AUDITING TOP SECRET

Security File Review

Control Options

Auditing Tools

The Audit Program

AUDITING TOP SECRET

SECURITY FILE REVIEW

Functional ACID Structure

User ACIDs for:

- General Users
- Emergencies
- Firefighting
- Consultants

AUDITING TOP SECRET

SECURITY FILE REVIEW

Functional ACID Structure

Division and Department ACIDs for:

- Miscellaneous Resources
- Temporary Resources
- Corporate Resources
- Major and Intermediate Organization Functions

AUDITING TOP SECRET

SECURITY FILE REVIEW

Reviewing the Functional Levels

Security Administrator ACIDs for:

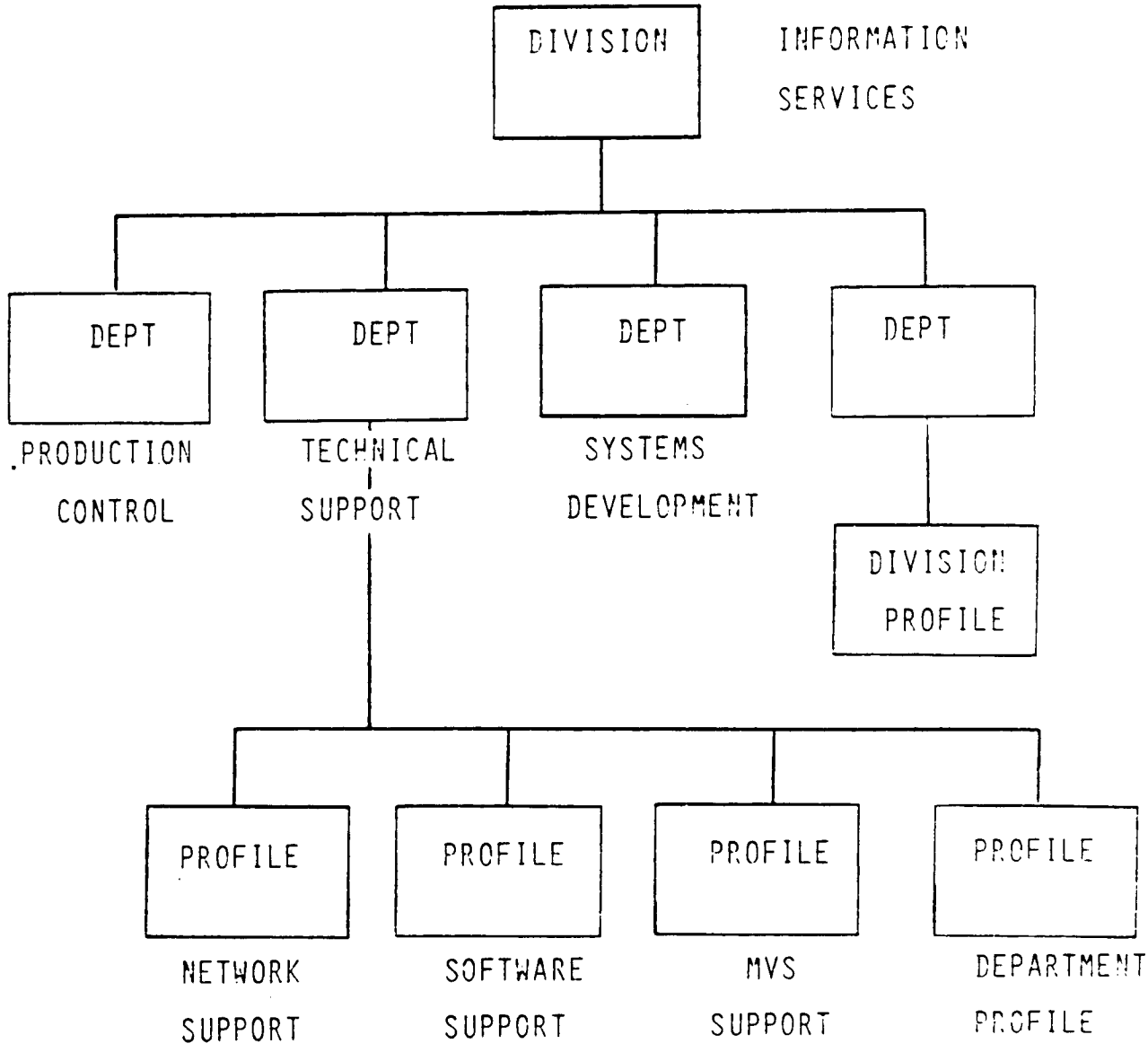
- Size of User and Resource Base
- Extent of Inter-User and Inter-Department Sharing of Resources
- Priority for Implementation
- Centralized or Decentralized Administration

TOP SECRET™

AUDITING TOP SECRET

SECURITY FILE REVIEW

Reviewing the Functional Levels



AUDITING TOP SECRET

SECURITY FILE REVIEW

Reviewing the Functional Levels

Implementation priority can affect definition of levels - for example:

- A logical division structure is implemented in segments
- Users to be implemented later are part of an existing division or department structure
- Resources with top priority for protection are accessed by only a few users in a logical division or department

AUDITING TOP SECRET

SECURITY FILE REVIEW

Reviewing the Functional Levels

TSSCHART

- Provides Graphic Representation of Database Structure
- Displays Resource Ownership Information
- Controlled by Administrator's Scope and MISC1 CHART Authority

CONTROL KEYWORDS

CHART

RESOURCE

PAGE

DIV (or XDIV)

DEPT (or XDEPT)

PROF (or XPROF)

USER (or XUSER)

AUDITING TOP SECRET

SECURITY FILE REVIEW

Reviewing the Functional Levels

TSSCHART

CHART Parameters

DIV **DEPT** **PROF** **USER**	Specifies ACIDs or groups of ACIDs to be included in chart
XDIV **XDEPT** **XPROF** **XUSER**	Specifies ACIDs or groups of ACIDs to be excluded from chart

Parameters

ALL
NONE
EJECT
DIV
acid list

AUDITING TOP SECRET

SECURITY FILE REVIEW

Correcting Design Errors

- Creating New Divisions
- Creating New Departments
- Moving Departments between Divisions
- Moving Users between Departments
- Consolidating, splitting and moving profiles
- Tightening Authorizations
- Changing Ownership
- Moving Ownership
- Moving Security Administrators
- Renaming ACIDs

AUDITING TOP SECRET

SECURITY FILE REVIEW

Correcting Design Errors

- Users may be moved from one department to another with no effect on their access characteristics

- They may be active when moved

  TSS MOVE(USER42) DEPARTMENT(TECHSUP)

- USER42 remains a TYPE(USER)

AUDITING TOP SECRET

SECURITY FILE REVIEW

Correcting Design Errors

- Profiles may be moved from one Department to another without detaching from Users who remain behind

TSS MOVE(BUDPRO) DEPT(APDEPT)

AUDITING TOP SECRET

SECURITY FILE REVIEW

Correcting Design Errors

Tighten Up Authorizations

Use TSSAUDIT to review the "User to Attribute" cross-reference

CONSOLE	Change Control Options
DUFXTR	Read Installation Data
DUFUPD	Update Installation Data
NOADSP	No automatic data set protection
NODSNCHK	Access/Use any data set
NOLCFCHK	Command/Transaction Bypass
NORESCHK	Use any resource
NOSUBCHK	Submit job with any ACID
NOVOLCHK	Access/Use any volume

AUDITING TOP SECRET

SECURITY FILE REVIEW

Correcting Design Errors

Tighten Up Authorizations

WHOHAS DSN(**)

WHOHAS VOL(*ALL*(G))

WHOHAS VOL(volume) ACC(ALL)

WHOHAS RES(*ALL*)

AUDITING TOP SECRET

SECURITY FILE REVIEW

Correcting Design Errors

Changing Ownership

- Must revoke all permissions

  TSS REVOKE(USER21) DSN(SAS.LOAD) etc.

- Must remove ownership

  TSS REMOVE(SOFSUP) DSN(SAS)

- Must define new resource

  TSS ADDTO(SOFSUP) DSN(SAS.)

- Must redo the permissions

  TSS PERMIT(USER21) DSN(SAS.LOAD) etc.

AUDITING TOP SECRET

SECURITY FILE REVIEW

Correcting Design Errors

Moving Security Administrators

- SCAs, VCAs, and DCAs can be moved between Departments and Divisions
- An ACID moved without a Department or Division designation becomes an SCA

TSS MOVE(USER36)

USER36 is now an SCA

- An ACID moved to a Division becomes a VCA

TSS MOVE(USER21) DIV(FINDIV)

USER21 is now a VCA

- An SCA or VCA moved to a Department becomes a DCA (A User ACID remains a User ACID)

TSS MOVE(SCADM) DEPT(TECHSUP)

SCADM is now a DCA

AUDITING TOP SECRET

CONTROL OPTIONS

Verify that Control Options

are being used as required

by the organization

AUDITING TOP SECRET

CONTROL OPTIONS

OPTION	*DESCRIPTION*
DATE	Sets format for date display. *DEFAULT*: (MM/DD/YY)
DEBUG	Controls the error debug feature. *DEFAULT*: (OFF)
DEFPROT	Controls default resource protection. *DEFAULT*: (NO)
DEFDSNPROT	Controls default data set protection. *DEFAULT*: (NO)
DIAGTRAP	Controls diagnostic traps. *DEFAULT*: (OFF)
DOWN	Selects down options for TSS. *DEFAULT*: (SB, TW, BW, OW)
DRC	Alters DRC table. *DEFAULT*: N/A

AUDITING TOP SECRET

CONTROL OPTIONS

OPTION	*DESCRIPTION*
JES	Identifies JES subsystem. *DEFAULT*: NOVERIFY
JOBACID	Locates ACID on batch job card. *DEFAULT*: (A,1)
LOG	Controls recording of security events. *DEFAULT*: (MSG,SMF,INIT,SEC9)
MODE	Sets global security mode. *DEFAULT*: (FAIL)
MSG	Alters TSS message table. *DEFAULT*: N/A
MSUSPEND	Allows automatic suspension of MSCA. *DEFAULT*: NO
NEWPW	Sets specifications for new passwords. *DEFAULT*: (MIN=4,NR,ID,RS,MINDAYS=1,WARN=3)
PRODUCTS	Indicates special products or options are active. *DEFAULT*: (TSO/E)

AUDITING TOP SECRET

CONTROL OPTIONS

OPTION	*DESCRIPTION*
STAT	Displays statistical counters. *DEFAULT*: N/A
STATUS	Shows settings of various controls options. *DEFAULT*: N/A
SUBACID	Controls derivation of batch job ACIDS. *DEFAULT*: (U,7)
SUSPEND	Suspends an ACID. *DEFAULT*: N/A
SWAP	Determines if TSS address space is swappable. *DEFAULT*: (YES)
SYNCH	Synchronizes resource authorization tables. *DEFAULT*: N/A
SYSOUT	Spins off TSS activity log. *DEFAULT*: N/A

AUDITING TOP SECRET

CONTROL OPTIONS

OPTION	*DESCRIPTION*
FACILITY	Selects options per facility.

SUBOPTION	*DESCRIPTION*
NAME	Changes the NAME of a facility
DEFACID	Default ACID for facility
AUDIT/NOAUDIT	Auditing of all activity
RNDPW	Allows random PASSWORD generation

AUDITING TOP SECRET

CONTROL OPTIONS

Five Ways to Specify

Parameter file at TOP SECRET start-up

Parm field of TOP SECRET started task JCL
// EXEC PGM = TSSMNGR,PARM = 'options'

MVS START command
S TSS,'options'

MVS MODIFY command
F TSS,'options'

TOP SECRET MODIFY command
TSS MODIFY(options)

AUDITING TOP SECRET

CONTROL OPTIONS

HIERARCHY

Parameter file overridden by

EXEC parameter overridden by

START parameter overridden by

MVS MODIFY command

or

TSS MODIFY command

Verify that Control Options are not incorrectly overridden

AUDITING TOP SECRET

AUDITING TOOLS

LIST Function

Displays information about ACIDs,
the ALL, STC and AUDIT records

Examples

- TSS LIST(ACIDS) DEPT(APDEPT) DATA(ALL)
- TSS LIST(APPROF) DATA(ALL)
- TSS LIST(USER13) DATA(ALL)
- TSS LIST(AUDIT)
- TSS LIST(ALL)

Will be displayed on-line

AUDITING TOP SECRET

AUDITING TOOLS

WHOOWNS Function

Determines if a resource is defined to **TOP SECRET**

Identifies who the owner is

Example

TSS WHOOWNS DSN(AP.)

TSS WHOO VOL(*)

AUDITING TOP SECRET

AUDITING TOOLS

SYSOUT Control Option

Causes the Activity Log (which records console activity and unexpected events) to be spun off and a new one dynamically allocated

No operands

Only valid from MODIFY command

AUDITING TOP SECRET

AUDITING TOOLS

Verifying DATASET Protection

- Security interface call dependent on security bit if you are not using DFP/370 1.1, DFP/XA 1.2, or VSAM in ICF catalog
- MVS sets bit for defined users

TSSPROT

Utility to set security bit by:

Volume
Catalog
Dataset or dataset prefix
Dataset type
ALL

SIM(ulate) option for auditing purposes

DEFDSNPROT(NO) in IMPL mode

AUDITING TOP SECRET

AUDITING TOOLS

TSSTRACK

On-line Tracking

Audit/Tracking file

Wrap-around file

Real time

For auditors and administrators

AUDITING TOP SECRET

AUDITING TOOLS

TSSSIM

Ability to Test or Audit Access Definitions

Online through TSO or ROSCOE

Simulate User Signon and Resource Access

Controlled by Administrator's Scope and MISC1 SIM Authority

AUDITING TOP SECRET

THE AUDIT PROGRAM

Pre-Audit

Using the TSS list function of TOP SECRET, determine that the auditor's security record is defined with sufficient authority to allow the audit to be carried out. This will include the proper administrator's level (SCA) as well as appropriate resource, ACID and data authority and CONSOLE attribute.

Review the corporate security policy.

Obtain a list of all security administrators and a detail list of the scope of their authority.

AUDITING TOP SECRET

THE AUDIT PROGRAM

- Obtain a list of all users and profiles

  TSS LIST(ACIDS) DATA(ALL)

- Obtain a list of ACIDs not in FAIL mode

  TSS WHOHAS MODE(D)
  TSS WHOHAS MODE(W)
  TSS WHOHAS MODE(I)

- Determine if all sensitive programs and libraries are protected

  TSS WHOHAS PGM(IE)
  TSS WHOHAS PGM(*)
  TSS WHOHAS PGM(TSS)
  TSS WHOHAS DSN(TOP SECRET DATA SETS)
  TSS WHOHAS DSN(SYS)
  TSS WHOHAS VOL(*ALL*)
  TSS WHOHAS RES(*ALL*)

AUDITING TOP SECRET

THE AUDIT PROGRAM

- Review the default ACIDs to ensure that they are not too powerful
- Determine if there are any unprotected data sets using TSSPROT P SIM for NON-ALWAYSCALL environments
- Examine all user written SVCs
- Determine if operator accountability exists over all STCs.
- Determine the method of tape protection in operation.
- Review logging and reporting of violations to ensure constant monitoring of security related activity.
- Determine if any customized controls are in use.
- Additional installation dependent considerations.
- Consider third party security review
  - to satisfy audit review requirements
  - to provide outside perspective