Information Systems: Auditing in an Automated Environment

OBJECTIVE

To ensure that automated information systems are managed, developed, and controlled effectively and efficiently in order to support the entity's mission by providing information for informed decision making and reporting.

BACKGROUND

Public and private organizations spend billions of dollars annually designing, constructing, and implementing automated information systems. Even organizations of modest size cannot operate today without support from information technology to streamline operations, improve services, and assist management in monitoring organizational performance (*Texas Lacks Effective Controls For Developing Automated Information Systems*, SAO Report No. 3-038, 1993).

In order to protect the investment in technology, processes must be in place to ensure that financial resources are used efficiently and effectively. Information systems should be carefully planned and guided. Implementing processes for project management, life-cycle development, and system controls will provide management with a means for making automated systems reliable and secure. In addition, *data* must be protected against unauthorized changes and access. Also, physical assets and property should be protected from unauthorized use or destruction.

[The Draft version of "How to Manage an Information Technology Project," written by the Department of Information Resources, was used for developing this module, except where other references are listed.]

DEFINITIONS

An **application** refers to a set of programs on a computer (such as a payroll system or accounting system) which support a particular business function or portion of a function.

Application controls are the controls designed for a specific automated information system application to help ensure that processed information is authorized, valid, complete, accurate, and timely. This category also includes requirements that ensure the system is secure and that an audit trail exists (Model Framework for Management Control Over Automated Information Systems, January 1988, Federal Government.).

Batch processing exists when inputs are captured and grouped in transactions files over a period of time, and these files are subsequently released to process and update application master files.

Controls are procedures or mechanisms used to protect assets, most notably data.

General controls are specific controls for developing, operating, managing, and assessing all automated information system applications. General controls include the organization's methods and procedures that apply to the overall computer operations in an agency (Model Framework, January 1988).

Information resources includes the procedures, equipment, and software that are designed, built, operated, and maintained to collect, record, process, store, retrieve, display, and transmit information, and associated personnel including consultants and contractors.

An **information system** is the combination of all communication methods in an organization (computers, telephones, personal contact). An information system collects, records, processes, stores, retrieves, and displays information. Its major purpose is to enable an organization to meet its mission. Major Information Resource" projects are subject to review by the Quality Assurance Team.

Major Information Resource projects are subject to review by the Quality Assurance Team. A Major Information Resource project is defined as an automation project whose development costs are over $1 million and either:

- has a development schedule of 1 year or more,
- involves more than one agency or governmental unit, or
- materially alters the work methods of agency personnel or delivery of services.

On-line batch processing exists when inputs are entered on-line (usually with some automated editing) to create a transaction file which is used to update application master files within a short period of time.

Post-implementation evaluations are reviews of computer systems after the system has been adequately tested and implemented for the organization's use. These reviews general focus on 1) inputs to the system, 2) processing by the system, and 3) outputs from the system.

Programmers write sets of related instructions (referred to as programs) that perform operations or tasks. Applications programmers write specific, task-oriented programs designed to satisfy particular user needs. Systems programmers write programs needed for a computer system to function. Programmers often work from program specifications developed by systems analysts. These specifications serve as a blueprint for program design.

The Quality Assurance Team (QAT) is composed of representatives from the Department of Information Resources and the State Auditor's Office. The team is responsible for approving major information resources projects (Quality Assurance Review Guide for Major Information Resources Projects, November, 1996).

Real-time or interactive processing exists when inputs are entered and immediately update or access the application master files.

Systems analysts develop program specifications for a project to guide programmers. Systems analysts define project information requirements, user requirements, and necessary system functions. They focus more on the design of a system and what it will do rather than on operational programming details.

A **system design development methodology** (SDDM) is a set of procedures intended to aid systems analysts, programmers, and users in creating and maintaining a computer application. It should guide the information system staff through needs analysis to design, development, testing, implementation, and maintenance. Frequently, these are purchased or "canned" packages, but some are internally developed. Some are also automated. (System Development Life Cycle Methodology is a synonymous term, but

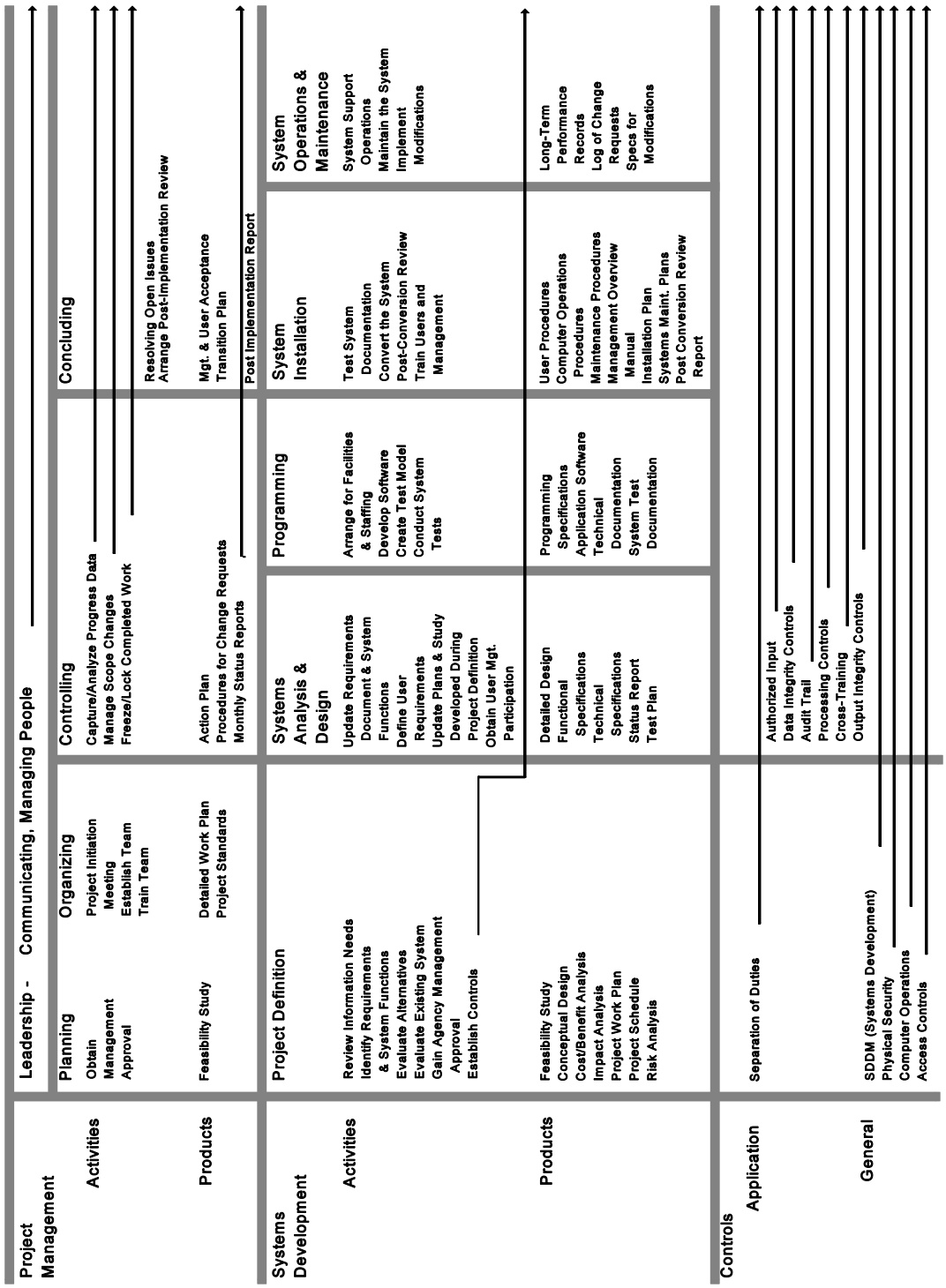
the acronym "SDLC" also identifies a telecommunications protocol and is not used here, to avoid confusion.)

OVERVIEW OF THE PROCESS

The principal steps in the process of managing the deployment of automated information technology are as follows:

- **Develop an understanding of the agency and its programs to identify automation opportunities.** (See the module on Managing Information for additional information.)
- **Establish an effective project management process.**
- **Implement an effective system design development methodology.**
- **Ensure that appropriate controls are built into the system to protect the investment.**

The table on the following page illustrates how the project management process relates to the phases of the system design development methodology and control functions.


Developing Automated Information Systems
Project Management
Leadership - Communicating, Managing People
Activities
Planning
Obtain Management Approval
Organizing
Project Initiation Meeting
Establish Team
Train Team
Controlling
Capture/Analyze Progress Data
Manage Scope Changes
Freeze/Lock Completed Work
Concluding
Resolving Open Issues
Arrange Post-Implementation Review
Products
Feasibility Study
Detailed Work Plan
Project Standards
Action Plan
Procedures for Change Requests
Monthly Status Reports
Mgt. & User Acceptance
Transition Plan
Post Implementation Report
Systems Development
Activities
Project Definition
Review Information Needs
Identify Requirements & System Functions
Evaluate Alternatives
Evaluate Existing System
Gain Agency Management Approval
Establish Controls
Systems Analysis & Design
Update Requirements Document & System Functions
Define User Requirements
Update Plans & Study Developed During Project Definition
Obtain User Mgt. Participation
Programming
Arrange for Facilities & Staffing
Develop Software
Create Test Model
Conduct System Tests
System Installation
Test System Documentation
Convert the System
Post-Conversion Review
Train Users and Management
System Operations & Maintenance
System Support Operations
Maintain the System
Implement Modifications
Products
Feasibility Study
Conceptual Design
Cost/Benefit Analysis
Impact Analysis
Project Work Plan
Project Schedule
Risk Analysis
Detailed Design Functional Specifications
Technical Specifications
Status Report
Test Plan
Programming Specifications
Application Software
Technical Documentation
System Test Documentation
User Procedures
Computer Operations Procedures
Maintenance Procedures
Management Overview Manual
Installation Plan
Systems Maint. Plans
Post Conversion Review Report
Long-Term Performance Records
Log of Change Requests
Specs for Modifications
Controls
Application
Separation of Duties
Authorized Input
Data Integrity Controls
Audit Trail
Processing Controls
Cross-Training
Output Integrity Controls
General
SDDM (Systems Development)
Physical Security
Computer Operations
Access Controls

PROCEDURES

The suggested procedures listed below are grouped into two categories; **Review Criteria** and **Assess Condition**. Project management should be tailored to the major issues identified while evaluating the agency's system of information management.

Review Criteria:

General criteria

The following are general criteria for a successful automated information system:

To be considered successful, the system must:

- satisfy the business needs of users
- be completed on schedule
- be completed within budget
- meet established standards

Specific criteria

The specific criteria related to the requirements for managing automated information are as follows:

I. Establish an effective project management process.
Project management entails five basic activities:

- planning
- organizing
- controlling
- leading
- concluding

A. **Planning** takes place before the beginning of the project. The planning process revolves around reviewing, confirming, and refining the feasibility study. The principal object of project planning is to ensure the project gets off to a good start.

- The feasibility study is a report which details the cost, benefits, schedule, and budget for the project. A good feasibility study should also:
  - serve to verify the content of the original needs analysis before beginning the project
  - estimate the level of effort required
  - quantify and detail assumptions made about the project
  - provide a baseline for initiating changes
  - serve as a basis for evaluating project results

- As the project progresses, the project manager should review and refine the initial assumptions and estimates to update the feasibility study. There should be checkpoints during the project to determine if the project should proceed based on revised estimates and assumptions There should be checkpoints during the project to determine if the project

should proceed or be changed based upon the updated estimates and assumptions.

- The final step in project planning is to obtain **management approval** to proceed with the project. The approval process should ensure that management, users, and team members understand and accept the scope and approach of the project.

B. **Organizing** the project should include developing the detailed project work plan, defining project standards, establishing project initiation, and training the team. Proper organization will contribute significantly to smooth operation of the team and the overall success of the project. Additional criteria for successful project organization are detailed as follows:

- The project's organizational structure should be well defined with responsibilities and lines of authority clearly stated.

- People with the necessary programmatic knowledge and technical skills should be assigned to the project team. Different people will be needed at different times. At various stages/phases of the project, people with various different skill sets will be needed on the project.
- A work plan outlining the work to be performed at the appropriate level of detail, the people assigned to each task, and the specific milestones and products that should be completed. Detail Planning is an on-going function as the project progresses. Initial tasks should be well defined. However, depending on the length of the project, major tasks that occur toward the end of a project may be scheduled, but have little detail.

- Project standards and formats should be defined. These standards relate to such activities as time reporting, expense control, review procedures and documentation.

- A Project Kick-off Meeting should be conducted as a forum for briefing the project team and ensuring that team members are committed to and understand the project.

- Project team training should be conducted during the organizational phase.

C. **Controlling the Project** is the most challenging project management responsibility. Controlling the project is time-consuming and often difficult. The process itself involves capturing progress data, preparing project control reports, developing an action plan, and managing project scope changes. The ultimate goal is to produce a

"successful" automation project. Criteria for effective project control are as follows:

- Project control should be an iterative process continuing throughout as the plan and organization of the project are adjusted.
- The project manager should have timely and accurate information to control the project schedule, budget, performance, and direction.
- The project manager should be engaged in the following activities:
  - capturing progress data
  - analyzing and interpreting variances from the budget and work plan
  - preparing project control reports
  - analyzing risks and developing action plans which highlight potential problems and propose remedial actions
  - identifying issues and problem resolution/elevation
  - issuing status reports with progress on milestones/issues
  - managing project scope changes by
    - establishing procedures for handling change requests
    - recognizing and controlling unapproved scope changes
    - freezing or "locking" completed project work from further changes
    - identifying and responding to deviations from the work plan and identifying and addressing changing needs

D. **Leading the project**, although less tangible than planning, organizing, and controlling the project, is essential to the role of project manager. In fact, it may be the most significant management function. The way the project manager communicates with people involved in the project can create a spirit of cooperation and teamwork that is essential to the project's success.

- Effective project leadership includes coordinating and running successful meetings. The following Meeting Matrix can be used as a guideline for determining the type and frequency of meetings to be held during the project.

Meeting Matrix

Meeting	Purpose	When	Who Attends
Project Steering Status	Keep management informed of progress on problems.	Monthly	Steering committee members *
Project Team Status	Keep efforts coordinated. Develop/Refine action plan.	Weekly	Team members
User	Update users. Discuss proposed changes. Gain input from users. Obtain sign-off on completed work.	Frequently	Representatives of user groups
Ad Hoc	Resolve/refer urgent problems.	As needed	Team members
Walk-through	Critique completed work for functional/technical requirements and technical quality.	As work is completed	Team members
Sign-off	Document management/user acceptance of the system.	Project conclusion	Management and users

***** The Steering Committee should include the upper management of the organization as well as the MIS executive/director.

- Leading the project also involves managing people. Effective management of people on a project should include the following:
  - motivating team members
  - delegating and assigning work
  - recognizing good work
  - improving poor performance

E. **Concluding the project** is much more than just stopping the work. It represents the most important milestone of the project: all segments of the system have been completed and frozen, and now the transition from the current project to any future projects begins. Criteria for a successful project conclusion should include the following:

- All open issues should be resolved or deferred.
- Acceptance tests should be successfully completed, verifying that management and users accept the system.
- A transition plan should be implemented.
- Post-implementation evaluation should be arranged.

II. Implement an effective system development methodology.

An information technology project is triggered by the needs of the agency. Once initiated, a successful project usually proceeds through a system life cycle development process comprised of five overlapping phases. Each phase has specific objectives, major activities, key products, and critical success factors. The phases build upon each other to ensure that the system will meet the agency's needs. Even though the phase name may vary, the major activities and the key products generally remain the same.

In general, the requirement for moving from one phase of the system development process to the next is user and management approval of the key products of the completed phase.

The five phases of the traditional (or "waterfall") system development process are:

- **project definition**
- **system analysis and design**
- **programming**
- **system installation**
- **system operations and maintenance**

In very large projects it is not unusual to see phases 2, 3 and 4 being worked on simultaneously. The main requirement is that a given module or set of programs will proceed like a waterfall down through the phases.

Another system development process that is sometimes used is called the iterative or prototyping methodology. This process contains the same basic phases. However, this process is marked by a module or group of programs moving back and forth between system analysis and design and programming. A major characteristic of this process is users are asked questions and then a "prototype" is built. The user then tries out the prototype and is asked additional questions. Based upon this another prototype is constructed (or major enhancements are made to the first prototype). This iteration continues until the user's needs are satisfied.

A. The focus of the **project definition phase** is needs assessment. The business needs of the agency, the needs of the users, and the needs of the project team to complete the project must all be determined.

In the State's information technology environment, the basic mechanism for project definition is the feasibility study which, in turn, is initiated through the agency's information management planning process. Most project definition activities are completed during the feasibility study process. Therefore, the focus of project planning during system development is on refining and updating the feasibility study.

During the project definition phase, the entity should:

- Identify and describe major information requirements and functions of the system.

- Ensure that the information system resulting from the project supports program objectives.
- Evaluate system alternatives based on cost/benefit, risk, and impact analyses.
- Obtain project approval from agency management.
- Establish plans for developing and implementing the system.
- Establish effective project controls.

Signals of problems with the project planning from SAO Report No. 3-038 are listed beginning on page 31.

More specific tasks which should be completed during this phase are as follows:

- Agency information needs should be reviewed.
- High-level evaluation of the existing system should be performed.
- High-level design for proposed system should be developed.
- Resource requirements should be refined.
- Documentation of a feasibility study performed to assess the implications of a proposed information technology project including refinement of system cost/benefit and risk analyses should be completed.
- Project work plan and high-level project schedule should be refined.

B. Once the feasibility study for the project has been approved and any necessary refinement completed, system development continues with the **system analysis and design phase**. This phase builds on the high-level information gathered and refined during the project definition phase. In system analysis and design, the team further defines the agency's information requirements, user requirements, and necessary system functions.

System analysis and design is a very critical phase in the project. Errors corrected early in the project cost considerably less in terms of time, money, and effort than those discovered and corrected during later phases of the project.

During the system analysis and design phase, the entity should:

- Ensure that the proposed system will meet user needs and expectations.
- Ensure that program management understands and accepts the design.
- Further define the program's information requirements and the system's functional specifications.

- Establish organizational and management structures to ensure successful development of the system.

Other more specific tasks which should be completed during this phase are as follows:

- User and management participation should be solicited.
- User requirements should be defined.
- Performance requirements should be determined.
- Hardware and system software needs should be determined.
- Cost/benefit analysis should be adjusted as needed.
- High-level system design should be expanded.
- Detailed system design should be completed.
- Test plans should be defined and developed.

By the conclusion of this phase of system development, several key deliverables should be completed:

- functional specifications - a complete model of the system as the user will view it
- technical specifications - a detailed description of software and hardware requirements
- detailed system design - a comprehensive blueprint for the proposed system, how it will function and what it will do
- system analysis and design management report - a status report of the system analysis and design phase
- test plan - a detailed plan for meeting the acceptance criteria and ensuring that the product meets functional and technical specifications

Signals of problems occurring in the systems analysis and design phase from SAO Report No. 3-038 are listed beginning on page 33.

C. Once system analysis and design has been completed, it is time to begin the **programming phase**, which focuses on the creation or development of the application software. Having completed documentation of the detailed design in the prior phase, the project team will begin creation of program code for the reports, screens, forms, files, data bases, and records described in the detailed design. During this phase, it is essential to document program specifications, with emphasis on coordination among team members. Planning and conducting the system test will also take place during the programming phase.

During the programming phase, the entity should:

- Plan and arrange for adequate facilities and realistic staffing.
- Develop an accurate, reliable, maintainable system that meets the needs reflected in the detailed design.
- Develop technical documentation.
- Create a test plan.
- Conduct unit, integration, and system test(s).

At the conclusion of the programming phase, the following key deliverables should be completed:

- software - programs that are accurate, reliable, and fully tested
- technical documentation - thorough documentation of system software and hardware
- system test documentation - specifications and results of system testing

Signals of problems from SAO Report No. 3-038 are listed beginning on page 31.

D. The **system installation phase** focuses on the work required to transform the newly developed system into a fully operational system. To ensure that the implemented system will be fully operational and accepted by the users and management, the project manager must determine that physical resources are complete and ready for conversion, users are trained so that they understand and can use the system, procedures are documented, the data is converted, and system performance is reviewed after it has been operational for a significant period of time.

The system installation phase includes what may be one of the largest tasks of the project - the system conversion. Every detail essential for the system's operation must be ready on time. Therefore, the primary management function is to control the project by continually monitoring project activity and progress.

During the system installation phase, the entity should:

- Convert data and introduce users to the new system.
- Prepare user personnel and management for implementation of the new system.
- Establish organizational and management structures to ensure the successful continuing operation of the system.

- Establish and document sound procedures for using, operating, and maintaining the system.
- Perform user acceptance test the system.
- Identify and document possible future system enhancements.

At the conclusion of the system installation phase, the following deliverables should be completed:

- installation plan - schedule and resources required for installation of the system, including site preparation and site testing
- updated system documentation - includes user procedures, computer operation procedures, maintenance procedures, and a management overview of the system
- training materials - tutorials and procedures for system operations and maintenance
- plans for ongoing system maintenance and training - description of requirements for maintaining the system and ongoing training
- post-conversion review report - report of results of system installation and conversion

Signals of problems from SAO Report No. 3-038 are listed beginning on page 31.

E. In the State's information technology environment, the system development process concludes with the completion of the system installation phase. The **system operations and maintenance phase** consists of the activities required for continued operation and ongoing maintenance of the operational system. During this phase, changes to the system are implemented as the agency's programs evolve and its information needs change.

System operations activities assist users on a day-to-day basis, handle operational emergencies, and analyze system performance and usage. System maintenance activities analyze, prioritize, implement, and control all changes to the system. Each change requires a mini-implementation phase, involving testing, coordinating necessary physical resources, preparing users, converting changes, updating documentation, and performing a post-conversion review.

During the system operations and maintenance phase, the entity should:

- Operate and maintain the implemented system in a manner that is cost-effective and meets the needs of the users.

- Identify and control all potential changes to the system.
- Provide management control over the cost, timetable, and sequence of changes made to the system.
- Ensure that changes are properly and effectively implemented.
- Assess the quality of the structure and performance of the system to assist in future information management planning.

Other more specific tasks which should be completed during this phase are as follows:

- System operations should be supported. This may involve:
  - user assistance
  - responding to emergencies
  - monitoring system performance factors
  - analyzing computer resource usage
  - training personnel

- The system should be maintained and enhanced.
  - investigate and initiate change requests
  - prioritize changes to the system
  - develop implementation schedule for system changes

Since this phase is ongoing, the following deliverables should be continuously produced:

- performance records - monthly and yearly data on system performance factors, such as on-line functions, adequacy of reports, response time, ease of operation, and level of support
- log of change requests and schedule of system modifications - record of proposed system changes and implementation schedule for approved changes
- system specifications for modifications - functional and technical description of approved system changes
- implemented modifications - installed system changes

Signals of problems from SAO Report No. 3-038 are listed beginning on page 31.

III. Ensure that appropriate controls are built into the system to protect the investment.

A. **General controls** are the structure, methods, and procedures that apply to the overall computer operations in the entity. They provide a control environment affecting the applications being processed. The entity must ensure that:

- Controls are in place to achieve specific management and business objectives.
- Controls have been designed according to management direction and known legal requirements.
- Controls are operating effectively to provide reliability of, and security over, the data being processed.

General controls ensure that information and information resources are protected against unauthorized changes, use, or destruction. Use of information systems should also be carefully planned and guided. The management of these functions is critical when the entity depends on information systems. Information and information resources residing in the various agencies of state government are strategic assets belonging to the people of Texas that must be managed as valuable state resources [Art. 4413 (32j), Section 1 (a) (1)].

General controls are categorized into organizational and management controls, security controls, and systems software and hardware controls. These controls tend to operate dependently with each other and can be classified as preventive, detective, and corrective control techniques, depending on where or how they are used in a process or system.

Preventive controls exist to stop errors from occurring. An example would be separation of duties reduces the likelihood of collusion occurring. Preventive controls usually are general types of controls exercised at early stages in the flow of data through a computer system.

Detective controls identify errors after they have occurred. An example would be an input validation routine that identifies data that falls outside an allowable range of values. Detective controls tend to be specific types of controls exercised at later stages in the flow of data through a computer system.

Corrective controls attempt to ensure that errors identified are corrected. An example would be controls that write data mis-matches to a suspense file and issue reminders if

they are not removed from the file, corrected and re-entered into the system. Once an error has been detected, some type of corrective control is always necessary. However, corrective controls also must be subject to detective controls since errors may occur once again in the error correction process.

Organizational and management controls

Organizational and management controls will help ensure that the organization's objectives are achieved and that errors or irregular acts are prevented or detected. The entity must ensure that:

- Responsibilities and accountability for planning, managing, and controlling the functions of the data processing organization are clearly assigned.
- Personnel are qualified and adequately trained and supervised.
- Duties are properly separated.

Systems software and hardware controls

Systems software and hardware controls protect the computer systems. Systems software and hardware controls are classified as detective controls. These controls identify and report expected errors as they occur. If preventive controls fail or are bypassed, detective controls can provide management reports when specific pre-determined thresholds have been reached or processing errors start to occur. Detective controls allows management to implement corrective or preventive controls after an undesirable event has been detected. The entity should ensure that:

- Procedures are in place to ensure that the systems software and hardware are functioning properly.
- Procedures exist to detect errors and make appropriate authorized corrective actions.
- Procedures are in place to recover loss data due to accidental or intentional destruction.

Examples of system and hardware controls:

- The wrong file is accessed by a program and the system software prevents processing and notifies the computer console;
- The tape drive malfunctions. The tape drive notifies the computer operator on the computer console so that corrective actions can be taken.

Following are the Control Procedures for General Controls included on the Internal Control Structure Questionnaires (ICSQ) developed by the State Auditor's Office for data processing audits specific to these areas mentioned above. Further detail is included on the ICSQs.

Computer Operations

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

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

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

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

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. (This plan should be in conformity with the *Guidelines for Contingency Planning for Information Resources Services Resumption* published by the Department of Information Resources on January 19, 1994.)

CONTROL POLICY #6 - There are methods which aid in processing recovery in the event of abnormal program termination.

Security controls

Security controls help ensure that only authorized persons are granted access to the computer system for authorized purposes. Security controls are generally classified as preventive controls, however, some would be classified as detective. These preventive control techniques keep undesirable events from occurring and are implemented through automated procedures to prohibit unauthorized system access. The entity should ensure that:

- Controls over the computer programs, data files, telecommunications network, and input and

output materials are in place. Controls include physical access to the computer system.

Examples of security controls include:

- restriction of user overrides
- requirements for passwords before accessing system or entering data
- cardkey protected entrance to data center

Following are the Control Procedures for General Controls included on the Internal Control Structure Questionnaires (ICSQ) developed by the State Auditor's Office for data processing audits specific to areas under security controls. Further detail is included on the ICSQs.

Physical Security

CONTROL POLICY #1 - The responsibility for physical security is assigned.

CONTROL POLICY #2 - Physical access to the computer room, libraries, and building is restricted to authorized persons.

CONTROL POLICY #3 - Data processing resources are protected from fire, water, and other potential hazards.

Access

Access controls are contingent upon the organization having already assigned a person to be responsible for access security and that the organization's data has been classified as to the level of security required. (These access controls should be in conformance with the *Information Resources Security and Risk Management Policy Standards, and Guidelines* published by the Department of Information Resources in March 1994**.)**

CONTROL POLICY #1 - There are written policies for security over access to automated resources.

CONTROL POLICY #2 - Access to systems software is controlled.

CONTROL POLICY #3 - Access to production programs is controlled.

CONTROL POLICY #4 - Access to production data files is controlled.

CONTROL POLICY #5 - Access to on-line systems is restricted to authorized individuals.

CONTROL POLICY #6 - Access to the data base is adequately controlled.

CONTROL POLICY #7 - There are procedures for the assigning, monitoring, and deleting of passwords.

B. **Application controls** are methods and procedures designed for each application (system) to ensure the authority of data origination, the accuracy of data input, integrity of processing, and verification and distribution of output. Controls are specific to the flow of transactions and are designed to prevent, detect, and correct errors as transactions flow and are processed through the system.

Applications should be managed in such a way that the functions of an application from start to finish are protected from unauthorized changes, corruption, and theft. The major functions of an application include documentation, input, processing, and output. Data integrity and protection of assets are the goals of these functions. Changes should be made only through appropriate management and user authorization.

Application controls should be in place to ensure the:

- completeness of inputs
- accuracy of inputs
- validity and authorization of inputs
- verification and proper distribution of output

Completeness of Inputs

For each transaction type, control techniques should be in place to ensure transactions were accepted and recorded completely.

Examples of control techniques are:

- computer matching with previously processed data
- agreement of established batch control totals
- rejection reports or online rejection

These control techniques ensure that:

- all rejected transactions were reported
- each transaction was accepted and processed only once

- duplicate transactions were reported

Following are the Control Procedures for Application Controls included on the Internal Control Structure Questionnaires (ICSQ) developed by the State Auditor's Office for data processing audits specific to this area. Further detail is included on the ICSQs.

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

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).

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

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

Accuracy of inputs

For each transaction type, control techniques should be in place to ensure that the proper data fields were accurately processed by these transactions. These controls consist of:

- batch totals with manual follow-up for differences
- edit checks on inputs performed by the system (e.g. validity checks, reasonableness checks, limit checks, existence checks)
- computer matching with manual follow-up for unmatched items
- one-for-one transaction checking

Following are the Control Procedures for Application Controls included on the Internal Control Structure Questionnaires (ICSQ) developed by the State Auditor's Office for data processing audits specific to this area. Further detail is included on the ICSQs.

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

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).

Validity and authorization of inputs

For each transaction type, control techniques should be in place to prevent or detect the processing of unauthorized transactions. These controls ensure data integrity and reliability. Examples of control techniques include:

- review and approval of the transaction by a responsible individual
- segregation of duties for data entry and corrections
- security software to restrict access to the particular applications or screens within an application

Following are the Control Procedures for Application Controls included on the Internal Control Structure Questionnaires (ICSQ) developed by the State Auditor's Office for data processing audits specific to this area. Further detail is included on the ICSQs.

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

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

Verification and proper distribution of output

For each input, output control techniques should be in place which provides assurance that the results of input processing are reported. Examples of output control techniques include:

- hardcopy reports for distribution
- file output to interface with other systems
- on-line data inquiry

These output control techniques ensure that:

- a complete audit trail is in place
- tracking of transactions from its source to end-of-file processing is available
- the audit trail allows tracing in either direction

Following are the Control Procedures for Application Controls included on the Internal Control Structure Questionnaires (ICSQ)

developed by the State Auditor's Office for data processing audits specific to this area. Further detail is included on the ICSQs.

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.

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

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

Assess Condition:

Determine the actual process used

Conduct interviews, observe operations, and identify and collect available documentation in order to gain an understanding of the entity's actual process and controls for managing automated information systems. Possible procedures include, but are not limited to:

- Determine where the responsibility for managing automated information systems resides in the entity, who participates in the process, and how the participants are selected.
- Obtain and review any manuals, policies, and forms that document how information technology is managed, including the relationship of information technology to entity goals, objectives, strategies, and plans.
- Determine if and how management consciously selects and employs the assumptions, criteria, methods, processes, and techniques used in automated systems development. Obtain and review available documentation on the assessment of risks, costs, and benefits.
- Review an inventory and configuration of information systems within the entity.
- Compare information resources expenditures to those of similar agencies using reports from the statewide accounting system.
- Review plans for personnel, hardware, software, and training.
- Review the make-up of the steering committee.
- Review information resources training activities for information systems personnel as well as users.

In addition to gaining an understanding of the actual process, also try to find out:

- whether executive management and the users perceive the management of Information Services as effective or not
- what parts of the process they see as successful or unsuccessful and why
- what they think is important about the process and why

This information may help identify causes and barriers.

Determine the strengths and weaknesses of the actual process

Using the tailored criteria, the understanding of the entity's process gained above and the procedures in this section, analyze the actual process to determine if it:

- is designed to accomplish the management objective(s)
- has controls that provide reasonable assurance that the process will work as intended
- is implemented and functioning as designed
- is actually achieving the desired management objective(s)

Suggested procedures for each of these four analysis steps are detailed below. In executing these procedures, remember to identify and analyze both strengths and weaknesses.

Identify and review the steps in the actual process to determine if the management of automated information systems is designed to accomplish the management objective(s). Possible procedures include, but are not limited to:

- Determine if all major steps in the criteria are included in the actual process. If steps are missing, determine if the absence is likely to have a materially negative effect on managing automated information systems at the entity you are reviewing.
- Determine if all the steps in the process appear to add value. If there are steps that do not appear to add value, try to get additional information on why they are included in the process.
- Review the order of the steps in the process to determine if it promotes productivity.
- Review the level of technology used in the process to determine if it is up-to-date and appropriate to the task. Besides computer, electronic, communications, and other mechanical technology, you should also consider what kinds of management techniques are used (Gantt charts, process maps, decision matrices, etc.). See the appendix to the module on problem-solving and decision-making for more information.

- Determine the adequacy of tactical planning and management for information systems.

- Determine the adequacy of planning for application software implementation. Determine the extent of project management.

- Determine if the steering committee has been meeting and making significant decisions.
- Determine the adequacy of progress or evaluation reporting.
- For major information system users, obtain any available documentation on user satisfaction with current systems.
- Determine the operational service effectiveness and efficiency by examining:
  - mainframe operations: down time, response time, job turnaround, preventive maintenance, necessity of shifts, and waste of supplies

- network: adequacy of support/assistance and down time
- maintenance of software: backlogs, prioritized lists, and timeliness
- procurement practices: right types of goods, low cost, quick deployment and maximizing use (see procurement module)
- help desk: problem tracking and resolution, expertise, and analysis of trends
- staffing: skills to match need, quantity, contractors managed, appropriate assignments, and turnover (see human resources module)
- training practices: policy, goals, cost, required skills are supported, records, and computer literacy of users (see human resources module)
- control reviews: general and application

Identify the controls over the process to determine if they provide reasonable assurance that the process will work as intended. These controls should be appropriate, placed at the right point(s) in the process, timely, and cost effective. Possible procedures include, but are not limited to:

- Draw or obtain a picture of the automated information management process, the controls, and the control objectives. (See page 13 of the Introduction for an example.) Flowcharts of the process can help identify inputs, processes, and outputs.
- Determine if the control objectives are in alignment with the overall management objective(s) (this module, page 1).
- Identify the critical points of the process (i.e., those parts of the process most likely to determine its success or failure or expose the entity to high levels of risk) and the controls related to them. Consider whether the controls are:
  - in the right location within the process (input, operations, output)
  - timely (real time, same day, weekly, etc.)
- Compare the cost of the control(s) to the risk being controlled to determine if the cost is worth the benefit.
- Determine what controls are in place for monitoring and evaluating the overall effectiveness of the automated information management process and making sure that changes are made in the process if it does not yield the desired results.
- Identify, describe, and assess the process used to gather input from employees who might reasonably discover flaws in the process.

Review observations, interviews, documentation, and other evidence and design specific audit procedures as needed to determine if the process and/or the controls have been implemented and are functioning as designed. Depending upon the objectives of the project, these procedures may include both tests of controls and substantive tests.

(More information can be found in *The Hub*, pp. 2-B-8, ff.) Possible procedures include, but are not limited to:

- Administer the Internal Control Structure Questionnaire for general control or for application controls (See the SAO EDP Specialist Team.)
- Determine if any evidence of management override exists.
- Walk through the actual process, i.e., follow a transaction through the people and documents involved, and compare to the official process.

Review and analyze any reports used by the entity to monitor the outcome(s) of the automated information management process and/or any other information available to determine if the process is actually achieving the desired management objective(s) (this module, page 1). Possible procedures include, but are not limited to:

- Analyze these process reports over time for trends.
- Discuss any apparently material negative or positive trends with management.
- Determine if and how management acts upon these trend reports and what changes, if any, were made in the process or controls as a result. Some process refinements, especially those affecting entity mission, goals, and outcome measures, may need to wait until the next appropriations cycle.

Determine causes

Determine what circumstances, if any, caused the identified weaknesses in the automated information management process. Possible procedures include, but are not limited to:

- Determine if the participants in the automated information management process understand the entity's mission, goals, and values and support them through their management of information.
- Determine if the participants understand both the purpose of and their role in the automated information management process.
- Determine if the relationship between the automated information management process and other entity processes is clear.
- If the process occurs at multiple locations, determine the nature and scope of the communication and coordination among them.
- Determine if the automated information management process has adequate human, dollar, time, information, and asset resources. If they appear inadequate, determine if entity resources have been allocated according to the materiality of the automated information management process relative to other entity processes.
- Determine if the entity has considered using alternative resources such as industry associations, non-profit organizations, academic institutions, or other governmental entities to meet its resource needs.

- Determine if resources available to the automated information management process have been allocated and used in a manner consistent with the importance of that resource to the process.
- If there are negative trends in the reports used to monitor the outcome(s) of the automated information management process, determine if these reports are communicated to and used by the appropriate parties to modify the process.

Determine what internal or external constraints or barriers, if any, must be removed in order to overcome these identified weaknesses. Possible procedures include, but are not limited to:

- Review the applicable entity, state, or federal laws or regulations to determine if any of them prevent the necessary changes from being made in the automated information management process.
- Determine if any key employees are unwilling to change the process and why they are unwilling.

Determine effect

Compare the actual entity process to a recommended alternative process(es) and determine if each weakness in the entity process is material. Alternatives can be developed by using the criteria contained in this module, applying general management principles to the process, using the processes at comparable entities, etc. Materiality can be measured by comparing the dollar cost, impact on services (either quantity or quality), impact on citizens, impact on the economy, risks, etc., of the actual process to the recommended alternative process(es). Possible procedures include, but are not limited to:

- Identify performance benchmarks (industry standards, historical internal data, other comparable entities, etc.) for the process in question and compare to actual performance. Measure the difference, if possible. Include the cost of the additional controls or changes in the process.
- Estimate the cost of the actual process and the alternative process(es) and compare.
- Estimate the quantity and/or quality of services provided by the actual process and by the alternative process(es) and compare.
- Identify the risks associated with the actual process and with the alternative process(es). Measure and compare the risks.

Develop recommendations

Develop specific recommendations to correct the weaknesses identified as material in the previous section. In developing these recommendations, consider the tailored criteria, kind of process and control weaknesses identified, causes and barriers, effects, and additional resources listed at the end of this module. Possible procedures include, but are not limited to:

- Identify alternative solutions used by other entities.
- Identify solutions for removing barriers.
- Provide general guidelines as to the objectives each solution should meet; then the entity can tailor the solution to its specific situation.

- Provide specific information, if available, on how each recommendation can be implemented.

RESOURCES

Articles

Davenport, Thomas, et al. "How Executives Can Shape Their Company's Information Systems" *Harvard Business Review* (March-April 1989).
Location: Methodology Information Resource Folders

Elam, Joyce, The University of Texas. *Guidelines for an IS Measurement Program in State Agencies*, submitted to the State Auditor's Office, (August 24, 1990).
Location: Methodology Information Resource Folders

Meeting the Government's Technology Challenge, Results of a GAO Symposium, United States General Accounting Office, February 1990.
Location: Methodology Information Resource Folders

Poschmann, Andrew W. "Management Reporting," *SCORE (STRUCTURED COMPANY OPERATIONAL REVIEW AND EVALUATION)*, 1985.
Location: Methodology Information Resource Folders

Shatsoff, Paul. "Managing with Information," *Open Forum* (a quarterly publication of the New York State Forum for Information Resource Management) (October 1990).
Location: Methodology Information Resource Folders

Wold, Geoffrey H. "Information Systems Planning," *Government Finance Review* (June 1989).
Location: Methodology Information Resource Folders

Books

American Institute of Certified Public Accountants, Computer Services Executive Committee, *Computer Assisted Audit Techniques.*
Location: SAO Library

Burkan, Wayne C., *Executive Information Systems; From Proposal through Implementation*, Van Nostrand Reinhold, N.Y., 1991.
Location: The University of Texas, Perry-Casteñada Library (T58.6 B874 1991)

Caudle, Sharon and Donald A. Marchand, *Managing Information Resources: New Directions in State Government*, School of Information Studies, Syracuse University (August 1989).
Location: The University of Texas Law Library, Microfiche (JK 2445 A8 M36 1989, 1-4)

Comptroller of Public Accounts, Texas Performance Review, *Against the Grain.*

Location: SAO Library

Department of Information Resources. *How to Manage an Information Technology Project*.
Location: Methodology Project Information Resource Folders

Department of Information Resources. *Instructions for the Entity Plans for Information Resources Management, Fiscal Years 1991-1995*
Location: Methodology Project Information Resource Folders

Department of Information Resources. *Security Guidelines*
Location: Patricia Perry-Williams or Angela Rodin's offices

Department of Information Resources, *State Strategic Plan for Information Resources Management*.
Location: SAO Central Files

EDP Auditing, Auerbach Publications, 1992.
Location: SAO Library

Gleim, Irvin N., *Third Edition CIA Examination Review*, vol 1, Chapter 6.
Location: Methodology Project Information Resource Folders

Institute of Internal Auditors Research Foundation, *Systems Auditability and Control, (SAC)*, (ongoing).
Location: Methodology Project Information Resource Folders

Nelson, James, Editor, *Gateways to Comprehensive State Information Policy*. Published by the Chief Officers of State Library Agencies through The Council of State Governments, Lexington, Kentucky (October 1988).
Location: The University of Texas, Perry-Casteñada Library (T58.64 G37)

United States General Accounting Office, *Assessing the Reliability of Computer-Processed Data*, GAO Publications.
Location: SAO Library

Thierauf, Robert J., *Executive Information Systems: A Guide for Senior Management and MIS Professionals*, Quorum Books, N.Y., 1991.
Location: The University of Texas, Perry-Casteñada Library (T58.6 T47 1991)

Treadway Commission, Committee of Sponsoring Organizations of the Treadway Commission, *Internal Control-Integrated Framework*, September 1992.
Location: Methodology Project Information Resource Folders

Watne, Donald A. and Peter B.B. Turney, *Auditing EDP Systems*, Prentice-Hall, Inc., New Jersey, 1984.

Location: The University of Texas, Perry-Casteñada Library (HF 5548.35 W37 1984)

Weber, Ron, *EDP Auditing: Conceptual Foundations and Practice*, McGraw-Hill, New York, 1st edition, 1982.
Location: Angela Rodin's Bookshelf

Weber, Ron, *EDP Auditing: Conceptual Foundations and Practice*, McGraw-Hill, New York, 2nd edition, 1988.
Location: The University of Texas, Perry-Casteñada Library (QA 76.9 A93 W43 1988)

Data Bases

Uniform Statewide Accounting System (USAS)
Human Resource Information System (HRIS)
Uniform Statewide Payroll System (USPS)
Automated Budget and Evaluation System for Texas (ABEST)
Public Education Information Management System (PEIMS)
State Real Property Inventory Data Base
Boards and Commissions System
Statewide EDP Application Risk Assessment
Higher Education Data Base
Statewide Consolidation
Agency Profile
Cash Management System
Statewide Property Inventory Data Base

Periodicals

"Datapro Reports," Datapro Research, monthly
Location: Department of Information Resources Library (475-4728)

"DIR Tech Times," Department of Information Resources, bimonthly
Location: Department of Information Resources Library (475-4728)

"EDPACS," Auerbach Publishers, monthly
Location: Department of Information Resources Library (475-4728)

"IS Audit and Control Journal" (formerly "The EDP Auditor Journal"), Information Systems Audit and Control Association (EDP Auditors Association), quarterly
Location: Department of Information Resources Library (475-4728)

Professional Associations

Information Systems Audit and Control Association (EDP Auditors Association), Rolling Meadows, IL, 708-253-1545

SAO Report # 3-038 Signals of Problems

By understanding some of the common risks to developing cost-effective information systems, these obstacles can be monitored. As a result, development methods will be improved. The risks discussed are derived from research conducted on the topic of information systems. Developers and reviewers can use this list to detect early signals of system development efforts going awry.

Obstacles to project planning

- There is a lack of senior management support
- Long-range planning for information technology is not part of the Long-Range Planning Cycle. Managers are often short-sighted and do not plan for information technology beyond the next budget cycle.
- Systems do not fit in with the organization's long-term business plans.
- Decisions to initiate and/or continue a project are not made by the developing organization.
- Project managers often focus on the needs of their individual areas rather than the organization's larger mission and goals.
- The focus is on technical solutions rather than the basic purposes and uses of the information system.
- The system is not flexible enough to meet the business needs for which it was designed.
- Systems are developed without inter-agency/intra-agency coordination.
- All systems affected by the new development have not been identified.
- Affected parties are numerous and have diverse needs and expectations.
- A noncooperative environment exists between parties involved in the design.
- Alternatives are limited to simply automating existing processes and procedures, instead of streamlining operations.
- The system is trying to automate processes that have not worked manually.

- Large systems are developed instead of breaking down tasks into smaller modules.
- Projections of system response times have not been made or validated.
- There is no long-term strategy that transcends personnel changes.
- Personnel and equipment resources are inadequate.
- Systems under development and existing systems cannot share data or work together.
- There are problems with the currency and reliability of the data for the system.
- Checks for data accuracy are not included in the design.
- The technology is new or new to the developers.
- Systems under development will become obsolete because of other planned hardware or software changes.
- The hardware is obsolete, and the vendor no longer manufactures spare parts.
- The software is obsolete, and the vendor no longer supports maintenance for it.
- There are no procedures for disaster recovery.
- Security measures have not been taken to prevent unauthorized use of the automated system.

- There are no plans for:
  - logic flow diagrams
  - data flow diagrams
  - output design
  - system conversion
  - system operations
  - oversight
- There is no system documentation, such as
  - needs statement
  - feasibility
  - cost/benefit analysis
  - system decision paper
  - system requirements
  - project budget
  - project schedule
- The original design and each major change in the system is not supported by a feasibility study and cost/benefit analysis.

<u>Factors that lead to ineffective project control</u>

- Project management skills or experience are inadequate.
- There are frequent changes in personnel on the project.
- Projects are moving targets: changing scope, requirements, and specifications.
- Project meetings are not held regularly.
- There are no clearly defined stages in the project that can be used by management as decision points to determine whether to continue the project.
- Original project deadlines were not reasonable.
- The project schedule and budget are not monitored.

- Product development exceeds the allotted time and budget.
- There is a lack of effective oversight for information resources development.
- Senior management approval is required for all system decisions.
- Problems identified during system development are not corrected.
- Task lists and task schedules have not been prepared, or the tasks have not been described in detail.
- Critical steps (e.g. testing) are skipped to meet the deadline.
- There is no parallel processing of old and new systems during conversion.
- There is inadequate documentation detailing the work performed.
- Agency personnel did not participate in development performed by contractors.

Identifiers of ineffective system design and development methodology

- There is no system design and development methodology, or the existing methodology is not utilized.
- There is inadequate definition of the system's requirements.
- System design is not traceable back to system requirements and tends to further diverge from the requirements throughout the project.
- The computer code does not reflect the system design.
- Documentation is nonexistent or incomplete.
- There are no standards for development and documentation.

Signs of inadequate user involvement

- Users' needs do not dictate how technology is used.
- The focus is on internal operational needs, with little regard for the needs of the customers.
- Information systems are limited by what the data processing department can handle, not based on what the users need.
- There is a lack of communication between users and data processing personnel.
- Users are not required to approve changes to tasks or requirements.
- The users, data processing department, and accounting department are not in agreement with the cost/benefit analysis.
- All affected parties are not involved in the development process through a Data Processing Steering Committee or other means.
- There is a tendency to rely on the users' perceived demands of the past, not on the reality of both the present and the future.
- Users are not adequately trained to use the automated systems.
- There are no formal procedures for users' requests.

Indicators of incomplete or inadequate testing

- There are no test plans to ensure that all system requirements are tested.
- Testing efforts fall victim to schedule constraints.
- Users are not involved in testing.
- Testing and production data are not maintained separately.