibility and authority, individual accountability, knowing what the control procedures are and that they are in place, knowing who has access to assets and records and controlling this access, and various auditing considerations.

Existing Corporate Policies

Almost every company or agency has some written policies already in place. Many of these do not relate to computer assets/data security. Others exist because of the factors mentioned in 1 through 5 above and may be reviewed as part of these other areas. But all existing policies relating to data security, access control, and computer control auditability should be identified and considered when selecting ACF2 options and building an overall installation security plan. Future planned or desired policies should not be overlooked, as they will probably be easier to implement and enforce if they are considered when designing the initial overall plan.

Organizational Impact

Sites normally want to implement data security that is transparent to the users. While ACF2 contains various features and options to assist in its implementation and in the transition phases, these alone will not make security "transparent". Normally a site is going from an environment with little or no data access control to one with appreciable controls. This in itself is a significant difference and cannot be totally transparent. However, proper planning, education, and phased implementation can alleviate most problems and can even create a positive, progressive attitude among users.

The IT could also make other decisions concerning implementation of ACF2 which might have an organizational impact. Such decisions would encompass the degree of functional separation and the degree of centralization/decentralization in the administration of ACF2 and related controls. The outcome would either (a) require organizational and job responsibility changes or, (b) if the selected approach is similar to existing procedures, minimize these changes.

Procedure Enforcement Needs

ACF2 can also be a valuable aid in enforcing various corporate policies not directly related to data protection. These would include items such as naming conventions for datasets, volumes, programs, and user identification. It can help enforce consistent policies throughout the corporation or agency, including multiple physical locations. Again, the IT should consider these needs when selecting ACF2 options and implementing its controls.

IDENTIFYING LOCAL OPERATING ENVIRONMENT

To select the most appropriate options and effectively use ACF2 controls, first identify local conditions which need to be taken into consideration.

Local Naming Conventions

Determine existing (or desired) naming conventions for:

- user identification for TSO, Wylbur, IMS, CICS, etc.
- dataset names
- volume-serial names, for example DASD, MSS, and tape
- physical device names for terminals, remote job entry stations, etc.
- IDMS tasks, programs, data areas, subschemas, and files.
- IMS or CICS transaction names
- CICS program and file names
- IMS Application Group Names
- program names
- library dataset names
- JCL DD statement names
- account numbers
- procedure names (for TSO and/or started tasks)

The significance of various naming conventions depends on which ACF2 options you use. Conversely, the options you select may depend on your naming conventions. ACF2 provides methods of controlling resource access based on all of the fields listed above. It also allows global rules to be written which reference name "patterns" for each of these fields. Thus, if consistent naming conventions are used for dataset names, program names, IMS transaction names, etc., ACF2 rules are much easier to write. And, once access rules are in place, ACF2 will help in turn to enforce compliance with your naming conventions.

Dataset Name High-Level Indices

Conventions used for high-level index names are important because of the way ACF2 validates an access request. When validating a request, ACF2 compares a value associated with the user making the request to the high-level index to determine if that user owns the dataset. If these values do not match, ACF2 then selects the appropriate high-level index rule set and interprets that rule to determine if the requested access should be allowed.

Standard Security Mechanisms

Identify current security mechanisms and decide which of these will eventually be replaced and which will be used in conjunction with ACF2. Before ACF2 is in system-wide ABORT mode, you may wish to keep all current security mechanisms active, because ACF2 does not actually deny dataset/resource access while in QUIET, LOG, or WARN mode. If you choose to implement the RULE mode option, you can phase in your selection of datasets to be placed under ABORT mode on a rule set basis. Controls such as ACF2 TSO command limiting can be independently activated, regardless of which mode ACF2 operates under.

ACF2 does not interfere with mechanisms such as OS password protection, expiration date protection, PCF (IBM's Program Control Facility), or most other local security mechanisms (e.g., those based on checking account numbers or job names in SMF exits). After ACF2 is in ABORT mode, you may elect to replace such mechanisms with ACF2 features. Others you may wish to retain permanently for additional security. For example, ACF2 also does not interfere with application-level security checks, such as special processing performed within a batch, IMS, or CICS application program. However, since ACF2 is not designed to replace or supercede these checks, most application-level checking should be retained even after ACF2 is in full ABORT mode. Of course, ACF2 might be used to implement these controls in a different way, such as by centralizing control information in ACF2 databases.

Uniqueness of User Identifications

Establish whether each system user is currently uniquely defined to the system. Identify all users and any existing individual or group ids. Sometimes a whole group of users will have a single system identity (e.g., a group of IMS operators sharing one terminal). In other cases, a single system user may currently have multiple ids or passwords for different tasks (e.g., a TSO user with multiple TSO passwords, an IMS signon id, and a Wylbur id). Plans should be established to positively identify each system user with a unique ACF2 Logonid and single password.

Another significant consideration in planning will be the selection of an ACF2 User Identification string (UID) format, which should be based on your individual id patterns, organizational groupings, etc. (See the "UID String Format" section later in this manual.)

Dependencies on Jobnames, Account Numbers, etc.

Determine if your installation is currently using batch jobnames, account numbers, or similar fields for any controls. Review if these functions should be replaced with ACF2 features, discontinued, or kept to coexist with ACF2. Also ensure that these controls will not interfere with ACF2.

Other Security Controls

Identify other automated or manual security-type procedures existing or desired at your site. Consider, for example, controls on:

- physical devices, such as terminals, RJE station, readers, etc.
- batch jobs versus TSO or other online sessions
- test versus production work
- systems programming activity

Operating System Configuration

Identify other subsystems and software packages used (or planned for) and review them to determine if there will be any impact on either ACF2 or these other systems. Particularly important are:

- tape management systems
- disk management systems
- archival systems
- library maintenance systems
- interactive or online systems
- job control or scheduling systems
- JCL maintenance/submission
- started tasks

The ACF2 Other Products Manual contains information on interfaces between ACF2 and various products from other vendors.

SELECTING ACF2 OPTIONS

The selection of appropriate ACF2 options to tailor the ACF2 implementation to your needs should be accomplished in several phases. Some options (like the NOSTC field in the OPTS GSO record) must be used for the first IPL (also see the section entitled "The First ACF2 IPL"). You can select temporary values for other options for transition purposes, in order to phase ACF2 protection into your system. For example, you may choose to control TSO and batch use of DASD only for the first week, expand to tape protection week two, IMS test region week three, IMS production week four, then CICS control after that. You can indicate these choices to ACF2 by setting up various ACF2 parameters.

The IT should review all the ACF2 options and select appropriate values for the first IPL and also those for later use (with target dates for changing the significant ones). Refer to Appendix B, "acf2/MVS Superceded Elements", for information on older ACF2 features which are currently available but will probably not be supported in future releases. New sites should avoid using these features, opting instead for the newer, more powerful alternatives.

Other system tailoring can be done using ACF2 exits. The various possibilities and combinations should be reviewed by the IT. Other manuals, such as the General Information Manual, the Administrator's

Guide, the System Programmer's Guide, and the CICS, IDMS and IMS Support Manuals should be used in studying the available options. However, a few special areas are highlighted below.

UID String Format

The structure of the ACF2 User Identification string (UID) involves special planning. If the current TSO USERIDs have a high information content, such as division, department, job responsibility, etc., then it may be adequate to carry over such conventions directly to the UID. However, if this is not the case, informational fields can be added to the Logonid record and ACF2 can be instructed to form the UID by concatenating these new fields and the Logonid.

A UID which is constructed with a high information content allows the ISO to manage groups of individuals very easily, since dataset sharing rules may specify UID patterns for access. In this way, all users in a department or location can be given access to a dataset or other protected resource through one simple rule instead of lists of the pertinent individual Logonids.

Boundaries of ACF2 Controls

Many ACF2 options are specified in the Field Definition Record (ACFFDR) macros, the online Global System Options (GSO) records, the special ACF2 IMS and IDMS macros and the CICS system initialization parameters. A number of ACFFDR, GSO, IMS, IDMS, and CICS parameters affect the overall bounds of ACF2 controls on your system. These include options such as:

- whether tapes are protected at dataset name level, volume-serial level, or not at all
- whether or not STCs, IMS users, IDMS users, CICS users, or other user and job groups are to be controlled by ACF2
- what mode (QUIET, LOG, WARN, ABORT, or RULE) the base system is running under
- what mode (LOG or ABORT for IMS and IDMS; QUIET, LOG or ABORT for CICS) each IMS, IDMS, or CICS region is running under
- whether any programs are specially controlled
- to what degree ACF2 administration will be centralized
- whether operator identification cards are required for terminal access

Since the values chosen for these options can have a significant effect on the scope and completeness of ACF2's controls, the IT should review each of the possible options very carefully. This should include an item-by-item review of each parameter in the Field Definition Record (see the System Programmer's Guide) and the GSO records (see the Administrator's Guide). If the optional IMS, IDMS, and or CICS interfaces will be utilized, see the appropriate ACF2 documentation manual for complete information about the available control options.

Use of UADS and UADS Conversion

In an MVS/TSO environment, ACF2 will run in a system using UADS or will totally bypass the UADS dataset. The advantages of bypassing UADS are faster LOGON processing and eliminating the need to maintain both UADS and the ACF2 Logonid database. However, multiple account and procedure structures are managed differently by ACF2, and the other TSO-related items formerly contained in UADS would have to be redefined in ACF2's database. Therefore, these items should be carefully reviewed. Note: The use of UADS and UADS conversion does not apply to a non-TSO environment.

ACF2 Exits

ACF2 exits can be used to resolve unique installation dependencies or provide specialized transition paths. An example is the logon pre-validation exit. This exit can obtain the Logonid and password and modify them or reject the logon attempt. Sample source code for such an exit (LGNIXIT) is supplied with the distribution tape. All exits are described in the System Programmer's Guide.

THE FIRST ACF2 IPL

The first IPL with ACF2 linked into the system should be done in a controlled environment. While the entire Implementation Team need not be present, at least the ISO and the system programmer responsible for the ACF2 install should be there. Various system testing functions should be performed, as well as some work with ACF2 (establishing Logonid records, writing rules, testing commands, etc.). There are normally some special considerations during the first IPL, most of which are documented in the ACF2 System Programmer's Guide. Information in the current version of the Guide (provided with the distribution tape) should always be reviewed in addition to the comments provided below.

TESTING THE SYSTEM

In addition to submitting the first jobs to establish ACF2 Logonid records and rules, there are a number of other items which should be tested soon after the first successful IPL. The other facilities noted below should be tested to ascertain that they are functioning correctly; additional local tests may be desirable for checking local modifications or special processes.

1. Test ACF2 startup procedures.

2. Test startup of all other basic systems (VTAM, TSO, ROSCOE, STCs, etc.).

3. Test batch job submission (initially under ACFUSER until Batch Default and/or other ids are established).

4. Test TSO logon procedures (also initially under ACFUSER until other Logonids are established).

5. Verify that job processing has not been affected. Special sample jobs may be used to ensure that ACF2 intercepts are working properly. The ACF2 SHOW ACTIVE subcommand displays the list of ACF2 intercepts, and will indicate which have currently gained control. Some sample jobs constructed to ensure that the intercept points are active (e.g., allocate, catalog, uncatalog, and scratch a dataset, perform a tape open, etc.) should be run, and then SHOW ACTIVE checked again.

6. Test all local exits and modifications.

7. Use ACF SHOW subcommands to verify that the correct ACFFDR options, GSO parameters, and ACF2 intercepts are active (e.g., SHOW STATE, SHOW SYSTEM, SHOW ACF2).

8. Run the ACF2 report generators to test the jobs themselves and produce reports which can be used to check other processing.

9. Test the ACF2 backup and recovery procedures.

10. Test the various ACF2 commands and subcommands to check that they all are working as expected, and to help test and display various Logonid and rule-related options.

11. Test interfaces with other products (FDR, ASM2, ROSCOE, etc.).

12. Review console logs and job logs as well as the ACF2 reports to ensure that all activity is proceeding as expected.

ESTABLISHING INITIAL LOGONIDS

When you bring the system up for the first time there is only one Logonid defined in the ACF2 Logonid database (default value is ACFUSER). Thus, until this Logonid logs on and uses the ACF2 commands (or submits a batch job to process these commands) to insert other Logonids into the database, no other Logonid can be used to run a job. Also remember that, regardless of which mode (QUIET, LOG, WARN, ABORT, or RULE) ACF2 is in, no job will run on the system unless the Logonid associated with the job is predefined on the Logonid database as a valid system user. Thus, for the first IPL you must also specify the NOSTC field in the OPTS GSO record. If STC, rather than NOSTC, were specified, ACF2 would attempt to validate started tasks and, not finding their Logonid in the database yet, would abend them.

Additional Logonids should be defined to ACF2 soon after the first IPL. Logonids cannot be created on the ACF2 database until ACF2 is running. The first few Logonids to establish will be the default Logonids. The Logonid you have specified in the DFTLID field (in the OPTS GSO record) is the one ACF2 will automatically assign to any batch job entering the system without a Logonid specified. Use the INSERT subcommand of the ACF command to create a Logonid record for this id. (For additional details on the syntax and use of the various ACF2 commands and their subcommands, see the ACF2 Administrator's Guide.) This default Logonid should minimally have the attributes RESTRICT, JOB, and JCL turned on.

If you will also be controlling started tasks via ACF2, establish a Logonid record for the STC default id (the value in the DFTSTC field in the OPTS GSO record) you have selected. This Logonid must have the STC attribute. The STC attribute implies RESTRICT, so the latter is only necessary if you want a record of usage to show up in the ACFRPTJL (Restricted Logonid Job Log) report. Similarly, if you will be using the IMS, IDMS, or CICS interfaces, create the appropriate default Logonid records as described in the applicable ACF2 documentation.

When STC control is selected, Logonid records for each individual authorized STC procedure name can be established in addition to the DFTSTC Logonid. These Logonids also need the RESTRICT and STC attributes. Some may also require NON-CNCL, SECURITY, and ACCOUNT privileges.

If you have any online systems which will immediately be controlled by ACF2 (TSO will, if used, and others such as ROSCOE, WYLBUR, CICS, IMS, IDMS, etc. will optionally), you will need to establish ACF2 Logonid records for each of the current users before they can logon or signon to the system. These Logonids should not have the RESTRICT attribute but should instead require passwords. Other attributes, such as the TSO attribute for TSO users, should also be turned on. If the UADS dataset is being bypassed, a number of other TSO-related fields must also be established for each TSO user. ACF2 provides sample UADS conversion CLIST to help convert each existing TSO user (defined with a TSO userid on UADS) to an ACF2 user by creating comparable ACF2 Logonid records. The CLIST should be tested and locally tailored ahead of time, and then

executed soon after the first ACF2 IPL to establish TSO users as valid system users. Additional manual updating of some of these Logonid records (to assign special privileges, such as security officers) will also be necessary. The TSO GSO record can be altered to establish basic default values for TSO users when UADS is being bypassed.

Other Logonid records (for batch users, special production ids, etc.) also must be established on ACF2's Logonid database before they can be used to submit jobs. The sooner specific Logonids are established and used, the sooner the ACF2 reports will contain specific information about individual system users (versus the default Logonids) and the easier it will be to use the report information to write rules and to research and follow up on potential problems.

Before determining the proper attributes and special powers to give each Logonid record, review the descriptions of all the individual Logonid record fields which are provided in the ACF2 Administrator's Guide. After ACFUSER (the initial Logonid) has been used to create appropriate new Logonid records with SECURITY and other powers, ACFUSER should be CANCELled or SUSPENDed (and later deleted).

ACCESS RULE WRITING

In any mode other than ABORT or RULE, ACF2 will not actually abend any job for a rule violation, even if no rules exist. Thus rules are not critical for startup, since the first IPL is normally done with ACF2 in LOG mode. However, in LOG or WARN mode ACF2 will write an SMF record for every unauthorized access, creating large reports until some rules are written. Therefore it is advisable to begin by writing a few general rules (e.g., for commonly used high-level indexes such as SYS1) so that the remaining records on the reports can be reviewed more easily. These initial general rules should be carefully reviewed later and refined.

If RULE mode is selected, individual dataset access rules can contain the 'mode' for that particular rule set. Access rules without this mode control card will be governed by the system-wide mode specified. See the section "Conversion to Full ACF2 Security" for more information on RULE mode.

To write ACF2 rules before ACF2 is running and is therefore available to compile and store rules on its database, separate partitioned datasets should be established for access rules (and generalized resource rules, if written). The PDS's will contain one member for each rule set written (i.e., one PDS member for each $KEY entry).

The first entry in each member will start in column 1 with $KEY(value), where "value" for access rule sets will be a dataset name high-level index (such as SYS1). Additional control entries in the rule record could be $MODE, $OWNER, $PREFIX, %RCHANGE, etc., plus comment lines, although none of these are mandatory. A skeletal rule set containing

only the $KEY and %CHANGE or %RCHANGE control cards can be created for future rule insertion by an authorized user (for information on control cards, see the ACF2 Administrator's Guide). The rule entry line begins with a dataset name (dsn or dsn pattern). It can contain various optional fields which further refine the conditions under which the rule applies to dataset accesses, and normally contains the access permission levels which apply (READ, WRITE, ALLOCate, and/or EXECute-only). Each of these access permission levels may be designated as Allowed (A), allowed and Logged (L), or Prevented (P). The default for each level is PREVENT.

The most general, permissive rule set that could be written for a high-level index is a one-rule entry which applies to all dsns with that high-level index and allows all access levels by anyone under any conditions. To write such a rule set for a high-level index of TEST would require only two lines in the PDS member (or two lines entered directly with the COMPILE command) as follows:

```
$KEY(TEST)
 - R(A) W(A) A(A) E(A)
```

The dsn value of dash (-) is an allowable use of ACF2's masking or pattern feature, meaning that the rule entry applies to any dsn with the high-level index of TEST, followed by any other values in any number of additional index levels (e.g., dsns of TEST.DATA, TEST.ACCTG.PGMGG.COBOL, TEST.A.B.C.D, TEST.WEEKLY.PAYROLL.G0000V03, etc.). Since no other conditions are specified in this rule entry (i.e., the rule entry does not specify that it only applies to certain users or to TEST dsns on certain volumes, etc.), the permissions specified apply to any user accessing any TEST dsns. The permissions of R(A) W(A) A(A) E(A) state that reading, writing (updating), allocating (creating, scratching, cataloging, renaming, etc.), and executing (running programs out of TEST.- libraries) are all "(A)", allowed. If your site has numerous accesses to test datasets whose high-level index names are TEST, compiling and storing this one rule record would eliminate all SMF records and ACF2 reports for all accesses to these datasets.

Obviously a few early rule sets like this one will greatly reduce the volume of reports immediately. However, from a true security point of view this type of rule is probably too general to be permanent. Thus, this technique should only be used selectively and only as a transition aid to reduce report volume, so that specific areas can be progressively secured. When you are ready to write a more specific TEST rule (while still in LOG mode), remove this temporary rule. This will cause all accesses to TEST datasets to be logged again; no rule applies, so they look like potential violations. Similarly, the access permissions in the existing rule could be changed from A (allow) to L (allow but log). The resulting ACF2 reports of TEST dsn accesses can then be used to help write specific TEST rules as appropriate.

Temporary rule entries are another useful ACF2 rule feature in this type of situation. A time limit can be added to a rule through the use of

the FOR operand. For example, the previous TEST rule could have been entered as

```
$KEY(TEST)
* TEMPORARY RULE TO REMOVE TEST RECORDS FROM REPORTS
 - FOR(30) R(A) W(A) A(A) E(A)
```

This rule, when compiled and stored by ACF2, would automatically expire 30 days later. With no rule left allowing everyone access at that point, accesses to TEST datasets would again appear on the logging reports. The security officer would not need to go back and refine the initial rule. This example also contains a sample of an optional comment card, which is defined as any line with an asterisk in column 1.

Based on the logging reports, additional rules can be written and existing rules refined until the site feels most rules are completed. WARN mode can be used as an additional period in which to refine rules before full ABORT mode is implemented. A detailed discussion of these modes, and ideas on selective phasing of different rule sets through modes, can be found in the next chapter, "Conversion to Full Security".

Your installation may have particular high-level indices under which numerous datasets exist (such as SYS1). The NEXTKEY feature of the ACF2 dataset access rule set allows what might be a very large rule set to be split into smaller rule sets or, conversely, the merging of multiple rule sets to one central rule. Refer to the next chapter, "Conversion to Full Security", and the ACF2 Administrator's Guide for details on the use of NEXTKEY in access rule writing.

For additional information on the fields in rule records and the syntax of writing rules, and for additional hints on rule writing, also see the ACF2 Administrator's Guide and the ACF2 Auditor's Guide.

GENERALIZED RESOURCE RULE WRITING

Generalized resource rules are similar to access rules in their use and syntax. They apply to the control of resources other than datasets and volumes. Some additional resources ACF2 may control include:

* Account numbers
* TSO procedure names
* IMS transactions and application group names
* CICS transactions, files, temporary storage, transient data, DL/I calls, programs
* IDMS tasks, programs, data areas, files, and subschemas.

Facilities for controlling all of these resources come with ACF2 and can be implemented independently. For the first IPL you may choose not to turn on any of these features, in which case no resource rules need be written, not even to reduce logging reports. Rules for the various resource types can then be written later as each type is selected for ACF2 control. (Also see the ACF2 Administrator's Guide and ACF2 Auditor's Guide for more detailed information on resource rules.)

CONVERSION TO FULL SECURITY

Many methods are available to ensure that the conversion to full ACF2 security proceeds smoothly without adversely affecting day-to-day activities. This chapter describes some of the conversion methods that have been used successfully by other installations.

SYSTEM-WIDE

The entire installation can move through the various phases together, by using the standard ACF2 system-wide option selections and no exits. This would normally include the following steps:

1. The ACF2 system is put into LOG mode. ACF2 will make all its decisions concerning dataset accesses, but will not deny them. It is essentially in a simulated protection mode. ACF2 reports will show accesses that would have been denied. The Security Officer will have to write, compile, and store access rules to reduce the number of violations. Either during this process or afterwards, the ISO will consult with the data owner to determine if the accesses are legitimate. Decentralized administration with multiple ISOs writing rules (each for his own department or group) may also be used.

2. The ACF2 system is put into WARN mode. For every dataset access that ACF2 would have prevented, an ACF2 warning message will be displayed on the user's terminal or printed in the job log. An installation-supplied message is also displayed, indicating the date on which the access will no longer be allowed. WARN mode should only be used for a limited period of time to ensure that rules are refined and users have had a chance to request changes before migrating to ABORT mode. Running too long in WARN mode tends to make the users ignore the messages or become impatient with the system.

3. Finally, the ACF2 system is put into ABORT mode, which is its final and normal mode of operation. Accesses considered invalid by the ACF2 system will be denied.

Alternatively, RULE mode may be selected for this transition period. Individual rule sets will contain the $MODE control card specifying QUIET, LOG, WARN, or ABORT mode for that particular rule set. The system-wide modes for the "rule sets/records not found" condition or for rule sets lacking the $MODE card can also be set through the MODE field of the OPTS GSO record.

SELECTIVE MIGRATION

Probably the most frequently used method of converting to full ACF2 security is the "selective migration" technique. The benefits of this approach are readily apparent, because it allows security to be enforced based on a combination of standard ACF2 controls and installation specified criteria. Some of the schemes used to implement selective migration are:

1. Migration according to rule set.
2. Migration by user group.
3. Other local criteria.
4. A combination of the above.

Migration According to Rule Set

Two standard ACF2 features allow dataset access decisions to be migrated based on information in the applicable access rule set. These are RULE mode and NEXTKEY support.

To use RULE mode, include a "$MODE(mode)" control card in each access rule set and set the MODE field of the OPTS GSO record to "(RULE,no-rule,no-$mode)". The "no-$mode" parameter specifies a default MODE for access rule sets that do not contain the $MODE control card. Similarly, the "no-rule" parameter specifies a default MODE if no access rule set is found. The "mode" can be any of the other four ACF2 MODES: QUIET, LOG, WARN, or ABORT. When in RULE mode, ACF2 will base its access decision on the value specified in the $MODE control card.

User TESTER requests write access to dataset "PAYROLL.PROD.MASTER" and access to this dataset is controlled by the following ACF2 rule (UID strings at this installation consist of the Logonid preceded by three other characters):

```
$KEY(PAYROLL)
$MODE(LOG)
 PROD.TEST UID(***TESTER) R(A) W(A) A(A) E(A)
 PROD.MASTER UID(***TESTER) R(A) W(P) A(P) E(A)
```

Even though the applicable rule (PROD.MASTER) indicates that TESTER is prevented from writing to the dataset, (i.e., W(P)), the $MODE(LOG) control card causes the access to be allowed but also logged. If $MODE(QUIET) was set, then access would be allowed and not logged. Similarly, the access would have been prevented if $MODE(ABORT) was set.

Also, if the rule set did not contain a $MODE control card:

```
$KEY(PAYROLL)
 PROD.TEST UID(***TESTER) R(A) W(A) A(A) E(A)
 PROD.MASTER UID(***TESTER) R(A) W(P) E(A) A(P)
```

then access would be denied, because ABORT MODE is the default when no $MODE control card is specified. The "no-rule" MODE value (ABORT) would have applied if no rule set for the high-level index (PAYROLL) could be found.

RULE mode provides a flexible method for selectively converting to full ACF2 security based on dataset high-level index names. Using RULE mode, the security officer or data owner is allowed to write access rules and put them in production, testing and refining them as appropriate. After the transition period, the entire rule set can be placed in ABORT mode by simply removing the $MODE control card (assuming the 'no-$mode' value is ABORT) or by changing the $MODE control card to ABORT. Additionally, the ISO can leave RULE mode and place all data under full ACF2 security by changing the MODE field of the OPTS GSO record to ABORT. Note that the $MODE values in a rule set have no effect on processing if the MODE field of the OPTS GSO record is set to anything other than RULE.

The NEXTKEY feature allows an installation to split a rule set into several smaller rule sets, each of which could contain its own $MODE. (For more details on NEXTKEY, see the Administrator's Guide.)

For example:

```
$KEY(PAYROLL)
$MODE(LOG)
 MASTER.- NEXTKEY(MASTER)
 TEST.- UID(***TESTER) R(A)

$KEY(MASTER)
$PREFIX(PAYROLL.MASTER)
$MODE(ABORT)
 SHOP1 UID(***PRODO1) R(A)
```

Here all datasets beginning PAYROLL.MASTER would be protected in ABORT mode, while any invalid PAYROLL.TEST dataset accesses would merely be logged.

Migration By User Group

Many installations convert to full ACF2 data security based on internal groupings, such as by department, unit, etc. ACF2 provides a number of standard features suitable for this purpose.

First, if the User Identification String (UID) includes a group identifier, then access rules may be used to accomplish this without requiring any local exit code. For example, if the UID is defined as "site,job-code,department,Logonid", then rules may be written based on a combination of these fields. All data accesses by users with a job-code of A can be fully controlled by ACF2, while accesses by job-code B users remain unaffected, merely by appropriate rule writing. Other combinations are also easily accommodated.

If the UID does not include appropriate group identifiers as outlined above, then a user exit may be written. Migration by user group can be accomplished using an installation-written exit routine. The exit routine can use information supplied in the Logonid record, information in the applicable access rule set, or both. A number of ACF2 dataset validation exit points are provided. See the ACF2 System Programmer's Guide for complete information about exits.

To use the Logonid record technique, one of the standard ACF2-defined fields of the Logonid record may be used, or a "local" field can be added for this purpose. For example, a field named "MIGRATE" (with ALLOW, LOG, WARN, ABORT values, for example) could be added to the installation portion of the Logonid record and then examined by an exit routine to determine whether or how ACF2 access rules will be used to validate the access. Similarly, the exit could treat all data accesses by users with the "TSO" attribute as if they were in ABORT mode, while accesses by other users are allowed to proceed in LOG mode.

Access rule sets can also be used to implement a migration by user group scheme. The $USERDATA and $OWNER access rule set control cards are provided for installation-specified data. Standard ACF2 routines do not use them. For example, a user exit can examine either or both of these and allow an access request, deny the request, or let ACF2 decide whether access is authorized.

There is also a rule DATA field available for each individual access rule entry. Rule DATA may also be used by the installation to contain information for each individual rule entry. Again, an installation exit routine can interrogate the field and determine how the access should be handled.

By combining various methods, it is possible to accommodate most approaches for conversion to full ACF2 security. Standard features, such as RULE mode and NEXTKEY, are easy to use and require no local coding, while user exit routines are available for unique installation requirements.

NOTE: When combining different migration techniques, ensure that the desired method takes precedence where overlapping occurs. For example, in migration by index level using RULE mode, the dataset high-level index of "SYS1" may be placed in ABORT mode and users attempting to access a SYS1 dataset will be aborted if a violation occurs. However, that same user may be outside the "migration by user group" method (such as the non-TSO technique outline above). The installation exit routine should enforce the correct choice out of the combination.

OTHER TRANSITIONAL CONSIDERATIONS

During these various phases (such as LOG, WARN, and ABORT modes) other activity is taking place besides rule writing. The system-wide options selected (ACFFDR, GSO records, IMS, IDMS, and CICS parameters) must be periodically reviewed and modified as various implementation schedule milestones are reached. Additional areas should be brought under ACF2 control if they were not defined initially, such as STC control, tape datasets, IMS and CICS regions, etc.

All system users should be identified, assigned individual Logonids, and defined to ACF2. Their privileges must be determined and defined. Some educational steps may be necessary. For example, users must be instructed to use their Logonids for batch jobs, and console operators may need some instruction on production job submission, recovery procedures, and/or new (ACF2) console commands and messages. In decentralized environments additional user training in rule writing and in using ACF2 commands may be necessary. User-level documentation distribution may be desirable, including information on general security topics and corporate security policies, plus general ACF2 information.

Also, throughout these phases and on a continuing basis after full ABORT mode has been reached, the ACF2 reports should be printed and carefully reviewed on a regular basis. These reports should be very useful in the early phases to help write rules and to define appropriate assignment of individual user privileges. As soon as certain privileges and rules have been established (even in LOG mode), the reports will identify "violations" which should be further researched and acted on appropriately. When used on an ongoing basis, these reports can be an invaluable aid in detecting data security threats.

GENERAL TECHNICAL CONSIDERATIONS

Detailed information on the technical aspects of ACF2 and the required installation and/or system maintenance steps is provided in the ACF2 Installation and Maintenance Guide and in the ACF2 System Programmer's Guide. Only general comments and explanations will be provided here, with some special areas for consideration highlighted.

SYSTEM COMPONENTS

The design of ACF2 provides for a phased installation. This includes technical portions which can be performed in phases. For example, the standard IBM Systems Maintenance Program (SMP) is used to establish ACF2 libraries and to provide tracking of system changes and controls over the normal maintenance activities. SMP physical installation processing should be performed prior to the actual installation date. For MVS Release 3.8 systems only, ACF2 is not activated until a special post-install job (named POSTJOB) is run which link-edits the ACF2 intercepts into the operating system.

These ACF2 intercepts are handled independently of any IBM or SKK maintenance, Selectable Units, or local modifications. The ACF2 program product itself consists of the following components:

ACFMAIN
: A subsystem used to initialize the ACF2 Communication Vector Table and perform automatic ACF2 VSAM cluster backups.

ACFRECVR
: Program used to recover the ACF2 VSAM clusters from backup datasets and SMF journal records (online or tape).

ACFRPT
: Report generators used to produce the various ACF2 reports.

ACFNRULE
: Program used to modify a set of rules.

ACFERASE
: Data disposal utility.

ACF2 SVCs
: ALTER
  : Manages the ACF2 databases, user entry authorization, and resource validation.

VALD
Performs dataset access validation and TSO command-limiting validation.

SPF Screens
For MVS installations with TSO/SPF, SKK supplies a set of SPF screens for processing certain ACF2 functions online. The ACF2 SPF selection menu includes options for:

RULES
To process access and resource rules.

LOGONIDS
To create and maintain ACF2 Logonid records.

SYSTEM
To execute ACF2 SHOW commands.

REPORTS
To generate ACF2 reports.

UTILITIES
To process ACF2 utilities.

GSO
To create, alter and activate GSO records.

Online SPF tutorials are also supplied.

TSO Commands
ACF
Contains various subcommands to manipulate Logonid records, dataset rules, resource rules, scope, shift, and GSO records, and entry lists, and to display these records and other information about ACF2 options which are active.

ACFCOMP
Compiles and stores a set of rules.

ACFDEL
Data disposal utility (online version of ACFERASE).

ACFNRULE
Modifies a set of rules.

ACFSUB
Allows for TSO submission of specially controlled job streams.

HELP Members
ACF command (available to Security Officer, Account Manager, and Auditor

ACS - ACF mode
ACSC - SCOPE mode
ACSE - ENTRY mode
ACSI - CONTROL mode
ACSL - LID mode
ACSR - RULE mode
ACSS - RESOURCE mode
ACST - SHIFT mode

ACF command (normal users without special authorities)

ACF - ACF mode
ACFC - SCOPE mode
ACFE - ENTRY mode
ACFL - LID mode
ACFR - RULE mode
ACFS - RESOURCE mode
ACFT - SHIFT mode

ACF400(general ACF2 information)

ACFCOMP command

ACFDEL command

ACFNRULE command

ACFRSRC (resource rule description)

ACFRULES (access rule description)

ACFSUB command

JESx Modifications
To authorize users for access to the system via jobs. ACF2 also:

* Provides optional validation of Logonid and password at all nodes in an NJE network.

* Provides optional network job inheritance for NJE jobs.

* Does not transit passwords in clear text format across NJE nodes.

* Supplies jobs submitted without a Logonid and password with a default Logonid at JES reader time.

* Supports all JESx systems.

ACF2 Intercepts
To authorize user access to TSO and TSO commands, and to validate dataset, volume, and resource accesses.

LOCAL MODIFICATIONS

There are two types of local modifications to be considered:

1. Existing or planned local modifications to the operating system and/or subsystems (e.g., TSO, JES, SMF, exits, etc.) which may need to interface with ACF2 processing due to their location or their logic. These local modifications should be reviewed before the installation of ACF2.

   In some cases, such as TSO logon processing, the local code may have been designed to perform some security-related function which will be replaced by ACF2. Under these circumstances, the local code can normally just be removed. In other cases, the code must remain to perform some needed local function and must reside in the same exit or front-end the same intercept point that ACF2 uses. This requires a decision as to which processing (ACF2's or the local modification) should come first. Normally ACF2 should come first, as it will be determining whether the requested function is legitimate. Then, only when ACF2 decides to allow the process to continue, would the local code be used.

   For example, a site with a local modification in the open SVC to produce automated external tape labels would allow the ACF2 front-end validation to come first to see if the open is authorized. If the open is denied, no tape label would be desired.

2. Local modifications to ACF2 for further tailoring beyond what can be done with provided options. Normally this requires producing local code for one or more of the provided ACF2 exits, or inserting local code in another software product, or a special application program to call ACF2 validation routines. Most sites find that these modifications can wait until the basic system is installed, tested, and operational; indeed, most sites install ACF2 without ever having to use the local exits.

While possible local modifications (due to some special naming conventions, transitional implementation plans, etc.) should be taken into account during installation planning, normally the actual coding and activation of these changes can be performed after the initial installation and IPL has established the base system.

MINIMUM SYSTEMS MAINTENANCE LEVEL

The exact current requirements for operating system and subsystem maintenance levels are provided with each ACF2 distribution or maintenance tape (see the System Programmer's Guide). In general, the system should be at a relatively recent level (maintenance provided by the system hardware vendor applied within 6 months of the release date). It also should have been running at that level (in production) a minimum of one week to provide a valid, stable base for ACF2 code installation and testing.

STORAGE CONSIDERATIONS

The "internal" storage that is used by ACF2 is approximately:

Link Pack Area (LPA) - 230K. This includes the two ACF2 SVCs, all of the intercepts, and the Field Definition Record. The ACF command is link-edited into SYS1.LINKLIB; it may be moved to LPA if desired and is 91K bytes in length. This storage is Key 0 and pageable.

Common Storage Area (CSA) - 36K plus resident rules. This includes the common control blocks and VSAM buffer pools used for database access. The resident rules are loaded at ACF2 initialization time and are those specified in the RESRULE and RESDIR GSO records within the Infostorage Control class. This storage is Key 1, fetch protected, and pageable.

System Queue Area (SQA) - 1K. This is the ACF2 Communications Vector Table (CVT) and other small control blocks. This storage is Key 0 and fixed in memory.

Local System Queue Area (LSQA, in individual address space) - 2K plus queued rules. This includes the ACF2 User Control Block, the Logonid Record, and the User Identification String (UID) which was constructed when the job was initiated. The queued rules are those whose indices were referenced by that user and were not in the RESRULE specification. This storage is Key 0 and is swappable.

The "external" storage considerations include:

SMF Datasets - ACF2 writes all of its attempted violation, logging, trace, and control database recovery records on the standard SMF datasets (e.g., SYS1.MAN1 and SYS1.MAN2). Thus, the installation of ACF2 will increase the volume of these datasets. The heaviest volume will occur immediately after installation (if running in any mode except QUIET mode) until a number of rules are compiled and stored. This period could cover only a few minutes if the necessary rules are pre-written in a dataset and immediately compiled and stored, or could cover weeks if rule writing has not started. This volume increase could nearly double the SMF output (actual percent of increase would depend on rule writing, ACF2 logging options, SE2/SMF options, local exits, etc.). The "permanent" volume of ACF2 SMF output will be much lower than the initial output, but is also dependent on all these factors.

ACF2 Control Databases - ACF2 requires three VSAM control databases (LOGONIDS, RULES, and INFOSTG). Alternate clusters for recovery use should also be defined. The location of these should be carefully considered, e.g., shared DASD used for multiple CPU systems and on a pack not heavily used for other system tasks. The alternates should be on a different pack than the primary datasets. For approximate space allocations for each dataset, see the chapter on Installation in the ACF2 System Programmer's Guide.

Backup Sequential Datasets - ACF2 requires three sequential datasets for backup processing of its control databases.

GENERAL INSTALLATION AND MAINTENANCE PLANNING

Planning for the technical installation of ACF2 and its ongoing systems maintenance should be progressing concurrently with the general implementation planning. Some of the topics that should be considered in the technical portion are listed below. These are in general chronological sequence but, with careful planning and coordination, many of these steps could be accomplished in parallel.

1. Planning and organizing for the ACF2 system installation, including schedules, responsibility assignments, check points, etc.

2. Establishing a stable operating system (and subsystems) at least at the minimum required maintenance level.

3. Reviewing special subsystems, started tasks and program products (such as data or operational management packages) which already exist on the system and planning for the resolution of any possible conflicts.

4. Reviewing local system modifications (such as local modifications to JES source code or local code in exits in SMF, TSO, IMS, or other areas), and planning for the resolution of any logical or physical conflicts.

5. Planning for the initial establishment of Logonid records so that users can access the system. This includes preparing for UADS conversion (for TSO users) and for the establishment of default Logonids for batch and STC jobs. Also consider whether or not UADS will be retained after ACF2 implementation and plan accordingly for the conversion and maintenance of the TSO-related use r data elements.

6. Planning for and processing the ACF2 Distribution Tape and steps such as:

   - unloading the packaging datasets.
   - running the SMP install jobs.
   - applying maintenance from pertinent FLASHes, etc. (if any).

   The tape is normally unloaded early in order to provide information necessary to proceed with the other steps described here.

7. Selecting the ACFFDR, GSO, CICS, IMS, and IDMS installation options (as applicable and preparing the assemblies, modules and online changes for ACF2 processing.

8. Completing the installation process, including:

   - creation of the final target system
   - making final adjustments for the local running environment
   - defining and initializing the three ACF2 VSAM-based files
   - IPLing the system (normally in LOG mode)
   - establishing the initial system users (running the UADCLIST conversion, inserting default Logonids, etc.)
   - testing the system, rules, etc.

9. Tailoring and testing the ACF2 database recovery procedures.

10. Tailoring and testing the ACF2 report generator JCL and running and reviewing the actual reports.

11. Establishing policies and procedures for:

    - the ongoing application of ACF2 and system maintenance
    - the periodic review and modification of ACF2 system options (e.g., updating the ACFFDR, including reassembly and re-IPL; reviewing GSO records)
    - the handling of new features and/or the migration of ACF2 controls to other areas, such as CICS, ROSCOE, etc.

OTHER PRODUCT INTERFACES

There may be numerous other software products running at your site besides ACF2 and the basic operating system and subsystems. These might include database systems, disk management and archiving systems, tape management systems, sorts, and other utilities and packages. A large number of these will continue to operate without any changes or special considerations related to the implementation of ACF2. With some software products, however, the user may notice some minor differences and special ACF2 interfaces that should be utilized to afford the best overall security level. For detailed information on a number of these systems, see other ACF2 manuals such as the IMS Support, CICS Support, and Other Products Manuals. However, a few comments about some of these subsystems and products are listed here for special consideration in implementation planning.

CICS (IBM'S CUSTOMER INFORMATION CONTROL SYSTEM)

The ACF2/CICS interface provides security for CICS transactions, programs, files, transient data, temporary storage, and DL/I requests. Each CICS region can be interfaced with ACF2 at different times and with different options, so that the desired CICS controls can also be phased in. ACF2/CICS system initialization parameters, which define many ACF2 options for CICS, can be defined in a dataset which is referenced at CICS initialization time so that no macros need to be assembled.

IDMS (CULLINET'S INTEGRATED DATABASE MANAGEMENT SYSTEM)

The ACF2/IDMS interface provides signon security as well as resource validation for IDMS programs, data areas, files, and subschemas. ACF2/IDMS security is implemented independently of the base ACF2 system. ACF2/IDMS options and control parameters for each IDMS address space are specified by means of ACF2/IDMS macros. Complete details about the interface can be found in the ACF2 IDMS Support Manual.

IMS (IBM'S INFORMATION MANAGEMENT SYSTEM)

The ACF2/IMS interface validates IMS users and the terminals, transactions, and/or application group names which they use. These interfaces and the IMS-related ACF2 options can be implemented either at the same time or later than the rest of ACF2's controls. In addition, each IMS control region can be interfaced separately with ACF2. Thus, for example, ACF2 could be implemented for TSO and batch users initially, for the test IMS system the following month, and for the production IMS system a few weeks later. And the test IMS control region could be in ABORT mode while the production IMS control region was in LOG mode.

TSO (IBM'S TIME SHARING OPTION)

At MVS sites with TSO users, it is important to realize that these users will come under ACF2's user validation immediately. ACF2 provides a CLIST to convert each TSO user defined on the TSO UADS (User Attribute Dataset) file to an ACF2 user (creates records to establish each TSO user onto ACF2's Logonid database). This should be done early in the installation process.

There are other aspects of TSO usage which are slightly different under ACF2. These should be planned for and publicized as needed. For example:

Logon Processing
: There are a few differences in how certain Logon parameters will be treated under ACF2. Most of these are dependent on selection of system options, such as whether UADS will be bypassed or still used with ACF2, and whether "quick logons" (passwords entered on the logon line) will be allowed. See the section on "TSO Logon Processing" and similar topics in the General Information Manual for more details.

TSO PROFILE PREFIX
: Under ACF2, two variables are of particular importance to the TSO user:

  a. The ACF2 owned dataset prefix (PREFIX) in the Logonid record indicates the high-level indexes the user "owns", for which no rules are required for full dataset access. This field is usually the same as the Logonid, but could be blank or a mask (high-level index "pattern" which matches multiple high-level indexes).

b. The TSO profile dataset prefix field (PROFILE PREFIX) becomes the high-level index for any type of unqualified dataset name reference. Usually this field is the same as the Logonid. However, the user may change this field for convenience when doing frequent references to non-owned datasets for which the user has access permission. Changing the PROFILE PREFIX to something other than the ACF2 PREFIX field may have significant ramifications, as detailed below. Additionally, if the UADS field of the OPTS GSO record has been specified, the change is permanent (from logon to logon) until it is reset with another PROFILE PREFIX command.

Some TSO commands create (allocate, catalog, open for write, scratch, and/or rename) intermediate datasets in order to accomplish the user's request. Some of these commands are OUTPUT, MERGE, and EDIT, and SUBMIT and RUN under EDIT. There may be other commands in your system which also implicitly cause new dataset allocations. If the user has changed his PROFILE PREFIX, then functions which create intermediate datasets will be aborted by ACF2 since the user may not have allocate or write privileges (even though the user may be allowed read access) for datasets of non-owned high-level indices. An exception to this is if the TSO Command Package (SU811) is on the system and the user is operating without the RECOVER option; then many of the intermediate datasets are VIO (virtual input/output) datasets, for which the creating address space has full control.

It is recommended that the full implications of the PROFILE PREFIX command (especially when ABORT mode is reached) be clarified to your TSO users.

TSO/E Broadcast Performance Support

The TSORBA field of the ACF2 Logonid record will specify the Mail Index Record (MIR) for TSO/E users. This feature reduces the logon processing time by providing a direct pointer to the MIR in the SYS1.BRODCAST dataset and requires both LIDRECL(1024) and NOUADS to be specified in the OPTS GSO record.

OS Password Protection

Prior to ACF2, if a user used OS Password protection on a dataset and specified an OS password equal to his TSO LOGON password, the system would not prompt for the OS password when accessing that dataset. Under ACF2, even if the OS password is the same as the TSO password, the user will be prompted for his OS password (since ACF2 does not retain the TSO password after logon).

JES (IBM'S JOB ENTRY SUBSYSTEM)

For detailed information on the installation of the ACF2/JES interfaces, see the ACF2 Installation and Maintenance Guide. However, a few general considerations should be recognized during the planning period, such as:

JES2 Multi-Access Spool Considerations

In a JES2 multi-access spool system it is not a requirement that ACF2 be installed on all processors simultaneously. Jobs submitted on a non-ACF2 CPU and run on an ACF2 CPU will be assigned the default Logonid. Jobs submitted on an ACF2 CPU will run normally on a non-ACF2 CPU. There is no incompatibility in SPOOL disk formatting. This feature allows for easy transition in this type of complex environment.

Network Job Entry (NJE) Considerations

JES2/NJE systems require a cold start of the SPOOL volumes at the node where ACF2 is installed (for the initial ACF2 IPL only) because of an internal control block incompatibility in an ACF2/JES2/NJE environment. There is no incompatibility with any mixture of ACF2 and non-ACF2 nodes in the NJE Net.

Jobs may enter the net at any type of node, be transmitted through any type of node, and execute at any type of node. The ACF2 Logonid and password information entered with the job will be transmitted to the "executing" site and if ACF2 is present, Logonid validation will occur.

If ENCRYPT(XDES) is specified in the PSWD GSO record, ACF2 will suppply a partially encrypted password which can be sent over the telecommunications network. The password is then fully encrypted by the execution node if validation is required.

JES3 Considerations

In a JES3 complex, all CPUs must use JES3 with the ACF2 modifications installed although it is not necessary to install the rest of ACF2 on all the systems. This will make the JES3 modifications passive on the systems without ACF2. There is no incompatibility in SPOOL disk formatting and no fixed JES3 control blocks are modified.

ACF2 should be initially installed on the processor with TSO and on the Global CPU. Other processors can be added as scheduling permits.

TAPE MANAGEMENT SYSTEMS

ACF2 operates with various tape management systems, such as University Computing Center's TMS and Calcomp's Automatic Tape Library, to optionally provide full dataset-level protection on tape with no additional support coding required. ACF2 operates with other systems, but in order to provide tape protection at a dataset name level an ACF2 exit may be required. This is because some systems do not record the full names of all datasets on the tape.

ROSCOE (APPLIED DATA RESEARCH)

ACF2 provides exits for signon validation, job submission, and the COPY and UTILITY processors for ACF2 control of ROSCOE users, dataset access, and the transferring of Logonid information without the need for passwords in ROSCOE-stored JCL. See the ACF2 Other Products Manuals for complete details.

ASM2 (CAMBRIDGE SYSTEMS GROUP)

ACF2 provides an authorization exit for the protection of datasets in ASM2 archive status. The ACF2/ASM2 interface is supported by CSG (via the ASM2 AUTHEXT code and documentation supplied by CSG). See the ACF2 Other Products Manuals for complete details.

FDR/ABR (INNOVATION DATA PROCESSING'S FAST DUMP RESTORE)

A front-end to FDR is available to validate that the datasets and volumes specified may be dumped, restored, or otherwise processed. See the ACF2 Other Products Manuals for complete details.

OTHER PRODUCTS

Interfaces with various other products are available through SKK, from other ACF2 users, or from the other package vendors. The ACF2 Other Products Manual contains information about other product interfaces to ACF2. This manual is supplied with the ACF2 package. Other documents (such as the bimonthly newsletter, SKK BROADCAST) should be reviewed for the most current information, and/or the appropriate vendor(s) to contact.

APPENDIX A - DOCUMENTATION

This Implementation Planning Guide represents only one of many manuals provided with the ACF2 system. Besides the manuals, other support documentation is also periodically distributed. In general, ACF2 documentation includes:

BASIC MANUALS

Overview
A short manual which gives a general management overview of the ACF2 product. This would normally be the first manual a new implementation team member would read.

General Information Manual
This is the general reference manual for the basic ACF2 system and describes the general design philosophies, features and functions of ACF2 and its various parts and subsystems. It should be reviewed early to get a general familiarity with ACF2. The General Information Manual gives descriptions of the various functions ACF2 performs (e.g., system access control, data access control, generalized resource control), the Logonid record, use of input source controls, ACF2 databases, etc. It contains basic information on topics covered in greater detail in other manuals (e.g., Administrator's Guide, Utilities Manual, etc.).

Utilities
This manual includes descriptions, parameters, sample job JCL, and sample outputs of all of the utilities, batch programs, and report generators provided with the ACF2 package. It is a good reference when using one of these programs, or when interpreting output from any of the reports.

Administrator's Guide
This manual provides detailed information on the use of the ACF command and subcommands for processing Logonid records, access rules, generalized resource rules, GSO records, etc. This manual provides detailed explanations of the ACF2 concepts and facilities briefly presented in the ACF2 General Information Manual. Different portions of this manual may be selected for distribution to various system users and special ACF2 administrative personnel (security officers, account managers, auditors, etc.) as appropriate for the tasks they need to perform. Additional local information (such as company policies and naming conventions) could be added to this manual and used to produce tailored in-house user guides.

Auditor's Guide

This manual should be useful to management and security administrators in making decisions about selecting ACF2 options, rule writing, assigning user privileges, and in implementing an overall security system. The manual will also be useful for the EDP auditor in reviewing the ACF2 and related internal controls implemented at the site.

System Programmer's Guide

This manual is directed primarily at the system programmer responsible for the technical aspects of ACF2 installation and maintenance. It contains detailed information on processing the ACF2 distribution tape, modifying JES, various installation tasks, the first IPL, optional PTFs, ACF2 macros, SVCs, exits, databases, subroutines, other product interfaces, control blocks, and similar technical aspects. Also included are descriptions of ACF2 Field Definition Record (ACFFDR) macros and LIDREC (Logonid Record Definition) values. It explains how to designate parameters for each ACFFDR macro and thus establish the local values or choices for the various system-wide ACF2 options. This information should be reviewed when first installing the product and used for reference later on, especially where local tailoring (exit writing, special product interface, etc.) is desired.

Messages Manual

This document contains an entry for each system message ACF2 might produce (to a user, the console, or the job log). The individual message id, the message text, and a description of the possible cause of the message are included. This is primarily useful in the operations and systems maintenance areas, but parts of this manual may be useful to special groups of users. The manual is separated into sections based on the interface/subsystem producing the message, such as IMS, CICS, ROSCOE, JES, ACF2 command processing, utilities, report generators, etc.

IDMS Support Manual

Contains information on the ACF2/IDMS interface, including option selection, use of macros, and Logonid record considerations.

IMS Support Manual

This manual includes detailed information about the ACF2/IMS interface, such as option selection, Logonid record considerations, and storage estimates.

CICS Support Manual

This manual contains information on the ACF2/CICS interface, including how to select and set ACF2 options, how to secure user-defined resources, and worksheets for calculating the amount of storage needed.

Implementation Planning Guide

This manual is designed primarily to be used during the initial planning and installation phase of ACF2 implementation at a site. It includes various hints and suggestions on how to go about the non-technical aspects of the implementation. These ideas can then be tailored and augmented according to local conditions and requirements to produce the best implementation plan for that site.

Other Products Manual

The OPM provides information on various software products on the market and their uses/interfaces to ACF2. The products are listed alphabetically. OPM entries may also be found in the Composite Index. The OPM also contains a catalog of usermods that describes user-written interfaces to ACF2. The physical usermods are supplied on the ACF2 distribution and maintenance tape.

Composite Index

Indexes are provided in each of the above manuals excluding the Overview. Additionally, a separate Composite Index is supplied with the ACF2 documentation package. This composite index contains the combined references from each individual manual for all entries. A code (such as GIM to denote General Information Manual and UTIL to denote Utilities Manual) is used to indicate which manual contains the information on each topic.

ACF2 Reference Card

The ACF2 Reference Card provided with the ACF2 package contains summaries of the various ACF subcommands and the syntax of each subcommand. Also listed are the fields of the Logonid record, access rule syntax, and resource rule syntax.

Each of these manuals is updated as necessary to reflect the current version of the product. Changes to these manuals are published periodically and distributed as TNLs (Technical Newsletters). It is important that sites file these changes in all copies of their manuals regularly to maintain up-to-date reference material.

Each site which orders ACF2 receives two sets of all the manuals listed above. Normally one copy should go to the security administrator (ISO) and the other to the systems maintenance person. Additional copies can also be ordered from SKK, either as one-time orders where the individual manuals are priced at cost, or on an annual subscription basis where the charge includes a complete set of manuals plus copies of any new manuals or updates (TNLs) distributed during the year. Contact SKK directly for current information on rates or to make changes to the mailing list.

FLASHES

These contain announcements of relatively severe problems (and their fixes) where SKK feels it is inappropriate to wait until a more formal document (e.g., a new version or release) is produced. The FLASH identifier contains the year issused and a sequential number (e.g., MVS85-02 would be the second acf2/MVS FLASH for 1985).

SKK BROADCAST

This document is a bimonthly newsletter which announces forthcoming product changes and events, reports on significant happenings, introduces new ideas and activities, and generally informs SKK customers of interesting current projects and user information.

DISTRIBUTION AND MAINTENANCE TAPE

Besides containing the basic system and its related utilities, report generators, install jobstreams, etc., the ACF2 Install Tape or Distribution Tape also contains various sample jobstreams, exit coding, other product interfaces, and other aids.

CUSTOMER EDUCATION CATALOG

This catalog provides a detailed description of the various sessions offered at the ACF2 Training Classes and/or available for onsite course requests. Request forms for both the regularly held classes and for requesting customized onsite classes are included in the catalog.

TRAINING COURSE HANDOUTS

Copies of the more than 600 transparencies used in the four-day ACF2 training classes, plus some other ACF2 reference materials, are included in the ACF2 Training Class binder which is provided to each class attendee. ACF2 training classes are held monthly in the U.S. and periodically elsewhere in the world. Contact your local ACF2 representative for current schedules and fees.

MISCELLANEOUS OTHER ANNOUNCEMENTS

Periodically other announcements and information will be mailed out from SKK. These include information on upcoming training classes, user conferences, official holiday schedules, documentation rates (for extra copies), questionnaires, etc. These mailings are sent to the same contact names at each site as the standard ACF2 documentation mailings.

APPENDIX B - ACF2/MVS SUPERCEDED ELEMENTS

SKK continually enhances ACF2 to meet the needs of installations concerned about information security. Some of these enhancements have resulted in new options and features which perform the same basic functions as older ones but with increased flexibility and power. One example of this would be the addition, in Release 3.1, of scope lists, which replaced all the functions of the much more limited LIDSCOPE, UIDSCOPE, and DSNSCOPE.

In each case where older features have been superceded by newer options, the old options have been temporarily retained to provide installations with easy upward compatibility. However, since these older fields and options have been fully superceded by newer more powerful facilities, they should be replaced.

To give existing ACF2 users ample time to change any related procedures and Logonid or rule records, we are notifying you now which items will be removed from acf2/MVS in future releases. Please note that the items listed in the left-hand column may not be supported under future releases of the acf2/MVS product. The features listed on the right-hand column are available now and provide the same or improved facilities. Some items are further highlighted to indicate they should be replaced during implementation of Release 4.0.

New acf2/MVS installations

Since the items listed in the left-hand column have all been superceded by the features identified in the right-hand column and will be deleted in future releases, it is highly recommended that no use of the left-hand items be made at your installation. Although many of these options are still available as part of Release 4.0, their use may necessitate otherwise unnecessary procedural or database changes in the future.

SUPERCEDED OPTION	ALTERNATIVE OPTION
Logonid Record Fields:	
LIDSCOPE (LIDASCOP, 8 characters) UIDSCOPE (LIDUSCOP, 24 characters) DSNSCOPE (LIDSSCOP, 8 characters)	SCPLIST (LIDSCPL, 8 characters) This field, introduced in Release 3.1, points to the name of a scope list record on the Infostorage database which can contain lists of scope masks applicable to any or all of the following areas: LIDs, UIDs, RULEs, Infostorage records.
PASSWORD (LIDPSWD, 4 characters)	PASSWORD (LIDNPSWD, 8 characters) This field, introduced in Version 3.1.4., contains the results of the XDES one-way encrypted password for that Logonid. Choosing the ENCRYPT=XDES option of the OPTS global system options (GSO) record automatically handles the maintenance of this field.

The 44 characters of the LIDREC previously used by these fields will become reserved fields in a future release of acf2/MVS and may be used for some other purposes in later releases.

SUPERCEDED OPTION	ALTERNATIVE OPTION
ACFFDR @PSWD Macro ENCRYPT=R221 option	Infostorage GSO type code PSWD record ENCRYPT(XDES)
The R221 encryption option will no longer be available as of Release 5.0. Note that Release 4.0 uses the XDES encryption method as a default.	The XDES encryption algorithm, first available in ACF2 Version 3.1.4, should be implemented prior to Release 5.0. Note that ENCRYPT(XDES) is the default in Release 4.0.
ACFFDR @OPTS LIDRECL=512	Infostorage GSO type code OPTS record LIDRECL(1024)
The option of a 512-byte Logonid record will be eliminated in a future release. Note that a 1024-byte LIDRECL is the default value shipped with Release 4.0.	For Release 4.0, Logonid records, by default, utilize the 1024-byte maximum record length option.
ACFFDR @OPTS T2741=YES/NO NCP=YES/NO ASCMOD=YES/NO XOUT17=YES/NO	The need to specify these options has been eliminated in Release 4.0, and any related program determinations have been moved into the standard code. No installation action is required for this migration, unless some local code referenced the related ACCVT entries which are no longer supported. However, related GSO records (TSOCRT, TSOTWX and TSO2741) are available on the ACF2 Infostorage database for any local tailoring of X-out character strings, etc. that may be desired.
These ACFFDR options are no longer supported at Release 4.0 and above. Their related ACCVT entries are also no longer maintained or supported at Release 4.0 and above.	

SUPERCEDED OPTION	ALTERNATIVE OPTION
ACFFDR @EXITS SMFJINT SMFSINT SMFTERM	ACF76DYN and ACF76DRV These are module samples supplied in source form. They provide optional expanded SMF driver support for sites desiring this facility.
These ACFFDR options are no longer supported in Release 4.0 or above, since ACF2 no longer uses the related SMF exits or requires an SMF exit driver for its processing.	
ACFFDR @CFDE PRTN=8 RRTN=8	ACFFDR @CFDE PRTN=11 RRTN=11
These processing and reconstruction routines for HEX fields have been superceded in Release 4.0 and above by PRTN=11 and RRTN=11. The previous specifications (PRTN=8, RRTN=8, FLAGS=SPECIAL) will continue to function unchanged. However, all SKK-supplied @CFDE defaults for HEX fields have been changed to specify PRTN=11 and RRTN=11 in Release 4.0 and above and it is recommended that installations also change any local @CFDE specifications to use these new routines. Support for PRTN=8 and RRTN=8 for HEX fields will be dropped in a future release.	These new routines supercede PRTN=8 and RRTN=8 and provide all the same functions. In addition, the use of these routines does not require the specification of FLAGS=SPECIAL as was previously needed with PRTN=8 and RRTN=8. Note that PRTN=11 and RRTN=11 will be selected by default for any @CFDE entry with type HEX specified if no PRTN and RRTN are specified.

SUPERCEDED OPTION	ALTERNATIVE OPTION
Technical Changes:	
VIOEXIT exit	DSNPOST exit
This exit point will be removed in a future release of acf2/MVS. All local processing accomplished in this exit can be performed in the DSNPOST exit.	This exit, available in Release 3.1, will monitor all dataset, volume, and program accesses which would have gone through the VIOEXIT. Note that if an installation has both a VIOEXIT and DSNPOST defined, only the DSNPOST exit receives control.
ACGRSRC parmlist	ACNTRY parmlist
Local code using the ACGRSRC parmlist at the acf2/MVS 3.1 level will continue to function the same at the Release 4.0 level for all existing Infostorage records. However, for the Infostorage records under storage class C, such as the GSO records, the ACNTRY parmlist must be used. Also, any installation written routines should use the ACNTRY parmlist rather than the ACGRSRC parmlist for all Infostorage classes except "R". Support in ACGRSRC for use with other than generalized resource rules will be dropped in a future release.	The new ACNTRY parmlist should be used for any local requests to access ACF2 Infostorage records except for class "R" generalized resource rule reocrds. In a future release, ACF2 will allow the use of ACGRSRC for generalized resource rule records and associated directories only. ACNTRY must be used for all other Infostorage records.

SUPERCEDED OPTION	ALTERNATIVE OPTION
ACCVT Location Routines	ACF79USR exit
A temporary exit (ACF79USR) has been provided with Release 4.0 to function as a transition aid for any sites who previously utilized their own ACCVT processing routine. Installations have the option of relinking their applications or coding this exit. This is a temporary exit which will be dropped in a future release and is provided as a transition aid for Release 4.0 only.	See ACF79USR discussion under ACCVT location routines in the other column. This exit is temporary and will be dropped in a future release.
ACDSV parmlist	ACDSV parmlist
This parmlist (for local ACFSVC TYPE=S requests) has been expanded for Release 4.0 and above. Any local code which currently uses this parmlist does not require reassembly at 4.0 time, until or unless the local code is modified to use some feature in the new expanded area.	A new compatibility bit is provided for transition during Release 4.0 but will be dropped in a future release. Note that all code using ACDSV would therefore require reassembly at a future date if not already using the fully extended Release 4.0 and above parmlist.

SUPERCEDED OPTION	ALTERNATIVE OPTION
SVC S Cleanup Request	SVC A Cleanup Request
Local requests for system exit processing which currently issue ACFSVC TYPE=S for cleanup should be converted to issue ACFSVS TYPE=A. This will reduce overhead and GETMAINs. Currently (Release 3.1 and 4.0) both SVC S and SVC A support cleanup requests. Support for use of the SVC S cleanup requests will be dropped in a future release.	Support for use of ACFSVC TYPE=A for system exit cleanup requests (ACTRM) has been available for many releases. This support has also been available via ACFSVC TYPE=S (ACDSV). Due to duplication and the extra overhead required when choosing to use TYPE=S versus TYPE=A, the cleanup support in TYPE=S will be dropped in a future release. Local code already using TYPE=A for this function will not require any modification or reassembly. Local code using TYPE=S should be changed to use TYPE=A to avoid possible future maintenance problems.
TSO Command Limiting, ACFSVC TYPE=C	TSO Command Limiting, SVC A TYPE=A
Locally coded requests for TSO Command Limiting validation previously used TYPE=C. These TYPE=C requests will continue to operate unchanged under Release 4.0. However, expanded capabilitity is provided by the new ACFSVC A TYPE=A request and installations should convert to using the new TYPE=A. Support for the TYPE=C option will be dropped in a future release.	This new Release 4.0 and above feature expands the facilities for local requests for TSO Command Limiting validations. A new parmlist ACLIMIT must be used. This feature is available in Release 4.0 and above.

SUPERCEDED OPTION	ALTERNATIVE OPTION
ACF62DSP program parmlist	ACFCDSPP DSECT supplied
This parmlist has also been expanded. All local code referencing ACF62DSP (also previously known under the alias ACFCDSP) to construct LIDREC display buffers, etc., must be reassembled at Release 4.0 time.	This DSECT maps the ACF62DSP parmlist and is provided with Release 4.0 and above to assist in identifying fields, offsets, etc.
ACVALD parmlist	ACVALD parmlist
This system entry validation parmlist was extended in Release 3.1.4, with additional fields added in Release 4.0. Reassembly of local installation code for Release 4.0 is required if OLDPARM=NO (the default) is specified on the macro ACVALD. Note that if OLDPARM=YES, OID card support is not available.	A macro parameter, OLDPARM, was introduced in Release 3.1.4 for compatibility reasons. This parameter will be dropped in a future release. By that time, all local code referencing this parmlist should be reassembled to use the expanded parmlist, since OLDPARM=YES will no longer be supported.

INDEX