Agency **Audit Program - Computer Operations**		Initials	Date
	Prepared By		
	Reviewed By		
	W / P Ref		
	Page **1** of **1**		

Procedures	Initials	Date	Reference/Comments
OBJECTIVE - To document the review of the computer operations controls. This program is used to itemize the procedures utilized to allow the auditor to assess the control environment..			
1. Utilize the Computer Operations Internal Control Structure Questionnaire to gain an understanding of the control procedures. In completing the ICSQ, include the following: **a. results from interviews that further describe the control procedures** **b. documentation that illustrates the current conditions pertaining to the control procedures.**			
2. Summarize control policies and procedures (initial assessment) identified in developing an understanding of the computer operations controls. Include the most significant control policies and procedures that might be tested to provide evidence of their operating effectiveness.			
3. If it is determined to be effective and efficient, design and perform tests which will provide evidence of the operating effectiveness for significant control policies and procedures determined in #2 above.			

Procedures	Initials	Date	Reference/Comments
4. Based upon the above procedures, include any weaknesses on a point disposition sheet. Weaknesses should be discussed with management and finding sheets should be written for reportable conditions.			
5. Include the audit results in an overall memo. Consider the effect of the results, combined with the results of any other ICSQ performed, on the overall control environment.			

Agency **Internal Control Structure Questionnaire** **Computer Operations** Updated: 10/95		Initials	Date
	Prepared By		
	Reviewed By		
	W/P Ref		
	Page **1** of **9**		

INSTRUCTIONS NEEDED FOR COMPLETION OF THE QUESTIONNAIRE:

1. The responses to the questions in the ICSQ will be used in gaining and documenting an understanding of the EDP General control structure.

2. Assess the level of control risk for each accounting system or control procedure listed on the ICSQ using the following measures of risk:

   0 - Low Risk
   1 - Moderate Risk
   2 - Slightly Less Than Maximum Risk
   3 - Maximum risk

   Document your justification for the level of risk assessed in the space provided.

3. Cross-reference to flowcharts, narratives, memorandums, etc. that support the control policies or procedures, when applicable.

4. The ICSQ will be maintained in the permanent file rather than the current workpapers. See new permanent file maintenance instructions for further information.

5. The ICSQ can have items added or deleted depending on the particular needs of the current audit.

For clarification or assistance, contact the EDP Audit Specialist Team Coordinator

Policy/Question	N/A	Yes	No	W/P - Remarks
CONTROL POLICY #1 - Computer operations tasks are scheduled and performed in an orderly manner.				
1. Are all data control and operations tasks, including program and equipment maintenance, computer system upgrades, and testing, scheduled in advance?				
2. Has management prioritized jobs in the event of contention for resources?				
3. Are schedules periodically reviewed by management for the following? a. if jobs are properly scheduled b. if the schedules are being followed c. to aid in planning for future resource needs				

Circle the level of Control Risk assessed for this Control Procedure:

0 - Low Risk
1 - Moderate Risk
2 - Slightly Less Than Maximum Risk
3 - Maximum risk

RISK ASSESSMENT JUSTIFICATION:

Policy/Question	N/A	Yes	No	W/P - Remarks
CONTROL POLICY #2 - The operations function is responsible for ensuring that the equipment and software operate as they are designed.				
1. Do procedures for operations include the following? a. recording hardware and software problems b. management of the tape library c. cleaning and performing preventive maintenance on the computer equipment d. powering up and shutting down the equipment e. procedures for running and correcting jobs				
2. Are there system utilities for the following? **a. the tape library management to check file labeling and help track tapes of large libraries** **b. batch processing scheduling** **c. automated system logging and reporting for the following:** **(1) system malfunctions** **(2) usage of the computer system resources**				

Circle the level of Control Risk assessed for this Control Procedure:

0 - Low Risk
1 - Moderate Risk
2 - Slightly Less Than Maximum Risk
3 - Maximum risk

RISK ASSESSMENT JUSTIFICATION:

Policy/Question	N/A	Yes	No	W/P - Remarks
CONTROL POLICY #3 - Plans for the routine backup of critical data, programs, documentation, personnel, and supplies exist.				
1. Do backup procedures include the following? **a. the backup of master files, tables, and transactions** **b. the backup of current and prior versions of application programs** **c. the backup of current and prior version of systems software** **d. the backup of job streams** **e. the backup of automated log data** **f. the labeling and identification of backup files** **g. the retention and timely rotation cycle of backup files** **h. the storage of application, system software, and other system operations documentation at an off-site storage facility** **i. the storage of a reserve supply of critical, nonstandard forms at an off-site storage facility** **j. the testing of critical backup tapes for readability** **k. cross-training of data processing staff** **l. removal to an off-site storage facility of the following:** **(1) daily backups** **(2) weekly backups** **(3) Biweekly backups** **(4) monthly backups** **(5) year-end backups** **(6) archival backups**				

Policy/Question	N/A	Yes	No	W/P - Remarks
2. Does cross-training of data processing staff include the following? **a. more than one programmer and analyst being familiar with each application** **b. more than one data control person being familiar with the handling of each application** **c. the rotation of operators on each application and operations function** **d. more than one person, either another systems programmer or a programmer or analyst (when there is only one systems programmer), being familiar with systems software** **e. more than one person, either another database administrator or a programmer or analyst (when there is only one database staff member), being familiar with each database**				

Circle the level of Control Risk assessed for this Control Procedure:

0 - Low Risk
1 - Moderate Risk
2 - Slightly Less Than Maximum Risk
3 - Maximum risk

RISK ASSESSMENT JUSTIFICATION:

Policy/Question	N/A	Yes	No	W/P - Remarks
CONTROL POLICY #4 - There is a secure off-site storage facility for the storage of backup files, documentation, and critical forms.				
1. Does the off-site storage facility meet the following criteria? **a. solid walls that are fire resistant and extend to the solid or true ceiling** **b. solid doors that are fire resistant** **c. doors that are attended or kept locked** **d. temperature and humidity monitoring and control** **e. heat and/or smoke alarms** **f. fire suppression**				
2. Is a log of the backup tapes, disks, documentation, and supplies kept at the off-site storage facility?				

Circle the level of Control Risk assessed for this Control Procedure:

0 - Low Risk
1 - Moderate Risk
2 - Slightly Less Than Maximum Risk
3 - Maximum risk

RISK ASSESSMENT JUSTIFICATION:

Policy/Question	N/A	Yes	No	W/P - Remarks
CONTROL POLICY #5 - There is a documented backup plan adequate for processing critical jobs in the event of a major hardware or software failure or temporary or permanent destruction of the data processing facility.				
1. Is there a backup plan to be used in the event of an emergency or disaster?				
2. Is there evidence of executive management support for the disaster recovery project?				
3. Was the disaster recovery plan developed by a disaster recovery committee that included data processing personnel and major users?				
4. Has a risk assessment been performed to identify those risks that the agency is subject to?				
5. Does the backup plan include the following? **a. consideration for the risks identified in the risk analysis** **b. a predetermined priority for application processing** **c. the minimum computer configuration, associated communication software, lines, data and application software, physical facilities, security, etc., necessary for processing critical systems for the following:** **(1) short periods of time** **(2) extended periods of time** **d. provisions for the use of manual procedures, if necessary** **e. identification and training of users, data processing personnel, and their backups in their responsibilities in the event of a disaster**				
6. Have hardware and software vendors been contacted as to the amount and cost of support they could provide in the event of a disaster?				
7. Has an alternate site agreement for the use of a compatible site for short periods, an arrangement for delivery of temporary equipment, or the use of a commercial site for longer periods been established?				

Policy/Question	N/A	Yes	No	W/P - Remarks
8. Does the agreement for the alternate or commercial site include the following? **a. specific resources available including the following:** **(1) hardware** **(2) software** **(3) personnel** **b. time available** **c. cost specifications** **d. duration of the assistance**				
9. Have purchases necessary for disaster recovery been identified?				
10. Is the backup plan tested to the degree practical at least once a year?				
11. Is the plan updated as the system components or personnel change?				

Circle the level of Control Risk assessed for this Control Procedure:

0 - Low Risk
1 - Moderate Risk
2 - Slightly Less Than Maximum Risk
3 - Maximum risk

RISK ASSESSMENT JUSTIFICATION:

Policy/Question	N/A	Yes	No	W/P - Remarks
CONTROL POLICY #6 - There are methods which aid in processing recovery in the event of abnormal program termination.				
1. Are there procedures for recovery when processing is abnormally terminated?				
2. Do applications have checkpoint and restart procedures when necessary to allow processing to continue from the record of the last checkpoint before an abnormal termination occurred?				
3. Are abnormal terminations logged?				

Circle the level of Control Risk assessed for this Control Procedure:

0 - Low Risk
1 - Moderate Risk
2 - Slightly Less Than Maximum Risk
3 - Maximum risk

RISK ASSESSMENT JUSTIFICATION:

Computer Operations Control Procedure Information

CONTROL POLICY #1 - Computer operations tasks are scheduled and performed in an orderly manner.

Computer Operations primarily involve the scheduling of daily computer processing jobs (regular and special requests). Job processing, software and equipment maintenance, computer system upgrades, and testing, should be scheduled by management in advance. Management should prioritize computer processing jobs in the event of contention for resources. Schedules should be periodically reviewed by management and changes appropriately made.

The auditor should interview the Manager of Operations. An understanding of the operations scheduling techniques should be documented. A review of automated or manual scheduling logs, maintenance, and testing schedules should be performed to ensure that they exist. The Operations Policies and Procedures manual should be obtained and reviewed to ensure it includes adequate instructions on job scheduling procedures and special processing requests.

CONTROL POLICY #2 - The operations function is responsible for ensuring that the equipment and software operate as they are designed.

Formal operations policies and procedures for should exist. Written procedures for recording hardware and software problems, the management of the tape library, cleaning and performing preventive maintenance on the computer equipment, powering up and shutting down the equipment, and procedures for running and correcting jobs should be documented.

A tape library management system that checks file labeling (specific to a mainframe) and helps track and rotate tapes maintained in a tape library should exist. Automated logging and reporting of system malfunctions and the usage of the computer system resources should also exist. Incident reports should be documented and reviewed by Operations Management.

The auditor should gain an understanding of the day to procedures. Discussions with the Manager

of Operations and staff operators on their responsibilities should be performed. **The Operations Policies and Procedures manual should be obtained and reviewed to ensure it includes adequate detail (no reliance is placed on personal knowledge). Incident Reports should be reviewed to determine the types of problems occurring.**

CONTROL POLICY #3 - Plans for the routine backup of critical data, programs, documentation, personnel, and supplies exist.

Data Backup - Data backup procedures of master files, tables, and transactions and the backup of current and prior versions of application programs should be in place. Backups of current and prior version of systems software, of job streams, and automated logs should be part of scheduled jobs.

In addition, procedures should include the labeling and identification of backup files, the retention and timely rotation cycle of backup files, the storage of application, system software, and other system operations documentation at an off-site storage facility.

Backup of data should consist of:

- **daily backups**
- weekly backups
- biweekly backups
- monthly backups
- year-end backups
- archival backups

Storage of a reserve supply of critical, nonstandard forms at an off-site storage facility, the testing of critical backup tapes for readability, cross-training of data processing staff, and the procedures to the off-site storage facility should be written.

The auditor should ensure that data backup procedures exist. Observations of the tape backup and rotation procedures should be performed. The Operations Policies and Procedures manual should be obtained and reviewed to ensure it includes adequate detail. A physical check of a sample of backup tapes should be traced to tape library reports.

Personnel Backup - Cross training is dependant on the staffing and resources available to the data processing department. Good practices consist of data processing staff with more than one programmer and

analyst being familiar with each application, more than one data control person being familiar with the handling of each application, the rotation of operators on each application and operations function, more than one person, either another systems programmer or a programmer or analyst (when there is only one systems programmer), being familiar with systems software, more than one person, either another database administrator or a programmer or analyst (when there is only one database staff member), being familiar with each database.

An Organization Chart of Computer Operations should be obtained and reviewed. Interviews with operations personnel should be done to assess the adequacy of personnel backup and knowledge. There should not be any reliance on personal knowledge.

CONTROL POLICY #4: There is a secure off-site storage facility for the storage of backup files, documentation, and critical forms.

An adequate storage facility for retaining and rotating backup files should exist. The off-site storage facility should have solid walls that are fire resistant and extend to the solid or true ceiling. Solid doors that are fire resistant, doors that are attended or kept locked, temperature and humidity monitoring and control, heat and/or smoke alarms, and fire suppression equipment should be in place. A log of the backup tapes, disks, documentation, and supplies kept at the off-site storage facility should exist and be maintained both onsite and offsite.

The auditor should visit and observe the storage facility. Rotation and storage procedures should be observed. A physical agreement of tapes at offsite storage should be reconciled to tape library reports.

CONTROL POLICY #5: There is a documented backup plan adequate for processing critical jobs in the event of a major hardware or software failure or temporary or permanent destruction of the data processing facility.

A comprehensive backup plan used in the event of an emergency or disaster should exist. There should be a Disaster Recovery Coordinator appointed. The plan should identify executive management approval and support for the disaster recovery project.

In addition to the Coordinator, there should be a disaster recovery committee composed of data processing personnel and major users. A risk assessment should be performed periodically to identify those risks that the agency is subject to. The plan should consider those risks identified in the risk analysis and that a predetermined priority for application processing exists. Documentation for the minimum computer configuration, associated communication software, lines, data and application software, physical facilities, security, etc., and the necessary for processing critical systems for both short and extended periods of time should exist. In addition, the plan should address the identification and training of

users, data processing personnel, and their backups in their responsibilities in the event of a disaster. Hardware and software vendors should be listed and the amount and cost of support they will provide in the event of a disaster.

An alternate site agreement for disaster recovery should be in force. The use of a compatible site for short periods, an arrangement for delivery of temporary equipment, or the use of a commercial site for longer periods should be established. The agreement should address the alternate or commercial site use and include the specific resources available for hardware and software, personnel, time available, cost specifications, and the duration of the assistance.

Test results of the last time the backup plan should be available. The degree of test, results, and updates to system components or personnel change should be summarized.

The auditor should interview the Disaster Recovery Coordinator. Procedures should be obtained and evaluated to ensure they include adequate detail on recovery activities. A review of tests performed should be done. Contracts in force should be evaluated.

CONTROL POLICY: There are methods which aid in processing recovery in the event of abnormal program termination.

Restart and recovery procedures should exist when regularly scheduled job processing abnormally terminates. (This is not part of the Disaster Recovery Plan). Abnormal terminations should be logged and investigated.

The auditor should discuss restart recovery procedures with Operations personnel. These should written in the Operations policies and procedure manual. Incident Reports should note any abnormal job terminations. Reoccuring problems should be noted and discussed with Operations.