Treasury Board Of Canada Office Of The Comptroller General

Series 500 Guide 507

Guide To The Audit Systems Under Development

Internal Audit Handbook

Volume III

Internal Audit Guides

Working Draft

March 1991

The Office of the Comptroller General (OCG) is an organization which provides bilingual services. please feel free to address your enquiries in the language of your choice.

Prepared on behalf of Treasury Board of Canada Comptroller General Interdepartmental Advisory Committee on Internal Audit

Ottawa, Ontario

K1A 1E4

Table of Contents

Preface

This guide is a product of the:

> Office of the Comptroller General
>
> Audit and Review Branch

It draws on the documents mentioned herein and on the experience and ideas of the following participants:

- Administrative Policy Branch, TBS

- Informatics and Management Audits Branch, Government Consulting and Audit Agency, Audit Services Group

- Financial Management Information and Systems Branch, OCG

- Management Audit and Evaluation, Public Works Canada

- Director General Audit, National Defence

- Internal Audit and Evaluation, Revenue Canada-Taxation

Introduction

Background

In late 1983, owing to the importance of the early output of the Task Force on Informatics, the Office of the Comptroller General decided to suspend publication of the preliminary version of this "Guide to the Audit of Systems Development Performance". The Task Force, established by Treasury Board on July 7, 1983, was expected to require 12 to 18 months to complete their job. During that period, however, a Policy Interpretation Notice (PIN) 1984-03 ("Pre-implementation Audit") was issued. That PIN defines the purpose and scope of this Guide.

The Task Force issued their report in 1985 and on July 22, 1986, an Information Management Policy Overview draft was issued by the Administrative Policy Branch of the Treasury Board Secretariat, partly in response to that Report. All these documents, while portraying the tremendous technological changes in the field of systems development, also underline the importance of the PIN's instructions about auditing systems development. The PIN states:

> "Pre-implementation audits should be undertaken for all major systems under development in departments and agencies; they should be reflected in the departmental/agency internal audit policies and plans; and the potential loss of auditors' objectivity can be minimized through appropriate terms of reference and a suitable assignment strategy".

It is in the belief that management control over systems under development through the audit process is important that this Exposure Draft is offered.

Purpose of Guide

This Guide is written for the senior internal auditor conducting a Systems Under Development (SUD) Audit. A SUD Audit is defined as:

> "A review and evaluation, at various stages in the systems development life cycle, of a selected system or large scale enhancement to an existing application. The audit includes a review of compliance with specified aspects of a department's systems development process and a review of the controls being built into the system to ensure completeness, accuracy, security, proper authorization and auditability of the data being processed."

The auditor should know that Information Technology audits, in addition to reviewing systems under development, can also evaluate the computer centre, post-implementation, on-going system, data dictionary, end user computing, data security, data management, Information Technology procurement, Information Technology management and any other type of audit project that may have an impact on issues that fall within a SUD audit. The preceeding are not objectives, they are areas for study. An audit of systems under development will examine the following (see PIN 1984-03):

1. The project management and systems development process.
2. Products reflect the control framework being designed in conjunction with (surrounding), or as an integral part of, the system under design.

Organization

In Chapter 1, we discuss the environment surrounding systems development in today's Public Service.

Chapter 2 provides a description and model of the systems development life cycle and the roles and responsibilities of the main players.

Chapter 3 set out objectives and criteria for conducting a SUD audit with reference to control, economy, efficiency, and operational effectiveness in each stage of the process. The chapter deals first with the five major activities of audit and how those activities relate to each of the seven system development life cycle stages. Each of the subsequent sections of chapter three then deals with project, data integrity, and systems management control objectives at each stage of the life cycle.

Appendix A contains a grid of suggested interviewees for each Detailed Criteria. Appendices B through H contain detailed criteria for each Systems Development Life Cycle Stage from Initiation through to Post-Implementation.

Finally, there is a bibliography in Appendix I, and a TB Policies and Standards listing in Appendix J.

The Value of the Systems Development Process

As stated in Policy Interpretation Notice 1984-3 on Pre-Implementation Audit:

> "systems development projects are notorious for cost/time overruns; implemented systems are equally notorious for not meeting all user requirements; systems, particularly EDP systems, often have under-designed control frameworks; and recent cost-reduction programs ... have focused increased attention on improving the productivity/efficiency of all processes. This puts the

spotlight particularly on the systems development process because of the costly down-stream effects of inadequate design and implementation."

When the investment in systems development and the dependence of departments on systems to manage and deliver their programs are both considered, the advantage of an early warning to management of any inadequacies in the systems development is clear. To this end, the existence of a formal departmental systems development life cycle provides essential standards for establishing management control over specific projects or major enhancements.

Reporting of the Audit of Systems Development

A SUD audit must take place as the system is being developed, not after the system has been implemented. In addition, the sooner the project developer is aware of audit findings, the easier it is for remedial action to take place. It is also axiomatic that solutions, to design or project management weaknesses, are more efficiently implemented the earlier, in the development process, that audit is involved.

In view of this, "Special Reporting Considerations" presents some detail methodology early in Chapter 3 (see figure 1).

Special Considerations

Auditing systems under development is different, from On-going and Post-implementation system's audit, in that one may "revisit" the same system's development up to seven times. Thus, much of the audit work accomplished in early stages of the development process becomes ground work for auditing in the later stages of development. Chapter 3 is written with this aspect in mind.

Figure 1: The Cost of Change

```
┌─────────────────────────────────────────────────┐
│                THE COST OF CHANGE                 │
├─────────────────────────────────────────────────┤
│  Relative Cost of              Place when error   │
│  Correcting Error              is detected        │
│                                                   │
│                ┌──────────────┐                   │
│                │            ╱ │                   │
│    1,000       │           ╱  │    Maintenance    │
│                │          ╱   │                   │
│                │         ╱    │    Program         │
│     100        │        ╱     │    Testing         │
│                │       ╱      │                    │
│                │      ╱       │                    │
│                │     ╱        │    Programming     │
│                │    ╱         │                    │
│                │   ╱          │                    │
│     10         │  ╱           │    Specification   │
│                │ ╱            │                    │
│      1         │╱             │    Initial Concept │
│                └──────────────┘                   │
└─────────────────────────────────────────────────┘
```
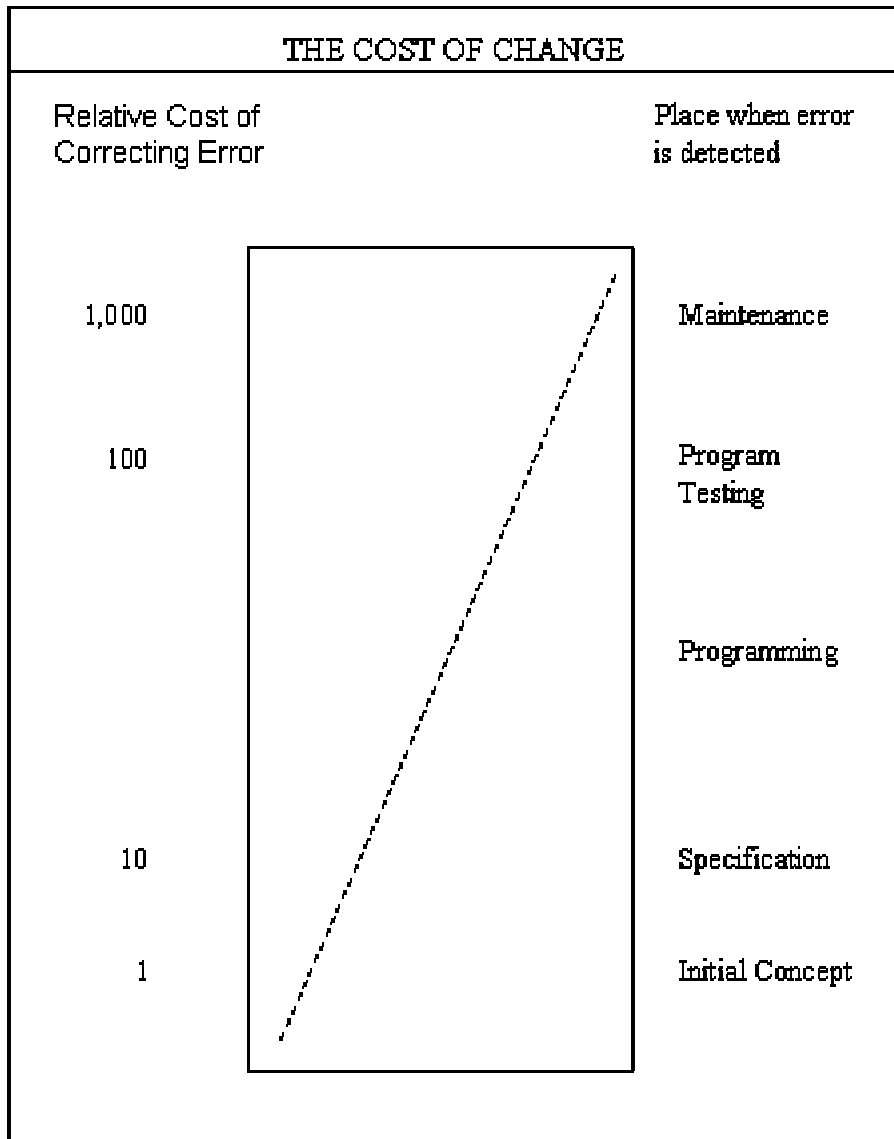
The importance of an audit concern for project activity to properly communicate human resource impact, and ensure that there are plans to cope with that impact, is covered in more detail at the start of Chapter Three and with control objectives in the Project Control (A) stream.

The auditor must also verify, early in the development process, that the project reflects departmental strategic planning and is directly related to senior management objectives. Project Control (A) Objectives (Chapter 3) are provided to deal with these points.

The auditor should consider the recommendation of the Verification and Validation contracting technique, based on a risk assessment, if the project is not using that technique. More detail is included early in Chapter 3.

The auditor's early involvement in the strengthening of controls may raise questions about his or her objectivity in auditing the on-going system at some much later date. This issue is discussed in more detail later in the report, but it can be said here that the assignment of different auditors in the on-going systems audit should adequately address this issue (see reference to PIN 1984-03, Page 1).

The Environment of the Systems Development Process

Introduction

This chapter provides some basic definitions and descriptions of internal and external factors that affect the systems development process in government. Its purpose is to provide a common understanding of terms used in describing systems under development, and to identify factors that auditors may consider significant in auditing the development of a system.

The chapter is organized as follows:

- definitions
- general factors:
  - departmental management infrastructure
  - SDLC Policies and Standards
  - planning and acquisition process
  - technological processes
  - central agency policies
  - common service requirements
  - security and privacy

Definitions

a) Systems Development Life Cycle (SDLC)

A structured approach that divides an information systems development project into distinct stages which follow sequentially and contain key decision points and sign-offs. This permits an ordered evaluation of the problem to be solved, an

ordered design and development process, and an ordered implementation of the solution. A final stage allows for management feedback and control through a post-implementation evaluation.

b) Systems Development Methodology

The particular department's adaptation of the SDLC. It may be a home-grown set of procedures, forms and processes within each of the usual stages of the SDLC or a purchased set of software, procedures, forms and processes that are considered more effective by the department.

c) Systems Development Project

An organized set of activities designed to execute the requirements of the particular Systems Development Methodology that is being followed to achieve a set of objectives and/or problem solutions. The activities are carried out by a project team acting under the leadership of a project manager. The manager is expected to follow all of the SDLC activities of management in completing the stages and requirements of the project.

The Systems Development Environment

During the 1980s, changes in the complexity of the Information Technology environment accelerated. Not only has the complexity of the systems development activity increased, but the range of functions included in systems design and development has also increased. The effect of this combination has been exaggerated by a shift towards systems created by the "end user".

We will continue to see increased use of Fourth generation languages (4GLs), prototyping, pilot implementations and CASE tools. Each of these will require adjustment of approach by internal audit, however, the fundamental principles

laid out in this guide will remain of value. Future amendments to this audit guide will address these recent advances in system development methodology more directly.

These trends will only increase in the future.

The internal auditor, therefore, will have to keep abreast of those environmental factors, both internal and external, that affect the systems development process. Figure 1.1 below, and the descriptions that follow, illustrate these factors.

Figure 1.1: Systems Development Life Cycle

```
┌────────────────────────────────────────────────────────────────┐
│   ┌──────────────┐                      ┌──────────────┐         │
│   │    SDLC      │                      │  PLANNING    │         │
│   │   POLICIES   │                      │     AND      │         │
│   │              │                      │ ACQUISITION  │         │
│   └──────┬───────┘                      └──────┬───────┘         │
│          │          ┌─────────────┐            │                 │
│          └──────────┤             ├────────────┘                 │
│                     │             │                              │
│  ┌──────────────┐   │             │    ┌──────────────┐          │
│  │ INFORMATION  ├───┤             ├────┤ DEPARTMENTAL │          │
│  │   PRIVACY    │   │             │    │  MANAGEMENT  │          │
│  └──────────────┘   │   SYSTEMS   │    │INFRASTRUCTURE│          │
│                     │ DEVELOPMENT │    └──────────────┘          │
│                     │    LIFE     │                              │
│                     │    CYCLE    │                              │
│  ┌──────────────┐   │             │    ┌──────────────┐          │
│  │ INFORMATION  ├───┤             ├────┤   COMMON     │          │
│  │   ACCESS     │   │             │    │   SERVICE    │          │
│  └──────────────┘   │             │    │ REQUIREMENTS │          │
│                     └──────┬──────┘    └──────────────┘          │
│        ┌───────────────────┼──────────────────┐                 │
│  ┌─────┴──────┐     ┌───────┴──────┐    ┌──────┴───────┐         │
│  │    TBS     │     │TECHNOLOGICAL │    │CENTRAL AGENCY│         │
│  │  SECURITY  │     │    TRENDS    │    │ POLICIES AND │         │
│  │  STANDARDS │     │              │    │  PROCEDURES  │         │
│  └────────────┘     └──────────────┘    └──────────────┘         │
└────────────────────────────────────────────────────────────────┘
```
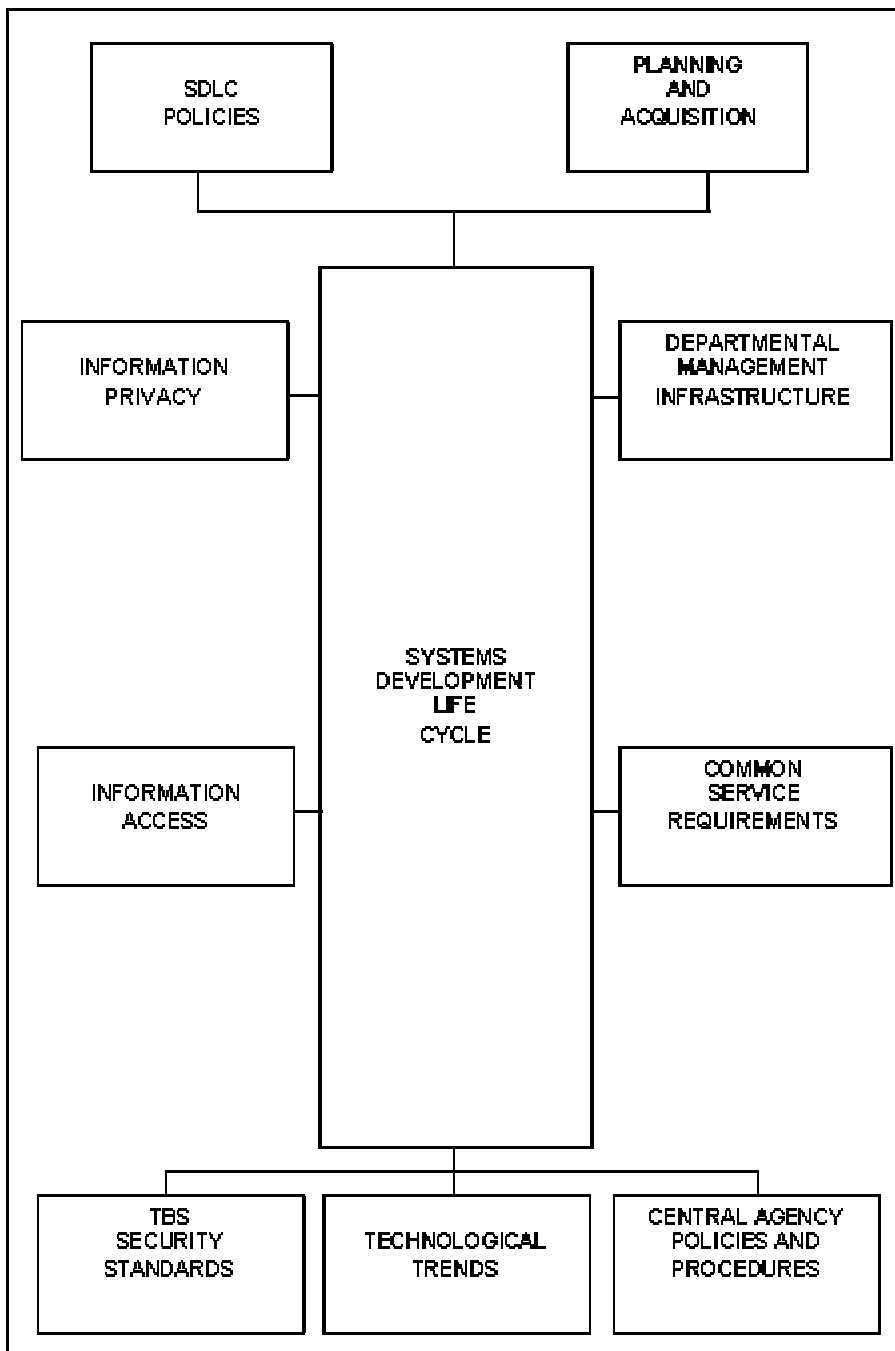
General Factor Descriptions

Departmental Management Infrastructure

The first area to consider is the general organization and infrastructure for systems development within the department. Of particular interest will be the roles and responsibilities of the information management organization (or organizations), the EDP advisory or user steering committees, and the senior management committee(s).

The auditor should find out how well coordinated these organizations are, and their "track record". This information will yield "clues" to possible issues or lines of inquiry, the extent of previous user involvement and an understanding of how effective management has been in developing systems within time and cost targets.

SDLC Policies and Standards

A second major factor that influences the development of a system is the department's SDLC policies and standards. They establish the basis for developing systems. Their purpose is to emphasize the definition of requirements before design begins, thereby minimizing costly modifications later.

The internal auditor should therefore review the department's policies and standards to ensure, on an on-going basis throughout the involvement in the SDLC, that the development project is satisfying departmental requirements.

Planning and Acquisition Process

A third major source of information for the auditor is the department's Information Management Plan (which evolved from the Information Technology and Systems Plan (ITSP)) and the capital budget. Both documents are prepared as part of the department's multi-year operational plan (MYOP).

While the name and the content of the TBS directed process known as the ITSP has changed since the first writing of this section, the principle of the auditor knowing all of the strategic, tactical, and operational planning of the department, in order to assure senior management that the project is supporting those planning thrusts, remains valid.

The ITSP reflects the EDP plans, for the on-going activities and for new initiatives, and the assignment of resources needed to carry out the EDP strategies, policies and programs. The ITSP also reflects the department's capital budget for new EDP acquisitions.

In addition the development should conform to applicable central agency policies and procedures (see Chapter 1 - Central Agency Policies and Procedures).

The internal auditor should review the ITSP and the capital budget to establish a proper link between these planning documents and the particular system under development. It is also important for the auditor to ensure that the planning for the systems development project is tied into and coordinated with the department's EDP acquisition process.

Technological Trends In The Public Service

The first external factor that influences the auditor's understanding of systems development is the technological trends that have an impact on information management in the Public Service. The Treasury Board's "Information Management Policy Overview - Strategic Direction in Information Technology Management in the Government of Canada - 1987", points out that:

> "The management of information systems on a life cycle approach
> is to receive increased importance in government, with due
> consideration, within increased ministerial responsibility, to the

investment in systems, the benefits received, and the need to plan the replacement of systems."

The Overview also provides an interesting assessment of the current situation and it is worth noting that each principle is relevant to a SUD audit:

"The present policies for EDP and telecommunications are based on policy principles that are still sound:

- Resources are used in support of government programs, and are not an end in themselves.

- Needs of the government are met through the services of the private sector, except when it is in the public interest, or is more economical to provide these services internally.

- Departments will develop annual plans, containing information on projects, equipment and personnel and these will be based on longer term plans.

- Efforts will be made to identify opportunities for the sharing of information plans, information itself and relevant expertise.

- Departments establish their own internal policies.

- The staged approval of systems development projects.

- The micro-computer policy, which also includes consideration of the impact on people and the need for training."

-

The Overview continues by outlining re-adjustments to the scope of systems development necessitated by the increasing complexity of the environment:

"Re-adjustments are, however, required to take into account the merging of information technologies, human resource considerations and recent developments, as noted above, in government information policies. Also factors such as the need to ensure departmental and government-wide data quality and

consistency in an environment where more computing power is placed in the hands of end users will require coverage in forthcoming policy updates."

A complete reading of the Overview reveals, in summary, that more factors have been, and will continue to be, introduced into the domain of systems development. Some of these factors are:

- importance of the quality and consistency of data

- end user computing and processing power

- complex and interactive systems

- where required, better development "tools" such as prototyping, fourth generation languages, Computer Assisted Systems Engineering (CASE) software, and interactive data base software (with active data dictionaries)

- more money, not less, to be invested in systems replacement

- critical human EDP resource issues

- the inclusion or integration of telecommunications

Central Agency Policies and Procedures

Two organizations that have an impact on the way public service systems are developed are the Administrative Policy Branch of the Treasury Board Secretariat (TBS) and the Financial Management Information and Systems Branch of the Office of the Comptroller General (OCG). These organizations are positioned by legislation to provide leadership in the management and control of information technology. They have created a general framework that departments and agencies are expected to follow.

The Administrative Policy Branch has promulgated policies and directives dealing with all aspects of the information and systems life cycle, such as project

management, access to information, common services, micrographics, EDP, telecommunications, and micro-computers.

The branch also reviews the Information Management Plans (IMP) submitted by departments and agencies and prepares an annual review of information technology and systems in the Government of Canada. Section 1.A.1.2 of Chapter Three recommends that the auditor verify that the project is appropriately established in the department's plans.

The Financial Management Information and Systems Branch (FMISB) fosters the development and monitors the implementation of sound managerial practices and controls in government. To assist financial systems implementors, the Branch has published and is currently developing guidelines, criteria and policies specifically for financial systems development. Appendix J, Items 13 through 18 contain references to those financial systems development aids. It is very important for auditors to be aware of these guidelines, criteria and policies as they emerge, since they will form part of the auditor's review of controls in financial systems under development.

The FMIS Branch is also responsible for the OCG's role in the currently emerging Financial Information Strategy. This joint undertaking, between the OCG and SSC, is better described in Appendix J, Item 19. Suffice it to say here that the auditor should know the Strategy and how it should fit departmental strategies inherent in any developing financial system.

Auditors should also be aware of their department's Increased Ministerial Authority and Accountability negotiations and the implication of these negotiations on any financial systems being developed. The Office of the Comptroller General is the reference point for IMAA reporting requirements.

Common Service Requirements

The nature and scope of common services is described in Chapter 303 of the Treasury Board's Administrative Policy Manual and in a series of directives. Common services are an important element in EDP operations and its management. Chapter 303 states that "it is the policy of the government to provide goods and services through common service organizations for maximum value for money, more uniform compliance with socio-economic policy decisions, and greater observance of prudence and probity". The fact that common services are government-wide gives them the attributes of a central service. They can significantly affect Information Technology management practices and system development.

The auditor should therefore determine whether management has considered the impact of common service requirements, such as the pay/pension, procurement, SSC, PWC, Communications, NLC (Archives) and other departmentally-provided services as a factor in their planning.

Security and Privacy

The issue of security and privacy in the information technology environment has been given a lot of attention recently, particularly by the Administrative Policy Branch of the Treasury Board Secretariat. The following documents have been published by the Treasury Board: Security Policy of The Government of Canada (revised Sept. 1987), Security In the Government Of Canada-Interim Security Standards: Operating Directives and Guidelines (1987); and TBS Circular 1987-52, the Review of Security Policy. See Appendix J for other listings.

While some of the following references are no longer current, they can provide useful information. The auditor should examine Administrative Policy Manual and other publications, particularly:

- (current) Security Policy and Standards of the Government of Canada

- (current) the OCG's draft Guide to the Audit of the Government's Security policy

- interim information technology standards (Part III Interim Security Standards)

- contingency measures, GES/NE1-14 - 4.1.2.7

- disaster plans, 4.1.2.7.3

- software security, 4.6

- design, development, and quality assurance. 4.6.2

Ideally, security and privacy should be addressed by the auditor at every stage of the systems development process. All relevant security and privacy requirements should be taken into account right at Project Initiation and who fulfils the responsibilities of EDP Security Co-ordinator and Departmental Security Officer established. The availability of relevant RCMP Security Evaluation and Inspection Team reports should also be ascertained at the beginning of the audit.

Detailing the Systems Development Process

Introduction

This chapter describes the Systems Development Life Cycle and the roles within that Cycle, in enough detail that an auditor can perform an audit of development at any phase of any department's interpretation of the SDLC into its own Systems Development Process (SDP). This means that the auditor should be able to assess any project's progress, layout the tangible accomplishments for comparison to those accomplishments deemed appropriate for the sequential stages of development considered standard by this guide, and so determine "where" the project is relative to the standard. This will then enable the auditor to select, from all audit objectives given to that point in the standard SDLC, the audit objectives appropriate for the particular project.

The Systems Development Life Cycle

The "Management of Information Technology" Policy June 1990 from Treasury Board supersedes Treasury Board Administrative Policy Manual 1978 Chapter 440.3 (Appendix J of this guide). Chapter 440 defined the Systems Development Life Cycle on which this guide was based. Although adherence to a specific SDLC is no longer prescribed by Treasury Board, this audit guide remains of value in defining the audit of an SDLC, which is still an accepted systems development practice.

The purpose of an SDLC is to allow system innovators and users to produce a controlled, economical, efficient and effective system. The following phases of the development process were suggested in Treasury Board Administrative Policy Manual 1978 Chapter 440.

- Project Initiation
- Feasibility Study

- General Design

- Detailed Design

- Implementation

- Installation

- Post-Installation

While the Standard SDLC describes seven life cycle stages, individual Departmental SDLCs may contain more or fewer than these seven. However, from the work content of each stage or combination of stages in a particular SDLC, parallels of progress can be drawn by comparison to the seven-stage standard of project work accomplishment (see Figure 3). Therefore, as was previously stated, appropriate audit objectives and audit criteria (discussed in Chapter 3) can be selected for a particular system's audit from those applicable at the same and previous stages of this Guide's sequenced set of objectives.

On the same note, one current school of thought holds that, in this day of micro computers and/or prototyping/fourth generation languages, organizations cannot afford the controlled constraints of a formal life cycle methodology. Nonetheless, the auditor's responsibility is to ensure that adequate management control points exist, whatever the individual life cycle in place. To this end, the content or deliverables of the development phases must exist and should have been completed in a logical sequence of the Standard SDLC.

Prototyping

Before showing a generic SDLC comparison table of the Standard SDLC and comparing it to another terminology example, we should discuss one particular recent development technique in more detail.

Application prototyping is defined in this Guide as "dynamic visual modelling that provides a communication tool for the user and developer that is more effective

than either narrative prose or static visual models for portraying functionality". It is an approach intended to simulate the ultimate system. The technique is an adjunct to a development methodology and not a replacement. Prototyping should be used at the Feasibility and General Design Stages, if a conscious decision has been made to use the technique at all, to determine functional and data requirements by permitting the user "hands on" involvement in the earliest stage possible. When the technique is chosen, the auditor should examine the decision of the project team and the control over the use of prototyping at the Feasibility and General Design stages.

Note that the auditor should ensure that Prototyping is not confused with Piloting. A prototype may be built with non-production software and thus could not be gradually expanded into the production version. A Pilot system is intended from inception to be expanded into the production version.

The auditor must insure that the difference is recognized by the project team or that formal, signed off decisions exist to extend the "prototype" beyond the General Design (or equivalent) stage.

Data Management

The auditor should be aware of the current tendency for departments to manage their data formally and the effect on systems development that data administration and data base administration are having or should have in their environments. An excellent reference is "Information Management Strategy For Common Systems Report - 1989", by the TBS Advisory Committee for Information.

Figure 2, below, illustrates a sample development methodology, in flow chart form, using data management and structured design techniques. This is not the Standard SDLC approach. However, many of the terms and deliverables of the

stages are similar to those used in the Standard SDLC. By matching the deliverable content of the standard stages and the deliverables of the audited system under development, the auditor will be able to select the equivalent standard stage objectives from this guide. This will provide the auditor with a core set of objectives, to be augmented dependant on the nature of the particular system, in order to yield optimum audit coverage during development (whatever the local SDLC and particular system characteristics).

Figure 3 (below beyond Figure 2) is a summary of deliverables by stage in the Standard SDLC.

Figure 2: A Sample of a Non-Standard Systems Development Life Cycle
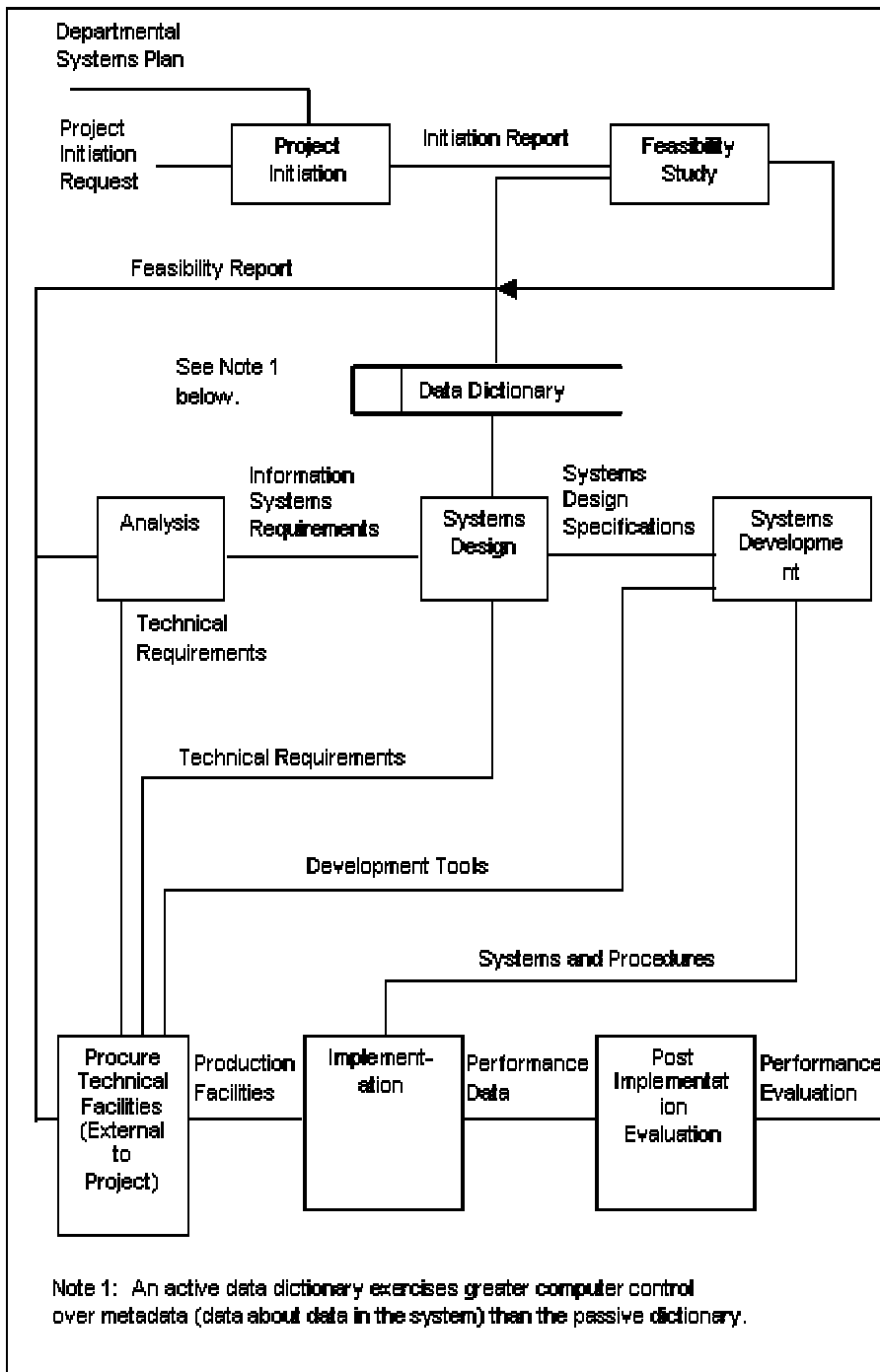
Note 1: An active data dictionary exercises greater computer control over metadata (data about data in the system) than the passive dictionary.

Figure 3: Standard SDLC - Deliverables by Stage

Stage	Activity	Deliverable
Initiation	• Screen Requests • Document Details • Planning and Approval	• Initiation Report • Problem Definition • Approach • Roles/Project Plan
Feasibility	• Data Gathering • Data Analysis • Develop Alternatives • Evaluation of Conceptual Design • Write Report	• Feasibility Report • Users' Requirements • Evaluation of Sys. Alternatives • Conceptual Design • Concept • Project Plan • Recommendations
General Design	• Data Gathering • Analysis • Outline System • Outline Controls • Quality Assurance • Security Goals • Validate User Reqmts • Planning & Approval	• General Design Report • Revised Cost/Benefit • Functional Specs • Controls • Perf Revised Tech. Reqmts • Revised Project Plan • Detail Design Plan
Detail Design	• Design Sub-systems • Create Sub-systems • Design User Aids	• Detail Design Report • Revised Cost/Benefit

	• Design System Test • Design Conversion • Prepare Report • Planning/Approval	• Revised Technical Requirements • System Description • User Procedures • Revised Project Plan • Implementation Installation Plans • Training plan
Development	• Software Coding • System/Unit Testing • Produce User Aids • Planning/Approval	• Implementation Report • Documented Programs • User Procedure Manual • Training/Operations Manual
Implementation	• Installation Equipment • Acceptance Testing • Training/Conversion • Operation/Approval	• Project Completion • Notice for Approval
Post Instal.	• System Adjustments	• Gathering • Post Instal. Data • Evaluation Report

Stage Descriptions

1. Project Initiation Stage

At this stage terms of reference for the project should be formally defined and the project control parameters established.

Procedures involve performing a preliminary review of the existing system (if any) to assess the need for change and the nature of the suggested changes. The "problem" must be defined. A potential solution should be conceptualized for reference during the feasibility study phase. The description of the solution should not be so detailed that it prejudices the alternatives examined during the feasibility study.

At this time all external and internal constraints (cost, time, legislation, departmental guidelines, user needs, etc.) should be determined and their impact on the problem and the solution assessed. Security, including disaster recovery requirements and Privacy issues should be assessed during this phase.
This phase produces a Project Initiation Report.

2. Feasibility Stage

When this stage is complete, an appropriate solution to the problem should have been determined and a preliminary plan for its implementation designed.
Users' Requirements may be documented or established by prototyping, thus providing a basis for identifying a solution.

It is of prime importance that enough alternative approaches be examined. A detailed analysis, at the conceptual level, of the various alternatives should support a formal justification for the suggested solution. This analysis should include cost benefit analysis (or similar techniques), consideration of financial and operational controls, and organization compatibility. As in the project initiation phase, care must be taken that evaluations are objective and complete and that there is no "built-in" bias towards one particular solution.

Resource requirements for the remainder of the project should be identified and time and costs estimated for management approval. Broken into appropriate project phases, these factors will be used to maintain and monitor project development.

Documentation of the above should be contained in a Feasibility Study Report.

3. General Design Stage

Work during this phase will translate the proposed conceptual solution, determined during the feasibility study, into a workable solution ready for detailed design and implementation.

This will require:

- the preparation of a system outline, including flowcharts, system performance criteria and the identification, definition and preliminary formatting of all inputs, outputs and files used or produced by the system. (This will require extensive liaison with users.)

- an overview of the internal control framework and operating procedures to ensure that they meet the objectives of the system being developed (The proposed system should satisfy all user requirements.)

- the selection of facilities and job specifications for suppliers or bureaux.

- an outline of all functional specifications to ensure that the general design meets all system objectives that have been determined.

- the revised costs, time estimates, and other criteria relating to future phases for management approval.

Documentation of the information gathered in this stage will typically be contained in a General Design Report. Some departments may prefer to prepare two reports, the second to highlight the Business System Design by itself. Either way, these elements of the system must be clearly documented.

4. Detailed Design Stage

Based on the functional specifications from the general design stage, detailed procedures and computer specifications are produced. All controls, procedures, work flows, input/output documents, processing logic, file/data base layouts, and data elements will be finalized.

Management and user approval of this design stage is paramount. Therefore, the final product of this phase, the Detailed Design Report, should contain, in addition to detailed program specifications, workflows, etc., a non-technical description of the entire system. This should encompass:

- a system description, objectives, inputs, outputs
- a system flowchart illustrating the conceptual design

Appropriate members of management should review the detailed specifications and technical requirements.

Documented system test plans and implementation and conversion plans should also be produced at this stage, and, in addition, a plan on how the activities in the implementation and installation phases will be coordinated. This will include preparing instruction manuals (users and operators), training, security, back-up and conversion procedures.

5. Implementation

This stage creates all computer programs, forms, manuals and training material needed for an operational system.

Detailed program logic will be designed and application software coded. User, operations and training manuals will be finalized and should cover, where appropriate:

- data capture

- data validation

- system audit trails and controls

- verification of analysis report

- computer operating instructions

- back-up and re-run procedures

- security procedures

All aspects of the system, including program logic and operational procedures, should be thoroughly tested. All procedures required for the installation of the system should be defined and scheduled.

6. Installation Stage

This stage converts the system to operational status. The work includes converting existing files (if any) or creating the initial information base, training all personnel involved with the system (user and EDP), and instituting control and operational procedures through pilot or parallel run phase-in. All documentation from previous phases should be finalized. Conversion and installation procedures should be reviewed and tested. The project manager should issue a formal Project Completion Notice for approval.

7. Post-Installation Stage

Work during this stage consists of examining the project performance and system performance against the original project documentation of system cost/benefit and project cost and time schedules.

A period of settling in is normally allowed between Installation and Post-Installation audit. The audit team could be changed at this point, as well, to

maximize objectivity, but decreased audit efficiency will offset the objectivity gained.

Thus, project reviews are important soon after system installation to assess the success of the systems development process and to identify any differences in control design and control operation.

Stage Description Conclusion

As we have noted, adequate departmental standards should exist and be adhered to for each SDLC stage to ensure consistent and complete management control over implementation. However, it may be appropriate for the department to have defined and approved a separate set of SDLC activities based on the type of project being undertaken (i.e. major or minor system development). It is normal to document management approval of the deviation from departmental standards.

In many cases of micro- or mini-computer end user development, examining the importance of the data/information to the corporate body may indicate that some or all of the control points of an SDLC should be present.

Lastly, in evaluating whether or not system development or change is minor enough to justify grouping or eliminating some of the SDLC stages, the auditor should keep in mind that some relatively small system changes could be very significant from a control point of view.

Roles

The typical roles in the systems development process illustrate the contribution of each stage in the SDLC model to management's assurance of control, economy, effectiveness and efficiency in systems development. These are very basic

descriptions, but they serve as examples of the roles an auditor should expect to find in a controlled environment. These roles, or their equivalents, and others are illustrated in Appendix A as interviewees for the questions related to the suggested Objectives and Criteria for each audit stage.

Management

Management has a review role, to ensure that the developed system meets the ultimate goals of the organization. Management sets priorities on projects, budgets, and target dates. Management establishes departmental policies and standards for system development, then demands the appropriate occasions to exercise its control over the development process by ensuring that an SDLC is in place and is functioning as designed.

A major management responsibility is to decide how much risk can be tolerated in any project.

Management may need third-party technical help with these management responsibilities.

Approval Authority and/or Steering Committee

Each departmental organization usually appoints a sign-off authority for each stage of the development process. Taken together, they represent the approval authority. Some departments have an EDP Steering Committee at the DM level, which should consider all systems audit reports. This is sometimes the final approval authority. The key issue for internal audit is that some evidence of a formal approval process with senior level sign-off, be in place.

Designer/Analyst

The designer/analyst works with the user requirements to develop a system that meets the objectives and needs of the user. The designer is responsible for ensuring that the system design is comprehensive and workable. The designer/analyst is also responsible for overall system control over data that transcends or integrates individual program controls. The designer also bears the responsibility for choosing the optimal technical design alternative. The auditor should ensure that the analyst's control role is not compromised by the project manager or anyone else.

Programmer

The programmer creates an effective and efficient program from a specification drawn up by the analyst/functional representative. The program could be a dialogue or module of the overall system and the controls in the specification must ensure that the data that are entered into the program retain their integrity throughout the program's processing. Control over data must be programmed in the input editing process, internal EDP program processing, and output displayed, communicated, or printed.

Users

It is the user who in the early stages of development clearly defines and supports the objectives and requirements to be satisfied by the system. It is also the user's responsibility to establish control requirements and to ensure that the resulting system delivers the required control. The user may need third-party technical help to ensure that the required control is in place.

Departmental Security Process

The Treasury Board's Security Policy and Standards, 1989, outlines the security responsibilities of the Department, the Royal Canadian Mounted Police (RCMP), the Department of Supply and Services, the Department of Communications, the

Department of Public Works, and the Security Evaluation Inspection Team (SEIT). The roles of the Departmental Security Officer and the Security Advisory Committee, within the two activities of Security Co-ordination and Security Administration, are briefly outlined. Every department should provide, directly or by consultation with the RCMP SEIT, advice, standards and evaluation of the physical (versus logical) controls required within that department over data, information and physical assets. Sign-off, from the approval authority should be evident at each required stage in the SDLC.

Other security references are contained in Item 12 of Appendix J.

Departmental Data Manager/Administrator

New emphasis is being placed by many departments on managing data and information as a critical corporate asset. Data Administration can be described as the functions of planning, administration, and control of the data-related activities of an organization, and the Data Administrator is that person or organization responsible for carrying out the Data Administration.

A person from the Data Management or Administration area should be identified as a key project team member.

Departmental Data Base Administrator

Data Base Administration plans, controls, and performs any other functions that directly lead to or have an immediate impact on operational data bases. The Data Base Administrator is the person or organization responsible for the functions of Data Base Administration. Where there is technical distinction between analyst and data base administrator, the auditor should ensure that data base administration is represented on the project team.

Internal Auditor

The auditor should review and evaluate the management controls used in developing new application systems or major enhancements. The auditor will look for evidence that there has been adequate user participation in the design and acceptance of the system and that there is adequate attention in the detail system and procedures design to accomplish general and application control.

The exact extent of the auditor's participation in systems development is determined by the risk to the organization of the development activity. The risk is comprised of elements of development cost, operational cost and the organization's dependence on the information processed. Today's systems design and development activity is growing as a significant portion of organizational time and expense and organizations rely more than ever on the continued functioning of their EDP systems. In much the same manner that the auditor would establish the materiality of their findings, the auditor should also establish the reason for choosing certain criteria over others in the Planning Phase of the audit. This is accomplished by establishing the extent of the risk to the department should a particular management control be poorly executed. In some cases, this approach may enable very few audit resources to handle very large systems development projects.

The auditor may find very complex documents, deemed necessary to explain the system development role relationship between product managers, communication system designers, data base administrators, data owners, users, clients (sometimes called users' users) and a host of other titles that have sprung up to deal with the more complex Information Technology world described in Chapter 1.

Other than for the development of system requirements for the audit group, as a user of the system, the auditor must never be held directly responsible for any

project activity. Auditors are "outside" the project team, even though they may offer advice on control, by letters or reports, to the project team. The auditor must, through all project development stages, verify that all of the issues and role/reporting concepts that will arise during the project are well documented. In all of its systems development review activities, auditors must ensure that the independence of the audit function is not compromised for later on-going system reviews. This is normally accomplished by assigning different auditors once the system has been installed, and through the manner in which the system development auditor makes observations and recommendations for the improvement of control. The auditor must always resist being involved in the actual system design.

Performing the Audit: Applied to the Systems Development Process

Introduction

This chapter deals with the audit process to be applied at each stage of a selected development project. The word "Stage" was selected for the sequential components of the SDLC in this Guide to avoid confusion with the word "Phase" that is used in audit methodology.

Scope and Purpose

The audit of Systems Under Development may have three main thrusts: first, to provide an opinion on the efficiency, effectiveness, and economy of project management; second, to assess the extent to which the system being developed provides for adequate audit trails and controls to ensure the integrity of data processed and stored; and third to assess the controls being provided for the management of the system's operation. These thrusts are clearly grouped for the auditor, in Chapter 3, by the presence of an A (Project Controls), B (Data Controls), or C (Systems Management Controls) letter as the second indicator in the Objective, Criteria and Detailed Criteria numbers.

The first thrust is pursued by having the auditor attend project and steering committee meetings, examining project control documentation and conducting interviews. The emphasis is on establishing, with the auditee, what project control standards are to be complied with, (such as a formal systems development process) and determining the extent to which compliance is being achieved. In carrying out this activity the auditor should keep in mind the requirements outlined in former Chapter 440 of the Treasury Board Administrative Policy Manual, the content of all circulars, policies and standards

listed in Appendix J, and the material covered in the OCG's "Guide to the Audit of The Management Process".

As for the second thrust, the auditor is limited to examining system documentation, such as functional specifications, to arrive at an opinion on controls. The auditor's opinion will be based on the degree to which the system satisfies the general control objectives that any Information Technology system should meet. A list of such objectives should be provided to the auditee. The same is true for the third thrust, the system's operational controls. The auditor should provide the auditee with a list of the standard controls, over such operational concerns as response time, CPU usage, and random access space availability, that the auditor has used as assessment criteria.

Audit Phases

The audit of a system under development involves the conduct of certain audit procedures in connection with each stage of the SDLC. While this may appear to segment the process into separate and distinct audits, that is not the case. The audit of any stage or group of stages should consider all previous audits (or the lack of audit presence) in the continuous process of developing a system.
In conducting audits of systems under development the following activities, common to all audits conducted to Treasury Board standards, should be included in each audit stage:

1. assignment planning
2. review
3. evaluation
4. verification
5. reporting and follow-up

For the most part, the above activities will be executed during a Systems Under Development audit, but there is some difference in how they are applied.

Special Planning Phase Considerations

All phases of an SDLC audit should be planned and be included in the initial planning for a system under development audit. As each subsequent stage of the SDLC is audited, the audit plan should detail the particular stage being audited and update plans for the remaining stages.

Review and Evaluation Phases

Compliance with an SDLC process will be reviewed and evaluated at each audit stage performed. However, as the documentation and/or programming of controls begins during the Feasibility Stage, review and evaluation of the data integrity and system controls can take place only at the Feasibility, General Design, Detailed Design, Implementation, Installation, and Post-Installation stages.

Verification Phase

Throughout the development process the auditor will verify compliance with the SDLC (see detailed approach in 4.A.10.1). The auditor will not, however, test the controls in the system being developed, but will review compliance with testing standards as per the SDLC. Where testing has been inadequate, the auditor should advise project management immediately. Testing is a project team and user function. Direct participation in the testing activity compromises the auditor's independence. However, the auditor may decide to re-perform selective tests to support control conclusions.

Special Report Timing Considerations

An important feature of Systems Under Development Audits is the avoidance of retrofitting costly controls. Such cost avoidance can be achieved only where communication between the auditor and auditee is at a level where action can be taken quickly in response to audit concerns. In order to fully support senior management, the audit reporting process must be guided by the systems development process. However, another important guiding principle is to ensure that audit findings are communicated, as soon as the auditor can support them, to the Project Manager level. To ensure audit independence and to keep senior management aware of SUD audit activity, summary audit reports should be made to coincide with project stages and check points. For example, if the process being followed provides for the stages shown below:

- Project Initiation
- Feasibility Study
- General Design
- Detailed Design
- Implementation
- Installation
- Post-Installation

the related audit outputs would involve an Audit Plan Memorandum to be released to all levels of management during the Project Initiation stage audit with summary audit reports, according to the regular audit report process, after all subsequent audit stages.

Another special timing consideration is that of scheduling SUD audit activity to enable providing assistance to senior management at the time when the departmental approval of Treasury Board submissions is required. This would normally be in the form of delivering an opinion of the reasonableness of

cost/benefit information contained in the submission, but could extend into the audit of other submission information.

General Note

The SDLC stages discussed above apply mainly to major new systems being developed or to major changes to existing systems. In developing smaller systems or where minor maintenance changes are made to existing systems, the SDLC stages may be grouped together or certain stages may be dropped completely. In the latter case, the project team must be careful that the system is not impaired. For example, inadequate consideration of alternatives in the Feasibility Study stage may lead to choosing an inappropriate alternative. Costs as a factor in a decision to drop a stage should be weighed against the degree of risk involved in doing so.

Prototyping, as a technique, has been described in Chapter 2. The concerns and expected controls in prototyping are included in the Initiation and Feasibility Stages.

Maintenance projects, that is the enhancements made to systems already in production, may be considered significant enough to be viewed as complete SUD projects in themselves. In that case, the audit concerns would be identical to those described below.

To ensure consistent development of all departmental projects, development standards should be in place and adhered to for each SDLC stage. However, it may be appropriate for the department to define a separate set of SDLC standards, based on the type of project being undertaken (i.e. major or minor system development). This will help ensure that minimum standards are applied in the minor systems development activities.

Lastly, in deciding whether a system is minor enough to justify grouping or eliminating some of the SDLC stages for an audit, the auditor should keep in mind that some relatively small system changes can be significant from a control point of view. The significance of a system amendment should be carefully assessed if it deviates from standards.

Control Objectives by Stage

Following are project management (A), data integrity (B) and Systems Management (C) control objectives, criteria, and detail criteria related to each stage of project development.

Project control is reviewed at every stage so that one can form an opinion about the efficiency, effectiveness and economy of project execution. Fortunately, the input, data integrity and system management controls being built into the system need be reviewed only at the Feasibility Study, General Design, Detail Design, and Implementation stages (see figure 4). The Feasibility Study stage is included in case control requirements are germane to selecting a design approach.
Note that while a few project control criteria are repeated from one audit stage to the next, the auditor should treat each audit stage of the guide as an independent stage. That means that the auditor must ensure that all objectives in all audit stages, prior to the one in which the auditor is working, are considered for application in the current audit stage.

Finally, the Chapter is organized by a combination of numbers and letters. This allows readers to situate themselves in a particular Stage and Audit Thrust at any point in the text. A diagram follows to ensure the numbering discipline is clear.

Figure 4: Activity by Stage Development

Stage	Project	Data	System
Initiation	YES	NO	NO
Feasibility Study	YES	YES	YES

General Design	YES	YES	YES
Detailed Design	YES	YES	YES
Implementation	YES	YES**	YES*
Installation	YES	NO	NO
Post-Installation	YES	YES**	YES**

YES means audit activity at this point.

NO means no audit activity possible or required.

* System Control concerns are covered as part of the review of Testing done at this stage. (See criterion 5.A.3.2 in Appendix F).

** Covers selective re-performing of testing of controls.

The audit information in the remainder of the chapter and associated appendices is organized and identified by means of a four field Dewey Decimal number (reference figure 5). This number will assist readers in identifying where they are at any point in the text.

Figure 5: Example of Dewey Decimal Numbering System

1.A.1.1

SDLC Stages:

- Initiation

- Feasibility

- General Design

- Detail Design

- Implementation

- Installation

- Post-installation

1.**A**.1.1

Objectives:

A = Project Controls

B = Data Controls

C = System Development

1.A.**1**.1

Criteria

1.A.1.**1**

Audit Steps

1. Project Initiation Stage

It is essential that the auditor's participation be communicated formally to the Departmental Systems Steering Committee, by issuing a formal memorandum stipulating the need to include the auditor in Project Team and Steering Committee meetings.

After the auditor has completed the Planning Phase of the audit of the Initiation stage, a formal audit plan memorandum should be issued, outlining audit participation in the remainder of the project.

When compliance with the requirements of the SDLC at this stage is reviewed, any major non-compliance issues should be sent to the Steering Committee.

Project Control (A) Concerns

The "User or USER Management" term used in any Objective, Criteria, or Detailed Criteria refers to the "community of users", usually represented by one or more persons on the project team. The "community of users" can be one or many seperate organizations in a department. The auditor must ensure that the "community" is adequately represented on the project team.

Developing a new system must be clearly justified, usually by an economic analysis. In some cases, however, it may take the form of an evaluation of the need for improved or additional services, or other non-quantifiable concerns. In any case, some form of project justification should exist.

To be sure that management has made an informed decision to go ahead with the project, the constraints the project faces should be documented in the project documentation, along with a preliminary identification of the prerequisites by which the effectiveness of the new system will be assessed.

Project control, organization, responsibilities and authorities should be very clearly established.

Key Risks

The audit plan should include activities to address the following key risks which could contribute to not meeting user or project requirements:

- vague identification of problem and project scope
- acceptance of a project plan that does not contribute to corporate objectives or strategic planning
- poor project management, including both human resource requirements and financial resource needs (i.e. budgeting)
- inadequate assessment of project risk
- inadequate documentation of security and privacy concerns, including the required and actual level of clearance and reliability of team members

Objective

1.A To establish that the project is formally initiated and that appropriate project control measures exist.

Criteria

1.A.1 The need for the project has been clearly stated in a Project Initiation Report or similar document.

1.A.2 The need for the project is acknowledged and financially supported by the appropriate level of user and Data Processing Management.

1.A.3 A project organization is outlined in the Project Initiation document.

1.A.4 A project development process is outlined in the Project Initiation document including tasks and responsibilities.

1.A.5 A work plan, including target dates, is provided in the Project Initiation document.

1.A.6 The project organization, the development process, and the work plan have been formally accepted by an appropriate level of management.

Note 1: This objective and its criteria correspond to identically named Audit Programs in Appendix B.

Note 2: As shown in figure 4, there are no objectives for Data controls (B) and System controls (C) for the Initiation Stage (1) as there is no documentation of controls required in this stage (see Figure 3).

2. Feasibility Study Stage

During the Project Initiation stage the problem was defined. The Feasibility Study Stage conducts a study of general User Requirements to determine the appropriate conceptual solution in terms of organizational compatibility, economic justification, and technical suitability. Detail specifications will be prepared in the

next stage based on these requirements, usually known as the USER REQUIREMENTS DOCUMENT.

Project Control (A) Concerns

The auditor should ensure that detailed user requirements have been properly identified and documented. The information contained in the User Requirements document should be gathered with great care directly from the users, by the project team, to be sure that they do not limit their definition of requirements because they are unaware of the new System's potential capabilities.

All practical alternatives should have been identified and analyzed. Facts and cost/benefit estimates used in the analysis must be reasonable and derived from valid sources. Conclusions made should follow logically from the analysis.

Resource estimates and time budgets must be complete and reasonable. Since these estimates are to be used for budget and project control, it is imperative that adequate detail be provided.

Key Risks

Audit activity, addressing the following key risks, should be incorporated into the audit plan.

- Information provided to management for evaluation, approval and planning purposes may be incomplete or inaccurate.

- The optimal alternative was not selected.

- Inadequate planning, control, and administration.

- Many users have difficulty in verifying their previously expressed needs when presented with a voluminous document. The auditor should determine that an optimum way of ensuring the user's active involvement in verifying User's Requirements (such as Prototyping described earlier in Chapter 2 of this Guide) was used by the project team.

- Senior Management may treat this approval stage lightly because it consumes relatively few resources. As a result, work could proceed on later stages before this significant stage is complete.

Objective

2.A To establish that a feasibility study, including an Overall Project Plan, has been undertaken to determine the most appropriate solution to a stated problem in terms of organizational capability, economic justification, and technical suitability.

Criteria

2.A.1 User requirements are addressed in a User Requirements Report or similar document.

2.A.2 The accuracy and completeness of user requirements has been acknowledged by the appropriate level of user, and by Data Processing management.

2.A.3 The analysis of alternative processing configurations has been described in a Feasibility Study or similar document.

2.A.4 The appropriate level user and Data Processing management have confirmed that the analysis of processing alternatives including constraints or risks is accurate and complete, and they agree with the recommendations.

2.A.5 Resource estimates and other financial data have been addressed in a Cost/Benefit Analysis Report or similar document.

2.A.6 The accuracy and completeness of the cost/benefit analysis and acceptance of the recommended alternative has been acknowledged by the appropriate level of user and Data Processing management.

2.A.7 Based on the alternative recommended in the cost/benefit analysis, a Personnel Skills Summary has been prepared by the Project Manager summarizing the following information:

- required skill categories (administrative and technical)
- required skill levels
- required number of skilled personnel
- required authority level

2.A.8 Minutes of Steering Committee Meetings or similar document.

2.A.9 The status of the project compared to the work plan contained in the Project Initiation document has been addressed in a Feasibility Stage Project Status Report or similar document.

2.A.10 The accuracy and completeness of the Feasibility Stage Status document has been acknowledged by the appropriate level of user, and by Data Processing management, or concerns have been satisfactorily dealt with.

Note 1: This objective and its criteria correspond to identically named Audit Programs in Appendix B.

Data (B) and System Management (C) Controls Being Built into the System

At this stage of development the user, who is ultimately responsible for data integrity, must make the data control requirements (B) known. These requirements must be considered when carrying out the feasibility study and cost/benefit analysis to ensure their inclusion in the system. Both processing and security/privacy control requirements must be included in the User Requirements document, or prototyping equivalent.

System Management (C) Controls are the controls required to ensure that the system will continue to operate efficiently and effectively after installation. These controls are different from data and information controls and have different control objectives. These management controls over the operation of the system must be in keeping with the requirements definition for the system itself and with the cost benefit analysis.

Key Risks

Audit activities addressing the following key risks should be incorporated into the audit plan:

- failure by user senior management to assess adequately the documentation of data control requirements and the chosen alternative's resolution of the requirements when they sign off this stage; and

- failure of the user or operator to specify system management control requirements.

Objective

2.B To ascertain that data processed and stored by the system will be complete, accurate, and authorized, and that security, privacy, and accessibility levels for the system's data are specified.

Criteria

2.B.1 The need for processing control requirements is identified in a System Processing Controls Specifications or similar document.

2.B.2 The level of security, privacy, and accessibility of system data has been documented by the user representative including the sensitivity of system and data to loss, destruction, unauthorized access and changes.

Note 1: This objective and its criteria correspond to identically named Audit Programs in Appendix C.

Objective

> 2.C To ensure that the system operates efficiently, effectively, and economically.

Criteria

2.C.1 System management control requirements have been outlined in a Minimum System Management Controls Specifications or similar document.

Note 1: This objective and its criteria correspond to identically named Audit Programs in Appendix C.

3. General Design Stage

In this stage a detailed specification of the user's requirements is prepared from the system design alternative that has been approved in the previous phase. The specification that results is expressed in terms of those executing the business functions concerned and is free of technical design considerations. The functional specifications will then be translated into a system design in the next phase.

Security concerns, as noted at the end of Chapter 2, should continue as an audit concern in this Stage.

Project Control (A) Concerns

Project performance during the general design stage in comparison to the plans and budgets established at the Feasibility stage should have been monitored and variances justified to the project authorities.

The system, as designed, should meet the user's requirements. Control considerations (both financial and operational) should have been addressed. In some cases, the audit mandate may require evaluation of these application controls.

Both the manual and automated elements of the new system should have been addressed.

Documentation should address all elements of the system in enough detail to permit the detailed design of the system.

Key Risks

The following key risks should be considered in the audit plan:

- incomplete/inaccurate identification and definition of key factors
- lack of correspondence between defined and actual needs
- inadequate assessment of the cost/benefit of the system
- approval/authorization not obtained at designated checkpoints

Objective

3.A To ensure that the general design of the system expands on the findings of the feasibility study, produces a functional description of the manual and EDP processes, and devises an overall system design that can be used to obtain a commitment for further development.

Criteria

3.A.1 System specifications are addressed in a System Specifications Report or similar document.

3.A.2 The accuracy and completeness of system specifications has been acknowledged by the appropriate level of user and by Data Processing management.

3.A.3 The data dictionary/directory has been updated to reflect the contents of the System Specifications document.

3.A.4 All required skills are still available to the project.

3.A.5 Dates for committee meetings and the items to be discussed at each meeting continue to be addressed in a Steering Committee Meeting Schedule or similar document.

3.A.6 The status of the project compared to the budget and schedule contained in the Feasibility Stage Status document has been addressed in a General Design Stage Project Status Report or similar document.

3.A.7 The accuracy and completeness of the General Design Stage Status document and agreement with it has been acknowledged by the appropriate level of user and Data Processing management.

3.A.8 A human resources impact analysis is planned.

Note 1: This objective and its criteria correspond to identically named Audit Programs in Appendix D.

Data (B) and System Management Controls (C) Being Built into the System

The project team, made up of user and Data Processing representatives, must select techniques to satisfy the control requirements developed at the Feasibility

stage. This selection is limited only by the team members' imaginations. The auditor's job at this point is to assess control, not the user's technical capability.

Key Risks

Audit activity, addressing the following key risks, should be incorporated into the audit plan:

- inaccuracy of project data must be incorporated into the audit planning, to determine the extent, nature and timing of audit procedures for this stage and all subsequent SDLC stages;

- failure of the user to specify techniques to satisfy System Management Control requirements, because "it's too early to know".

Objective

3.B To establish that data processed and stored by the system will be complete, accurate, and authorized.

Criteria

3.B.1 Processing control techniques to satisfy the requirements outlined in the List of Minimum System Processing Controls document have been outlined in a Processing Controls Specifications Report or similar document.

3.B.2 The accuracy and completeness of the processing control technique specifications have been acknowledged by the appropriate level of user and by Data Processing management.

Note 1: This objective and its criteria correspond to identically named Audit Programs in Appendix D.

Objective

3.C To ensure that the system will operate efficiently and effectively.

3.C.1 Control techniques to satisfy the requirements outlined in the List of Minimum System Management Controls are outlined in a System Management Controls Specifications Report or similar document.

3.C.2 The accuracy and completeness of the system management control technique specifications have been acknowledged by the appropriate level of user and by Data Processing management.

Note 1: This objective and its criteria correspond to identically named Audit Programs in Appendix D.

4. Detailed Design Stage

During the Detailed Design stage, the functional specifications prepared in the previous stage are translated into a description of the system that will meet the specified functional requirements. The system design will then be implemented in computer-based and manual systems in the Implementation stage.

The main objective of this stage is to translate the user design specifications into systems, processes and data bases that will operate within hardware and systems software constraints.

Project Control (A) Concerns

Project performance during the detailed design stage compared to the plans and budgets established at the Feasibility stage (or as revised subsequently) should have been monitored and variances justified to the project authorities.

All elements of the system must have been designed in detail. Both the manual and computerized elements and the control features of the system must have been addressed.

If the audit mandate includes the evaluation of application controls an examination, as described in the "Guide to the Audit of Application Controls", may be required.

The detailed design is the complete and final design of the operational system. That is, there must be no apparent technical flaws or inconsistencies. Depending on the audit mandate, the auditor may either examine evidence that this has been established or satisfy himself by re-evaluating.

Key Risks

Audit activity, covering the following key risks, should be incorporated as part of the audit plan.

- The underlying principles on which the testing approach is designed may be inappropriate and therefore lead to faulty conclusions.
- Insufficient information on hardware and software characteristics and contract terms may prohibit optimal selections.
- Inaccurate/incomplete assessments of the cost and benefits of the system.
- The Implementation stage is begun before required planning for testing is complete.

Objective

4.A To ascertain that a detailed system design is developed from the functional specifications created in the general design.

Criteria

4.A.1 Programming specifications are addressed in a Detailed System Design Report or similar document.

4.A.2 The accuracy and completeness of Detailed System Design specifications has been acknowledged by the appropriate level of user and by Data Processing management.

4.A.3 The data dictionary/directory has been updated to reflect the contents of the Detailed System Design document.

4.A.4 Testing has been addressed in a Test Plan or similar document.

4.A.5 The accuracy and completeness of the Test Plan has been acknowledged by the appropriate level of user and by Data Processing management.

4.A.6 The testing covers all user requirements.

4.A.7 All required skills continue to be available to the project.

4.A.8 Dates for Committee meetings and the items to be discussed at each meeting continue to be addressed in a Steering Committee Meeting Schedule or similar document.

4.A.9 The status of the project compared to the budget and schedule contained in the General Design Stage Status document has been addressed in a Detailed Design Stage Project Status Report or similar document.

4.A.10 The accuracy and completeness of the Detailed Design Stage Status document and agreement with it has been acknowledged by the appropriate level of user and by Data Processing management.

4.A.11 A human resources impact analysis has been performed.

Note 1: This objective and its criteria correspond to identically named Audit Programs in Appendix E.

Data (B) and Systems Management Controls (C) being designed into the System

In this Detail Design Stage, the application control techniques, identified in the previous stage, have been developed into input, processing, and output controls. In many respects, auditing data and system management controls now begins to resemble the auditing of an ongoing system. The main difference is that the auditor has to audit the test plan/design of the project team and should plan to re-perform control tests only selectively.

Input controls will involve the transmission, acceptance, conversion, and validation of data and the correction of errors. Processing controls will involve access restrictions and verification of data integrity between processing steps and within data bases. They will also minimize the impact of system failures in on-line systems. Output controls consist of overall reconciliation and balancing of output files and reports and the safeguards over them.

To a certain extent, the nature of the application controls developed will be a function of the particular system application. It is therefore not practical to try to anticipate the detailed systems design specifications associated with each control technique to be included. Again, Appendix I contains references dealing with the audit of Ongoing Systems. As well as reviewing the testing to be undertaken by the project team to verify that it covers control requirements, the auditor should begin to identify those controls that should be re-tested (note RE-TESTED, not TESTED) once the first programs are available, probably in the late Implementation or early Installation Stages.

Key Risks

Audit activity, addressing the following key risk, should be incorporated into the audit plan:

- failure to include all control requirements in the test plan.

Objective

4.B To ensure that the data processed and stored by the system are complete, accurate and authorized.

Criteria

4.B.1 Processing control techniques outlined in the Processing Controls Specifications Report have been included for testing in the Test Plan or similar document.

Note 1: This objective and its criteria correspond to identically named Audit Programs in Appendix E.

Objective

4.C To ensure that the system will operate efficiently and effectively.

Criteria

4.C.1 Control techniques to satisfy the requirements outlined in the System Management Controls Specifications document have been included for testing in the Test Plan or similar document.

Note 1: This objective and its criteria correspond to identically named Audit Programs in Appendix E.

5. Implementation Stage

Based on the system design specifications documented in the previous stage, the system under development is implemented in computer-based and manual systems and put into operational status in the next stage.

Computer programs and manual procedures are written and tested. Training material and the Installation Schedule are prepared.

Project Control (A) Concerns

Project performance during the Implementation Stage compared to the plans and budgets established at the Feasibility stage (or revised subsequently) should have been monitored and variances justified to the project authorities.

System and program testing must be comprehensive and thoroughly documented. Problems encountered should have been addressed and rectified. The auditor may choose to re-perform selectively some tests but should never be perceived as being responsible for testing.

User manuals, input and output formats, screen layouts and any other form of user interface should be designed to optimize user efficiency.

Key Risks

Audit activity, covering the following key risks, should be incorporated as part of the audit plan:

- Adequate site preparation may not have been performed. The auditor should take care to assess that telecommunication line installation, hardware delivery and physical site preparation activity have not been compromised because the installation date is close to the expiration of budgeted resources

- Adequate training plans may not have been developed and adequately shared with the user

- Systems personnel may not completely understand the users' needs

- There may be inadequate documentation of systems design, programs/dialogue, and the user's manuals

- Testing may be inadequate owing to time or other resource constraints

Objective

5.A To establish that all appropriate forms, manuals, programs and training materials are created from the detailed systems specifications.

Criteria

5.A.1 All manuals and other outputs required have been completed before installation begins.

5.A.2 The accuracy and completeness of the required manuals and outputs has been acknowledged by the appropriate level of user and by Data Processing management.

5.A.3 Testing results have been addressed in a Test Report or similar document.

5.A.4 The accuracy and completeness of the Test Report have been acknowledged by the appropriate level of user and by Data Processing management.

5.A.5 All required skills continue to be available to the project.

5.A.6 Dates for Committee meetings and the items to be discussed at each meeting continue to be addressed in a Steering Committee Meeting Schedule or similar document.

5.A.7 The status of the project compared to the budget and schedule contained in the Detailed Design Stage Status document has been addressed in an Implementation Stage Project Status Report or similar document.

5.A.8 The accuracy and completeness of the Implementation Stage Status document and agreement with it has been acknowledged by the appropriate level of user and by Data Processing management.

Note 1: This objective and its criteria correspond to identically named Audit Programs in Appendix F.

Data (B) and Systems Management Controls (C) Being Built into the System

At this stage of development, to ensure that data integrity and systems management will exist, controls are being built into the new system. While the auditor's main efforts are focused on auditing testing activity, which has been covered in the section above on Project Control Concerns, there is the opportunity now to re-perform selected tests of key controls.

Appendix I contains reference material for determining appropriate techniques to re-test the selected controls, depending on the nature of the system and its environment. Real-time on-line systems, using data base management systems under the control of separate data administrative management will demand more sophisticated re-tests than typical batch input, tape master file systems. The judicious use of the reference material will enable an auditor with substantial EDP experience to perform efficient and effective re-testing.

Key Risks

Audit activity, addressing the following key risks, should be incorporated as part of the audit plan:

- The total reliance by the auditor on the project team's documentation of its own team testing could result in erroneous judgements on the overall completeness and accuracy of project team testing

- The auditor could expend effort in re-testing controls that are in the process of being re-programmed. It is important to determine how stable the test system is before re-performing selected control tests

Objective

5.B To ensure that key data controls are effective.

Criteria

5.B.1 Re-perform selected data integrity control tests.

Note 1: This objective and its criteria correspond to identically named Audit Programs in Appendix F.

Objective

5.C To ensure that key system controls are effective.

Criteria

5.C.1 Re-perform selected system integrity control tests.

Note 1: This objective and its criteria correspond to identically named Audit Programs in Appendix F.

6. Installation Stage

During this stage the system is put into operational status. Training is undertaken and files are converted.

The system is installed in accordance with the plan developed in the previous stage. This may require a phased installation, by geographical location, by

organizational component, or location determined by need for instance. The last case requires needs criteria. "Sign-off" of acceptance is required from the user.

Project Control (A) Concerns

Project performance during the Installation Stage compared to the plans and budgets established at the Feasibility stage (or as revised subsequently) should have been monitored and variances justified to the project authorities.

Data conversion should be accurate. Testing of the data conversion process should be well documented. Depending on the quality and coverage of the testing performed by the auditee, auditors may wish to re-perform their own tests.

Key Risks

Audit activity, addressing the following key risks, should be considered during this audit stage:

- inaccurate or incomplete conversion of files

- inadequate training of personnel

- poor management of cut-over

- improperly functioning system, owing to incomplete testing or ineffective user involvement during acceptance testing

- as fiscal year end, or any other type of calendar/time/money constraint approaches, training, testing, and project control can be short-changed, compromising the project team's reaction to the audit recommendations from previous stages

- a tested contingency plan may not be available to the operators of the system

Objective

6.A To ensure that the system and any file conversions properly move from development status to operational and maintenance status.

Criteria

6.A.1 The accuracy, completeness, and authenticity of the files created by conversion are ensured through the use of appropriate control techniques.

6.A.2 Training has been carried out in accordance with the schedule prepared.

6.A.3 Installation was carried out in accordance with the schedule prepared.

6.A.4 The status of the project relative to the budget and schedule contained in the Implementation Stage Status document has been addressed in an Installation Stage Project Status Report or similar document.

6.A.5 The accuracy and completeness of the Installation Stage Status document and agreement with it has been acknowledged by the appropriate level of user and Data Processing management.

Note 1: This objective and its criteria correspond to identically named Audit Programs in Appendix G.

Note 2: As shown in figure 4, there are no objectives for Data controls (B) and System controls (C) for the Installation Stage (6).

7. Post-Installation Stage

During this phase, the system will be in operation and will be adjusted using controlled system changes, to run correctly and according to current needs. A project report should be prepared, three to six months after installation, to

indicate the degree of adherence to user functional requirements and the degree to which predicted costs/benefits were achieved.

Project Control (A) Concerns

Audit activity in this phase involves a review of the Post-Installation report and working papers against all earlier documentation, to ensure compliance with the SDLC and to attest to the accuracy and completeness of the findings.

Key Risks

Audit activity, addressing the following key risks, should be included in the audit plan:

- An adequate number of trained operators, quality system and user documentation, and an availability of appropriate support may not exist
- Support, in the form of "hot line" technical advice, Information Centre technicians, or any other appropriate form, may not exist
- Documented operational inadequacies, so that management can prevent future inadequacies of the same type, may not exist

Objective

7.A To establish that the system operates in accordance with the design objectives and other measurement criteria, and project costs/benefits have been achieved.

Criteria

7.A.1 A formal post-installation review has been undertaken and the results reported to management.

Note 1: This objective and its criteria correspond to identically named Audit Programs in Appendix G.

Note 2: As shown in figure 4, there are no objectives for Data controls (B) and System controls (C) for the Post Installation (7).

SUD Interview Matrix

Legend

- DBA = Data Base Administrator
- D/A = Designer/Analyst
- DDM = Departmental Data Mgr
- Mgt = Management
- Pgm = Programmer
- PM = Project Manager
- SC/AA = Steering Committee/Approval Authority
- Sec = Departmental Security Officer
- Usr = Users

Audit Step	PM	Mgt	SC/AA	D/A	Pgm	Usr	Sec	DDM	DBA
1.A.1.1	X	X	X						
1.A.1.2	X	X				X		X	
1.A.2.1	X	X	X			X			
1.A.2.2	X			X		X			
1.A.3.1		X							
1.A.3.2									
1.A.3.3	X								
1.A.3.4									
1.A.3.5	X	X							
1.A.4.1	X								
1.A.4.2	X		X						
1.A.4.3	X			X					
1.A.5.1	X								
1.A.5.2	X								
1.A.5.3	X								
1.A.6.1			X						
1.A.6.2	X		X						

Audit Step	PM	Mgt	SC/AA	D/A	Pgm	Usr	Sec	DDM	DBA
2.A.1.1				X		X			
2.A.1.2				X		X			
2.A.2.1	X		X						
2.A.2.2	X			X					
2.A.3.1	X					X			
2.A.3.2	X					X			
2.A.3.3	X					X			
2.A.4.1	X		X						
2.A.4.2	X		X			X			
2.A.5.1	X								
2.A.5.2	X					X			
2.A.6.1	X		X						
2.A.6.2	X		X			X			
2.A.7.1	X		X						
2.A.8.1	X		X			X			
2.A.8.2	X		X			X			
2.A.9.1	X		X			X			
2.A.9.2	X					X			
2.A.9.3	X					X			
2.A.9.4	X								
2.A.10.1	X		X						
2.A.10.2	X					X			
2.B.1.1	X			X		X	X	X	
2.B.1.2				X		X			
2.B.2.1	X		X						
2.B.3.1	X					X	X		
2.C.1.1	X			X		X			
2.C.1.2	X			X		X			
2.C.2.1	X		X						

Audit Step	PM	Mgt	SC/AA	D/A	Pgm	Usr	Sec	DDM	DBA
3.A.1.1	X			X		X			
3.A.1.2	X			X		X			
3.A.2.1	X		X						
3.A.3.1	X			X				X	X
3.A.4.1	X								
3.A.5.1	X		X			X			

Audit Step	PM	Mgt	SC/AA	D/A	Pgm	Usr	Sec	DDM	DBA
3.A.5.2	X		X			X			
3.A.6.1	X								
3.A.6.2	X					X			
3.A.6.3	X					X			
3.A.6.4	X					X			
3.A.6.5	X								
3.A.6.6	X					X			
3.A.7.1	X		X						
3.B.1.1	X			X		X			
3.B.1.2	X			X		X			
3.B.2.1	X		X						
3.C.1.1	X			X		X			
3.C.1.2	X			X		X			
3.C.2.1	X		X						

Audit Step	PM	Mgt	SC/AA	D/A	Pgm	Usr	Sec	DDM	DBA
4.A.1.1	X			X					
4.A.1.2				X		X			
4.A.2.1	X		X						
4.A.3.1				X				X	X
4.A.4.1	X			X		X			
4.A.4.2				X					
4.A.5.1	X		X			X			
4.A.6.1				X					
4.A.7.1	X								
4.A.8.1	X		X			X			
4.A.8.2	X		X						
4.A.9.1	X					X			
4.A.9.2	X					X			
4.A.9.3	X					X			
4.A.9.4	X					X			
4.A.9.5	X					X			
4.A.9.6	X					X			
4.A.10.1	X		X						
4.B.1.1	X			X					
4.B.1.2				X					
4.B.2.1	X		X						
4.C.1.1	X			X					

4.C.1.2				X					
4.C.2.1	X		X						

Audit Step	PM	Mgt	SC/AA	D/A	Pgm	Usr	Sec	DDM	DBA
5.A.1.1	X			X		X			
5.A.2.1	X			X		X			
5.A.3.1	X			X		X			
5.A.3.2	X			X					
5.A.4.1	X		X						
5.A.5.1	X								
5.A.6.1	X		X			X			
5.A.6.2	X		X						
5.A.7.1	X					X			
5.A.7.2	X					X			
5.A.7.3	X					X			
5.A.7.4	X					X			
5.A.7.5	X					X			
5.A.7.6	X					X			
5.A.8.1	X		X						

Audit Step	PM	Mgt	SC/AA	D/A	Pgm	Usr	Sec	DDM	DBA
6.A.1.1	X					X			
6.A.1.2	X			X		X			
6.A.2.1	X					X			
6.A.3.1	X			X		X			
6.A.3.2	X					X			
6.A.4.1	X					X			
6.A.4.2	X					X			
6.A.4.3	X					X			
6.A.4.4	X					X			
6.A.4.5	X					X			
6.A.4.6	X					X			
6.A.5.1	X			X		X			

Audit Step	PM	Mgt	SC/AA	D/A	Pgm	Usr	Sec	DDM	DBA
7.A.1.1	X					X			
7.A.1.2	X					X			

7.A.1.3	X					X		
7.A.1.4	X					X		
7.A.1.5	X					X		

Appendix B: Audit Program for the Project Initiation Stage

Stage: 1. Project Initiation

Objective: 1.A To establish that the project is formally initiated and that appropriate project control measures exist.

Criterion: 1.A.1. The need for the project has been addressed in a Project Initiation Report or similar document.

Audit Step: 1.A.1.1 Has a Project Initiation document been prepared and released by the Project Manager?

Y	N	N/A	Comments	XREF

Audit Step: 1.A.1.2 Verify that Project Initiation document contains at least the following:

- a clear statement of the project definition prepared by the user group

- a clear link between the departmental Information Management Plan (IMP)and Multi Year Operational Plan (MYOP)

- assurances that the data and the system are not already provided for by existing systems or other projects

- an evaluation of the present system to ensure that the proposed system is required

- a statement of internal and external constraints, such as organizational changes required, legislative changes required, impact on other systems

- special security requirements

- a preliminary cost/benefit and risk analysis of viable alternatives

- an explanation of the source of funds for the project, including reference to any special requirements, like Treasury Board submissions, which may be involved.

Criterion: 1.A.2 The need for the project acknowledged by the user at the appropriate level, and Data Processing management.

Audit Step: 1.A.2.1 Has the Project Initiation document been reviewed and approved by management at least one level above those who will be held directly accountable for the project?

Y	N	N/A	Comments	XREF

Audit Step: 1.A.2.2 Have steps been taken by the project team to identify and consult all affected parties?

Y	N	N/A	Comments	XREF

Audit Step: 1.A.2.3 Has the project received financial approval?

Y	N	N/A	Comments	XREF

Criterion: 1.A.3. An appropriate project organization has been outlined in the Project Initiation documentation.

Audit Step: 1.A.3.1 Determine by examining the Project Initiation document that:

- Project Team members and representatives and their responsibilities have been named including:

    o Project Director

    o Project Manager

    o User Manager/Director

    o Technical Representatives

    o User Functional Representatives

- a Steering Committee or Sign Off Authorities have been established

- if appropriate, a TB Program Branch official has been identified, and his or her role in the project determined

Audit Step: 1.A.3.2 Evaluate the background and qualifications of project members for their assignment to specific project tasks.

Y	N	N/A	Comments	XREF

Audit Step: 1.A.3.3 Has the user department management appointed personnel from its department to participate in the project?

Y	N	N/A	Comments	XREF

Audit Step: 1.A.3.4 Do user department personnel and the project team have the same understanding of the scope and objectives of the project?

Y	N	N/A	Comments	XREF

1.A.3.5 Verify that the Project Manager or one of the team members is responsible to ensure the complete and accurate accumulation of project costs.

Y	N	N/A	Comments	XREF

Audit Step: 1.A.3.6 Determine that the Steering Committee/Sign Off Authority is representative of management at least one level higher than the Project Manager and that it represents all interested parties.

Y	N	N/A	Comments	XREF

Audit Step: 1.A.3.7 Determine that the required and actual level of security and reliability clearance for team members is established and verified.

Y	N	N/A	Comments	XREF

Criterion: 1.A.4 An appropriate project development process is outlined in the Project Initiation documentation.

Audit Step: 1.A.4.1 Determine, by referral to the Project Initiation document, that a formal process for carrying out the project is outlined. (In the absence of a departmental process, the process outlined in Chapter 440, Section 3 of the Treasury Board Administrative Policy Manual could still be used as a guide).

Y	N	N/A	Comments	XREF

Audit Step: 1.A.4.2 Have variations from the approved departmental process been highlighted and reasons for the variances stated?

Y	N	N/A	Comments	XREF

Audit Step: 1.A.4.3 Has prototyping (see the start of Chapter 2) been considered as a development technique, with appropriate consideration for:

- the prevention of too much prototyping (see Chap. 2, page 16 for a brief description of prototyping)

- its use at stages of the development process (ie., during the Feasibility stage through General Design)

- effective user involvement with the prototype (by seeing that the user needs are reflected in the prototype)

Y	N	N/A	Comments	XREF

Criterion: 1.A.5 A work plan, including reasonable target dates and resource requirements for each stage, is provided in the Project Initiation document.

Audit Step: 1.A.5.1 Determine from the Project Initiation document that a work plan, including target dates and resource requirements, has been prepared.

Y	N	N/A	Comments	XREF

Audit Step: 1.A.5.2 Verify that the total resource requirements indicated in the work plan are in keeping with those outlined in the preliminary cost/benefit analysis.

Y	N	N/A	Comments	XREF

Audit Step: 1.A.5.3 Verify that the target dates indicated in the work plan are in keeping with the resource requirements outlined and any constraints involved.

Y	N	N/A	Comments	XREF

Audit Step: 1.A.5.4 Verify that the work plan includes the development of a human resources plan for all employees to be affected by the new system.

Y	N	N/A	Comments	XREF

Criterion: 1.A.6 The project organization, the development process, and the work plan have been formally accepted by an appropriate level of management.

Audit Step: 1.A.6.1 Has the Initiation Document been reviewed by management levels at least one above those who will be on the Steering Committee/Sign Off Authorities? Have they signified acceptance of the organization, the development process, and the work plan?

Y	N	N/A	Comments	XREF

Audit Step: 1.A.6.2 Is there a plan for the project manager to present periodic reports to management indicating the project costs and actual achievements compared to the project plans?

Y	N	N/A	Comments	XREF

Appendix C: Audit Program for the Feasibility Stage

Stage: 2. Feasibility Study

Objective: 2.A To establish that a feasibility study, including an Overall Project Plan, has been undertaken to determine the most appropriate solution to a stated problem in terms of organizational capability, economic justification, and technical suitability.

Criterion: 2.A.1 User requirements are addressed in a User Requirements Report or similar document.

Audit Step: 2.A.1.1 Has a User Requirements document been prepared and released? Does it include the following expression of need in terms of the organization's mission:

- A description of the current function.

- Deficiencies of the current function.

- Resources expended on the current function.

- Volume of work produced with the current function, including peak processing performance and projected growth.

- Internal control and security requirements.

- Justification for improvement and changes.

- Scope and objectives of proposed system.

- Alternative solutions to solving the need.

- Relationships with other systems.

- Relationships with long-range plans and other information resource management initiatives.

Note: See Gane and Sarson, Appendix I, Item 22, contains further areas of investigation concerning user requirements.

Y	N	N/A	Comments	XREF

Criterion: 2.A.2 The accuracy and completeness of user requirements has been acknowledged by the appropriate level of user, and by Data Processing management.

Audit Step: 2.A.2.1 Has the User Requirements document been reviewed by the Steering Committee/Sign Off Authorities?

- Have they signified acceptance of the need to continue the project? Note any conditional acceptance for follow-up in later stages.

Y	N	N/A	Comments	XREF

Audit Step: 2.A.2.2 Have steps been taken by the project team to identify and consult all affected parties?

Criterion: 2.A.3 The analysis of alternative processing configurations has been described in a Feasibility Study or similar document.

Audit Step: 2.A.3.1 Has a Technological Feasibility Study been prepared and documented?

- Are there organizational standards for the content and conduct of Technological Feasibility Studies?

- Is the proposed technology feasible, considering the technical sophistication existing or available through the organization?

Y	N	N/A	Comments	XREF

Audit Step: 2.A.3.2 Review the technology feasibility report to see if it has adequately addressed:

- Hardware needs and availability.

- System software needs and availability.

- Communications hardware and software needs availability. Valid time constraints in the user department's information requirements and the manner of satisfying them.

- Operational feasibility (eg. whether the new project fits into the current mix of hardware, software, and communications).

Y	N	N/A	Comments	XREF

Audit Step: 2.A.3.3 Verify that there is a consensus among user departments and designers concerning the technological aspects of the system's configuration.

Y	N	N/A	Comments	XREF

Audit Step: 2.A.3.4 Determine the organizational capability to manage the related technologies and to decide whether the technologies should be developed or bought, operated in-house or out, and maintained in-house or out.

Y	N	N/A	Comments	XREF

Audit Step: 2.A.3.5 Confirm with independent sources the reliability and track record of the recommended hardware and software.

Y	N	N/A	Comments	XREF

Criterion: 2.A.4 The user of an appropriate level and Data Processing management have acknowledged that the analysis of processing alternatives is accurate and complete and agrees with the recommendations.

Audit Step: 2.A.4.1 Has the Feasibility Study document been reviewed by the Steering Committee/Sign Off Authorities?

- Have they signified acceptance of the recommendations and the need to continue the project? Note any conditional acceptance for follow-up in later stages.

Y	N	N/A	Comments	XREF

Audit Step: 2.A.4.2 Have steps been taken by the project team to identify and consult all affected parties?

Y	N	N/A	Comments	XREF

Criterion: 2.A.5 Resource estimates and other financial data have been addressed in a Cost/Benefit Analysis Report or similar document.

Audit Step: 2.A.5.1 Has a Cost/Benefit document been prepared and released? Are all costs identified as operating or capital?

Note: Information from the Advisory Committee on Information Management (ACIM) committees should also be used as reference material at this point in the audit.

Y	N	N/A	Comments	XREF

Audit Step: 2.A.5.2 Ensure that the analysis of the project costs and benefits was prepared to evaluate the economic feasibility of each alternative:

- the assumptions and constraints in the cost/benefit analysis for reasonableness

- the user and system costs cover all stages of the life cycle

- the estimated costs for each alternative include hardware and software enhancements needed to support that alternative

- estimated costs for each alternative includes cost of security and internal controls, data preparation and entry, file conversion, testing, parallel operations, acceptance, and related costs

- the basis of estimation and computation of costs is reasonable

- there is a consensus among end users, designers,and implementors concerning system costs, benefits, and contractual agreements

Y	N	N/A	Comments	XREF

Audit Step: 2.A.5.3 Ensure that the analysis of the project costs and benefits takes into consideration the impact on human resources. Verify that estimated costs for each alternative includes:

- training, and

- redeployment of staff.

Y	N	N/A	Comments	XREF

Criterion: 2.A.6 The accuracy and completeness of the cost/benefit analysis and acceptance of the recommended alternative has been acknowledged by the appropriate level of user and by Data Processing management.

Audit Step: 2.A.6.1 Has the Cost/Benefit document been reviewed by the Steering Committee/Sign Off Authorities?

- Have they signified acceptance of the recommended alternative and the need to continue the project? Note any conditional acceptance for follow-up in later stages.

Y	N	N/A	Comments	XREF

Audit Step: 2.A.6.2 Have steps been taken by the project team to identify and consult all affected parties?

Y	N	N/A	Comments	XREF

Criterion: 2.A.7 Based on the alternative recommended in the cost/benefit analysis, a Personnel Skills Summary has been prepared by the Project Manager summarizing the following information:

- required skill categories (administrative and technical)
- required skill levels
- required number of skilled personnel
- required authority level

Audit Step: 2.A.7.1 Has the Project Manager prepared a Personnel Skills Summary?

Y	N	N/A	Comments	XREF

Audit Step: 2.A.7.2 Does the Personnel Skills Summary address the following:

- required skill categories (administrative and technical)?

- required skill levels?

- required number of skilled personnel?

- required authority level?

Y	N	N/A	Comments	XREF

Audit Step: 2.A.7.3 Does the Project documentation show that the skills of the staff employed on the project (as Team Members or Steering Committee/Sign Off Authority members) meet the requirements specified in the Personnel Skills Summary?

Y	N	N/A	Comments	XREF

Criterion: 2.A.8 Dates for Committee meetings and the items to be discussed at each meeting have been addressed in a Steering Committee Meeting Schedule or similar document.

Audit Step: 2.A.8.1 Has a Steering Committee Meeting Schedule document been prepared and released to all interested parties, including EDP and user management?

Y	N	N/A	Comments	XREF

Audit Step: 2.A.8.2 Review the minutes of the Committee meetings and note the following:

- that EDP and user management were represented at each meeting, and

- that meetings were held regularly.

Y	N	N/A	Comments	XREF

Criterion: 2.A.9 The status of the project compared to the work plan contained in the Project Initiation document has been addressed in a Feasibility Stage Project Status Report or similar document.

Audit Step: 2.A.9.1 Has a Feasibility Stage Status document been prepared and released?

Y	N	N/A	Comments	XREF

Audit Step: 2.A.9.2 Verify that it contains at least the following:

- actual resources used to date, compared to planned, with reasons for variance

- actual milestones achieved to date, compared to planned, with reasons for variance

- detailed plan for General Design Stage, including reference to the following:

- analyzing and specifying the user's detailed requirements

- establishing change control processes

- updating the cost/benefit analysis

- obtaining management approval

- updated budget and reasons for any changes

- updated schedule and reasons for any changes

- recommendation to continue or discontinue the project

Y	N	N/A	Comments	XREF

Audit Step: 2.A.9.3 Verify actual resources used in the source documents.

Y	N	N/A	Comments	XREF

Audit Step: 2.A.9.4 Verify that the updated budget and schedule are in keeping with the feasibility study and cost/benefit analysis.

Y	N	N/A	Comments	XREF

Criterion: 2.A.10 The accuracy and completeness of the Feasibility Stage Status document has been acknowledged by the appropriate level of user, and by Data Processing management, and they agree with it.

Audit Step: 2.A.10.1 Has the Feasibility Stage Status document been reviewed by the Steering Committee/Sign Off Authorities? Have they confirmed its acceptance?

Y	N	N/A	Comments	XREF

Audit Step: 2.A.10.2 Have steps been taken by the project team to identify and consult all affected parties?

Note: The auditor is likely to find that the Cost/Benefit Analysis and the Feasibility Stage Status documents are combined. In any event, management acceptance of the cost/benefit analysis recommendation will be tantamount to accepting the updated budget. The updated schedule is a different matter.

Y	N	N/A	Comments	XREF

Objective: 2.B To ascertain that data processed and stored by the system will be complete, accurate, and authorized, and that security, privacy, and accessibility levels for the system's data are specified.

Criterion: 2.B.1 The need for processing control requirements are identified in a System Processing Controls Specifications or similar document.

Audit Step: 2.B.1.1 Does the Feasibility Study identify the need for a System Processing Controls Specifications or similar document?

Y	N	N/A	Comments	XREF

Criterion: 2.B.2 The level of security, privacy, and accessibility of system data has been documented by the user representative.

Audit Step: 2.B.2.1 Determine that a statement of the level of security, privacy and accessibility needed for system's data conforms to the TB policies (see Appendix J for a list of relevant documents) or government Acts, and that the statement is included with the documentation to be reviewed by the Steering Committee/Sign Off Authorities.

Y	N	N/A	Comments	XREF

Objective: 2.C To ensure that the system operates efficiency, effectively, and economically.

Criterion: 2.C.1 The need for system management control requirements is identified in a System Management Controls Specifications or similar document.

Audit Step: 2.C.1.1 Does the Feasibility Study identify the need for a System Management Controls Specifications or similar document?

Y	N	N/A	Comments	XREF

Appendix D: Audit Program for the General Design Stage

Stage: 3. General Design

Objective: 3.A To ensure that the general design of the system expands on the findings of the feasibility study, produces a functional description of manual and EDP processes, and devises an overall system design that can be used to obtain a commitment for further development.

Criterion: 3.A.1 System specifications are addressed in a System Specifications Report or similar document.

Audit Step: 3.A.1.1 Has a Systems Specifications document been prepared and released?

Y	N	N/A	Comments	XREF

Audit Step: 3.A.1.2 Verify that it contains at least the following:

- system objectives and scope

- general system concept and design considerations

- chart showing function structure in terms of processes

- logical data flow diagram showing flow among processes and data stores at the data element level

- process descriptions, including complete and detailed definitions of processes for all business cases involved. Descriptions will include algorithms and validity checks

- system interfaces: definitions at the data element level

- system inputs and outputs: definitions at the data element level with the medium to be used for input and output specified

- data stores: definitions of logical data stores at the data element level

- volumes, timings, highs and lows, and quality specified for inputs, outputs, and data stores

- service levels: Complete description of performance requirements. This will be used in later stages to confirm the technical feasibility and resources requirement of the system

- audit, control, and security requirements - implementation requirements, including conversion

- (see Gane and Sarson reference, Item 22 in Appendix I, for a description of some of the terms.)

Y	N	N/A	Comments	XREF

Criterion: 3.A.2 The accuracy and completeness of system specifications has been acknowledged by the appropriate level of user and by Data Processing management.

Audit Step: 3.A.2.1 Has the System Specifications document been reviewed by the Steering Committee/Sign Off Authorities? Have they signified acceptance of the need to continue the project? Note any conditional acceptance for follow-up in later stages.

Y	N	N/A	Comments	XREF

Criterion: 3.A.3 The data dictionary/directory has been updated to reflect the contents of the System Specifications document.

Audit Step: 3.A.3.1 Has the data dictionary/directory been updated to contain the system specifications?

Y	N	N/A	Comments	XREF

Criterion: 3.A.4 All required skills are still available to the project.

Audit Step: 3.A.4.1 Do the skills of the staff being employed on the project (as Team Members or Steering Committee/Sign Off Authority members) continue to meet the requirements specified in the Personnel Skills Summary?

Y	N	N/A	Comments	XREF

Criterion: 3.A.5 Dates for committee meetings and the items to be discussed at each meeting continue to be addressed in a Steering Committee Meeting Schedule or similar document.

Audit Step: 3.A.5.1 Has a Steering Committee Meeting Schedule document been prepared and released to all interested parties, including EDP and user management?

Y	N	N/A	Comments	XREF

Audit Step: 3.A.5.2 Attend or review the minutes of the committee meetings and note the following:

- representatives from EDP and user management were represented at each meeting, and

- meetings were held regularly.

Y	N	N/A	Comments	XREF

Criterion: 3.A.6 The status of the project compared to the budget and schedule contained in the Feasibility Stage Status document has been addressed in a General Design Stage Project Status Report or similar document.

Audit Step: 3.A.6.1 Has a General Design Stage Status document been prepared and released?

Y	N	N/A	Comments	XREF

Audit Step: 3.A.6.2 Verify that it contains at least the following:

- actual resources used to date, compared to planned, with reasons for variance

- actual milestones achieved to date, compared to planned, with reasons for variance

- detailed plan for the Detailed Design Stage, including the following activities:

    - updating the data dictionary/directory

    - carrying out the final design of all inputs and outputs

    - developing a detailed implementation plan - verifying that security concerns have been met

    - developing a detailed testing plan

    - estimating performance and resource requirements

    - updating project plans and budgets

    - updating the cost/benefit analysis

    - obtaining management approval

- the preliminary plan for the Implementation Stage, includes the following:

    - identification of manual procedures to be developed

    - manuals that will be affected

    - facilities needs

    - communications needs

    - training

- an updated budget and reasons for any changes

- an updated schedule and reasons for any changes

- an updated cost/benefit analysis

- a recommendation to continue or discontinue the project

Y	N	N/A	Comments	XREF

Audit Step: 3.A.6.3 Verify actual resources used in source documents.

Y	N	N/A	Comments	XREF

Audit Step: 3.A.6.4 Are the updated budget and schedule in keeping with the updated cost/benefit analysis?

Y	N	N/A	Comments	XREF

Audit Step: 3.A.6.5 Verify the updated cost/benefit analysis against the cost/benefit analysis from the previous stage and from source documents.

Y	N	N/A	Comments	XREF

Audit Step: 3.A.6.6 Determine that the updated cost/benefit analysis has taken into consideration the human resource impact requirements.

Y	N	N/A	Comments	XREF

Criterion: 3.A.7 The accuracy and completeness of the General Design Stage Status document and agreement with it has been acknowledged by the appropriate level of user and by Data Processing management.

Audit Step: 3.A.7.1 Has the General Design Stage Status document been reviewed by the Steering Committee/Sign Off Authorities and have they signified acceptance of it?

Y	N	N/A	Comments	XREF

Criterion: 3.A.8 A human resources impact analysis is planned.

Audit Step: 3.A.8.1 Does the detailed plan for the Detailed Design Stage take into consideration a human resources impact analysis? Does the planned analysis cover all personnel to be affected? i.e. those to be trained for new system and those to be re-deployed.

Y	N	N/A	Comments	XREF

Audit Step: 3.A.8.2 Does the detailed plan for the Detailed Design Stage take into consideration the marketing of the new system? i.e. communicating to all those affected, the impact of the system on the department and themselves.

Y	N	N/A	Comments	XREF

Objective: 3.B To establish that data processed and stored by the system will be complete, accurate, and authorized.

Criterion: 3.B.1 Processing control techniques have been outlined in a System Processing Controls Specifications or similar document.

Audit Step: 3.B.1.1 Has a System Processing Controls Specifications or similar document been prepared and released?

Y	N	N/A	Comments	XREF

Audit Step: 3.B.1.2 Verify that it addresses at least the following (see Appendix for further references to data controls):

I. Completeness

    1. There should be some method of ensuring that all data are initially recorded and identified.

    2. Control should be established close to the source of the transaction.

    3. Output should be reconciled to input.

4. There should be some method of ensuring that corrections for all identified errors are re-entered into the system.

5. The timing of input submissions and output distribution should be properly coordinated with processing.

6. Procedures are needed to ensure that output reports are independently reviewed for completeness and form.

II. Accuracy

1. Procedures should exist to prevent errors in the preparation of input or source data, and to detect and correct any significant errors that do occur.

2. Procedures should exist to prevent errors arising when data are converted to machine processable form, and to detect and correct any significant errors that do occur.

3. There should be procedures to ensure that data are transmitted accurately to the computer centre.

4. Procedures should ensure that only valid files are used.

5. Controls must ensure that the accuracy of data is maintained during processing.

6. Procedures should ensure that program computations are performed correctly.

7. There should be a system of control over the physical operations of the computer system.

8. Procedures should exist to ensure that all significant errors that have been identified at various stages in the system have been corrected, re-entered and properly reflected in the output.

9. Procedures are needed to ensure that all required output reports are delivered to the proper user departments.

III. Authorization

1. To ensure that only authorized data is processed.

2. Security, privacy, and accessibility level classifications (see 2.B.2.1) for data related to the system should be determined and appropriate measures devised to ensure proper storage, transmittal, access, privacy and destruction.

3. There should be some method of identifying and locating the component file records and input/output documents involved in the processing of a given transaction or in the accumulation of a given total.

IV.   Backup/Recovery

   1.   Procedures for system backup/recovery should be documented and related training plans prepared.

   2.   Procedures for data preparation, transcription, data control, and output distribution should be documented and related training plans prepared.

V.   Audit Trail

   1.   There should be some way to identify and locate the component file records and input/ouput documents involved in the processing of a given transaction or in the accumulation of a given total.

Note: Different control concepts apply to different types of systems (e.g. batch versus on-line). See the Bibliography in Appendix I for books on controls for various types of system.

Y	N	N/A	Comments	XREF

Criterion: 3.B.2 The accuracy and completeness of the processing control technique specifications has been acknowledged by the appropriate level of user and Data Processing management.

Audit Step: 3.B.2.1 Has the Processing Control Specifications document been reviewed by the Steering Committee/Sign Off Authorities? Have they signified acceptance of it? Note any conditional acceptance for follow-up in later stages.

Y	N	N/A	Comments	XREF

Objective: 3.C To ensure that the system will operate efficiently and effectively.

Criterion: 3.C.1 System management control techniques are outlined in a System Management Controls Specifications Report or similar document.

Audit Step: 3.C.1.1 Has a System Management Controls Specifications Report or similar document been prepared and released?

Y	N	N/A	Comments	XREF

Audit Step: 3.C.1.2 Verify that it addresses at least the following:

I.   Efficiency

    1.   There should be a standard or set of standards to determine system efficiency.

    2.   There should be a mechanism to compare performance with standards and to report variances.

    3.   There should be procedures for managers to follow up on variances from standards and for recording action taken.

II. Effectiveness

    1.   Effectiveness standards for the system's objectives should be established.

    2.   There should be a mechanism to determine and report situations where systems are no longer able to meet their original objectives.

III. Economy

    1.   Management should have formal procedures to review projects and their resulting applications system regularly for economy.

Y	N	N/A	Comments	XREF

Criterion: 3.C.2 The accuracy and completeness of the system management control technique specifications have been acknowledged by the appropriate level of user and Data Processing management.

Audit Step: 3.C.2.1 Has the System Management Controls Specification document been reviewed by the Steering Committee/Sign Off Authorities? Have they signified acceptance of it? Note any conditional acceptance for follow-up in future stages.

Y	N	N/A	Comments	XREF

Appendix E: Audit Program for the Detailed Design Stage

Stage: 4. Detailed Design

Objective: 4.A To ascertain that a detailed system design is developed from the functional specification created in the general design.

Criterion: 4.A.1 Programming specifications are addressed in a Detailed System Design Report or similar document.

Audit Step: 4.A.1.1 Has a Detailed Systems Design document been prepared and released?

Y	N	N/A	Comments	XREF

Audit Step: 4.A.1.2 Verify that it covers at least the following:

- system flow and description, by function
- data element dictionary
- system files
- system inputs, including design of forms and video screens
- system outputs, including design of forms, reports and video screens
- system interface specifications
- system software specifications
- hardware specifications
- communications specifications
- system management utility specifications

- audit, control, and security specifications

- common processing module specifications

- conversion specifications

Y	N	N/A	Comments	XREF

Audit Step: 4.A.1.3 Review system specifications for each application within the system for clarity, completeness, and consistency.

Y	N	N/A	Comments	XREF

Audit Step: 4.A.1.4 Review flow charts, decision tables, or narratives to assess the reasonableness of program logic incorporated in applications.

Y	N	N/A	Comments	XREF

Criterion: 4.A.2 The accuracy and completeness of Detailed System Design specifications has been acknowledged by the appropriate level of user and Data Processing management.

Audit Step: 4.A.2.1 Has the Detailed System Design document been reviewed by the Steering Committee/Sign Off Authorities? Have they signified acceptance? Note any conditional acceptance for follow-up in later stages.

Y	N	N/A	Comments	XREF

Criterion: 4.A.3 The data dictionary/directory has been updated to reflect the contents of the Detailed System Design document.

Audit Step: 4.A.3.1 Has the data dictionary/directory been updated to contain the detailed system specifications?

Y	N	N/A	Comments	XREF

Criterion: 4.A.4 Testing has been addressed in a Test Plan or similar document.

Audit Step: 4.A.4.1 Has a program and system test plan been developed and released?

Y	N	N/A	Comments	XREF

Audit Step: 4.A.4.2 Verify that it covers at least the following both for program and system testing, and for volume and operational testing:

- overview of the software to be tested, including vendor software and conversion software and the work environment it operates in

- test schedule

- locations, including any special travel and accommodation requirements

- materials and supplies including equipment, software, storage facilities (magnetic and physical), personnel, documentation, test input, sample output, and special forms

- training requirements

- list of user requirements to be tested

- list of operational requirements to be tested

- overview of test progression

- description of the test to be performed on each requirement including the type of input to be used, the method for recording results, constraints such as equipment or personnel availability, evaluation criteria and any data manipulation required for reporting purposes

Y	N	N/A	Comments	XREF

Audit Step: 4.A.4.3 Compare the information included in the test plan with one of the following standards or guides:

- The Institute for Electrical and Electronics Engineers System Test Plan Standard and Unit Test Plan Standard.

- Auerbach's A Standard for Testing Application Software.

Y	N	N/A	Comments	XREF

Criterion: 4.A.5 The accuracy and completeness of the Test Plan has been acknowledged by the appropriate level of user and by Data Processing management.

Audit Step: 4.A.5.1 Has the Test Plan document been reviewed by the Steering Committee/Sign Off Authorities?

Y	N	N/A	Comments	XREF

Criterion: 4.A.6 The testing covers all user requirements.

Audit Step: 4.A.6.1 Are all of the items in the User Requirements document being tested? Appropriate tests may include: walk throughs, simulations and prototypes. Where items are not being tested, check that a suitable explanation has been provided and accepted by the Steering Committee/Sign Off Authorities.

Y	N	N/A	Comments	XREF

Criterion: 4.A.7 All required skills continue to be available to the project.

Audit Step: 4.A.7.1 Do the skills of the staff being employed on the project (as Team Members or Steering Committee/Sign Off Authority members) continue to meet the requirements specified in the Personnel Skills Summary?

Y	N	N/A	Comments	XREF

Criterion: 4.A.8 Dates for Committee meetings and the items to be discussed at each meeting continue to be addressed in a Steering Committee Meeting Schedule or similar document.

Audit Step: 4.A.8.1 Has a Steering Committee Meeting Schedule document been prepared and released to all interested parties including EDP and user management?

Y	N	N/A	Comments	XREF

Audit Step: 4.A.8.2 Attend or review the minutes of the Committee meetings and note the following: - EDP and user management representatives attended each meeting, and - meetings are held regularly.

Y	N	N/A	Comments	XREF

Criterion: 4.A.9 The status of the project compared to the budget and schedule contained in the General Design Stage Status document has been addressed in a Detailed Design Stage Project Status Report or similar document.

Audit Step: 4.A.9.1 Has a Detailed Design Stage Status document been prepared and released.

Y	N	N/A	Comments	XREF

Audit Step: 4.A.9.2 Verify that the status document contains at least the following:

- actual resources used to date, compared to planned, with reasons for variance

- actual milestones achieved to date, compared to planned, with reasons for variance

- detailed plan for the Implementation stage, including the following activities:

    o designing the structures, logic, and flow of each system component

    o designing all data bases and files

    o estimating system performance and resource requirements and confirming that service levels will be met

    o designing conversion tools

    o coding and testing programs

    o purchasing and testing vendor software

- integrating programs into subsystems and systems

    o developing user manuals and procedures

    o developing conversion, training and operational manuals

    o conducting volume and operational tests

    o documenting programs and systems

- o   updating project plans and budgets

- o   updating the cost/benefit analysis

- o   obtaining management approval

- preliminary plan for the Installation Stage including reference to the following:

  - o   conversion of files

  - o   training

  - o   instruction manuals

  - o   redeployment of staff

  - o   cut-over

- updated budget and reasons for any changes

- updated schedule and reasons for any changes

- updated cost/benefit analysis

- recommendation to continue or discontinue the project

Y	N	N/A	Comments	XREF

Audit Step: 4.A.9.3 Verify actual resource use in source documents.

Y	N	N/A	Comments	XREF

Audit Step: 4.A.9.4 Verify that the updated budget and schedule are in keeping with the updated cost/benefit analysis.

Y	N	N/A	Comments	XREF

Audit Step: 4.A.9.5 Verify the updated cost/benefit analysis against the cost/benefit analysis from the previous stage and from source documents.

Y	N	N/A	Comments	XREF

Audit Step: 4.A.9.6 Does the updated cost/benefit analysis take into consideration the human resource impact requirements?

Y	N	N/A	Comments	XREF

Criterion: 4.A.10 The accuracy and completeness of the Detailed Design Stage Status document and agreement with it has been acknowledged by the appropriate level of user and by Data Processing management.

Audit Step: 4.A.10.1 Has the Detailed Design Stage Status document been reviewed by the Steering Committee/Sign Off Authorities and have they signified an acceptance of it?

Y	N	N/A	Comments	XREF

Criterion: 4.A.11 A human resources impact analysis has been performed.

Audit Step: 4.A.11.1 Has a human resources impact analysis been performed?

Y	N	N/A	Comments	XREF

Audit Step: 4.A.11.2 Have the results from the analysis been reviewed by the Steering Committee/Sign Off Authorities?

Y	N	N/A	Comments	XREF

Objective: 4.B To ensure that the data processed and stored by the system is complete, accurate and authorized.

Criterion: 4.B.1 Processing control techniques outlined in the Processing Controls Specifications Report have been included for testing in the Test Plan or similar document.

Audit Step: 4.B.1.1 Has a Test Plan been prepared and released?

Y	N	N/A	Comments	XREF

Audit Step: 4.B.1.2 Verify that it addresses the control requirements outlined in the Processing Control Specifications (See objective 3.B.1).

Y	N	N/A	Comments	XREF

Objective: 4.C To ensure that the system will operate efficiently and effectively.

Criterion: 4.C.1 Control techniques to satisfy the requirements outlined in the System Management Controls Specifications document have been included for testing in the Test Plan or similar document.

Audit Step: 4.C.1.1 Has a Test Plan been prepared and released?

Y	N	N/A	Comments	XREF

Audit Step: 4.C.1.2 Verify that it addresses the control requirements outlined in the System Management Control Specifications document (see objective 3.C.1).

Appendix F: Audit Program for the Implementation Stage

Stage: 5. Implementation stage

Objective: 5.A To establish that all appropriate forms, manuals, programs and training materials have been created from the detailed systems specifications.

Criterion: 5.A.1 All manuals and other outputs required have been completed before installation begins.

Audit Step: 5.A.1.1 Determine that the following have been prepared:

- conversion tools

- user manuals

- conversion manuals

- training manuals

- operations manuals

- program and systems documentation.

Y	N	N/A	Comments	XREF

Audit Step: 5.A.1.2 Verify that the user manual does the following:

- Describes the functions sufficiently,

- Contains non-DP terminology,

- Indicates how and when it is to be used,

- Serves as a reference document,

- Explains how to prepare input data and parameters,

- Explains how to interpret output results,

- Provides a full description of the application,

- Describes how to correct errors,

- Describes how to recover operations.

Y	N	N/A	Comments	XREF

Criterion: 5.A.2 The accuracy and completeness of the required manuals and outputs have been acknowledged by the appropriate level of user and by Data Processing management.

Audit Step: 5.A.2.1 Have the required manuals and outputs been reviewed by all members of the Project Team and have they signified acceptance? Note any conditional acceptance for follow-up in later stages.

Y	N	N/A	Comments	XREF

Criterion: 5.A.3 Testing results have been addressed in a Test Report or similar document.

Audit Step: 5.A.3.1 Has a Test Report been prepared and released?

Y	N	N/A	Comments	XREF

Audit Step: 5.A.3.2 Verify that it covers at least the following both for program and system testing, and for volume and operational testing:

- test results

- reasons for any testing not completed

- follow-up action taken where required as indicated by test results

Y	N	N/A	Comments	XREF

Criterion: 5.A.4 The accuracy and completeness of the Test Report have been acknowledged by the appropriate level of user and by Data Processing management.

Audit Step: 5.A.4.1 Has the Test Report document been reviewed by the Steering Committee/Sign Off Authorities and have they signified acceptance? Note any conditional acceptance for follow-up in later stages.

Y	N	N/A	Comments	XREF

Criterion: 5.A.5 All required skills continue to be available to the project.

Audit Step: 5.A.5.1 Do the skills of the staff being employed on the project (as Team Members or Steering Committee/Sign Off Authority members) continue to meet the requirements specified in the Personnel Skills Summary?

Y	N	N/A	Comments	XREF

Criterion: 5.A.6 Dates for Committee meetings and the items to be discussed at each meeting continue to be addressed in a Steering Committee Meeting Schedule or similar document.

Audit Step: 5.A.6.1 Has a Steering Committee Meeting Schedule document been prepared and released to all interested parties, including EDP and user management?

Y	N	N/A	Comments	XREF

Audit Step: 5.A.6.2 Attend or review the minutes of the Committee meetings and note the following:

- representatives from EDP and user management attended each meeting, and

- meetings were held regularly.

Y	N	N/A	Comments	XREF

Criterion: 5.A.7 The status of the project compared to the budget and schedule contained in the Detailed Design Stage Status document has been addressed in an Implementation Stage Project Status Report or similar document.

Audit Step: 5.A.7.1 Has an Implementation Stage Status document been prepared and released.

Y	N	N/A	Comments	XREF

Audit Step: 5.A.7.2 Verify that it contains at least the following:

- actual resources used to date, compared to planned, with reasons for variance
- actual milestones achieved to date, compared to planned, with reasons for variance
- detailed plans for the Installation stage, including the following:
  - file conversion, including any reconciliations and sampling of results
  - training, including schedules and distribution of materials
  - distribution of user and operations manuals
  - redeployment of staff
  - cut-over schedule
- updated budget and reasons for any changes
- updated schedule and reasons for any changes
- updated cost/benefit analysis
- recommendation to continue or discontinue the project

Y	N	N/A	Comments	XREF

Audit Step: 5.A.7.3 Verify actual resource use in source documents.

Y	N	N/A	Comments	XREF

Audit Step: 5.A.7.4 Verify that the updated budget and schedule are in keeping with the updated cost/benefit analysis.

Y	N	N/A	Comments	XREF

Audit Step: 5.A.7.5 Verify the updated cost/benefit analysis against the cost/benefit analysis from the previous stage and source documents.

Y	N	N/A	Comments	XREF

Audit Step: 5.A.7.6 Determine that the updated cost/benefit analysis has taken into consideration the human resource impact requirements.

Y	N	N/A	Comments	XREF

Criterion: 5.A.8 The accuracy and completeness of the Implementation Stage Status document and agreement with it has been acknowledged by the appropriate level of user and by Data Processing management.

Audit Step: 5.A.8.1 Has the Implementation Stage Status document been reviewed by the Steering Committee/Sign Off Authorities and have they signified acceptance of it?

Y	N	N/A	Comments	XREF

Objective: 5.B To ensure that key data controls are effective.

Criterion: 5.B.1 Re-perform selected data integrity control tests.

Audit Step: 5.B.1.1 Re-perform selected data integrity control tests.

Note: Appendix I contains reference material for determining appropriate techniques to re-test the selected controls, depending on the nature of the system and its environment. For example, real-time on-line systems, using data base management systems under the control of separate data administrative management, will demand more sophisticated re-tests than typical batch input, tape master file systems.

Y	N	N/A	Comments	XREF

Objective: 5.C To ensure that key system controls are effective.

Criterion: 5.C.1 Re-perform selected system integrity control tests.

Audit Step: 5.C.1.1 Re-perform selected system integrity control tests.

Note: Appendix I contains reference material for determining appropriate techniques to re-test the selected controls, depending on the nature of the system and its environment. Real-time on-line systems, using data base management systems under the control of separate data administrative management, will demand more sophisticated re-tests than typical batch input, tape master file systems.

Y	N	N/A	Comments	XREF

Appendix G: Audit Program for the Installation Stage

Stage: 6. Installation Stage

Objective: 6.A To ensure that the system and any file conversions properly moves from the development status to the operational and maintenance status.

Criterion: 6.A.1 The accuracy, completeness, and authenticity of the files created by conversion are ensured through the use of appropriate control techniques.

Audit Step: 6.A.1.1 Review the conversion plan before it is executed, referring to the List of Minimum System Processing Controls. Verify that control techniques are being included in the conversion process to satisfy all control concerns.

- This is an extremely critical process. No doubt about the integrity of the data in the new files should be tolerated. Control techniques such as one-to-one checks, may have to be used.

Y	N	N/A	Comments	XREF

Audit Step: 6.A.1.2 Verify that the conversion was carried out according to plan.

Y	N	N/A	Comments	XREF

Criterion: 6.A.2 Training has been carried out in accordance with the schedule prepared.

Audit Step: 6.A.2.1. Verify that training was carried out according to the schedule prepared in the Implementation Stage and that any variations have been agreed to by user management.

Y	N	N/A	Comments	XREF

Criterion: 6.A.3 Installation was carried out in accordance with the schedule prepared.

Audit Step: 6.A.3.1 Have installations been carried out according to the schedule prepared in the implementaion Stage and have any variations been agreed to by the user management?

Y	N	N/A	Comments	XREF

Audit Step: 6.A.3.2 Has user acceptence been formally ageed to, as appropriate, according to schedule? For example, if stand-alone processing locations are being installed on an independent basis, each location should sign-off its acceptance of the system.

Y	N	N/A	Comments	XREF

Criterion: 6.A.4 The status of the project relative to the budget and schedule contained in the Implementation Stage Status document has been addressed in an Installation Stage Project Status Report or similar document.

Audit Step: 6.A.4.1 Has an installation Stage Status document been prepared and released?

Y	N	N/A	Comments	XREF

Audit Step: 6.A.4.2 Verify that it contains at least the following:

- actual resources used to date, compared to plan, with reasons for variance.

- actual milestones achieved to date, with reasons for variance.

- updated budget and reasons for any changes.

- updated schedule and reasons for any changes.

- updated cost/benefit analysis

- recommendations to continue or discontinue the project.

Y	N	N/A	Comments	XREF

Audit Step: 6.A.4.3 Verify actual resource use in source documents.

Y	N	N/A	Comments	XREF

Y	N	N/A	Comments	XREF

Audit Step: 6.A.4.4 Verify that the updated budget and schedule are in keeping with the updated cost/benefit analysis.

Y	N	N/A	Comments	XREF

Audit Step: 6.A.4.5 Verify the updated cost/benefit analysis against the cost/benefit analysis from the previous stage and from source documents.

Y	N	N/A	Comments	XREF

Audit Step: 6.A.4.6 Determine that the updated cost/benefit analysis has taken into consideration the human resource impact requirements.

Y	N	N/A	Comments	XREF

Criterion: 6.A.5 The accuracy and completeness of the Installation Stage Status document and agreement with it has been acknowledged by the appropriate level of user and by Data Processing management.

Audit Step: 6.A.5.1 The accuracy and completeness of the Installation Stage Status document and agreement with it should be acknowledged by the appropriate level of user and Data Processing management.

Y	N	N/A	Comments	XREF

Appendix H: Audit Program for the Post-Installation Stage

Stage: 7. Post-installation Stage

Objective: 7.A To establish that the system operates in accordance with the design objectives and other measurement criteria, and project costs/benifits have been achieved.

Criterion: 7.A.1 A formal post-installation review has been undertaken and the results reported to management.

Audit Step: 7.A.1.1 Has a Post-Installation report or similar document been prepared?

Y	N	N/A	Comments	XREF

Audit Step: 7.A.1.2 Verify that it contains the following:

- documentation of the system's actual achievements

- comparison of those achievements against the original objectives

- recommendations for improvements

- actual resource use, compared to the original plan, with reasons for variance

- actual milestones achieved, compared to the original plan, with reasons for variance

- updated cost/benefit analysis

Y	N	N/A	Comments	XREF

Audit Step: 7.A.1.3 Verify actual resource use in source documents.

Y	N	N/A	Comments	XREF

Audit Step: 7.A.1.4 Verify the updated cost/benefit analysis against source documents.

Y	N	N/A	Comments	XREF

Audit Step: 7.A.1.5 Determine that the updated cost/benefit analysis has taken into consideration the human resource impact requirements.

Y	N	N/A	Comments	XREF

Appendix I: Bibliography

1. The Canadian Institute of Chartered Accountants. Computer Control Guidelines. CICA, 1986.

2. The Chartered Institute of Public Finance and Accountancy. Computer Audit Guidelines. London, England: CIPFA, 1984.

3. Gallegos, Richardson, and Bortheck. Audit and Control of Information Systems. Cincinnati: South-Western Publishing, 1987.

4. Halper, Davis, O'Neil-Dunne and Pfau. Handbook of EDP Auditing. Boston: Warren, Gorham and Lamont, 1985. Chapter 7 deals with system development. Additional information appears in a supplementary publication - the 1986 and 1987 Handbook of EDP Auditing Supplements by the same authors.

5. Institute of Internal Auditors. Guidelines to Controls for Data Processing Environments. Altamonte Springs, Florida: IIA, 1983.

6. Jenkins and Pinkney. An Audit Approach to Computers. London, England: Leighton-Straker, 1978.

7. Mair, Wood, and Davis. Computer Control and Audit. Altamonte Springs, Florida: The Institute of Internal Auditors, 1984.

8. Rothberg. Structured EDP Auditing. Belmont, California: Lifetime Learning Publications, 1983. (Note: The above references are available in the OCG's audit resource centre.)

9. Auerbach. A Standard For Auditing Computer Applications Using Audit Software Packages. Boston: Warren, Gorham and Lamont.

10. Auerbach EDP Publications Inc. Auerbach EDP Auditing. Ponnsouhen, New Jersey, 08109.

11. Boar, Bernard H. Application Prototyping: A Project Management Perspective. New York: American Management Association, 1985.

12. Boar, Bernard H. Application Prototyping; A Requirement. Toronto: John Wiley & Sons, 1984.

13. 13. Office of the Auditor General. Audit Guides - Auditing EDP: Planning of the EDP Audit.

14. 14. DMR Group, Information System Delivery Series, Prototyping Guide, Ottawa, 1987

15. EDP Auditor's Foundation. Control Objectives.

16. Fitzgerald, Jerry. Designing Controls into Computerized Systems.

17. FTP Technical Library, Auditing Computer Systems, Vol.III. 492 Old Town Road, Port Jefferson Station, New Jersey, 11776.

18. Gane, Christopher P. Structured Systems Analysis: Tools and Techniques. New York: Improved Systems Technologies, 1977. 2nd Edition: Englewood Cliffs, New Jersey: Prentice-Hall, 1979.

19. The Institute of Internal Auditors. Managing The Information Systems Audit: A Case Study.

20. Kuong, Javier F. Controls for Advanced On-line/Data-Base Systems. Wellesley Hills, Massachusetts: Management Advisory Publications (P.O. Box 151-44 Washington Street, Wellesley Hills, Mass., 02181). Part 2 is also available.

21. Lowry, Christina and Little, Robert. The Perils of Prototyping, Volume 8, Number 4. Ann Arbor, Michigan: University of Michigan, 1985.

22. MacEwan, Glenn H. Specification Prototyping. Kingston: Queen's University, Department of Computing and Information Science, 1982.

23. Martin, James. Security Accuracy, and Privacy in Computer Systems. Englewood Cliifs, New Jersey: Prentice-Hall, 1973

24. Martin, James. Strategic Data Planning Methodologies. Englewood Cliffs, New Jersey: Prentice-Hall, 1982.

25. Perry, William E. Ensuring Data Base Integrity. New York: John Wiley and Sons, 1983.

26. Roder, Martha H. and Stroka, John M. Prototyping Increases Chance of Systems Acceptance. Data Management Magazine, March, 1985.

27. Willson and Root. Internal Auditing Manual. Boston: Warren, Gorham, and Lamont. See Chapter 6.

28. Yourdon, Edward. Managing the Structured Techniques. 2nd Edition. New York: Yourdon Press, 1979.

Appendix J: TB/OCG Policies and Standards

Treasury Board And Office Of The Comptroller General Policies And Standards Applicable To Systems Under Development

Administrative Policy Manual - Chapter 440 - Electronic Data Processing

- Treasury Board

- 1978

Administrative Policy Manual - Chapter 540 - Management and Control of Projects

- Treasury Board

- 1978

Financial Systems Development:

- Common Evaluation Criteria for Financial Management Systems (CGC 1197)

  - Office of the Comptroller General

  - 1988

- Financial Management Systems Handbook Modules, Office of the Comptroller General:

  - Revenue Management 1989 (CGC 1193)

  - Expenditure Management (CGC 1207)

  - Financial Planning and Budgeting (to be released)

- Financial Management Information and Systems - Risk Assessment Methodology (CGC 1189)

  - Office of the Comptroller General

  - 1989

- DRAFT: Factors for the Successful Implementation of a Financial management System

  - Office of the Comptroller General

  - 1988

- SLIDES: Financial Information Strategy, A concept for the 1990s and beyond - Financial Management Information and Systems

    o Office of the Comptroller General

    o 1989

- See also Treasury Board Circular 1988-25 below.

Guide to an Audit of the Management Process

- Office of the Comptroller General

- 1987

Guide to the Audit of Systems Under Development

- Draft

- Office of the Comptroller General

- 1988

Information Management Policy Overview - Strategic Direction in Information Technology Management in the Government of Canada 1987

- Treasury Board

Policy Interpretation Notice: Pre-Implementation Audit

- PIN 1984-03

- Office of the Comptroller General

Security Policy and Standards

- Treasury Board

- 1989

Security Policy of the Government of Canada

- Treasury Board

- 1987

Security in the Government of Canada - Interim Security Standards: Operating Directives and Guidelines - 1987

- Treasury Board

Standards for Internal Audit in the Government of Canada (CGC 1009)

- Office of the Comptroller General

- 1982

- Treasury Board Circulars:

- 1980-33 EDP - make/buy

- 1982-17 EDP - make/buy procedures

- 1983-36 Approval of EDP Systems Development Process

- 1985-8 Policy on microcomputers

- 1987-47 Government information technology standards policy

- 1987-52 Review of security policy implementation

- 1988-25 Financial Management Systems software development, procurement, and operation.