

PROGRAM CHANGE CONTROL - by: James Smith jsmith@securanceconsulting.com

Objective:

The purpose of this review is to independently evaluate the adequacy, effectiveness, and efficiency of the system of control and the quality of ongoing operations within the Change Control / Configuration Management process. While originating in a mainframe environment, this program can be adapted, as necessary, to client-server based production environments.

The system of control should be designed to:

1. Provide reasonable assurance that assets are safeguarded, information is timely and reliable, and errors and irregularities are discovered and corrected promptly.
2. Promote operational efficiency.
3. Encourage compliance with managerial policies, laws, regulations, and sound fiduciary principles.

Scope:

The scope includes:

- a. Documentation, policies and procedures and software governing the change control process.
- b. Modifications to production and development to ensure that they are authorized.
- c. Modules placed in the production environment to ensure they are documented by a development listing and supported by related program change forms according to standards.
- d. Procedures to ensure the Quality Assurance / Control group, if applicable, monitors all changes to production and development environments.
- e. Access Security restrictions to production.
- f. Controls specific to the source control system are in place.

		W/P Ref.	Done By
1.0	General		
	1.1 Modify this program as necessary to address each type of change control environment controlling modifications made to application or system software. Prepare questionnaires and/or checklists for the program steps where they are appropriate.		
	1.2 Obtain and review audit workpapers, report and follow-up of prior audit recommendations. Plan and perform such additional audit steps as appropriate to verify management actions to correct previous deficiencies (if not already accomplished by prior audit follow-up).		
	1.3 Summarize any management plans for changing software, hardware, organization or control procedures.		
	1.4 To perform a Program Change Control Audit, obtain the following data: <ul style="list-style-type: none"> a. An organization chart of all related functions in IIS showing names and position titles, with associated position charters. b. Departmental policies and procedures concerning the change control process. c. Current vendor documentation for any library management or change control software in use. d. Listing of all production and test applications including source, and production environments. e. Access security requirements to development and production libraries. 		
	1.5 Arrange an "Entrance Conference" meeting with the Data Center operations management to discuss the purpose and scope of the planned audit.		
	1.6 Discuss with auditee management any problem areas that might require investigation.		
	1.7 Obtain or prepare a simple organization chart, indicating the reporting relationships involved in the Change Control Process. Determine that adequate separation of duties has been established between users, programming groups (applications and technical support), and the computer operations area.		
	1.8 Review the Change Control methodology for application programs used to ensure it encompasses appropriate controls as outlined in SEI (Software Engineering Institute) and accepted audit controls.		

		W/P Ref.	Done By
	1.9 Ensure that contracts governing all contract programmers/consultants are on file and that a unique user ID has been established for each contract programmer. The contract should indicate requirements for complying with departmental policies & procedures.		
2.0	Change Control Process		
	2.1 Obtain a list of source control applications used in the program Change control process.		
	2.2 Determine if backup and recovery procedures have been implemented, and tested for all development & prod environments. Obtain details of these procedures.		
	2.3 Review access security privileges to the various environments for appropriateness. Applications programming should not have "update" authority to production or staging environments.		
	2.4 Determine if users review test results and approve changes before programs are moved into production.		
	2.5 Evaluate procedures and controls for emergency program changes.		
	2.6 Review the procedures for recovery when a new version of a tested program fails to work in production.		
	<p>2.7 Select a sample of program changes from application source and production environments that evidence a software change and verify the following:</p> <ul style="list-style-type: none"> a. All related changes are received / reviewed by a Quality Assurance / Control function before the changes go into production. b. All related changes are supported by any appropriate documentation. c. All program changes are received/reviewed by a Quality Assurance function prior to going into production. d. All program changes are supported by properly authorized documentation. e. A copy of the reports produced by the move and the original move documents are reviewed by the appropriate programming manager. f. Trace Change Request Forms to supporting documentation such as trouble reports, etc. g. Verify that each module has an audit trail linking source and object versions. Record the data for step. h. Ensure that all documentation and procedures for each sample follows SPG policies (these should be at SEI level 3). 		

		W/P Ref.	Done By
	2.8 Using the sample selected previously, verify that the most recent version of the executable program corresponds to the most recent version in the source control.		
	2.9 For selected members from the program sample verify current listings are maintained in the Data Processing department. Check program size against production.		
3.0	Librarian Procedures		
	3.1 Determine that the LIBRARIAN Management Code (MCD) is used for controlling all production LIBRARIAN files.		
	3.2 The base MCD code should be controlled by the control group and changed on a frequent basis.		
	3.3 Run batch LIBRARIAN index listing against production LIBRARIAN files to determine module security status for production programs. There should be no TEST or PROD0 status modules. Review the security status of PROD1 and PROD2 programs to determine if they are appropriate.		
	3.4 Determine from the index listing that all programs are being archived. Review the archiving levels for adequacy.		
	3.5 If the source-load-audit-trail facility is used in compiles, trace a sample of programs from LIBRARIAN files to production load libraries.		
	3.6 Determine which LIBRARIAN exit routines are being used and what controls or features are being implemented through them. Ensure that exit routines can not be circumvented.		
	3.7 Review access controls to the batch LIBRARIAN for adequacy. Access to production LIBRARIAN files through batch should be restricted to appropriate personnel.		
	3.8 Access to the batch File Access Interface Routines (FAIR) should be restricted to appropriate personnel. The FAIR programs can be used to hack the LIBRARIAN file MCD codes.		
	3.9 Review the DASD blocking factors for LIBRARIAN master files to ensure compliance and efficiency per vendor recommendations.		
	3.10 Review implementation and controls over other LIBRARIAN features including LIB/AM, LIB/CCF, ELIPS, and other on-line interfaces.		

		W/P Ref.	Done By
5.0	Client-Server Application Change Control Procedures		
	Note: The industry is making progress in providing change control packages for client-server based systems (e.g., BindView's by-Control for SAP). This audit program should be adapted to non-mainframe change control packages as appropriate.		
	5.1 Review adequacy of change control procedures used for client-server based production applications. Evaluate version control maintenance controls.		
	5.2 As in Section 2.0 above, review source and production changes. Evaluate adherence to SPG change control, authorization, and documentation criteria.		
	5.3 Evaluate the security access privileges granted to programming personnel.		
6.0	Conclusion of Audit		
	6.1 Document any weaknesses or concerns noted during the audit and discuss with appropriate persons to validate your understanding.		
	6.2 Ensure that the audit objectives have been completely addressed and document the conclusions reached.		
	6.3 Ensure work papers are complete and cross-referenced especially in regard to the concerns noted.		
	6.4 Summarize findings and draft recommendations and discuss with audit management.		
	6.5 Arrange a closeout meeting with the auditee management to discuss findings and recommendations. Attempt to obtain auditee management concurrence for issues discussed. Document the issues discussed in memorandum form and file in workpapers.		
	6.6 Prepare a draft audit report and submit report and workpapers to audit manager for review. Obtain management responses for inclusion in the report.		
	6.7 Clear any review notes based on Audit manager's review of workpapers and report.		
	6.8 Issue the draft audit report to action persons, the IIS Audit coordinator, and appropriate management personnel.		
	6.9 Document proposed modifications to the audit program and/or points of interest for follow-up audit in the workpapers.		