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

The SAO follows control objectives established by the Information Systems Audit and Control Association (ISACA) for EDP audits. ISACA has updated the existing objectives and will release the Control Objectives for Information and Related Technology (COBIT) in April of 1996. Once released, the control objectives will be reviewed and the current application ICSQ and audit program will be enhanced to reflect the changes.

Procedures	Initials	Date	Reference/Comments
OBJECTIVE - To document the review of the application controls. This program is used to itemize the procedures utilized to allow the auditor to assess the control environment..			
1. Utilize the Application 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 application controls. Include the most significant control policies and procedures that might be tested to provide evidence of their operating effectiveness.			

Procedures	Initials	Date	Reference/Comments
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.			
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.			

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 PROCEDURE #1 - The preparation and input of transactions are authorized.				
1. Are transactions authorized and approved before input?				
2. Is authorization to input transactions controlled by terminal id (not usually used), user id, and/or transaction type?				
3. Are there manual controls (such as restrictions on access to records, to batch numbers, or to any pre-input information) in addition to system level controls that limits who can input data?				
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 PROCEDURE #2 - There are controls which provide reasonable assurance that transactions are not lost, duplicated, or added before or during data entry and editing.				
1. Are preprinted sequential numbers used on source documents to establish controls?				
2. Are there controls to account for the movement of transactions from origination to data entry such as turnaround transmittal documents, batching techniques, record counts, predetermined control totals, and logging techniques? **Which controls?**				
3. Are control totals for source documents reconciled with accumulated totals of transactions that have been entered?				
4. Are control totals for transactions which have been entered reconciled with transactions which have been edited?				
5. After data entry of each source document, is the document canceled to prevent duplicate entry?				

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 PROCEDURE #3 - There are controls which provide reasonable assurance that input data is correct.				
1. Are source documents designed to guide the initial recording of data in a consistent format?				
2. Do input documents facilitate the input of information by having data aligned in the same manner as the input screen?				
3. Have edits been designed to validate all critical data fields (dates, codes, account numbers, values)?				
4. Is input data edited and validated close to the point of origination? **If not, does editing and validation occur as part of the application processing?**				
5. Do edits check the contents of critical data fields for reasonableness, valid combination of fields, validity, format, mathematical accuracy, check digit verification, and range?				
6. To ensure update of the correct master file record, is new data to be processed matched with the master file record (Is the key of the update record matched back to the original master record)?				
7. Is data entry verified by someone other than the person who did the original data entry?				
8. Is the ability to override and bypass data validation and editing controlled by the following? **a. limiting the capability to supervisors for only a limited # of situations** **b. logging and reviewing of all overrides and bypasses**				

Policy/Question	N/A	Yes	No	W/P - Remarks
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 PROCEDURE #4 - There are controls which provide reasonable assurance that transactions with errors are prevented from updating files.				
1. Are transactions that do not pass the edits rejected?				
2. Is the reason for each error identified with some type of message?				
3. Are the rejected transactions investigated, corrected in a timely manner, and resubmitted? **a. Are the applicable batch control totals corrected?** **b. Are these procedures documented?** **c. Has responsibility for investigating, correcting, resubmitting and adjusting control totals been assigned?** **Who is responsible?**				
4. Are rejected transactions which have been corrected and resubmitted subjected to the same edits and validation as original transactions?				

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 PROCEDURE #5 - There is an audit trail so that transactions can be traced from source documents to edited data and from processed data back to the source documents.				
1. Are source documents retained and stored in a manner that aids in tracing of the audit trail and recreation of lost data?				
2. Is there a cross-reference number for each transaction that can be used to trace information to and from the source document?				
3. Does the audit trail (manual and automated) include the following for each transaction? **a. batch id number** **b. user id** **c. terminal id** **d. transaction type** **e. the date and time the transaction was entered/edited**				
4. Are listings of accepted and rejected transactions produced and reviewed to verify that everything entered has been processed?				
5. Do output transaction documents, records, ledger accounts, journal entries, etc., include a transaction source reference?				
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 PROCEDURE #6 - Adequate separation of duties exists within the user department.				
1. Are duties separated so that no individual performs more than one of the following operations? **a. data origination** **b. data authorization** **c. data input** **d. data verification** **e. data correction**				
2. Are duties separated to ensure that one individual does not prepare more than one type of transaction (i.e., establishing new master records plus changing or updating master records)?				

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 PROCEDURE #7 - Controls exist to provide reasonable assurance that data is processed completely (i.e., that all data entered into and accepted by the computer is updated to the proper file).				
1. Are control totals of transactions submitted for processing reconciled to totals of items that have updated the master file(s)? **If control totals are not used, is there a substitute method to verify that all accepted transactions are processed?**				
2. Are there methods to ensure that each transaction is applied to a file only once during update processing?				
3. Are amount field balances on the master file(s) periodically calculated and reconciled with cumulative transaction totals?				

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 PROCEDURE #8 - Controls exist to ensure that transactions are accurately processed (i.e., that all input data is accurately carried through processing and updates the correct files).				
1. Are internal header and trailer labels on files tested for the following? **a. correct file identifier** **b. proper date** **c. correct sequence of files** **d. record count** **e. control and hash totals** **f. date file retention has passed**				
2. When performing sequential updates, is the sequence of records on the input file checked?				
3. Does processing halt or is an operator notified if there is an error with an input/output file?				
4. Are other procedures followed to ensure the use of correct files and the detection of processing the wrong data file? **What are they?**				
5. Are reports of transactions that update the master file produced and reviewed (reconciliations)?				
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 PROCEDURE #9 - 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? **Are procedures to recover from abnormal terminations documented?**				
2. Does the application have checkpoint and restart procedures to allow processing to continue from the record of the last checkpoint before an abnormal termination occurred?				
3. Are abnormal terminations logged? **Has responsibility been assigned for periodic review of logged abnormal terminations?**				
4. Has responsibility for recovery from abnormal termination been assigned?				

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 PROCEDURE #10 - There is adequate cross-training of personnel and application backup to allow for continued operation of the application.				
1. Have personnel (programmers, users, operators, and data control personnel) been cross-trained so that the continued operation of the application is not dependent upon one individual?				
2. Are the application's current documentation and program/data files backed up and maintained at an off-premise storage location?				
3. Have manual procedures been developed for use in the event of a computer outage?				
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 PROCEDURE #11 - There are controls for ensuring that output is correct.				
1. Is someone responsible for reviewing output for completeness?				
2. Are control totals reconciled? **When control totals cannot be reconciled, is the problem reviewed and corrected?**				

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 PROCEDURE #12 - There are controls to ensure that all output is distributed and that it is only distributed to authorized users.				
1. Are there procedures to ensure that output is only distributed to the owner of the data?				
2. Is there a log of all output produced and distributed? **Are these logs maintained?**				
3. Are turnaround transmittal documents used to verify that output has been received by the authorized recipient?				
4. Is there a distribution list of who is to receive output?				
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:**

Application Control Procedure Information

CONTROL PROCEDURE #1 - The preparation and input of transactions are authorized.

CONTROL PROCEDURE #2 - There are controls which provide reasonable assurance that transactions are not lost, duplicated, or added before or during data entry and editing.

CONTROL PROCEDURE #3 - There are controls which provide reasonable assurance that input data is correct.

These control procedures ensures the input of data into the computer system is authorized, accurate, complete, and timely. Management relies on correct information in their planning and decision process. Therefore, the integrity of data is important.

The auditor begins the review by gaining an understanding of the input process. Ordinarily, the auditor obtains this knowledge and understanding through review of system documentation, such as a user operations manual, and through discussions with appropriate users and application personnel.

The auditor should determine and evaluate the adequacy of controls over the input preparation, collection, and the automated processing of inputs. This will ensure that no data is added, lost, or changed before it is processed by the computer system. Input forms and documents should be used to create and approve data going into the system. Majority of inputs processed by the systems are manually entered through terminals.

It is recommended that the auditor obtain system level documentation, job control language, and other pertinent information. A flowchart of the transaction flow should be prepared. The key input file processing, programs, output files, reports, and interfaces to other systems should be documented showing manually or generated inputs to the system. Assistance from an experience EDP Auditor may be required to understand and review system level documentation.

The auditor should identify and document the major transactions, key data fields on the transactions, method of data input or generation. This is indicated in systems documentation. Data input can be through a batch or on-line entry, or automatic generated by the computer system. Input controls can consist of restrictions on specific computer terminals, use of user access identification (Ids), and transaction types and codes. The auditor should determine the method of input and evaluate the controls to ensure accuracy, completeness and timeliness of inputs.

If the auditor determines that input controls are weak, the effect of this weakness could cause unauthorized, incomplete, and incorrect information to exist. This will lead to inaccurate representation of reality. Ultimately, decisions can be made on inaccurate data.

Tests of controls are performed for those controls that the auditor intends to rely on to obtain reasonable assurances that they are operating effectively. Examples of testing include:

- **Ensuring authorization to input transactions are controlled by terminal id, user id, and transaction type.**
- **Identify those users responsible for input preparation, the review, and authorization.**
- **Identify and evaluate the manual controls (authorization and reviews of source documents) in addition to system level controls that limits who can input data.**
- **Identify and test the control total balancing, exception or audit trails of each significant transaction.**
- Identify and test the controls which account for the movement of transactions from origination to data entry or generation. (These could consist of transmittal documents, batching techniques, record counts, predetermined control totals, and logging techniques.)
- Identify and test the process that ensures that transactions are entered and processed once**.**
- **Determine and test the procedures to reconcile the source documents with the transactions which have been entered.**
- Review documentation and document the function or control procedures performed by each major software program.
- Identify and test the preprogrammed keying formats used to aid in recording data in the proper field, format, etc.
- **Identify and test the edits that have been designed to validate all critical data fields (dates, codes, account numbers, values.)**
- **Determine and test the stage of editing and validation of input data. Identify and test edits which check the contents of critical data fields for reasonableness, valid combination of fields, validity, format, mathematical accuracy, checks digit verification, and range.**
- **Determine that data entry is verified by someone other than the person who did the original data entry.**
- **Identify and test the ability to override and bypass data validation and editing. Ensure the following: limiting the capability to supervisors for only a limited # of situations/ logging and reviewing of all overrides and bypasses**

After testing, the auditor again evaluates the controls based on his understanding of the

procedures and the results of testing. Control risk can be assessed depending on the assurance provided by test results.

A memo summarizing the test results is then prepared that includes a final assessment of the control procedure. Written and oral findings are prepared for weaknesses in controls and discussed with the client and their management.

CONTROL PROCEDURE #4 - There are controls which provide reasonable assurance that transactions with errors are prevented from updating files.

Data updates to files containing information should be error free. Automated editing in the system on inputs should occur. Typical edits include numeric checks, reasonableness, format, check digit, and valid field checks. Any errors noted during processing should be rejected and logged. Corrective procedures should consist of resubmission and subjected to editing and validation as original transactions. There should be manual procedures for investigating, correcting, and resubmitting transaction plus adjusting control totals.

The auditor should review documentation and document the process to ensure that transactions that do not pass the edit are rejected and maintained on a file. Each error should be identified with some type of message. Obtain copies of exception reports and evaluate the information reported. Determine and document the process to ensure rejected transactions are investigated and corrected in a timely manner, and resubmitted. Ensure the applicable batch control totals are corrected. Ensure procedures documented. Identify the person responsible for investigating, correcting, resubmitting and adjusting control totals been assigned. Through discussion, ensure that rejected transactions which have been corrected and resubmitted are subjected to the same edits and validations as original transactions. Document and evaluate the control procedure.

CONTROL PROCEDURE #5 - There is an audit trail so that transactions can be traced from source documents to edited data and from processed data back to the source documents.

Source documents should be used to submit inputs into the system. These should be stored in a manner that aid in the tracing and recreation of data. Through discussion with persons responsible for data input, determine if source documents are retained and stored in a manner that aids in tracing of the audit trail and recreation of lost data. The retention period should be adequate for data reconstruction. The auditor should obtain examples of the significant output and document the key fields. The audit trail (manual and automated)

should include the batch id number, user id, terminal id, transaction type, and that date and time the transaction was entered/edited.

The auditor should document the listings of accepted and rejected transactions produced. A review to verify that everything entered has been processed should be performed. The relationship between transaction documents, records, ledger accounts, journal entries, etc. should be understood.

As part of testing, the auditor should obtain copies of these documents and trace a sample of transactions. An evaluation and assessment based on testing should determine the quality of information and referencing.

CONTROL PROCEDURE #6 - Adequate separation of duties exists within the user department.

Duties within a department should be separated so that data authorization, validation, processing and review are not performed by the same person. An organization chart should identify the people (or position) responsible for all the functions. However, through discussion, and review of organization charts, the auditor should identify the individuals who perform the following operations:

Data Origination	New or changed data is created
Data Authorization	Inputs must be properly authorized prior to entry
Data Input	Data entry process
Data Verification	Reports are reviewed
Data Correction	Mistakes are corrected

It should be determined that duties are separated to ensure that one individual does not prepare more than one type of transaction (i.e., establishing new master records plus changing or updating master records). Compensating controls should be in place for departments that do not have adequate resources to supply an adequate segregation of duties.

CONTROL PROCEDURE #7 - Controls exist to provide reasonable assurance that data is processed completely (i.e., that all data entered into and accepted

by the computer is updated to the proper file).

Processing of data should be complete without any interruptions or manual manipulation. An understanding of the processing of data should be performed. The auditor should review documentation and document the significant files and data elements (fields) which are accessed by or updated by the significant transactions. Master files, transaction files, and history files are usually the key files in a mainframe application. Document the process for reconciling the control totals of transactions submitted for processing to the totals of items that have updated the master file(s). If control totals are not used, identify the substitute method to verify that all accepted transactions are processed.

Identify and document the methods to ensure that each transaction is applied to a file only once during update processing.

CONTROL PROCEDURE #8 - **Controls exist to ensure that transactions are accurately processed (i.e., that all input data is accurately carried through processing and updates the correct files).**

Document the process to ensure internal header and trailer labels on files test for the following:

- correct file identifier
- proper date
- correct sequence of files
- record count
- control and hash totals

Determine that the sequence of records on the input file is checked. Determine that computer processing halts or that an operator is notified if there is an error with an input/output file. Identify and document other procedures to ensure the use of correct files and the detection of processing the wrong data file. Determine if computer console and output messages used to indicate bypass file identification. Identify the transaction reports that show updates to the master file. Ensure they are produced and reviewed. Identify and document the controls in place to ensure the master file records after updates are correct.

CONTROL PROCEDURE #9 - **There are methods which aid in processing recovery in the event of abnormal program termination.**

Obtain and review the documented procedures to recover from abnormal terminations.

Evaluate the checkpoint and restart procedures to allow processing to continue from the record of the last checkpoint before an abnormal termination occurred. Ensure that abnormal terminations are logged. Obtain copies of the most recent logs and evaluate the extent of such activities. Identify the person responsible for the periodic review of logged abnormal terminations.

CONTROL PROCEDURE #10 - There is adequate cross-training of personnel and application backup to allow for continued operation of the application.

Identify and document the personnel (programmers, users, operators, and data control personnel) which have been cross-trained so that the continued operation of the application is not dependent upon one individual. Determine that the application's current documentation, and program and data backup files backed up and maintained at an off-premise storage location. Determine that manual procedures been developed for use in the event of a computer outage.

CONTROL PROCEDURE #11 - There are controls for ensuring that output is correct.

Obtain and document an understanding of the review process on output produced from the system. Document the review process over the reconciliation and input/output review.

CONTROL PROCEDURE #12 - There are controls to ensure that all output is distributed and that it is only distributed to authorized users.

Document the procedures to ensure that output is only distributed to the appropriate recipient. Determine and obtain the distribution lists used to verify that output has been received by the authorized recipient. Obtain a distribution list of who is to receive output.