

IBM AS400 Security Procedures

Table of Contents

	<u>Page</u>
A. Purpose and Scope	1
B. Preparatory Steps	2
C. General information	3
D. Standards	5
E. Documentation	6
F. Physical Security	8
G. Backup Procedures	9
H. Disaster Recovery	11
I. Implementation & Change Control	12
J. Operations/Processing (Job Scheduling, Tape Library Management, Output Handling)	16
K. System Security - General	19
System Security Values	20
User Group Profiles	27
Libraries	34
Objects	35
System Utilities	36
System Commands	37
System Logs	39
L. Physical Inventory	41
M. Systems Performance	42
N. Preventative Maintenance	43

Auditor(s) Assigned _____

Audit Date

Audit Objectives and Procedures

Workpaper
Ref. By

A. Purpose And Scope

This program is designed to enable the auditor to examine and test the effectiveness of controls and procedures at data centers using IBM System/34, 36, 38 and AS/400 computers.

Included in the audit program are suggested audit steps that are designed to obtain evidence that key control procedures are operating effectively.

The audit approach includes: background information, standards, documentation, implementation/change controls, backup procedures (including those financial files required by law - such as general ledger, payroll, receivables, sales, cost of sales and any master file/tables required to complete the financial information - such as chart of accounts, cost, price masters), disaster recovery, computer operations and logical access security.

This guide should be read through in its entirety before an audit is commenced in order to gain a thorough understanding of the audit approach.

The Appendix contains added information on classifying data and background information on the various machines that are covered in this audit program.

Auditor(s) Assigned _____

Audit Date

Audit Objectives and Procedures

Workpaper
Ref. By

B. Preparatory Steps

1. Review existing corporate computer policies and guidelines and evaluate their impact on the planned audit scope.
2. Review the workpapers and response to the prior audit report.
3. Obtain and review the current organizational chart for the relevant data center location.
4. Review the letter of recommendations issued by the external audit firm when evaluating the audit scope.
5. Document interviews and meetings with key audited personnel.

Auditor(s) Assigned _____

Audit Date

Audit Objectives and Procedures

Workpaper
Ref. By

C. General Information

1. Document the type of data processing equipment, ownership, capacity and future expansion plans.
2. Document the type of major software applications currently in production, who owns them and future development plans.
3. Review insurance coverage for hardware, software, facility, etc.
4. Determine if outside service bureaus or contract programmers are employed and list all applications processed or programmed.
5. Review procedures for obtaining these services.
6. Determine if any additional controls are provided to ensure all work performed by contract programmers is reviewed and approved.
7. Evaluate the contract with the service bureau(s) or outside programmer(s) for ownership of data, confidentiality statements, etc.
8. Review relevant job descriptions to ensure adequately defined duties, lines of responsibilities, etc.
9. Verify that procedures are in place for management review of the daily history log of computer processing activity and program changes.
10. Review EDP staffing policies relating to absenteeism, training, transfers and employee terminations.
11. Verify that an EDP steering committee has been established and review objectives, members and frequency of meetings.

GENERAL

C/PROG

Page 1 of 2

Auditor(s) Assigned _____

Audit Date

Audit Objectives and Procedures

Workpaper
Ref. By

C. General Information (continued)

12. Review minutes of steering committee and management policy meetings to identify EDP activities and progress on these projects.
13. Review management reports for evidence of management review and coordination of EDP activities.
14. Review EDP budget versus actual cost reports to ascertain whether data center resources are properly monitored.
15. Review procedures that are in place for the evaluation and approval of computer equipment and software packages prior to acquisition and implementation.

Auditor(s) Assigned _____

Audit Date

Audit Objectives and Procedures

Workpaper
Ref. By

D. Standards

1. Document who is responsible for creating and updating policies and procedures for the *EDP Standards Manual*.
2. Verify that the *EDP Standards Manual* contains an adequate explanation of the policies for EDP procedures.
3. Verify that the *EDP Standards Manual* contains:
 - a. Detailed procedures regarding the preparation of documentation for application systems.
 - b. Conventions to be used in the development of programs.
 - c. Standard forms, illustrations and their use.
 - d. Security requirements for both the applications and the computer itself.
 - e. Operational standards for the EDP department and surrounding areas.

STANDARDS

D/PROG

Page 1 of 1

Auditor(s) Assigned _____

Audit Date

Audit Objectives and Procedures

Workpaper
Ref. By

E. Documentation

1. Document who is responsible for creating, maintaining and distributing application documentation.
2. Verify that there is a formal, signed approval of each element of documentation at an appropriate management level.
3. Verify that the documentation is maintained in secure on-site and off-site storage facilities.
4. Verify that all major applications processed on the computer system have appropriate levels of corresponding documentation.
5. Review selected application documentation against corresponding software programs to ensure that documentation is accurate, complete and current.
6. For each application, verify that corresponding System Documentation contains an overview that includes:
 - a. The general nature and purpose of the system.
 - b. The functional requirements of the system.
 - c. The logical flow of the system or flow charts.
7. For each application, verify that corresponding Program Documentation contains:
 - a. Descriptions of each program and system interfaces.
 - b. Input and output description.
 - c. Description of program logic and flow.
 - d. Record layouts and file descriptions.

DOCUMENTATION

E/PROG

Page 1 of 2

Auditor(s) Assigned _____

Audit Date

Audit Objectives and Procedures

Workpaper
Ref. By

E. Documentation (continued)

8. For each application, verify that corresponding User Manuals are developed, which describe the operations performed and contain:
 - a. Application description.
 - b. Procedural requirements.
 - c. Sample reports and input screens.
 - d. Source documents required.
 - e. Description of screens, edits, etc.
9. Verify that current computer Operating Instructions contain:
 - a. Set-up instructions.
 - b. Operating system requirements.
 - c. Restart and recovery procedures.
 - d. Emergency procedures.
 - e. Listing of program messages, responses, etc.

Auditor(s) Assigned _____

Audit Date

Audit Objectives and Procedures

Workpaper
Ref. By

F. Physical Security

1. Verify that the building is protected by an automatic fire extinguishing system, appropriate to the environment.
2. Verify that the computer room is equipped with appropriate classes and sufficient number of clearly visible fire extinguishers.
3. Determine whether there are sufficient fire and smoke alarms appropriate to the environment.
4. Ensure that all exits and evacuation routes are clearly marked.
5. Ensure that smoking is prohibited in the computer room.
6. Document the provisions made to detect and report fires on a timely basis.
7. Review provisions for preventing water damage to the equipment.
8. Verify that the computer room is accessible to only authorized personnel.
9. Document computer room layout and location of all major hardware components.
10. Document the procedures in place for notifying security when an employee is no longer allowed access to the building.
11. Review established emergency procedures for the data center, which should include at a minimum:
 - a. Turning off data processing equipment.
 - b. Turning off electrical power to the computer room.
 - c. Evacuation of personnel.
12. Ensure that all emergency procedures have been posted or distributed to all personnel.
13. Review procedures for maintenance of appropriate temperature levels, periodic maintenance/inspection of equipment.

Auditor(s) Assigned _____

Audit Date

Audit Objectives and Procedures

Workpaper
Ref. By

G. Backup Procedures

1. Obtain a copy of the formal backup schedule for creating copies of production program and data files.
2. Describe how the company determines which files are to be saved and how often. Also, describe the number of generations of files kept.
3. Describe backup procedure for the following:
 - a. Production programs and procedures for both source and object code.
 - b. Systems documentation.
 - c. Operating system or other software.
4. Verify that the frequency of backups is appropriate for the environment.
5. Describe the secured area designated for on-site storage of backup media.
6. Document who has authorized access to on-site backup area.
7. Describe the off-site storage facility and the contents.
8. Ensure that access to the off-site storage facility is restricted to only authorized personnel. List their names and functions.
9. Review the arrangement for a computer backup site, for appropriate telecommunications facilities, operating systems, etc.

Auditor(s) Assigned _____

Audit Date

Audit Objectives and Procedures

Workpaper
Ref. By

Testing (Backup Procedures)

1. Select a critical application to be tested based on the scope of the review.
2. Obtain a current backup schedule for the programs and data files selected.
3. Identify critical files used with this application on the Volume Table Of Contents (VTOC) listing.
4. Trace files on the VTOC to the backup schedule.
5. Locate backup files in on-site storage.
6. Verify that dates on backup media agree with backup schedule.
7. Locate backup files on off-site storage.
8. Verify that dates on backup media agree with backup schedule.
9. Describe the contents of off-site storage facility.

Auditor(s) Assigned _____

Audit Date

Audit Objectives and Procedures

Workpaper
Ref. By

H. Disaster Recovery

1. Obtain a formal copy of the company's current disaster recovery plan.
2. Obtain the company's list of employees and vendors to be contacted in the event of an emergency.
3. Describe the method and extent of user involvement in the creation and maintenance of the plan.
4. Ensure that all critical systems have been identified.
5. Review interim manual procedures, prepared for users to continue processing critical transactions, for completeness.
6. Review the documented results from the test of the disaster recovery plan.
7. Review the disaster recovery plan for completeness. Some items to be considered in the review are:
 - a. Possible alternate processing sites.
 - b. Alternate sites tested at least annually.
 - c. Agreement exist for the use of the alternate sites.
 - d. Availability of peripheral equipment.
 - e. Defining critical systems to be processed.
 - f. Ability to process without key personnel.
 - g. Ability to adapt plan to lesser disasters.

DISASTER RECOVERY

H/PROG

Page 1 of 1

Auditor(s) Assigned _____

Audit Date

Audit Objectives and Procedures

Workpaper
Ref. By

I. Implementation/Change Controls

1. Verify that a formal method of project control has been established which covers all phases for the development of new/modified systems.
2. Document the method and reports used to control and prioritize projects.
3. Review the justification proposal created for all new systems, or major enhancements to existing systems, which may include:
 - a. Scope and purpose of the system
 - b. User requirements.
 - c. Cost analysis.
 - d. Time estimates.
4. Document the approval process to ensure that a steering committee or top management is involved.
5. Ensure that a detailed plan has been prepared and documented which should include:
 - a. The assignment of programmers.
 - b. Target dates for completion.
 - c. Adherence to programming standards.
 - d. Required approval points.
 - e. Completion of a programming checklist.
6. Ensure the programming phase is properly supervised by EDP management.

CHANGE CONTROL

I/PROG Page 1 of 3

Auditor(s) Assigned _____

Audit Date

Audit Objectives and Procedures

Workpaper
Ref. By

I. Implementation/Change Controls (continued)

7. Verify that programmers perform all development work only in test libraries and using test data.
8. Document testing procedures established for all new/modified systems.
9. Ensure that users participate in the creation of test.
10. Verify that test results are reviewed by both EDP and User management to provide compliance with specifications.
12. Review the plan for converting new/modified systems from development to production. Does it include at a minimum:
 - a. The training of users.
 - b. Completion of documentation.
 - c. Defining user access requirements.
13. Document the process used to transfer completed programs from test to production libraries.
14. Verify that programs are recompiled after modifications, prior to being placed into production.
15. Verify that all program changes are supported by appropriate authorization.
16. Ensure that a designated official regularly reviews changes not yet implemented.

CHANGE CONTROL

I/PROG Page 2 of 3

Auditor(s) Assigned _____

Audit Date

Audit Objectives and Procedures

Workpaper
Ref. By

I. Implementation/Change Controls (continued)

17. Verify that procedures are in place for saving current versions of programs to diskette/tape prior to substituting the new programs to allow for restoration of the older version in case of program problems.
18. Review procedures in effect to ensure that changes are correctly made and approved, when immediate modifications have to be made to production programs, bypassing normal procedures.
19. Examine evidence for documentation being created or updated, including:
 - a. Operator instructions.
 - b. Data entry instructions.
 - c. User manuals.
 - d. System Documentation.
20. Review evidence of final approval before project is transferred to projection library.
21. Review evidence that old versions of programs are saved before making final changes.
22. Describe how user access requirements are defined, how passwords are assigned and who are authorized to perform these activities.

Auditor(s) Assigned _____

Audit Date

Audit Objectives and Procedures

Workpaper
Ref. By

Testing (Implementation/Change Controls)

Select a representative number of completed program changes or new programs and trace from the initial request to the completion phase, performing or reviewing the following steps:

1. Ensure that user management has evidenced their approval on the initial project request form.
2. Describe the method of prioritizing requests submitted to steering committee or management for major projects.
3. Review log or method used to control all requests to ensure they are being followed up.
4. Determine if cost for purchase versus in-house development was considered.
5. Document method of assigning programmers to the project.
6. Review procedures for approval and progress reporting.
7. Examine project progress reports for evidence that systems development is controlled in accordance with established procedures.
8. Detail method used to create test data.
9. Ensure that EDP and user management evidence their review and approval of test results.
10. Review evidence of programmer having completed all necessary steps:
 - a. File specifications.
 - b. Program specifications.
 - c. Files created.
 - d. Test results filed.

CHANGE CONTROL

I/TEST

Page 1 of 1

Auditor(s) Assigned _____

Audit Date

Audit Objectives and Procedures

Workpaper
Ref. By

J. Operations/Processing

1. Obtain a copy of the EDP department work schedules for computer processing to ensure:
 - a. There is adequate staffing for each area of work.
 - b. All tasks are accomplished in a timely manner to meet user requirements.
2. Ensure schedules are periodically reviewed to determine if they are current.
3. Review the computer activity log, which is maintained for all work performed and any errors that occur, and compare it to the workload schedules to determine if schedules are satisfactorily met.
4. Describe how frequently the computer activity utilization reports are reviewed.
5. Review the operator's manual, which should include job control procedures, operating instructions and computer facility maintenance requirements.
6. Document the procedures in place for the periodic review and update of the operator's manual.
7. Describe the times the computer is operational and the various shifts that are maintained.
8. Ensure adequate cross training of EDP personnel has occurred for continued functioning of the computer if the operator is absent.
9. Determine if a concentration of duties exists and if compensating controls are in place.

OPERATIONS/PROCESSING

J/PROG

Page 1 of 3

Auditor(s) Assigned _____

Audit Date

Audit Objectives and Procedures

Workpaper
Ref. By

J. Operations/Processing (continued)

10. Review procedures in place which would allow management to detect if operators process unauthorized jobs.
11. Review procedures to control access to and usage of production files stored on diskette or tape.
12. Review procedures for the proper handling of diskettes or tapes, which include:
 - a. External labeling requirements.
 - b. Internal labeling requirements.
 - c. Provisions to ensure only the correct diskettes or tapes are used.
13. Describe the transmittal form used to control the movement of each batch of source documents or input forms between the users and data entry.
14. Ensure that batches are identified by a serial number or sequence number to provide subsequent accountability and for reference purposes.
15. Review completed batches for specially marked indicators to prevent duplication or omissions.
16. Obtain a copy of the log maintained in the data entry area to record the flow of batches. Is a similar log maintained in user departments.
17. Review procedures for requirement of data entry personnel to contact users if there are any errors in batches prior to input.
18. Describe the method of storing the source documents while they are in the custody of the EDP department.

OPERATIONS/PROCESSING

J/PROG

Page 2 of 3

Auditor(s) Assigned _____

Audit Date

Audit Objectives and Procedures

Workpaper
Ref. By

J. Operations/Processing (continued)

19. Obtain a copy of the current output distribution list. **What about output ques? Are they separated for confidential reports (payroll, accts payable, etc.)?**
20. Review output distribution list for accuracy, completeness, etc.
21. Document flow of output, to ensure proper safeguards are placed on the output, until it arrives in the user departments.
22. Review procedures for output, which should include:
 - a. Review of all output for completeness.
 - b. All errors are recognized and reported.
 - c. Batch totals match output totals.
 - d. Confidential outputs handled properly.
23. Review the tape inventory list.
 - a. Are scratch tapes all accounted for (in scratch bin and missing from tape rack).
 - b. Are other empty slots accounted for.
24. If the tape inventory is separated by machine:
 - a. are the tapes physically segregated?
 - b. are the tapes identified in some way so as to distinguish one set of tapes from the other (color coordinated - as an example)?
 - c. is the serial number sequence unique?

OPERATIONS/PROCESSING

J/PROG

Page 3 of 3

Auditor(s) Assigned _____

Audit Date

Audit Objectives and Procedures

Workpaper
Ref. By

K. SYSTEM ACCESS CONTROLS

Objective: To ensure that system security options are appropriately set to provide an adequate level of logical security.

Procedures:

K.1 System Access Security - General

- K.1.1 Ensure that all security files are backed-up to diskette/tape every time they are changed.
- K.1.2 Document who has access to the system console.
- K.1.3 Document applications that cannot be secured using built-in system security and ensure that the following controls are programmed into the application:
 - 1. edits on data fields.
 - 2. secondary passwords.
 - 3. exception reports.
 - 4. audit trails.
- K.1.4 Ensure that EDP duties are separated from user department duties.
- K.1.5 Ensure that the responsibility of controlling diskettes/tapes is separated from that of programming or processing transactions.
- K.1.6 Ensure that the responsibility of monitoring computer activity is separate from that of programming and operating.
- K.1.7 Review cross training procedures to ensure there is no segregation of duties problem.
- K.1.8 Determine if procedures have been developed for reporting and following-up on security violations.
- K.1.9 Determine the required length of passwords. [Recommend 6 to 8]
- K.1.11 Review the procedure in establishing the initial user-id. [How is the user-id established, how is the user informed, is the password set at expired, etc.]

Auditor(s) Assigned _____

Audit Date

Audit Objectives and Procedures

Workpaper
Ref. By

K.2 System Security Values - Cont'd

K.2.1.1 Determine who is/are assigned the QSECOFR profile.

All system inquiries in this section must be made with the QSECOFR profile as any others won't have enough privilege. The person holding the QSECOFR profile is typically the master security officer or someone of high management level.

K.2.1.2 Review other duties performed by the Master Security Officer (MSO) to ensure they do not conflict with the responsibilities required by the MSO position (e.g. if the MSO is a programmer).

K.2.2 System values are defined by the client. Obtain the system values report which lists all system values together with a brief description of each value by entering the following command:

WRKSYSVAL

The system values can also be displayed one by one on the terminal by using this command:

DSPSYSVAL SYSVAL (system value)

To print one by one use the command:

WRKSYSVAL *SEC OUTPUT(*PRINT)

System values are defined by the client according to their specific and unique security requirements. Security could be compromised if options are changed or inappropriate.

All possible options of each system value are listed and explained in this audit program as a guide. IBM default values are underscored.

Auditor(s) Assigned _____

Audit Date

Audit Objectives and Procedures

Workpaper
Ref. By

K.2 System Security Values - Cont'd

K.2.2.1 Determine the system security level:

QSECURITY

10: No user authentication, no resource protection.

20: User authentication through password security only, no resource protection.

30: User authentication and default resource protection.

40: Similar to level 30 but controls privileged instructions and the machine interface.

E&Y recommended value: 30.

Level 40 should be considered for clients with high inherent risk. It prevents direct access to objects, data of other jobs and internal system programs.

K.2.2.2 Determine the maximum number of sign-on attempts allowed:

QMAXSIGN

NOMAX: the system allows an unlimited number of sign-on attempts.

15: a user can try to sign on a maximum of 15 times.

After the specified maximum number of invalid sign-on attempts is reached, the terminal is varied (forced) off and a message is logged.

E&Y recommended value: maximum of 3.

Auditor(s) Assigned _____

Audit Date

Audit Objectives and Procedures

Workpaper
Ref. By

K.2 System Security Values - Cont'd

K.2.2.3 Determine action taken by system when QMAXSIGN is exceeded:

QMAXSGNACN

- 1: disable terminal.
- 2: disable user profile.
- 3: disable terminal and user profile.

E&Y recommended value: 3.

K.2.2.4 Determine the user-selected options related to password security:

∃ QPWDEXPITV - password expiration interval

*NOMAX: unlimited number of days.

1-366: valid range of days.

E&Y recommended value: 30-90 days.

∃ QPWDRQDDIF - duplicate password control.

0: can be identical as the previous 32 passwords.

1: must be different from the previous 32 passwords.

E&Y recommended value: 1.

∃ QPWDMINLEN - minimum password length

1: minimum of 1 character.

1 - 10: valid range of number of characters.

E&Y recommended value: 6 or more.

Auditor(s) Assigned _____

Audit Date

Audit Objectives and Procedures

Workpaper
Ref. By

K.2 System Security Values - Cont'd

∃ QPWDMAXLEN - maximum password length.

10: Maximum of 10 characters.

1 - 10: Valid range of number of characters.

E&Y recommended value: 7-8 if connecting to systems other than AS/400 or S/38.

∃ QPVDVLDPGM - password validation program.

*NONE: no password validation program is used.

Review specified program(password exit routine) used, if any, and ensure that it does not allow user to bypass password security and does not contain hard-coded passwords.

K.2.2.5 Determine if users with all object (*ALLOBJ) or service (*SERVICE) special authorities may sign on to only work stations they have specific authority to access.

QLMTSECOFR - limit security officer device access.

0: allows all users with *ALLOBJ authority to sign on to any display station, and users with *SERVICE can sign on to any display station with public authority of *CHANGE.

1: not allow users with *ALLOBJ or *SERVICE authorities to sign on any work stations unless they have specific authority to access.

E&Y recommended value: 1.

Auditor(s) Assigned _____

Audit Date

Audit Objectives and Procedures

Workpaper
Ref. By

K.2 System Security Values -Cont'd

K.2.2.6 Determine the appropriateness of time-out system value:

QINACTITV - inactive job time-out.

*NONE: no time out.

5 - 300: valid range for maximum minutes before time-out.

E&Y recommended value: 15.

Terminals left unattended for an extended period of time may be used by unauthorized persons to perform functions that are available under that session, possibly affecting production data and processing. In addition, unauthorized users of unattended terminals may remain unidentifiable.

*Authorized users can re-key their user-ids and passwords to continue from the screen left off in the previous session. This is possible when we set the disconnect job (*DSCJOB) value to disconnect any interactive, secondary or group jobs. Alternatively, *ENDJOB can be used. However, this will end any job, secondary or group.*

K.2.2.7 Determine if concurrent device sessions are limited:

QLMTDEVSSN - limit device sessions.

0: does not limit the use of a user-id to one work station at a time.

1: limits the use of a user-id to one work station at a time.

E&Y recommended value: 1.

K.2 System Security Values -Cont'd

K.2.2.8 Determine if sign-on information is displayed on screen.

QDSPSGNINF - sign-on display information control.

0: no sign-on information is displayed upon sign-on.

1: users are shown:

☐ date and time of last sign-on.

☐ invalid sign-on attempts since last sign-on.

☐ when applicable, a warning that the password is due to expire in seven days or less.

This information can alert users to unauthorized attempts to use their profiles to access the system.

The sign-on screen should show a restricted access message such as "For Authorized Users Only. Unauthorized Use Is Prohibited." It should also not show the company, system, and application names.

E&Y recommended value: 1.

K.2.3 Changing the Automatic Configuration of Virtual Devices Value

The QAUTOVRT values controls the creation of virtual device descriptions on a remote system when users pass-through to that system.

The system value QAUTOVRT specifies if pass-through virtual devices (as opposed to the workstation function virtual device) are automatically configured. This value can only be changed by the security officer or someone with all object (*ALLOBJ) and security administrator (*SECADM) special authority.

The value of QAUTOVRT should be set as low as possible. In most cases the value of 0 (zero) or 1 (one) is recommended. However in some locations where the passthrough activity is higher, it should be set as low as possible to minimize logon opportunities of unauthorized users.

K.2 System Security Values -Cont'd**K.2.4 Changing the Remote Sign-on Value**

The QRMTSIGN value controls if users can bypass the sign-on display on the remote system when using the display station pass-through function or the workstation function of PC support.

The possible values are:

- ! FRCSIGNON: All pass-through sessions that begin on the system must go through the normal sign-on procedure.
- ! SAMEPRF: Pass-through sessions without going through the sign-on procedure are allowed only for users whose user profile name on the remote system is the same as the user profile name on the local system
- ! VERIFY: Pass-through sessions without going through the sign-on procedure are allowed for all pass-through requests and no checking of passwords is done if the QSECURITY value is 10. Must sign-on if QSECURITY value is 30.
- ! REJECT: Pass-through sessions are not allowed to start on the remote system.

K.2.5 Create Authority Parameter in System Value

Review the QCRTAUT parameter on the system values report, and ensure that it has been changed from the default value of *CHANGE, to a setting of *USE or less.

Determine that the production database and production source code files are maintained in a library with appropriately restricted access. Or, use the Display Object Authority command and determine whether the Public Authority Access (PUBAUT) access parameter for each significant individual production database and production source code file is *EXCLUDE and individual access allowed are appropriate.

K.3 User/Group Profiles

Objective: To ensure that user or group profiles are authorized and defined appropriately to maintain adequate segregation of duties.

Procedures:

K.3.1 Obtain all user and group profiles by entering the command:

DSPAUTUSR SEQ (*GRPPRF)

K.3.2 Inspect each significant group profile to ensure that it is authorized by appropriate management personnel and covers a common group of users with a common function. Ensure that only one group profile is assigned to a user.

K.3.3 Inspect selected user profiles to ensure that they are authorized by appropriate management personnel and that their settings are compatible with their work functions.

K.3.4 A number of IBM user profiles are pre-defined when the system is shipped. The passwords to these user profiles are identical to the user profile names, except for DST's which is "QSECOFR". Determine that the client has changed the passwords for these user profiles:

<u>User Profile</u>	<u>Description</u>
QSECOFR	security officer
QSRV	full service functions
QSRVBAS	basic service functions
QSYSOPR	system operator
QPGMR	programmer
QUSER	work station user
DST	Dedicated Service Tools

Note: QSRVBAS and QSRV passwords should be changed after every maintenance trip by authorized IBM personnel. Vendor-supplied passwords for any commercial software products should also be changed.

Auditor(s) Assigned _____

Audit Date

Audit Objectives and Procedures

Workpaper
Ref. By

K. 3 User/Group Profiles - Cont'd

K.3.4.1 Signing on with IBM-supplied user profiles that are designed to be object owners is not permitted. Use a DSPAUTUSR list to verify that the following IBM-supplied user profiles have a password of *NONE:

QDBSHR	QDFTOWN	QDOC
QTSTROS		
QDSNX	QFNC	QGATE
QLPAUTO	QLPINSTALL	QSNADS
QSPL	QSPLJOB	QSYS

K.3.5 Obtain a listing of user and group profiles using the following command:
To get to magnetic file: Enter [DSPUSRPRF]: press (PF4): Select output file and name the file: have the file transferred to a PC or XCOMM to mainframe where Office Services will copy the file/s to audits cc 0820 G drive.
DSPUSRPRF USRPRF(profile name) TYPE(*BASIC)

For each profile review the following settings:

K.3.5.1 GROUP (Group Profile)

Determine if members of each group are related to a common user function.

K.3.5.2 PWDEXPITV (Password Expiration Interval) *UPGRPF*

*SYSVAL: system default specified in QPWDEXPITV

If a number is specified it means that a specific interval has been set for this user.

K.3.5.3 CURLIB (Current Library) *UPCRLB*

Determine that the specified library is suitable to the user function. Ensure that this library is adequately secured.

K.3 User/Group Profiles - Cont'd**K.3.5.4 LMTCPB (Limited Capability) UPLTCP**

Specifies whether the user can change the initial program, initial menu, current library and attention-key-handling program values.

*NO: user may change all the values in his own user profile with the CHGPRF command.

*PARTIAL: the initial program and current library values cannot be changed. The initial menu value can be changed (using CHGPRF) and commands can be run from the command line of a menu.

*YES: the initial program, initial menu and current library values cannot be changed. Some commands can be run on the command line of a menu.

*E&Y recommended value: *YES for production users.*

K.3.5.5 SPCAUT (Special Authority) UPSPAU

- *ALLOBJ - allows unlimited access to almost every object
- *SECADM - allows administration of user profiles
- *SAVSYS - for saving and restoring the system and data
- *JOBCTL - allows manipulation of work queues and subsystems
- *SERVICE - allows many uncontrolled functions
- *SPLCTL - allows control of spool functions

*USRCLS: - user given special authorities that are appropriate for his class

*NONE - no special authority assigned

Determine if the special authority assigned to each user class is suitable.

*Generally, users and programmers should not have any special authorities. SECADM, QSECOFR, and SYSOPR by default, have *SAVSYS and *JOBCTL special authorities. IBM engineers may have *SERVICE.*

*E&Y recommendation: *PUBLIC must be set to *EXCLUDE.*

K.3 User/Group Profiles - Cont'd

K.3.5.6 INLPGM (Initial Program) *UPINPG*

*NONE: No initial program is used. User is given access to the command level.

The initial program may not provide a way to exit from the program except to sign-off.

If a menu name is specified in the initial menu parameter then that menu is displayed. Ensure that there is no option in the menus/sub-menus to exit and access the command level.

K.3.5.7 INLMENU (Initial Menu) *UPINMN*

*SIGNOFF: the user will be signed off the system once the initial program ends.

Menu security limits a user's capabilities and restricts the user to a predefined secured environment. The initial menu appears after the initial program terminates. Ensure that users are assigned menus and menu options that are suitable for their job functions.

The advantages of menu security are that it is easy to implement and therefore, incurs low security management cost; and provides ease to use interface.

Caveat: Initial menus are mostly user-defined and therefore, may contain loop-holes. The application design is critical to menu security.

E&Y recommendation: Use the limited capability approach where appropriate with library and object security.

K.3.5.8 LMTDEVSSN (Limit Device Sessions) *UPLDVS*

*(SYSVAL): the system value selected determines if the user is limited to one device session.

*NO: does not limit the use of a user-id to one device session.

*YES: limits the use of a user-id to one device session.

*E&Y recommended value: *YES or *SYSVAL and QLMTDEVSSN - Set to Option One(limit number of device sessions to one).*

Auditor(s) Assigned _____

Audit Date

Audit Objectives and Procedures

Workpaper
Ref. By

K.3 User/Group Profiles - Cont'd

K.3.5.9 STATUS (Status of user profile) *UPSTAT*

Specifies whether the user profile is usable or not.

*ENABLED: profile is usable.

*DISABLED: profile is not usable.

*E&Y recommendation: Inactive or dormant user profiles should be set to *DISABLE to prevent unauthorized usage.*

*Note that system profiles such as QSYS, QSECOFR, etc. must be set to *ENABLE.*

K.3.5.10 Obtain a list of user profiles and review for the following:

1. Identify the users permitted access to individual and each group profile.
2. Determine if all users are permitted access based on written authorization by Departmental Management.
3. Confirm that all users are currently employed.

K.3.5.11 Determine whether unauthorized users can process critical functions from their menu(s).

K.3 User/Group Profiles - Cont'd

K.3.6 List all programs which adopt the privileged QSECOFR authority:

DSPPGMADP USRPRF(QSECOFR) [optional AOUTPUT(*PRINT)≡
to print]

Plan for running the above command overnight as it slows down the system.

Adopted authority provides a means to handle situations where programs or commands called by a user may require a higher level of authority than is normally available to that user. It allows a user to adopt the authority of the owner of a program whenever it executes, in addition to the authority of the user. This provides a method to give a user more access to objects, but the user is limited to the program function during execution.

K.3.6.1 Determine if the security officer is aware of such programs and if he/she evaluates any new ones that use the adopted authority.

E&Y recommendation: The security officer should monitor programs that adopt the privileged QSECOFR authority.

K.3.7 Ensure that a security and password policy or guideline has been developed which includes:

1. the secure assignment and distribution of passwords.
2. password selection criteria.
3. change or immediate removal of terminated employee's passwords. (Obtain report on Previous Signon Date)
4. periodic changing of passwords.
5. training users in the necessity of password secrecy and sign-off of workstations when not in use.
6. actions to be taken for attempted security violations.

Auditor(s) Assigned _____

Audit Date

Audit Objectives and Procedures

Workpaper
Ref. By

K.3 User/Group Profiles - Cont'd

K.3.7 Obtain a list of authorized users using the following command.

DSPAUTUSR

This list contains user profile, password last change date and user profile description. By reviewing the password last change dates, determine if passwords are changed within a reasonable interval of time [i.e., within a reasonable QPWDEXPIV value (see Procedure K.3.2.4)].

Auditor(s) Assigned _____

Audit Date

Audit Objectives and Procedures

Workpaper
Ref. By

K.4. Libraries

Objective: To ensure that appropriate access authority is defined at the library level in order to protect production data files and programs from unauthorized access.

Library security establishes security at the library level and it assumes that a nonspecific protection is adequate. To have specific protection over individual objects within a library, object level security is needed. See section 2.4..

Procedures:

K.4.1 Obtain a list of all libraries in the system:

DSPOBJD OBJ(QSYS/*ALL) OBJTYPE(*LIB) OUTPUT(*PRINT)

Determine that the production objects are segregated in separate libraries from the development objects.

K.4.2 Select a sample of significant production libraries. List the contents (objects) of the selected libraries:

DSPLIB (Library Name)

Ensure that only production objects are in production libraries.

K.4.3 List the object authorities for the above significant production libraries:

DSPOBJAUT OBJ(QSYS/library name) OBJTYPE(*LIB)

Determine that only authorized users or groups have access. Development users should have no access to production libraries. Also determine if the owner of the library is appropriate.

K.4.4 Review administration and authorization procedures for granting access to significant libraries.

E&Y recommendation: Library level security is strongly recommended as it provides a relatively easy and effective method of securing objects within libraries. Libraries should be structured in a way that all objects within a library have identical security requirements.

Auditor(s) Assigned _____

Audit Date

Audit Objectives and Procedures

Workpaper
Ref. By

K.5 Objects

Objectives: To ensure that appropriate access authority is defined at the object level in order to protect specific production data files and programs from unauthorized access.

Object security establishes security at the specific object level. It is used when different objects require different protection requirements. The client may choose to protect specific sensitive objects at the object level if their inherent risk is high or if library level protection is not used. It can also be used as an exception to the general authorization rules.

Procedures:

K.5.1 Select a sample of sensitive production objects (data files or source programs) and print their specific object authorities:

DSPOBJAUT OBJ(library/file) OBJTYPE(*FILE) (for files), and

DSPOBJAUT OBJ(library/program) OBJTYPE (*PGM) (for programs).

K.5.2 Ensure that only authorized users or groups may access or use the sensitive objects.

K.5.3 Review administration and authorization procedures for granting access to significant objects.

E&Y recommendation: Since assignment of object authorities to specific objects is tedious, specific object authority should only be defined to handle exceptions; otherwise, the default public authority should be used.

Auditor(s) Assigned _____

Audit Date

Audit Objectives and Procedures

Workpaper
Ref. By

K.6 System Utilities

Objective: To ensure that powerful system utilities are adequately restricted from unauthorized access and use.

The following are powerful system utilities:

SST	System Service Tools
DST	Dedicates Service Tools
DFU	Data File Utility
SEU	Source Entry Utility
SDA	Screen Design Aid
PDM	Programming Development Manager
QUERY	Query Language

Procedures:

K.6.1 Determine who has access to the above utilities:

- ∃ DSPOBJAUT OBJ(QSYS/STRDFU) OBJTYPE (*CMD).
- ∃ DSPOBJAUT OBJ(QSYS/STRSEU) OBJTYPE (*CMD).
- ∃ DSPOBJAUT OBJ(QSYS/STRSDA) OBJTYPE (*CMD).
- ∃ DSPOBJAUT OBJ(QSYS/STRPDM) OBJTYPE (*CMD).
- ∃ DSPOBJAUT OBJ(QSYS/STRQRY) OBJTYPE (*CMD).

Only authorized programmers should have access to these utilities.

*E&Y recommendation: *PUBLIC access should be set to *EXCLUDE, not *USE.*

K.7 System Commands

Objective: To ensure that powerful system commands are adequately restricted from unauthorized use.

The following are powerful system commands:

- * CRTUSRPRF Create User Profile
- * CHGUSRPRF Change User Profile
- * DLTUSRPRF Delete User Profile
- * RSTUSRPRF Restore User Profile
- Ⓜ CHGDSTPWD Change Dedicated Service Tool Password
- RSTAUT Restore Authority
- # STRSST System Service Tools
- ~ CRTAUTHLR Create Authority Holder
- M DLTAUTHLR Delete Authority Holder
- M □ SAVSYS Save the System
- ~ CHGSYSLIBL Change System Library
- CHGSYSVAL Change System Value

- * Restricted to the security administrator (QSECADM) and security officer (QSECOFR) only. PUBLIC access is irrelevant. A user cannot use these commands even if he/she has *ALLOBJ special authority.
- # Restricted to the service engineer (OSRV) only.
- ~ Restricted to the security officer (QSECOFR) only.
- ⓓ You need the DST *security* password to change the DST passwords.
- Restricted to *SAVSYS capability holder.
- M *PUBLIC should be set to *EXCLUDE.

See the sensitive command object authority matrix.

Auditor(s) Assigned _____

Audit Date

Audit Objectives and Procedures

Workpaper
Ref. By

K.7 System Commands - Cont'd

Procedure:

K.7.1 Review the object authority to the above significant security related commands:

DSPOBJAUT OBJ(QSYS/cmd) OBJTYPE(*CMD).

Ensure that only authorized personnel may use these commands.

*E&Y recommendation: Public authority of these commands should be set at *EXCLUDE.*

*Command source object contains the source code for all the CL commands and is used to recompile any one or all commands. Only the security officer and users with the *ALLOBJ special authority may access this object. It is not necessary for a user to have access to this object in order to access the CL commands.*

Auditor(s) Assigned _____

Audit Date

Audit Objectives and Procedures

Workpaper
Ref. By

K.8 System Logs

Objective: To ensure that system access and operational activities are monitored regularly by appropriate personnel.

Procedures:

- K.8.1 Obtain the printed system log, if any, and scrutinize it for evidence of review (e.g., initials, sign-offs) by appropriate personnel, typically the Systems Administrator or the Security Officer.

Note: Typically, the full system log is not printed because it is too voluminous. They normally review the log on-screen.

The following is a general format of the command to display messages recorded in the history log:

*DSPLOG LOG(QHST) PERIOD (start-time start-date) (end-time end-date)
MSGID (message-identifier) OUTPUT(*PRINT){of OUTPUT(*)}*

Most security messages are in the range CPF2201 to CPF2299. The message number CPF2200 should be entered if all messages in the range is required. For example, CPF2234 means incorrect password. CPF2240 means inadequate authority to object.

- K.8.2 Print the "Display Object Authority" list of the QHST object by the following command:

DSPOBJAUT OBJ(QHST) OBJTYPE(*MSGQ) OUTPUT(*LIST).

Determine that only the Security Officer has access to the QHST object and that PUBLIC be set to *EXCLUDE.

K.8 System Logs -Cont'd

K.8.3 If the system log is not used, determine if the auditing journal (QAUDJRN) is generated and reviewed.

The Security Officer can monitor security by gathering audit information about specific security-related events. This can be achieved by performing the following steps:

(1) Create journal receiver:

```
CRTJRNRCV JRNRCV(user-lib/user-name1) AUT(*EXCLUDE)
```

(2) Create journal:

```
CRTJRN JRN(QSYS/QAUDJRN) JRNRCV (user-lib/user-name1)  
AUT(*EXCLUDE)
```

(3) Change system value:

```
CHGSYSVAL QAUDLVL VALUES ('AUTFAIL *SECURITY  
*PGMFAIL ...')
```

The QAUDLVL values control which security-related events are logged to this journal. E&Y recommended QAUDLVL values are as follows:

- ⊘ AUTFAIL - logs all access authorization failures;
- ⊘ SECURITY - logs security-related activities, such as those related to object authority, user profiles, and system values; and
- ⊘ PGMFAIL (security level 40) - creates an authorization failure entry for each object domain, blocked instruction or program validation check failure.

K.8.4 Ensure that there are inquiry letters written by the Security Officer to the users' heads of department when significant access violations are detected by the logging facility. Also review the responses received from the users' heads of department explaining the violations.

K.8.5 Determine if a procedure is in place to provide a report to each user department identifying the respective department's responsible transactions (especially update) and the authorized users for those transactions. The reports should be provided not less than every 6 months. Verify the authorizations.

Auditor(s) Assigned _____

Audit Date

Audit Objectives and Procedures

Workpaper
Ref. By

L. Physical Inventory

1. Leases/contracts are available and in force for hardware, including peripheral equipment, and software.
2. Lists of existing equipment is complete and current (including all PCs).
3. Determine procedure for disposing of equipment.
4. Validate equipment to the Asset list.

Auditor(s) Assigned _____

Audit Date

Audit Objectives and Procedures

Workpaper
Ref. By

M. System Performance Monitoring

1. Are there performance standards established?
If not, what is the allowable limits of:
 - a. Response time
 - b. Disk Capacity
2. What capacity planning is performed with new systems development?
3. Is a report provided management depicting system performance?
If yes, how frequent?

N. Preventative Maintenance (PM)

1. Insure Preventative Maintenance agreements are available.

Auditor(s) Assigned _____

Audit Date

Audit Objectives and Procedures

Workpaper
Ref. By

- a. Time period (Start and ending PM dates).
 - b. Equipment description.
 - c. Frequency of PM
 - d. Charge per call or per year.
2. Insure PM is performed on contracted equipment only.

PREVENTATIVE MAINTENANCE

N/PROG

Page 1 of 1