		Initials	Date
Agency	Prepared By		
Audit Program - System Design, Development, and Maintenance	Reviewed By		
	W / P Ref		
	Page **1** of **1**		

Procedures	Initials	Date	Reference/Comments
OBJECTIVE - To document the review of the system design, development, and maintenance (SDDM). This program is used to itemize the procedures utilized to allow the auditor to assess the control environment..			
1. Utilize the System Design, Development, and Maintenance 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 SDDM 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.			

Agency
Internal Control Structure Questionnaire
System Design, Development, and Maintenance

Updated:10/95

	Initials	Date
Prepared By		
Reviewed By		
W/P Ref		
Page **1** of **12**		

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 - A systems development life cycle (SDLC) methodology or equivalent procedures to monitor the development or acquisition process of automated applications is followed.				
1. Are applications developed according to a SDLC methodology?				
2. Does the SDLC methodology include the following? **a. needs analysis** **b. system analysis and design** **c. testing** **d. program promotion** **e. implementation** **f. post-implementation reviews**				
3. Is there participation and approval by users, management, data processing, quality assurance group, and internal auditors throughout the various phases of the SDLC process?				
4. Is authorization and approval by management and the principal user(s) obtained at key points in the SDLC process (such as after developing the general system design, after detailed system specifications, after system testing, and at system acceptance)? If so, when?				
5. Are internal auditors provided the opportunity to participate in systems design to provide an independent evaluation of proposed controls in the system and to recommend the inclusion of computerized audit routines?				

Policy/Question	N/A	Yes	No	W/P - Remarks
6. Do personnel responsible for quality assurance assist in the following? **a. formulating systems and programming standards** **b. examining systems design documentation to ensure compliance with standards and that the new system has incorporated adequate functions to facilitate effective control** **c. reviewing program testing, systems testing, and parallel or pilot runs to ensure compliance with standards** **d. reviewing data conversion procedures for compliance with standards** **e. ensure systems and programming practices are in accordance with the standards**				
7. Is a project master plan developed for large projects?				

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 - A needs analysis is performed before the system is designed and developed.				
1. Do the standards for the needs analysis include the following? a. a formal request from the user(s) who desire the application b. a thorough review of the present system or procedures to evaluate the present system's deficiencies and capabilities and decide if a change is necessary c. a feasibility study for large projects that includes identification of all costs and benefits d. defining and analyzing existing and new information requirements e. identification of the effect of the new system requirements on other systems f. review of alternative courses of action (including purchasing software vs. developing it in-house) that satisfy the information requirements of the new system g. justification for the selected alternative				
2. Is the needs analysis phase documented?				

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 is a controlled process for designing and developing applications.				
1. Are detailed input, output, file, and processing specifications defined and documented?				
2. If a database is to be used, is the content and organization of the database, including logical data relationships, physical storage strategy, and access strategy included in the design?				
3. Are there written programming standards?				
4. Do programming standards include naming conventions and coding standards?				
5. Are programmed controls and audit trails incorporated in the detail design to promote data integrity?				
6. Are the specifications reviewed and approved by management and application users before programming starts?				
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 - Testing procedures are controlled for new and modified programs.				
1. Have system and program testing procedures been established?				
2. Does system testing include both the manual and computerized phases of the system?				
3. Are programmers prohibited from testing programs against production data files?				
4. Is system testing a joint effort of both users and data processing personnel?				
5. Is parallel processing performed where applicable? **a. Are the results of parallel processing reconciled before placing the new system into operation?**				

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 - Control procedures are established for the implementation of new and modified systems and programs.				
1. Do procedures exist to prevent unauthorized changes to data files during conversion from manual records to machine-readable records?				
2. Do these procedures require that manual records be retained until conversion is complete and it is determined that the system is operating correctly?				
3. Do final acceptance test criteria need to be met before a new system is placed into operation?				
4. Do program promotion standards require: **a. a person, such as the programming manager, to perform the following:** **(1) examine the code to ensure it does what is specified and nothing more** **(2) review program documentation** **(3) test the new or modified program to confirm that it operates as specified** **(4) approve the program for production** **b. once a programmer turns a program in for review, he no longer has access to the program** **c. the operations section or a systems programmer use a utility not available to the application programmers to place the program into production status** **d. only programs in official production status be used for live work** **e. each version of a modified program be saved with a historical number that will distinguish it from all other versions** **f. each version of a modified program is archived**				
5. Are there procedures for controlling changes to production programs in an emergency?				

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**:
CONTROL PROCEDURE #6 - A post-implementation review is performed for major projects.				
1. Are post-implementation reviews performed?				
2. Does the post-implementation review determine the following? **a. if the project has met the user's requirements** **b. if each of the SDLC phases have been satisfactorily completed and documented** **c. if additional improvements are needed**				
3. Does Internal Audit or quality assurance conduct the post-implementation review?				
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 - Maintenance of applications is adequately controlled.				
1. Is written authorization from the user obtained for all modifications?				
2. Is user approval received for system and program changes?				
3. Are all program changes approved, thoroughly tested, and reviewed by an independent EDP reviewer and user management?				
4. If there is a database, are there procedures relating to the following? **a. data changes** **b. data dictionary maintenance, including adding new data names and changing data descriptions**				

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 - There are procedures in place to provide control over changes to systems software.				
1. Are there procedures for the following? **a. requesting and authorizing modifications to systems software** **b. testing of changes** **c. the review of changes by someone other than the original programmer** **d. implementation (loading) of changes by someone other than the original programmer** **e. controlling changes to systems software during an emergency** **f. performing a review to determine that the changes operate properly**				
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 standards for system, program, user, and run documentation.				
1. Do documentation standards include the following? **a. system level documentation** **b. program documentation** **c. user documentation** **d. run documentation for use by operations personnel**				
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**:

System Development Life Cycle Control Procedure Information

CONTROL PROCEDURE #1 - A systems development life cycle (SDLC) methodology or equivalent procedures to monitor the development or acquisition process of automated applications are followed.

Applications should be developed according to an SDLC methodology. The **SDLC written procedures should cover areas such as needs analysis, system analysis and design, program promotion, implementation, and post-implementation reviews. There should be participation and approval by users, management, data processing, quality assurance group, and internal auditors throughout the various phases of the SDLC process.**

Authorization and approval by management and the principal user(s) should be obtained at key points in the SDLC process. These would occur after developing the general system design, after detailed system specifications, after system testing, and at system acceptance. Internal auditors should be provided the opportunity to participate in systems design to provide an independent evaluation of proposed controls in the system and to recommend the inclusion of computerized audit routines.

A Quality Assurance function should exist and be incorporated within SDLC process. Quality assurance assists in the formulating systems and programming standards by examining systems design documentation to ensure compliance with standards and that the new system has incorporated adequate functions to facilitate effective control and reviewing program testing, systems testing, and parallel or pilot runs to ensure compliance with standards. Data conversion procedures for compliance with standards to ensure systems and programming practices are in accordance with the standards should be reviewed.

The auditor should obtain and assess the SDLC procedures to ensure they are comprehensive in outlining a system design methodology.

CONTROL PROCEDURE #2 - A needs analysis is performed before the system is designed and developed.

A needs analysis should include a formal request from the user(s) who desire the

application. This should initiate a review of the present system or procedures to evaluate the present system's deficiencies and capabilities to decide if a change is necessary. A feasibility study for large projects should be performed which identifies all costs and benefits, define and analyzes existing and new information requirements, and identifies the effect of the new system requirements on other systems. A review of alternative courses of action (including purchasing software vs. developing it in-house) that satisfy the information requirements of the new system should also be part of the study and include a written justification for the selected alternative.

The auditor should ensure that a needs analysis segment is part of the system design methodology. A needs analysis should be included in the project development file.

CONTROL PROCEDURE #3 - There is a controlled process for designing and developing applications.

The SDLC written procedures should include programming standards, naming conventions, and coding standards. The auditor should obtain project development files to review the contents and ensure the project is in compliance to written system design standards.

CONTROL PROCEDURE #4 - Testing procedures are controlled for new and modified programs.

SDLC procedures should include system and program testing procedures. System testing should include manual and computerized phases of the system. Programmers must be prohibited from testing programs against production data files. System testing is a joint effort of both users and data processing personnel. Parallel processing should be performed where applicable and the results of parallel processing reconciled before placing the new system into operation.

The auditor should interview a system project manager and determine that testing and verification procedures are formally done by users and system developers.

CONTROL PROCEDURE #5 - Control procedures are established for the implementation of new and modified systems and programs.

Procedures to prevent unauthorized changes to data files during conversion from manual records to machine-readable records should exist. Manual records should be retained until conversion is complete and the system operating correctly. Final acceptance should be formally met by user testing and sign-offs before a new system is placed into operation.

Adequate program promotion standards require a person, such as the programming manager, or quality assurance group to examine the code to ensure it does what is specified and nothing more, review program documentation, test the new or modified program to confirm the program operates as specified, and approve the program for production status. Once a programmer turns a program in for review, write/update access to that program should not be allowed. Development tools such as CASE automate and structure the coding process.

The Operations or Systems sections commonly use a utility (PANVALET, CHANGEMAN) to place the program into production status. These utilities should not be accessible to the application programmers. Only programs in official production status should be used to process against master datafiles. Each version of a modified program should be saved with a historical number that will distinguish it from the new and all earlier versions. Each version of a modified program should be archived. There should be procedures for controlling changes to production programs in an emergency. Any use of emergency passwords or login ids should be documented and reviewed by Operations Management.

The auditor should gain an understanding of the implementation process. Change control procedures with or without automated or manual processes should be identified. An assessment of the process should be done. Use of emergency passwords or login ids to make a change in production systems should be assessed.

CONTROL PROCEDURE #6 - A post-implementation review is performed for major projects.

A post-implementation review should be performed to ensure users' requirements were sufficiently met, each of the SDLC phases has been satisfactorily completed and documented, and if additional improvements are needed. Internal Audit or quality assurance should be involved in the post-implementation review.

The auditor should ensure that post-implementation activities are performed. These

should be documented in the project design files.

CONTROL PROCEDURE #7 - Maintenance of applications is adequately controlled.

Written authorization from the users should be obtained for all types of modifications. User approval should be received for system and program changes. Change control documentation should indicate that all program changes approved, thoroughly tested, and reviewed by an independent EDP reviewer and user management. Modification procedures relate to data changes, data dictionary maintenance, including adding new data names and changing data descriptions

The auditor should gain an understanding of the change control process on existing applications (not under development). Automated or manual processed should be identified and assessed. Change control documents, logs, and reports should be obtained and evaluated. **Access to Change control utilities should be evaluated.**

CONTROL PROCEDURE #8 - There are procedures in place to provide control over changes to systems software.

Change control policies include requesting and authorizing modifications to systems software, testing of changes, and the review of changes by someone other than the original programmer. Implementation (loading) of changes should be done by someone other than the original programmer. Changes to systems software during an emergency should be controlled. A review should be performed by management to determine that expedited or emergency changes are appropriate and tested.

The auditor should gain an understanding of the change control process on existing systems (not under development). Automated or manual processed should be identified and assessed. Change control documents, logs, and reports should be obtained and evaluated. **Access to Change control utilities should be evaluated.**

CONTROL PROCEDURE #9 - There are standards for system, program, user, and run documentation.

Written documentation standards for system level, programs, and user documentation should be formalized and in compliance to documentation standards (part of SDLC methodology standards). Run documentation for use by operations personnel should also be standardized.

The auditor should obtain production copies of system, program, and run documentation and review for compliance to system design standards.