

GUIDELINE 3613.01

The following Information Systems Auditing Standards have been adopted by the DISC Bureau of Information Resource Management, and apply to all State agencies effective June 30, 2000. They have been reformatted and edited slightly for presentation here. To view the original, go to <http://da.state.ks.us/disc/pubs/guidelines/G3613.01.html>.

PURPOSE: To publicize existing audit standards and describe their application to state information systems development activities.

BACKGROUND: In 1992 DISC published guidelines for safeguarding the integrity of computer systems. These guidelines incorporated the general and applications control objectives published by the EDP Auditor's Foundation. The Foundation is now known as the Information Systems and Audit Controls Association. The guideline updates the previous guideline published in 1992 and adopts ISACA's new control objectives as the state standard. These objectives are similar to the ones promulgated by the Foundation in 1990. The EDP Auditors Foundation (EDPAF) is the internationally recognized standards setting body in this area. EDPAF has published Control Objectives (September 2000) to provide standards. The publication is available from the EDP Auditors Foundation, P.O. Box 88180, Carol Stream, Illinois 60188-0180, (708)-682-1200, and costs \$49.95 plus \$3.00 shipping.

Control Objectives standards embrace development systems. DISC has adopted the following selected standards. As resources and interest permit, the state may adopt more standards, and may audit against them. While the standards are for major systems development, they are be useful, in part, to development of small(er) systems, projects, and telecommunications activities.

Agencies should recognize that other entities have interests in this area, such as the Division of Legislative Post Audit and the federal Department of Health and Human Services (which audits state agencies for the federal government). These and similar external entities will most likely pattern their audit activities around these same standards. Therefore, agencies should structure their information systems development and management activities in concert with these standards.

Adopted standards are below in regular type. *Italicized* material is explanatory or structural.

GUIDELINE: The following standards are adopted:

Planning

To assure it contributes to the agency's successful realization of overall goals, the information technology (IT) function should have long and short range plans. The plans should be consistent with the agency's broader plans for attaining agency goals.

Long Range Planning for the Agency - The IT function's long range plans should address issues pertinent to its contribution to the agency's achievement of its long range goals. The agency's senior management should be involved in the development of the IT function's long range plan. This involvement of top management should ensure the IT function's plan is integrated into the agency's overall plan.

Planning or Steering Committee for the IT function – The agency's senior management should appoint a planning or steering committee to oversee IT function activities. Committee membership should include representatives from senior management, the IT function, and user department management.

Long Range Planning for the IT function - Long range plans for the IT function should be consistent with,

and integrated into, senior management's long range plans. Long range plans for the IT function should recognize organizational goals, organization changes, technological advances, and regulatory requirements.

Short Range Planning for the IT function – Senior management's short range plans for the IT function should ensure that appropriate IT function resources are allocated on a basis consistent with the overall agency's short range plans.

Policies, Standards, and Procedures

Policies, standards, and procedures should exist to serve as a basis for management planning, control, and evaluation of IT function activities.

Policies - Senior management's policy directives defining the relationship between the IT function and user departments should be developed and communicated to all those affected by them.

Standards - Standards governing the acquisition of IT function resources; the design, development, and modification of information systems; and the operation of the IT function should be defined, coordinated, maintained, and communicated to all affected personnel.

Procedures - Procedures describing the manner and responsibilities for performance governing relations between the IT function and user departments should be established, coordinated, maintained, and communicated to all affected departments.

Organizational Responsibilities and Personnel Management

The IT function should be sufficiently important in the agency hierarchy to enable it to meet its established overall objective and to promote its operational independence from user departments. Sound personnel management techniques should be employed to promote effective use of the IT function's human resources and to facilitate performance evaluation within the IT function.

Segregation of duties - Senior management should provide for segregation of duties within the IT function, such as between systems development and operations, operations and data control, and data base administration and system development.

External Requirements

External requirements relevant to agency goals and plans and responsibilities and activities of the IT function should be considered.

External Requirements - In planning for the work of the agency and the IT function, external requirements related to computer system practices and controls (for example in the areas of maintenance, operations, accounting, and privacy) and to the manner in which computers, programs, and data are used should be considered. Special attention should be given these issues in those functions which historically have been regulated closely.

Information System Development, Acquisition, and Maintenance Controls

System Development Life Cycle Methodology and Responsibility

The process followed in the development, acquisition, and maintenance of information systems should attempt to achieve system effectiveness, economy and efficiency, data integrity, resource safeguarding, and compliance with laws and regulations. The use of an effective system development methodology should provide senior management with a reasonable assurance that these objectives will be achieved.

Systems Development Life Cycle Methodology - The agency's senior management should issue a written policy statement establishing a system development life cycle methodology as a means for structuring and controlling the process of developing or acquiring computerized information systems.

Roles and Responsibilities - The systems development life cycle methodology adopted by the agency should establish the roles and responsibilities of the IT function, user departments, and others for planning, developing, reviewing, implementing, and auditing the end product of the system development process.

Updating the System Development Life Cycle - The system development life cycle methodology used by the agency should be reviewed periodically by the agency's senior management to ensure its provisions reflect current generally accepted techniques and procedures.

Project Initiation

An agency's system development life cycle methodology should provide for user department involvement in identifying the general nature and scope of a system development project. The information requirements to be satisfied by the new or modified system should be defined carefully in written form and the development of a proposed system should be approved before the development process begins.

Project Definition - The agency's system development life cycle methodology should provide for creation of a clearly stated written definition of the nature and scope of every system development project before project work begins.

User Department Participation in Project Initiation – The agency's system development life cycle methodology should provide for participation by the affected user department management in the definition and authorization of an information system development or modification project.

Project Team Membership and Responsibilities - The agency's systems development life cycle methodology should specify the basis for assigning individual staff members to project team membership and define the responsibilities of the various team members.

Definition of Information Requirements - The agency's systems development life cycle methodology should provide that the information needs to be satisfied by the existing and the proposed new or modified system should be defined clearly before a development or modification project is approved.

Project Approval - The agency's systems development life cycle methodology should provide for the approval by designated members of management of the work done in each phase of the cycle before work on the next phase begins.

Feasibility Study

The agency's systems development life cycle methodology should provide, for each proposed project, that a technological feasibility study be prepared in which alternative means for reaching the project's goals are formulated along with a cost-benefit analysis of each alternative being considered. Among the issues to be considered are the possibility of a null alternative and the feasibility of a make or buy decision. If a decision is made to proceed with work on the proposed project, a project master plan should be issued in writing.

Formulation of Alternative Courses of Action - The agency's systems development life cycle methodology should provide for the analysis of the alternative courses of action that will satisfy the information requirements established for a proposed new or modified information system.

Technology Feasibility Study - The agency's systems development life cycle methodology should provide for an examination of the technological feasibility of each alternative for satisfying the information

requirements established for the development of a proposed new or modified information system.

Economic Feasibility Study - The agency's systems development life cycle methodology should provide, in each proposed information system development or modification project, for an analysis of the costs and benefits associated with each alternative being considered for satisfying the information requirements established for the project.

Risk Analysis Report - The agency's systems development life cycle methodology should provide, in each proposed information system development or modification project, for an analysis of the security risks, internal controls needed, and the feasible safeguards for reducing or eliminating the vulnerabilities.

Project Approval - The agency's systems development life cycle methodology should provide, in each proposed information system development or modification project, for the agency's senior management to review the reports of the relevant feasibility studies, its decision on whether to recommend the project, and its identification of one of the alternatives examined in these studies as a basis for the project team's work. The life cycle methodology is an integral part of ITEC's project management standards.

Project Master Plan - The agency's systems development life cycle methodology should provide, for each approved project, that a project master plan be created which is adequate for maintaining control over the project throughout its life.

Cost Monitoring - The agency's systems development life cycle methodology should provide, for each approved information system development or modification project, that a project master plan be created which includes a method of monitoring the costs incurred throughout the life of the project.

Design Phase

The agency's system development life cycle methodology should provide, for each information system development or modification project, that the system requirements are incorporated adequately into the specifications for the design of the system. A design methodology should be used to structure the development of input, output, file, and processing specifications which describe the physical solution to the system requirements. This design methodology also should be used to specify the source documents, control mechanisms, security features, and audit trails to be included in the system.

Design Methodology - The agency's systems development life cycle methodology should provide that an appropriate procedure be selected for creating the design specifications for each information system development or modification project.

Output Requirements Definition and Documentation – The agency's systems development life cycle methodology should provide that an appropriate procedure be selected for creating the output requirements for each information system development or modification project.

Input Requirement Definition and Documentation – The agency's systems development life cycle methodology should provide that an appropriate procedure be selected for creating the input requirements for each information system development or modification project.

File Requirement Definition and Documentation - The agency's systems development life cycle methodology should provide that an appropriate procedure be selected for defining the file format and organization requirements for each information system development or modification project.

Processing Requirement Definition and Documentation – The agency's systems development life cycle methodology should provide that an appropriate procedure be selected for defining the data processing step requirements for each information system development or modification project.

Program Specifications - The agency's systems development life cycle methodology should require that detailed written program specifications be prepared for each information system development or modification project.

Source Data Collection Design - The agency's systems development life cycle methodology should require that adequate mechanisms for the entry of information be specified for each information system development or modification project.

Controls and Security Design - The agency's systems development life cycle methodology should require that adequate mechanisms for assuring the integrity of the data stored and processed by an information system and for safeguarding the systems resources be specified for each information system development or modification project.

Audit Trails Design - The agency's systems development life cycle methodology should require that adequate mechanisms for audit trails be specified for each information system development or modification project.

Design Approval - The agency's systems development life cycle methodology should require that the design specifications for all information system development or modification projects be reviewed and approved by the management of the IT function, the affected user departments, the agency's senior management, and Kansas Information Technology Office for Executive Branch CITO approval, when appropriate.

Program Documentation Standards - The agency's systems development life cycle methodology should incorporate standards for program documentation that have been approved by the IT function planning or steering committee, communicated to the staff of the IT function, and enforced to ensure that documentation created during information system development or modification projects conforms to these standards.

Validation, Verification, and Test Plan - The agency's systems development life cycle methodology should require that a validation, verification, and test plan be created for each information system development or modification project.

Development and Implementation

An agency's systems development life cycle methodology should provide, for each information system development or modification project, that the programming objectives should be established for the project and responsibilities for the actual programming be assigned, the system manuals be prepared, the program and system testing standards be defined, the system validation and acceptance criteria be created, and the acceptance of the system by the management of the affected user departments be secured.

Programming Objectives - The agency's systems development life cycle methodology should require that a written statement of the programming objectives to be realized be created for every information system development or modification project.

Program Narrative Description - The agency's systems development life cycle methodology should require that a written narrative of the programming logic employed within the project, be created for every information system development or modification project.

Application Software Packages - The agency's systems development life cycle methodology should require that the availability be determined for commercial software packages that satisfy the needs of a particular information system development or modification project. The commercial software packages should be compatible with existing IT function operations before the IT function's staff is assigned to do any programming related to these projects. Software product acquisition procedures should follow the state's

procurement policies, and these products should be tested and reviewed prior to their being used and paid for.

Contract Application Programming - The agency's systems development life cycle methodology should provide that the procurement of contract programming services be justified with a written request for service from a project manager. (The end products of completed contract programming services should be tested and reviewed by the IT function's quality assurance group before payment for the work and the end product of it is authorized).

Operations and Maintenance Manual - The agency's systems development life cycle methodology should provide that adequate operations and maintenance manuals be prepared as a part of every information system development or modification project.

User Manual - The agency's systems development life cycle methodology should require that adequate user manuals be prepared as a part of every information system development or modification project.

Training Plan - The agency's systems development life cycle methodology should require that adequate plans for training the staff of the affected user departments and the IT functions operations and maintenance groups be prepared as a part of every information system development or modification project.

Program Testing Standards - The agency's systems development life cycle methodology should provide standards for the testing and implementation of the software created as a part of every information system development or modification project.

System Testing Standards - The agency's systems development life cycle methodology should provide standards for the testing of the system itself as a part of every information system development or modification project.

System Testing Documentation - The agency's systems development life cycle methodology should provide, as a part of every information system development or modification project, that the results of testing of the system be included in the written record of the project team's activities.

Evaluation of Test Results - The agency's systems development life cycle methodology should provide, as a part of every information system development or modification project, that the results of testing of the system be evaluated and approved by the management of the affected user departments and the IT function.

Conversion Plan - The agency's systems development life cycle methodology should provide, as a part of every information system development or modification project, that a plan be developed for converting the system from development to production.

Parallel Testing - The agency's systems development life cycle methodology should define the circumstances under which a parallel testing of both existing and new systems will be conducted and should specify the criteria for terminating the testing process.

Final Acceptance Test - The agency's systems development life cycle methodology should provide, as a part of the final acceptance of quality assurance testing of every information system development or modification project, for an evaluation of the test results by the management of the affected user departments and the IT function.

Operation and Maintenance

The agency's systems development life cycle methodology should provide, as a part of every information system development or modification project, that operation and maintenance procedures be established that assure that data is processed consistently and accurately and that system content will be modified only with

proper authorization.

Operations Control Procedures - The agency's systems development life cycle methodology should provide, as a part of every information system development or modification project, that adequate procedures have been installed for controlling the data processing activities.

Cost Monitoring - The agency's accounting system routinely should record, analyze, and report the costs associated with the operation of a new information system.

System Modifications - The agency's system development life cycle methodology should establish procedures for monitoring and controlling changes to all operational information systems.

Re-evaluation of User Requirements - The agency's system development life cycle methodology should provide for the periodic review of the user requirements for specific information systems to determine whether and how those requirements may have changed.

Post-Implementation Review

An agency's system development life cycle methodology should provide for a comprehensive review, after the information system has been implemented, of each development or modification project to assure that the effort produced a system that meets user needs and stated objectives, is realizing anticipated benefits, and adheres to the requirements of the methodology.

Post-implementation Review Plan - The agency's system development life cycle methodology should provide, as an integral part of the project team's activities, for the development of a plan for a post-implementation review of every new or modified information system.

Results Evaluation - The agency's system development life cycle methodology should require that a post-implementation review of an operational information system assess whether that system's objectives are being achieved.

Evaluation of Meeting User Requirements - The agency's system development life cycle methodology should require that a post-implementation review of an operational information system assess whether that user's needs are being achieved by the system.

Evaluation of Cost-benefit Analysis - The agency's system development life cycle methodology should require that a post-implementation review of an operational information system assess whether the system's cost effectiveness conforms to the original costs and benefits projected for it.

Evaluation of Adherence to Development Standards - The agency's system development life cycle methodology should require that a post-implementation review of an operational information system assess whether the project team adhered to the provision of the methodology.

Reporting Post-Implementation Review Findings - The agency's system development life cycle methodology should require that the results of a post-implementation review of an operational information system be submitted to the management of the user departments affected by the system and to the management of the agency's IT function.