

## XIII-2

# Auditing Systems Under Development

*Frederick Gallegos*

*Daniel P. Dow*

---

---

**T**he primary objective of a systems development audit is to ensure that internal controls outlined by systems personnel are adequate to protect the system's integrity. It is relatively easy to make changes to a system during the development process; after the system becomes operational, modifications may not be practical or economically feasible. Specific benefits that result from auditor involvement during the development phase include the following:

- System validity and reliability are monitored.
- Auditability of systems design and operation is ensured.
- Production of appropriate documentation also is ensured.
- Omissions, weaknesses, and anomalies in the development process are identified.
- Scheduling or budgetary problems are detected.
- Inappropriate or disregarded system specifications are identified.

Because systems developers, for the most part, object to having their work checked every step of the way, a practical approach for auditor involvement in the systems development process calls for reviews at key points in the development cycle. These key points and suggested levels of involvement are listed in Exhibit XIII-2-1. This chapter describes these review points and discusses the auditor's role at each.

### THE DEVELOPMENT PROCESS

Systems development can be categorized into three broad phases:

- Planning.
- Development.
- Implementation and operation.

A brief explanation of these phases follows.

#### Planning

The planning phase of systems development includes the following activities:

Review Point	Suggested Audit Involvement (%)
1. Project organization	1
2. Review of the present system	2
3. Conceptual design	2
4. Cost/benefit analysis	3
5. Project team formation	1
6. Output report design	5
7. Computer processing design	3
8. Equipment requirements	2
9. Data file documentation	3
10. Detailed system design	30
11. System development	3
12. Operations and user control	15
13. System testing	15
14. Conversion	15
<b>Total</b>	<b>100%</b>

Exhibit XIII-2-1. Key Review Points for a Systems Development Audit

- Needs analysis—A study is conducted to determine whether a new system should be developed.
- Review—The current system is evaluated.
- Conceptual design—The systems flow and other information illustrating how the new system will operate are prepared.
- Cost/benefit analysis—A detailed financial analysis is conducted to determine the cost to develop and operate the new system, the cost saving or additional expense that it will incur, and its projected return on investment.

### Development

The following activities take place during the development phase:

- Project team formation—The group of MIS personnel, users, and others who will design the new system is formed.
- Output report design—The reports to be generated by the system are described.
- Computer processing design—A detailed flowchart that shows how transactions will be processed through the computer is prepared.
- Equipment requirements—The equipment necessary for system operation is determined.

### Implementation and Operation

During system implementation and operation, the following activities occur:

- Data file documentation—A field-by-field listing of what will be con-

tained in each file and a listing of the values that can be contained in each field are prepared.

- Detailed system design—Specifications of the programs contained in the system are prepared.
- System development—The various programs, the job control language, and other software support needed by the system are coded and tested.
- Control procedures definition—Descriptions of system operation and the way in which the user will control the system once it is in operation are created. This activity includes training for operations and user personnel.
- System testing—In addition to the testing performed by MIS, users conduct acceptance testing and independent parties conduct other tests.
- Conversion—Data is transferred from the old to the new system.
- Operation and maintenance—Change control processes are implemented to monitor and evaluate any changes made to the system and to maintain the system's control integrity.

In reviewing these phases, the auditor examines critical control points: how controls are developed, implemented, and enforced throughout the key phases of the development cycle. The completion of each phase usually corresponds to the key point at which the auditor should perform a review.

The auditor's first step in the systems development review process is to determine the amount of time to be allocated to a particular development project. Once the total hours have been determined, they can be broken down as shown in Exhibit XIII-2-1. The auditor's next step is to develop a systems development audit plan that includes a schedule for the specific review points. Although these dates are only estimates, they ensure that audit resources are available when needed.

## **THE AUDITOR'S ROLE IN THE DEVELOPMENT CYCLE**

The auditor's role in the systems development process generally falls into two areas:

- Reviewing and evaluating the adequacy of controls over the systems development process.
- Reviewing and commenting on the auditability of the application being developed.

There is a definite correlation between a well-managed systems development process and a well-controlled automated application. The use of a proven systems development methodology increases the probability that the system's internal controls will be effective and reliable.

The responsibility for the auditability of new applications lies jointly with the user department, systems analysts, and programmers. The user department is responsible for specifying the application system controls; implementing these controls is the responsibility of the systems analysts and programmers. The auditor should interact with each of these groups during the development phase to determine the adequacy of auditability provisions. By becoming involved at strategic points, the auditor can, with a limited amount of effort, ensure an adequate control system.

### KEY REVIEW POINTS FOR AUDITORS

The review points listed in Exhibit XIII-2-1 represent checkpoints in the systems development process. Auditors use these checkpoints to determine both the status of the internal control system and the status of the development project itself. These reviews eliminate the necessity of devoting large amounts of audit resources to the development effort. As long as the development process is progressing to the auditor's satisfaction, the need for audit involvement is minimal. At each checkpoint, the auditor meets with the systems professionals to:

- Determine the accomplishments since the last review point.
- Review the questions on the review point questionnaire developed by the auditor.
- Verify and validate selected answers to questions asked by auditors.
- Determine the adequacy of the internal control system to date.
- Make a judgment on the status of the project.

After completing the review, the auditor makes appropriate recommendations. If problems arise, a meeting with management may be required. Before concluding the review, the auditor and systems personnel set a date for the next review (usually at the end of the next development phase).

### The Planning Phase

As shown in Exhibit XIII-2-1, the largest blocks of time are devoted to the detailed system design, operations and user control, system testing, and conversion phases. This does not mean, however, that the earlier development phases and their review points are less important. In fact, greater benefits can be realized by attention to these initial phases of the life cycle. In these phases, auditors should stress the following concerns:

- The need for control.
- The importance of risk evaluation.
- The cost-effectiveness factor in control design.
- The usefulness of sample control guidelines.
- The importance of user involvement.
- The importance of assigning control responsibilities.
- The importance of feedback mechanisms for evaluating controls.

In the early phases, auditors do not determine how controls will be implemented, but they should establish the need for considering these concerns. This effort helps MIS personnel understand audit objectives.

Another reason for the importance of the auditor's involvement in the planning phase is that at the end of this phase the organization determines whether a project should be continued. If a project is continued, it is unlikely that it will be terminated in the future. The decision to proceed is critical because the organization will commit a considerable amount of time and resources to the project. Budgets are usually increased and time schedules extended to allow for modifications and unforeseen circumstances. The auditor should be prepared to recommend that the project be delayed or terminated if the system of internal controls is inadequate, the project plan is not detailed enough, or resources are insufficient to implement the proposed system on time and within budget.

The following paragraphs discuss each of the review points of the planning phase.

**Project Organization—Review Point 1.** The auditor should determine whether all personnel who have an interest in the development project are also part of a study team that evaluates the competence of project team members. The purpose of this study team is not to eliminate members but to recommend the addition of new members who possess skills that the team may lack.

**Review of the Present System—Review Point 2.** An auditor who is not familiar with the current system should review the areas that the new system will affect or replace. This familiarizes the auditor with the strengths, weaknesses, and procedures of the existing system. The auditor should also review the project team's analysis of the current system. To assist the project team in its analysis, the auditor should provide copies of system-related audit reports.

**Conceptual Design—Review Point 3.** The conceptual design of the system describes the key elements of the final system as well as a methodology for controlling the development or operation of the system. It also determines the resources needed to implement these controls. The auditor should ensure that appropriate audit and control needs are considered and met in the conceptual design of the system.

**Cost/Benefit Analysis—Review Point 4.** The auditor should conduct an independent review to verify the accuracy of the project team's cost/benefit analysis. After implementation, it should be determined whether both the cost and benefit estimates have been met. Deviations from the original estimates should be explained and documented for reference in future projects.

### **The Systems Development Phase**

The four key checkpoints included in the systems development phase determine in detail what the system does. The system's framework and control objectives are established. Management, including user management, usually pays little attention to the system during the development phases. The auditor, however, should ensure that users are involved.

The auditor's primary concerns during the review of this phase are:

- Have adequate resources been allocated to complete the project?
- Have the user's needs been satisfied by the new system?
- Are the control objectives met through the design criteria?
- Are there adequate feedback mechanisms to verify that controls are functioning correctly?
- Does the systems development methodology provide feedback to management on issues requiring revision or correction?

The following paragraphs review the key control points in the systems development phase.

## AUDITING

**Project Team Formation—Review Point 5.** During this review, the auditor should determine whether all personnel affected by the development project are adequately represented on the project team. The auditor must have the opportunity to interact with the project team. This phase should be evaluated with the same criteria used during project organization (Review Point 1).

**Output Report Design—Review Point 6.** The auditor, as a system user, should determine the reports needed for audit purposes. The auditor must also determine whether users have requested the reports needed to control the system. Because a system's usefulness depends on the type of information it generates, output reports must be correct and complete. When evaluating system output, the auditor should be concerned with reports on the following:

- Error conditions.
- Control information.
- Override conditions.

In addition, the *usefulness* of report data to system users is a major concern of the auditor.

**Computer Processing Design—Review Point 7.** The auditor should verify that audit and control requirements have been taken into consideration in the design of the system. This includes determining whether:

- The control objectives can be met by the design.
- The user specifications are met by the design.
- The design is practical from the user's viewpoint.

**Equipment Requirements—Review Point 8.** The auditor should verify that the equipment allocated for this system will be used effectively and efficiently and should review any financial analysis prepared for the purchase of new equipment.

### The Implementation Phase

Most of the auditor's time—approximately 80%—is spent reviewing activities in this phase. During the implementation phase, the auditor's primary concerns are that:

- The system as implemented meets the system specifications and incorporates sound control objectives.
- The system is implemented on time and within budget.
- Adequate documentation has been developed at all required levels.
- Users have been adequately trained.
- Users are satisfied with the system as it is being implemented.
- Users are involved in the system testing process.
- The conversion system is adequately controlled.
- The system is auditable.
- There are adequate audit trails and backup facilities.

The following paragraphs discuss the key review points in the implementation phase.

**Data File Documentation—Review Point 9.** The accuracy and completeness of the system can be determined by its control of data input and storage. The auditor's objectives are to determine the contents of the data file for potential audit purposes and to provide an independent opinion as to the completeness of the data. Data controls usually include:

- Identifying types of data that can be included in a record.
- Determining the audits to be executed on the data.
- Establishing procedures for handling rejected data.
- Identifying who has responsibility for data input.
- Establishing the retention period for the data.
- Documenting how the data will be used and by whom.
- Assigning a security classification to the data.
- Analyzing the risk to the organization if the data is lost, compromised, or modified.
- Assigning a location for data storage.
- Identifying where the data will be used.

**Detailed System Design—Review Point 10.** The auditor is most heavily involved in the detailed system design. Here, the auditor must perform detailed analysis to verify that design and control objectives have been met and must review and specify the control requirements of the system. This is a difficult task because it requires negotiations with systems personnel to determine how controls can be installed to meet control requirements economically.

**System Development—Review Point 11.** The auditor must ensure that the system design and control specifications have not been changed. The programmers code and debug the system during this phase, and the auditor should be available to answer questions concerning the purpose and implementation of controls.

**Operations and User Control—Review Point 12.** The documentation needed by operations and users to use the system effectively and efficiently is generated at this stage. The auditor's primary function is to assist and advise in the development of procedures and methods that operations personnel and users can implement to determine whether the system is operating properly. Because the primary cause of system failure is the user's inability to use the system effectively, users must be provided with adequate system documentation.

**System Testing—Review Point 13.** The auditor should verify that test data is complete and adequate to ensure that the system is functioning properly and that the user is participating in the system test. At the end of system testing and before implementation, the auditor should provide management with an opinion on the system's adequacy.

**Conversion—Review Point 14.** The auditor should ensure that sufficient controls have been implemented to maintain the integrity of the system during the conversion process. During conversion, the auditor should verify that:



- The procedures usually followed in systems development are adhered to in developing conversion routines.
- Data controls are maintained during conversion.
- The conversion is judged successful before the new system accepts live data.

### System Evaluation, Certification, and Maintenance

When all development phases have been completed, the auditor should evaluate the system as a whole and issue an opinion to management as to whether the system should be put into production. This report should mention any deficiencies in the system that need to be corrected and should also explain the risk that the organization is taking by implementing the new system. It is important that all audit involvement in the development project be thoroughly documented in audit workpapers to support all of the auditor's findings and recommendations.

This set of audit documentation can be reused during maintenance to validate, verify, and test the impact of any changes made to the system. The system should periodically undergo a recertification process to ensure that control integrity remains intact. These certifications should continue until the system is discontinued or replaced.

### SUMMARY

The use of the review point technique is an effective and efficient method for auditing and monitoring the systems development process. Exhibit XIII-2-2 presents a checklist that facilitates the implementation and use of this methodology. The review point technique can be adapted to any standardized development methodology. If an organization does not use a standardized methodology, MIS management should see that one is established.

#### Recommended Reading

- Davis, G., Adams, D., and Schaller, C. *Auditing and EDP*. New York: AICPA, 1984.
- Davis, K., and Perry, B. *Auditing Computer Applications*. New York: John Wiley & Sons, 1982.
- EDP Auditors Foundation for Education and Research. *Control Objectives*. Carol Stream IL, 1983.
- FAIM Technical Library. "Audit Participation in System Design." *Auditing Computer Systems*.
- Fitzgerald, Jerry. *Designing Controls into Computerized Systems*. Jerry Fitzgerald and Associates, 1981.
- Gilhooley, Ian A. "Auditing System Development Mythology." *EDP Audit, Control and Security* (July 1984).
- Helms, G.L., and Weiss, I.R. "Auditor Involvement in the Systems Development Life Cycle." *The Internal Auditor* (December 1983).
- Mair, Wood, and Davis. *Computer Control and Audit*. Wellesley MA: OED Information Sciences, 1978.
- Pleier, Joseph R. "Documentation of the System Development Audit." *EDP Audit, Control and Security* (September 1982).
- US General Accounting Office. *Audit Guide for the Evaluation of Internal Controls*. Washington DC, 1981.



	Yes	No	Comments
<b>A. The Systems Development Process</b>			
1. Does the organization have a formal, management-controlled approach to systems development?			
2. Does the systems development process include the following steps: Definition of user needs? Conceptual system design? Feasibility study? Cost/benefit analysis? Detailed systems analysis and design? Programming? Testing? Procedure preparation? Conversion? System acceptance? Operations? Postimplementation audit?			
3. Are formal requests for new or revised systems prepared by users and submitted with proper authorization signatures?			
4. Is the conceptual design based on user needs?			
5. Is the conceptual design used to determine the technical and operational feasibility of the system?			
6. Is a cost/benefit analysis performed to ensure that the conceptual system will economically produce results?			
7. Were additional hardware or systems software needs considered in the cost/benefit analysis?			
8. Are any additional hardware or systems software requirements consistent with the organization's short- and long-range plans?			
9. Is the detailed system design consistent with the conceptual design, and is it based on the feasibility study and cost/benefit analysis?			
10. Was the detailed system design used to prepare computer programs?			
11. When all programming is completed, are the programs, interrelated subsystems, and the entire system thoroughly tested?			
<b>B. Documentation</b>			
1. Does the organization have standards for documenting various MIS functions?			
2. Has a project request document been prepared to provide the means for a user to request the development, procurement, or modification of software or other MIS-related services?			
3. Does the project request document include the following: A statement of objectives to be accomplished by the proposed project? A description of the service to be performed? The reason for the request?			

**Note:**

All responses should be indexed to appropriate supporting documents or records of interviews. Explain negative answers and identify alternate control procedures.

**Exhibit XIII-2-2. Checklist for a Systems Development Audit**

# AUDITING

	Yes	No	Comments
<p>A description of how the requested project relates to other systems?</p> <p>A statement on privacy and security considerations?</p> <p>A list of those functions that will be affected by the proposed project?</p> <p>A list of pertinent reference documents on the project?</p> <p>4. Has the project request document been annotated by the receiving organization with the following:</p> <p>The date the request was received?</p> <p>The individual assigned to investigate the request?</p> <p>The disposition of the request?</p> <p>An estimated cost for completing both a feasibility study or other analysis and the project as a whole?</p> <p>Any additional information (e.g., problems encountered or references to other pertinent information)?</p> <p>5. Has a feasibility study document been prepared to provide the following:</p> <p>An analysis of the objectives, requirements, and system concepts?</p> <p>An evaluation of alternative approaches?</p> <p>An identification of a proposed approach?</p> <p>6. Does the document include the following:</p> <p>A description of the proposed system's requirements?</p> <p>A statement of the proposed system's major performance objectives?</p> <p>An analysis of existing systems that currently address the proposed system's requirements and objectives?</p> <p>A detailed description of the proposed system?</p> <p>A discussion of alternative systems or approaches?</p> <p>The rationale for recommending the proposed system?</p> <p>A proposed schedule for system development?</p> <p>7. Has a cost/benefit analysis document been prepared to give managers, users, designers, and auditors adequate cost and benefit information from which to analyze and evaluate approaches?</p> <p>8. Does the document include the following:</p> <p>A description of alternative systems or approaches?</p> <p>The cost of development and operation of each alternative?</p> <p>The benefits associated with the development of each alternative?</p> <p>A comparative cost/benefit summary?</p> <p>Sensitivity analysis assessing the extent to which costs or benefits would be affected by changes in key factors?</p>			

Exhibit XIII-2-2. (Cont)

	Yes	No	Comments
9. Has a functional requirements document been prepared to provide a basic understanding between users and designers of the system?			
10. Does the document include:			
A statement of objectives to be met by the new computer-based system?			
A description of existing methods and procedures?			
A description of proposed methods and procedures?			
A summary of expected improvements?			
A summary of impacts?			
11. Has a user manual been developed that documents the functions of the computer-based system?			
12. Does this manual include:			
A narrative description of the computer-based system?			
A description or diagram of the computer-based operation?			
A description of the equipment needed to process the system?			
The structure and role of each system component?			
The performance capabilities of the system?			
A description of all data files used by the system?			
A description of input, flow of data through the processing cycle, and output?			
The step-by-step procedures required to initiate processing?			
The requirements for preparing and entering input data?			
The requirements relevant to each output (e.g., format and frequency)?			
A list of error codes or conditions generated by the system and the corrective actions to be taken by the user?			
The detailed instructions necessary to initiate, prepare, process, and receive a query applicable to the data base?			
13. Has an operations manual been developed that describes the computer-based system and its operational environment for computer operations personnel?			
14. Does this manual include:			
A diagram showing the input, output, data files, and sequence of operations of the computer-based system?			
An inventory of all programs included in the system?			
An inventory of each permanent file that is referenced, created, or updated by the system?			
A list of the various runs possible and a summary of each run's purpose?			
A description of the manner in which the system advances from one run to another to complete the entire run cycle?			
The job control statements needed for each run?			

Exhibit XIII-2-2. (Cont)

# AUDITING

	Yes	No	Comments
<p>Operator instructions for each run?</p> <p>The output reports for each run?</p> <p>The output reports that need to be reproduced by other means?</p> <p>The restart and recovery procedures for each run?</p> <p>Any emergency procedures?</p> <p>A description of procedures for running the computer-based system through remote devices?</p> <p>15. Does the operations manual exclude:</p> <p>Program logic charts or decision tables?</p> <p>Copies of program listings?</p> <p>16. Are program listings inaccessible to computer operations personnel?</p> <p>17. Are computer operations personnel denied access to other program and system documentation?</p> <p>18. Has a program maintenance manual been developed that gives the maintenance programmer sufficient information to understand the programs, their operating environment, and their maintenance procedures?</p> <p><b>C. Program Testing and System Acceptance</b></p> <p>1. Are all computer programs desk-checked by the programmer and supervisor before program assembly or compilation?</p> <p>2. Are all computer programs reviewed after assembly or compilation to ensure that errors disclosed by these translator routines are corrected?</p> <p>3. Is test data, not live data, used to test computer programs?</p> <p>4. Is each program and subsystem tested, followed by a test of the entire system?</p> <p>5. Is test data treated like live data, instead of carrying special codes to indicate it is not production data?</p> <p>6. Are sufficient volumes of test transactions having a wide range of valid and invalid conditions entered?</p> <p>7. Is sufficient time allocated for thorough testing?</p> <p>8. Have sufficient personnel been allocated for testing purposes?</p> <p>9. Are there test cases that evaluate the following:</p> <p>Mainline and end-of-job logic?</p> <p>Each routine?</p> <p>Each exception?</p> <p>Abnormal end-of-job conditions?</p> <p>Combinations of parameter cards and switch settings?</p> <p>Unusual mixtures and sequences of data?</p> <p>10. Does the test data include cases that test for the following types of valid conditions:</p> <p>Codes?</p> <p>Characters?</p> <p>Fields?</p> <p>Combinations of fields?</p> <p>Transactions?</p>			

Exhibit XIII-2-2. (Cont)

	Yes	No	Comments
Calculations? Missing data? Extraneous data? Amounts? Units? Composition? Logic decisions? Limit or reasonable checks? Sign? Record matches? Sequence? Check digit? Crossfooting of quantitative data? Control totals? Record mismatches?			
<b>D. Program Changes</b>			
1. Are computer programs revised only after written request by users and approval by user management?			
2. Do these written requests describe the proposed changes and reasons for them?			
3. Do these requests include security and privacy specifications?			
4. Is a change request form or other means of documentation used to originate program modifications?			
5. If so, are all change request forms sequentially numbered and accounted for?			
6. Are program modifications thoroughly tested to ensure that the modification functions properly?			
7. Are program modifications subjected to system acceptance before being placed in operation?			
8. Is there a limit on the number of times a program can be changed?			
9. Are departments that initiate changes in master files or program instructions furnished with a notice or other documentation showing changes actually made?			
10. Do users make the final decision on whether the modification meets their needs?			
11. Is program documentation changed to reflect program modifications?			
12. Is system documentation changed to reflect program modifications?			
13. Is operations documentation changed to reflect program modifications?			
14. Is user documentation changed to reflect program modifications?			
15. Are procedures in place to determine whether any other system is affected by the program modification?			
16. Does the volume of regularly scheduled program modifications indicate a problem with program procedures, or the computer-based system?			
17. Do computer operations personnel have a list of individuals to notify if a computer-based system requires an emergency or immediate modification?			

Exhibit XIII-2-2. (Cont)

## AUDITING

	Yes	No	Comments
18. Are individuals on the preceding list the only application programmers allowed in the computer room?			
19. Are outdated source programs deleted from the production source library?			
20. Are outdated load modules deleted from the executable load module library?			
21. Are job control statements that relate to outdated programs discarded?			
22. Is documentation that relates to outdated programs discarded?			
23. Is there a procedure to prevent suspended programs from being used?			
24. Is a special library used for source programs or executable load modules during the testing and system acceptance phases?			
25. Is an executable load module library used for production processing?			
26. Does the executable load module library keep track of such information as date, sequence, who made the change, and the change?			
27. Does the organization use automated methods (e.g., a program library systems software package) to restrict access to computer programs?			

Exhibit XIII-2-2. (Cont)