

Management Systems Consulting, Inc.

Information Systems Auditing Standards

Control Objectives standards embrace all transaction based processing systems. MSC, Inc. has adopted the following selected standards. As resources and interest permit, the Client may adopt more standards, and may audit against them. While the standards are targeted to address major systems, they are useful when addressing smaller systems, projects, and network based activities.

Planning

To assure it contributes to the Client'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 Client's broader plans for attaining Client goals.

Long Range Planning for the Client - The IT function's long range plans should address issues pertinent to its contribution to the Client's achievement of its long range goals. The Client'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 Client's overall plan.

Planning or Steering Committee for IT functions – The Client'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 Client'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

Management Systems Consulting, Inc.

The IT function should be sufficiently important in the Client 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 Client goals and plans and responsibilities and activities of the IT function should be considered.

External Requirements - In planning for the work of the Client 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 Client'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 Client 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 Client should be reviewed periodically by the Client's senior management to ensure its provisions reflect current generally accepted techniques and procedures.

Project Initiation

A Client'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.

Management Systems Consulting, Inc.

Project Definition - The Client'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 Client'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 Client'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 Client'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 Client'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 Client'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 Client'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 Client'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 Client'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 Client'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 Client's systems development life cycle methodology should provide, in each proposed information system development or modification project, for the Client'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

Management Systems Consulting, Inc.

as a basis for the project team's work. The life cycle methodology is an integral part of project management standards.

Project Master Plan - The Client'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 Client'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 Client'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 Client'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 Client'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 Client'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 Client'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 Client'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 Client'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 Client'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.

Management Systems Consulting, Inc.

Controls and Security Design - The Client'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 Client'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 Client'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 Client's senior management, and Kansas Information Technology Office for Executive Branch CITO approval, when appropriate.

Program Documentation Standards - The Client'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 Client'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 Client'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 Client'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 Client'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 Client'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 Client's procurement policies, and these products should be tested and reviewed prior to their being used and paid for.

Contract Application Programming - The Client'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

Management Systems Consulting, Inc.

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 Client'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 Client'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 Client'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 Client'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 Client'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 Client'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 Client'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 Client'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 Client'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 Client'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 Client'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.

Management Systems Consulting, Inc.

Operations Control Procedures - The Client'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 Client's accounting system routinely should record, analyze, and report the costs associated with the operation of a new information system.

System Modifications - The Client'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 Client'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 Client'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 Client'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 Client'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 Client'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 Client'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 Client'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 Client'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 Client's IT function.