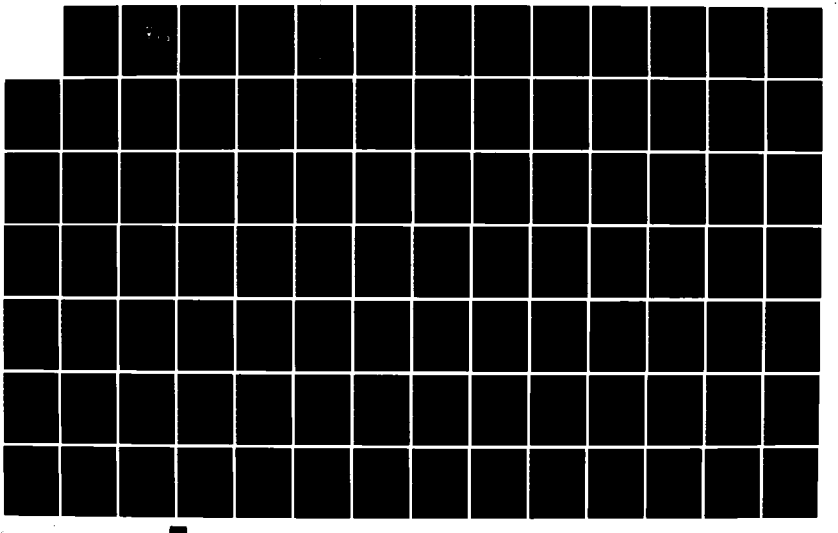
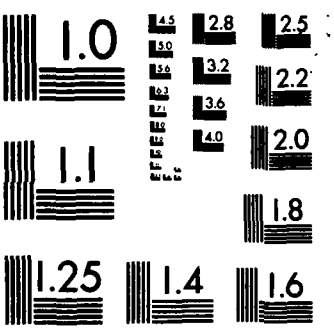
AD-A145 785 EVALUATION OF MANAGEMENT SYSTEMS PERFORMANCE AT NAVY REGIONAL DATA AUTOMATION CENTERS(U) NAVAL POSTGRADUATE SCHOOL MONTEREY CA G J SCOTT MAR 84 1/2

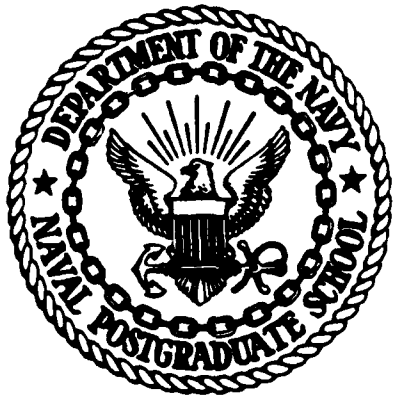
UNCLASSIFIED F/G 5/1 NL





(2)

NAVAL POSTGRADUATE SCHOOL
Monterey, California



THESIS

EVALUATION OF MANAGEMENT SYSTEMS PERFORMANCE AT NAVY REGIONAL DATA AUTOMATION CENTERS

by

Gloria Jean Cummings Scott
March 1984

Thesis Advisor: C. R. Jones

Approved for public release; distribution unlimited

SECURITY CLASSIFICATION OF THIS PAGE (When Data Entered)

REPORT DOCUMENTATION PAGE	READ INSTRUCTIONS BEFORE COMPLETING FORM
1. REPORT NUMBER / 2. GOVT ACCESSION NO. AD-A145 785	3. RECIPIENT'S CATALOG NUMBER
4. TITLE (and Subtitle) Evaluation of Management Systems Performance at Navy Regional Data Automation Centers	5. TYPE OF REPORT & PERIOD COVERED Master's Thesis March, 1984
	6. PERFORMING ORG. REPORT NUMBER
7. AUTHOR(s) Gloria Jean Cummings Scott	8. CONTRACT OR GRANT NUMBER(s)
9. PERFORMING ORGANIZATION NAME AND ADDRESS Naval Postgraduate School Monterey, California 93943	10. PROGRAM ELEMENT, PROJECT, TASK AREA & WORK UNIT NUMBERS
11. CONTROLLING OFFICE NAME AND ADDRESS Naval Postgraduate School Monterey, California 93943	12. REPORT DATE March, 1984
	13. NUMBER OF PAGES 125
14. MONITORING AGENCY NAME & ADDRESS(if different from Controlling Office)	15. SECURITY CLASS. (of this report) UNCLASSIFIED
	15a. DECLASSIFICATION/DOWNGRADING SCHEDULE

16. DISTRIBUTION STATEMENT (of this Report)

Approved for public release; distribution unlimited

17. DISTRIBUTION STATEMENT (of the abstract entered in Block 20, if different from Report)

18. SUPPLEMENTARY NOTES

19. KEY WORDS (Continue on reverse side if necessary and identify by block number)

Navy Industrial fund, Rate stabilization, cost liquidation, chargeback, operational auditing, internal control

20. ABSTRACT (Continue on reverse side if necessary and identify by block number)

The Navy Regional Data Automation Centers (NARDACs) became a Navy Industrial Fund (NIF) activity on 1 October 1983. This change requires that NARDACs bill customers for all data processing (DP) services provided. The impact of the change to NIF accounting on the evaluation of management performance is addressed within the context of the defined control structure. The purpose of this thesis is to present background information on the NIF concept, NARDACs, and operational audits, and to provide general (Continued)

DD FORM 1 JAN 73 1473 EDITION OF 1 NOV 65 IS OBSOLETE

S/N 0102-LF-014-6601

SECURITY CLASSIFICATION OF THIS PAGE (When Data Entered)

ABSTRACT (Continued)

recommendations for the design and application of operational auditing for a NARDAC. It is also to discuss benefits to be derived by managers of a NARDAC examined by an operational audit. A guide for performing an operational audit of a NARDAC IS outlined.

Approved for public release; distribution unlimited

Evaluation of Management Systems Performance at Navy Regional Data Automation Centers

by

Gloria Jean Cummings Scott
Lieutenant Commander, United States Navy
B.S., Southern University, 1968

Submitted in partial fulfillment of the requirements for the degree of

MASTER OF SCIENCE IN INFORMATION SYSTEMS

from the

NAVAL POSTGRADUATE SCHOOL
March 1984

Author: Gloria C. Scott

Approved by: _____ Thesis Advisor

_____ Co-Advisor

Richard S. Elster
Chairman, Department of Administrative Sciences

Kneale T. Marshall
Dean of Information and Policy Sciences

ABSTRACT

The Navy Regional Data Automation Centers (NARDACs) became a Navy Industrial Fund (NIF) activity on 1 October 1983. This change requires that NARDACs bill customers for all data processing (DP) services provided. The impact of the change to NIF accounting on the evaluation of management performance is addressed within the context of the defined control structure. The purpose of this thesis is to present background information on the NIF concept, NARDACs, and operational audits, and to provide general recommendations for the design and application of operational auditing for a NARDAC. It is also to discuss benefits to be derived by managers of a NARDAC examined by an operational audit. A guide for performing an operational audit of a NARDAC is outlined.

TABLE OF CONTENTS

LIST OF TABLES

LIST OF FIGURES

I. INTRODUCTION

A. GENERAL

In an attempt to understand the environment in which the Navy Regional Data Automation Centers (NARDACs) operate, it is essential to examine the fundamentals of the business of managing information services in general. This requires taking a wider view of computers, information resources management, and the events that led to the formation of the Naval Data Automation Command (NAVDAC). A review of the factors leading to the establishment of NAVDAC as a Navy Industrial Fund (NIF) activity is also necessary.

The Navy Regional Data Automation Centers (NARDACs) can be likened to an information services department in a large business corporation. NARDACs are information processing centers operating under the central management of the Naval Data Automation Command. They exist to provide high quality, low cost, non-tactical data processing services to operational customers in regions of extensive Navy activity. Each NARDAC is a support organization dedicated to improving the quality of computer support available to Navy activities in its region. Automated data processing (ADP) services offered by the NARDACs range from one-time technical consultations to full responsibility for processing applications on a scheduled production basis. Clients negotiate as requirements arise for the level of support needed. Thus, the extensive literature dealing with corporate information services management is applicable to NARDACs.

B. COMPUTERS--A HISTORICAL PERSPECTIVE

Managing information resources has become a task of overwhelming size and complexity. Technological, social, cultural, and political issues interact with one another making it increasingly difficult to distinguish which issue is important and which is not. Yet making these distinctions is essential to any organization with a large investment in information resources--people, machines, and technologies.

Unit costs of hardware continue to decline [Ref. 1]. Because computer needs continue to rise, total hardware costs continue to rise. Purchased software costs are rising slightly and people costs are rising at an ever increasing rate. These economic trends affect both the manager and users' perception of system efficiency.

Over the past thirty years, the rapid evolution and spread of computers, telecommunications, and office automation has created a major new set of managerial changes. Attempts to resolve these challenges has resulted in the creation of new departments, massive recruiting of staff, major investments in computer hardware and software, mechanization of routine tasks--inventory, payroll and accounts receivables--and installation of systems which have had a profound impact on how the organization operates.

Managing these challenges is complex because far too many members of the computer professional community received both their education and early work experience in a time prior to the wide-scale introduction of computer technology. The cultural impact has resulted in managers who feel somewhat uneasy about the subject and lack confidence that they have the appropriate background to provide managerial oversight. Their firsthand technical experience was with technologies vastly different from those of the 1980s.

In the early 1960s, the computing business began to look so different because of software development and stored programming. Only a small percentage of the professionals managed the transition to that new and totally different information management culture. Understanding the programming challenges of the rotational delay of the drum of machines in that era, however, provides no value in dealing with the challenges posed by today's sophisticated computer operating systems. [Ref. 2]

Moreover, understanding of what makes acceptable management practice in this field has changed dramatically since the early 1970s. Virtually all major, currently acceptable frameworks for thinking about how to manage in this field have been developed since then. Consequently, a special burden has been placed on information systems management, not just to meet day-to-day operating problems and new technologies, but to assimilate and implement quite different ways of managing the activity. If not committed to a process of self-renewal, occupational obsolescence very quickly results.

C. CHALLENGE OF INFORMATION SERVICES MANAGEMENT

It would be a serious mistake, of course, to consider the problems of computer systems management as being totally unique and separate from those of general management. The various elements of the data processing function require a high level of continuing communications and cohesive interrelationships to ensure adequate planning, development, and implementation of complex systems. The issues of information services organization, planning, control, strategy formulation, budgeting, transfer pricing, profit centers, cost centers, and so forth, are relevant here. The individual aspects of computer management problems thus are not

unique. What is unique is the combination of these issues in running an efficient and evolving function.

Because of this combinaton of issues, data processing is unlike any other activity within an organization. It combines a highly technical skill level with creativity. It requires a broad management outlook in its design stages, but an extremely detailed outlook in its implementation stages. Its managers must be concerned about the impact of their work on overall policy, procedure, and organization structure, while still maintaining an interest in individual data fields. It is a service function, yet it significantly influences the procedures of those it serves. It may be organizationally placed as one function, yet must maintain an objectivity in meeting the needs of functions crossing many organizational lines. To accomplish its job, its managers must have a line manager's knowledge of other functions within the company and still maintain a staff advisory outlook.

Each of these facets places a special burden on the selection of the appropriate information systems organizational structure. Data processing management must be continually alert to the fact that today's appropriate organization structure may not meet tomorrow's conditions or needs. Organization structure seldom remains static, and should be modified to meet changing conditions of assigned responsibilities, service role, and growth.

D. NAVAL DATA AUTOMATION COMMAND (NAVDAC)

This section provides a brief look at the Naval Data Automation Command (NAVDAC) organization, its mission and the field activities under NAVDAC. NAVDAC, and the NARDACs and NAVDAFs, were formed as the result of the "Navy Automatic Data Processing (ADP) Reorganization Study

Implementation Plan" of October, 1976. The reorganization was in response to the major ADP problems brought to light by a General Accounting Office (GAO) report that was critical of Navy ADP. In October 1977, NAVDAC became operational. The mission of the NAVDAC is to administer and coordinate the Navy non-tactical ADP program. This responsibility includes collaboration of ADP matters with all Navy ADP claimants; development of policy and procedures; approval of systems development, acquisition and utilization of ADP equipment and service contracts; sponsoring of ADP technology; and career development and training of ADP personnel. NAVDAC consists of a headquarters staff located in the Washington Navy Yard and field activities situated throughout the country in areas of high concentration of Naval activities. Figure 1.1 displays a diagram of the NAVDAC organization. These field activities are called NARDACs and Navy Data Automation Facilities (NAVDAFs).

Each NARDAC established under the NAVDAC was formed from existing facilities and operations in a particular geographical area. The seven NARDACs are located in Washington, D. C., Norfolk, Virginia, Jacksonville and Pensacola, Florida, San Francisco and San Diego, California and New Orleans, Louisiana. Each activity is designed to provide a full range of data processing services to their assigned geographic area. A standard NARDAC organization is depicted in Figure 1.2. Each center, however, may have specialized units to meet special requirements. The goal was to provide the Navy with "centers of excellence" that would provide data processing services, programming support, technical expertise, trouble shooting, telecommunicatons networking, distributed processing, and other ADP related services. [Ref. 3]

The NARDACs became Navy Industrial Funded (NIF) activities on 1 October 1983. This requires that NARDACs bill

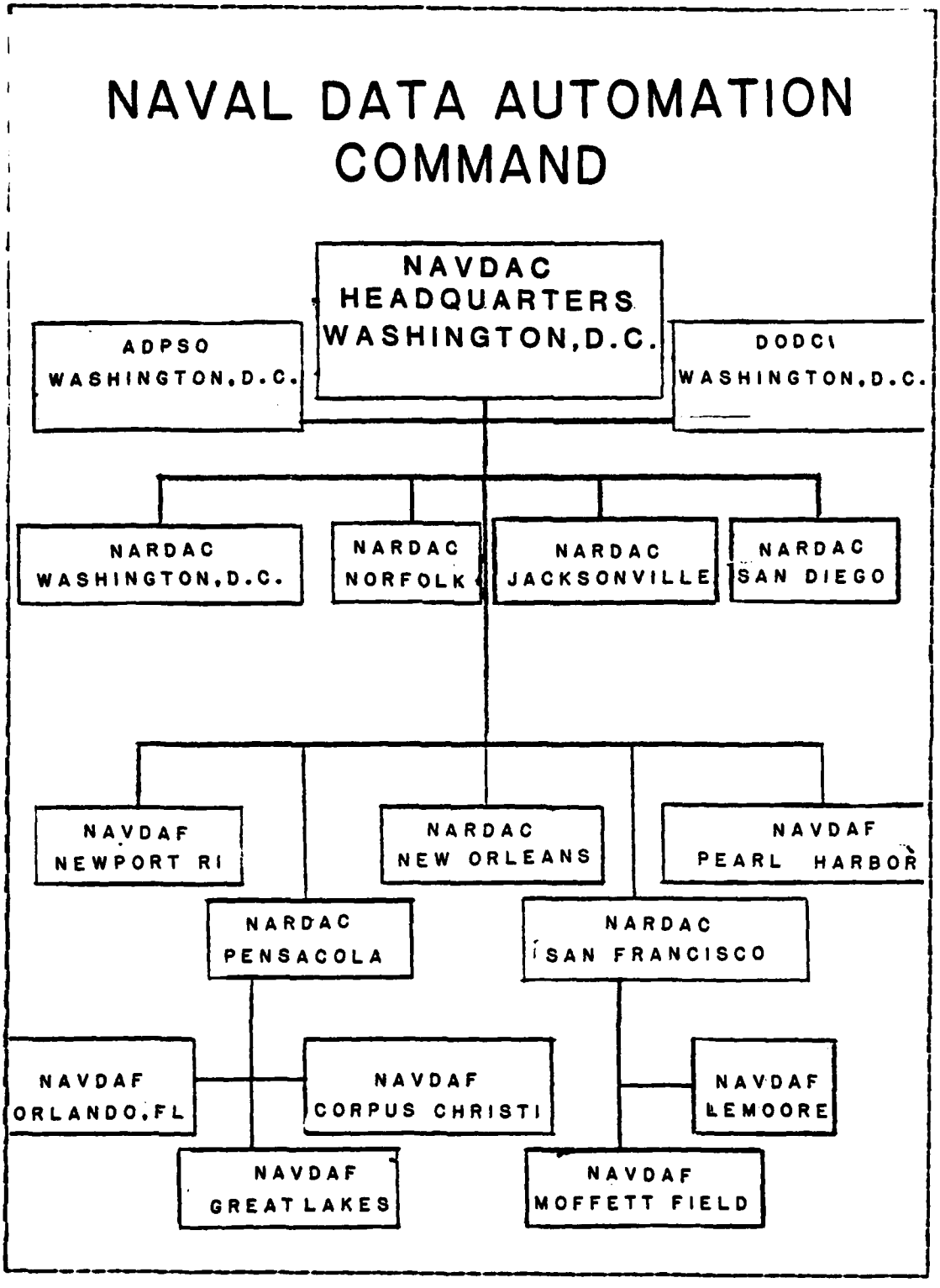


Figure 1.1 NAVDAC Organization Chart.

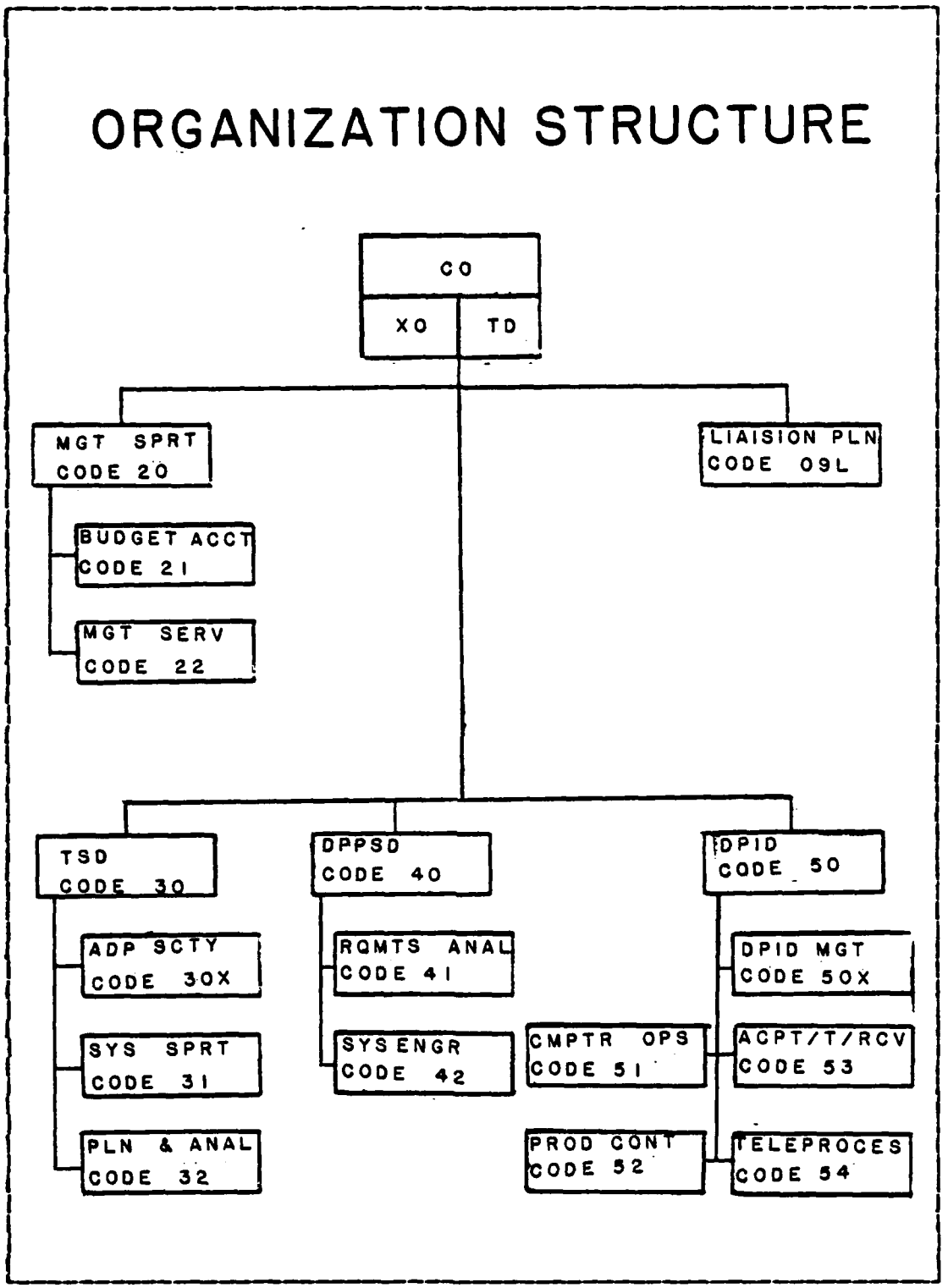


Figure 1.2 A NARDAC Organization Chart.

customers for services provided. The problem began on February 7, 1978, with the delivery of a report by the General Accounting Office (GAO) to the Congress entitled "Accounting for Automatic Data Processing Costs Needs Improvements" [Ref. 4]. After studying the cost accounting practices of twenty six federal organizatons, the GAO concluded that all were using inadequate accounting methods. The report stated that without accurate costs, computer center managers may choose uneconomical alternatives when replacing or adding to computer facilities. They may also fail to charge users of computer facilities equitable amounts for services rendered. Further, functional managers cannot make the best decisions when they are not aware of the total cost of implementing and operating their applications systems. GAC stated that cost records should be structured so that costs for both data processing and the agencies' programs can be identified. The report concluded that the mission funded concept was not adequate for the cost acccunting necessary for computer operations

The strongest point made in the GAO report was that the cost of computer services as reported by federal agencies often excluded major items of costs, such as military labor and overhead. Computer services cost had traditionally been stated in terms of Operations and Maintenance, Navy (O&MN) costs, since these costs were the only costs billable to the customer under the Resources Management System (RMS). The report indicated that an accounting system was necessary that would reflect the true cost of providing the computer services. [Ref. 5]

The GAO issued guidelines for accounting for ADP costs which state that "all significant elements of cost directly related to acquiring computers and associated assets and to performing data processing functions should be collected and accounted for in ways useful for management, budgeting, and

external reporting. Organizational boundaries and differences in financing methods should not prevent reasonable compilation of all ADP-related expenses in cost accounts." The categories of cost required for full cost accounting are: [Ref. 6]

1. Personnel. Salaries and fringe benefits for civilian and military personnel who perform and manage ADP functions: ADP-related custodial services, security, building maintenance, and contract management.
2. Equipment. Nonrecurring expenditures for acquisition and recurring costs for rental, leasing, and depreciation of computers and associated on-line and off-line ADP equipment.
3. Computer Software. Nonrecurring expenditures for acquisition, and conversion and recurring expenses for rental, leasing, and depreciation of all types of software--operating, multipurpose, and application.
4. Space Occupancy. Funded and unfunded costs for : (a) rental, lease, and depreciation of buildings and general office furniture; (b) buildings maintenance; (c) regular telephone service and utilities; and (d) custodial services and security.
5. Supplies. Expenditures for noncapital office supplies and general-purpose and special-purpose data processing materials.
6. Intra-agency Services and Overhead. The costs of normal agency support services and overhead, either billed or allocated, and the costs of central management, policy, and procurement services.
7. Contracted Services. Any of the above services if procured contractually.

In response to both the GAO report and a congressional study conducted by the House Appropriations Committee's (HAC) Survey and Investigation Staff, the Navy recommended the addition of the NARDACs to the Navy Industrial Fund as part of Fiscal Year 1984 Navy input to the President's Budget.

II. THE NAVY INDUSTRIAL FUND

A. BACKGROUND

The Navy Industrial Fund (NIF) was established as a means of helping certain Navy activities to function more efficiently and in a business-like manner. The reasoning behind the establishment of the Industrial Fund was that commercial/industrial type of activities that are qualified to operate under NIF could be freed from many of the worries arising from the total dependence on the cycle of annual appropriations (authorizations from Congress to set aside certain funds for specific purposes for limited time periods). For this reason, the Navy Industrial Fund Appropriation was established by Congress. The NIF Appropriation has indefinite life from which qualified commercial/industrial activities can be given working capital (cash) to operate on a revolving fund basis similar to private enterprise. [Ref. 7]

> The term "revolving fund" means that working capital (called NIF corpus) is used to finance operations from the time that specific work is begun to the time that payment is received from the customer. [Ref. 8]

All commercial/industrial enterprises need working capital. The difference between private industry and government is, of course, the profit motive. With NIF, the financial goal is to break even. This means the NIF activity should charge the customer the same prices as it costs the NIF activity to do the work. The NIF fund "revolves" in that payment received from the customers replenishes the working capital fund which is continually used to finance operations. The attempt to break even

requires rigorous ccntrol of costs, and projection of billing rates, because if NIF has cost overruns, it incurs losses (not just making a little less profit as is the case of private industry). [Ref. 9]

The Navy operates 51 activities under the Navy Industrial Fund. Figure 2.1 is a listing of the various NIF Activity Grcups, and relative volume of customer orders as

NIF ACTIVITY GROUP STRUCTURE

Activity Group	Number of Activities	FY 1984 Budget $Millions
Navy Research Lab	1	$ 324
Military Sealift Command	1	2,334
Shipyards	8	3,557
Ordnance Facilities	10	1,328
Air Rework Facilities	6	1,536
Air Labs	3	647
Air Engineering Center	1	142
Aviation Center	1	155
Public Works Centers	8	967
Construction Engineering Lab	1	41
Publications and Printing Service	1	187
Missile Facilities	2	64
Navy Research Labs	7	2,039
Regional Data Automation Centers	1	157
Totals	51	$13,478

Figure 2.1 NIF Activity Group Structure.

budgeted for Fiscal Year (FY) 1984. The Navy Regional Data Automation Centers (NARDACs) are operating as a single member activity group under the NIF for the first time, beginning FY 1984, in keeping with the Congressional intent of the FY 1982 DOD Appropriation Act. [Ref. 10]

The activity groups are organizationally controlled by and responsible to Activity Group commanders such as Naval Sea Systems Command (NAVSEA) for all shipyards and Naval Data Automation Command (NAVDAC) for all NARDACS. Overall

NIF management is the responsibility of the Comptroller of the Navy (NAVCOMPT) who must not over obligate the corpus as a whole.

The specific directive under which Industrial Funds have been implemented within the Department of Defense is DOD Directive 7410.4.

> The Navy Industrial Fund is a one-time appropriation of working capital provided by Congress from which the Comptroller of the Navy allocates required amounts to activities approved for operations under the Navy Industrial Fund. [Ref. 11]

This appropriation was established in 1949. The corresponding NIF Accounting System, rather than the appropriation itself, is usually referred to as "NIF". The Comptroller Manual, Volume 3, Chapter 8, entitled "Navy Industrial Fund" is the Navy implementation of DOD directive 7410.4.

The inception of the Navy Industrial Fund with application of modern business methods was widely heralded by the public as an effort on the part of the military to end inefficiency and waste, to create cost consciousness at all levels, and to reflect tangible savings as the result of sound financial management.

The Comptroller of the Navy, in reporting on the effect of industrial funding, stated:

> "It should be re-emphasized that the installation of NIF financing and its related "custom-built' budgeting, accounting, and reporting system at an industrial-type or commercial-type field activity, of itself does not assure an efficient and economical operation. Many potent management tools are inherent in these NIF systems, however, especially in the cost control and finarcial control areas; and the proper use of these tools should materially assist in the effective management of industrial-commercial type activities." [Ref. 12]

An important aspect of the NIF System is the concept of a revolving fund and its inherent flexibility. The fund is used as operationally required to finance work for customers on a self-sustaining basis. The Industrial Fund Activity takes orders for work from Navy customers, performs the work with dollars from the fund, bills the customers for the work, and receives reimbursement from the customers. The fund is reimbursed for supplies and materials used, services rendered, or labor performed by charges to applicable customer appropriations or payments received in cash. Consequently, the NIF provides the following advantages:

1. A modern business-type budgeting and accounting system permitting "tailor-made adaptations.
2. A basic accounting system that has been stable for years and promises to continue relatively unchanged (especially important in this age of automation).
3. Authority, though limited, to start emergency work on a sponsor's order prior to receipt of funds (Commanding Officer's orders).
4. A means of financing and carrying inventories of non-standard material.
5. The convenience of using working capital for initially charging all costs.
6. A method for developing total costs of each task or project, including overhead.
7. A means for producing management cost data by job orders, cost centers, or other organizational breakdowns.
8. Assistance for management to better control money, manpower, material, and facility resources.

Figure 2.2 is a list of all NIF activity groups and activity group managers.

Basic to the functioning of NIF activities is the division of effort into functional units called <u>cost centers</u>. Under the cost center concept, any level of the orgainzational structure might be a cost center. It could be an entire department or a subdivision of one.

GROUP	MANAGER
R & D Centers	Chief of Naval Material
Shipyards	Naval Sea Systems Command
Ordnance Activities	Naval Sea Systems Command
Air Rework Facilities	Naval Air Systems Command
Test and Eval. Activities	Chief of Naval Material
Public Work Centers	Naval Fac. Eng. Command
Civil Engineering Lab	Naval Fac. Eng. Command
Navy Printing & Pubs.	Navy Supply Systems Command
Strategic Weapons Fac.	Strategic Sys. Prog. Command
NARDACS	Naval Data Automation Command

Figure 2.2 Activity Group Managers.

All orders are accepted on the basis of a fixed price or on a cost reimbursable basis. In either case, the estimated costs are based upon the published stabilized rates pertaining to the product or service ordered. These stabilized rates are based upon budgeted costs. Customers are billed at the stabilized rate regardless of the actual cost. Non federal government customers are exempt from the rate stabilization program and are charged actual costs incurred. Fixed price orders are negotiated and billed on the basis of stabilized rates. When actual costs are less than the billed price, the activity makes a profit. A loss occurs when actual costs are more than the billed price.

NIF activities submit their budget (A-11 Budget) directly to NAVCOMPT into the Navy Industrial Funs Reporting Systsem (NIFRS). NAVCOMPT operates the NIFRS and maintains a budget data base for use by the NIF Activity Group Managers and for Department of the Navy (DON) NIF budgets and reports. The NIFRS also captures individual NIF activityl monthly reports, summarizes the data by NIF Activity Group and prepares the monthly reports for DON. It allows evaluation of NIF activities performance in comparison to the budget.

B. RATE STABILIZATION

Prior to the implementation of the rate stabilization program, most NIF activities developed and revised the rates charged to customers on a quarterly basis. The rates were devised to return to customers any profits previously made by the NIF activity or to recover any losses with the objective of achieving a zero accumulated operating results account balance at the end of the following quarter. Under the rate stabilization concept, however, rates to be charged for services by NIF activities are based upon the President's Budget. Thus, for example, during the summer and fall of 1982, NIF activities, Activity Group Commanders, NAVCOMPT, DOD and OMB reviewed and submitted budgets for FY 1984 which assumed a rate equal to that budgeted for FY 1984 which assumed a rate equal to that budgeted for FY 1984. Moreover, these rates reflected actual/projected performance through FY 1982 and FY 1983 and were intended to achieve a zero accumulated operating results balance for the fiscal year ending in 1984.

A principal objective of stabilized rates was to shelter DOD customers from inflation induced variances in cost increases in excess of those budgeted. This was to allow better financial planning by the DOD and the Navy. Industrial fund rate increases during the years prior to rate stabilization sometimes made it necessary for customers to reduce their programs in order to remain within their appropriated fund availability. These reductions, in turn, created further imbalances within the NIF activities which ultimately were also passed on to customers.

NAVCOMPT Note 7111 of 10 June 1975 announced to Navy activities the DOD requirements for the establishment of stabilized rates, and target dates for implementation were set. Stabilized rates have been in effect for all NIF activities since the start of FY 1977.

NAVCOMPT Instruction 7600.23B provided amplifying guidance as follows:

> "In developing and establishing rates, each activity will adhere to the principle of aligning rates to recover operating costs. Activities should devise a sufficient number of rates to ensure that the rate system is a reasonable model of the actual cost of performing the various categories of work or services covered by the rates. Stabilized rates submitted by the activities will be reviewed and adjusted by the Activity Group manager, to provide the necessary changes to offset the total prior year gains or losses thereby achieving zero profit and loss in the Accumulated Operating Results Account of the Activity Group. Gains and losses will normally be fully offset during the year following their occurence, and will be reflected uniformly in the rates of the Activity Group. Changed conditions resulting from the Office of the Secretary of Defense review of the Activity Group manager's A-11 Budget, and changes in the customer programs occuring during the budget review cycle will result in stabilized rates being again reviewed and additional changes made where appropriate." [Ref. 13]

Rates established for NIF activities are expected to remain in effect for the entire fiscal year. Shipyard rates, however, are normally in effect for the entire period that a ship is in the yard regardless of the number of fiscal years involved. Rates for work unrelated to the ship will change with the fiscal year. Rate changes during the fiscal year are expected to be rare, and may be made only upon approval of the Assistant Secretary of Defense (Comptroller). In a major sense, rate stabilization did help the Navy to cope with the radical swing in inflation, utilities, and fuel prices during Fiscal Year 1978 through Fiscal Year 1981.

A significant problem associated with stabilization is the failure of the process to make known the stabilized rates to the customers early enough to be useful in budget preparation at the local level. The process of attempting to balance the customer budget requests with the NIF funding in the President's Budget is done by NAVCOMPT, a level considerably higher than local customer budgeting, causing imbalances that are not discovered until a year later.

Any variance between stabilized-rate billing and actual costs become profits or losses of the NIF activity and are absorbed by the corpus. By the time a profit or loss is realized, however, the next year's rates are already established. These profits or losses are not offset, therefore, until the next rates are set. The NIF activity, consequently, essentially cperates on a three-year cycle.

The essence of rate stabilization is that rates are set annually for the entire fiscal year. The combination of rate stabilization and NIF budgeting results in rates being set one to two years in advance of actual use in billing. The rates charged represent modifications by the NIF Activity Group commander, NAVCOMPT and the Office of the Secretary of Defense (OSD) to those proposed by the NIF activity. As a consequence, individual NIF activity commanders do not directly determine rates or change stabilized rates when a flaw is found. Stabilization has resulted in a rather substantial loss of autonomy by NIF activities because they are no longer in control of the inflow of resources to their command and can not control the profit or loss for a particular period. The cash balance is also beyond their ccntrol. In spite of this lack of control, the performance of NIF activity commanders has been evaluated with the financial position of the individual activity as a factor. It seems obvious that the control system was weakened by rate stabilization and the loss of autonomy by NIF activities.

III. NAVY ACCOUNTING PROCEDURES

A. NAVY ACCOUNTING AT THE HEADQUARTERS LEVEL

Accounting in the Federal Government provides financial information for use by the management of a particular agency and for use by the Department of Treasury, Office of Management and Budget (OMB), and the Congress. Such information is used for these various reasons:

1. Facilitate efficient management.
2. Support budget requests.
3. Show the extent of compliance with legal provisions.
4. Report (in financial terms) to other agencies, to the Congress, and to the public, the status and results of the agencies activities.

The forerunner to today's budget and accounting system was the Budget and Accounting Act of 1921. This act provided for a budget system under the Department of Treasury. (This function was later transferred to the Executive Office of the President.) The act also established the General Accounting Office (GAO) headed by the Comptroller General of the United States. The Comptroller General was given the responsibility for developing government accounting systems and was also given authority to make expenditure analyses; maintain ledger accounts, investigate the receipt, disbursement, and application of public funds, examine books, documents, papers, and records of financial transactions; perform audits, etc. Since 1921, there has been a continuing attempt made, through legislation and executive orders, to establish effective fiscal control over all governmental activities. The respective headquarters

components maintain control of funds allocated to them [Ref. 14].

B. WORKING CAPITAL FUNDS

In 1949, when Congress amended the National Security Act of 1947 establishing the Department of Defense (DOD), originally named the National Military Establishment, the need to promote "efficiency and economy" through use of uniform budgeting and fiscal procedures was recognized. Among the features of the National Security Act was authorization (10 U. S. C. 2208) for the Secretary of Defense to establish working capital funds for the purpose of financing supply inventories and the capitalization of industrial type activities. Thus what we know today as "industrial funds" resulted from the National Security Act of 1947.

A fund has been defined as a "separate enterprise, having assets, liabilities, net worth, income and expenditures of its own." In government practice, a fund is not tied to profit making, hence, the emphasis is not on maximizing income. The fund is used to isolate a particular area and allow management to focus on it as an entity.

The goal of a DOD working capital fund is to recover all costs exactly--work to a zero profit [Ref. 15]. A working capital fund is not controlled by an annual appropriation.

C. RESOURCE MANAGEMENT SYSTEMS (RMS) ACCOUNTING

1. Background of RMS

The Resource Management System (RMS) was introduced to the Navy through a Priority Management Effort (Project PRIME) in Fiscal Year 1968. One basic change was to require the costing of military personnel. Another major change was the separation of procurement costs from operating costs.

The separation of expense and investment costs allow a differentiation between those costs influenced by management and those over which there is little control.

In operating RMS all activities are charged for operating resources consumed by them at the time of consumption. An expense is recognized when and where materials, supplies, services or labor are used to accomplish a mission. To distinguish between the time of purchase of resources and the time of consumption, working capital is used just as inventory accounts are used in commercial practice. RMS changed traditional accounting systems to improve and integrate accounting and reporting with programming and budgeting.

2. RMS Accounting

Resource Management Systems (RMS) accounting includes all procedures for collecting and processing recurring quantitative information that (1) relates to resources, and (2) is for the use of management. Resources are people, materials, services and money. There are four principal systems:

1. Programming and budgeting
2. Management of resources for operations
3. Management of inventory and similar assets
4. Management of acquisition, use and disposition of capital assets

The Department of the Navy has promulgated a series of publications for implementation of the Resource Management Systems for operations within the Navy. A handbook of instructions and procedures applicable at the field activity level and at the departmental level and another one for the operating forces have been developed [Ref. 16].

These handbooks set forth the resource management concepts as they apply to operation and maintenance.

IV. THE MANAGEMENT CONTROL SYSTEM

A. INTRCDUCTION

The information services (IS) management control system is a critical network which integrates the information systems activities with the rest of the organizatcn's cper-ations. Information services include a central hub of oper-ations linked by telecommunications to remote devices that may or may not have their own extensive data files and processing power. IS integrates the separate technologies of computers and telecommunications. While individual projects often last more than a year, and planning takes a multiyear view, the information services management control system focuses on guidance primarily on a year-to-year basis. The broad objectives an effective information services management control system must meet include the following: [Ref. 17]

1. Facilitate appropriate communication between the user and deliverer of IS services and provide moti-vational incentives for them to work together on a day-tc-day, mcnth-to-month basis. The management control system must encourage users and IS to act in the best interests of the organization as a whole. It must motivate users to use IS resources appropri-ately and help them balance investments in this area against those in other areas.

2. Encourage the effective utilization of the IS department's resources, and ensure that users are educated on the potential of existing and evolving technology. In so doing, it must guide the transfer of technology consistent with strategic needs.

3. It must provide the means for efficient management of IS resources and give necessary information for investment decisions. This requires development of both standards of performance measures and the means to evaluate performance against those measures to ensure productivity is being achieved. It should help facilitate make-or-buy decisions.

Four specific inputs appear to be critical to the structuring of an appropriate information services management control system for an organization. These are: [Ref. 18]

1. The control system must be adapted to a very different software and operations technology in the 1980s than was present in the 1970s. An important part of this adaptation is development of appropriate sensitivity to the mix of phases of IS technologies in the company. The more mature technologies must be managed and controlled in a tighter, more efficient way than ones in an early start-up phase which need protective treatment appropriate to a research development activity.
2. Specific aspects of the corporate environment influence the appropriate IS Management Control System. Key issues here include IS sophistication of users, geographic dispersion of the organization, stability of the management team, the firm's overall size and structure, nature of relationship between line and staff departments, etc. These items influence what is workable.
3. The general architecture of the organization's overall corporate management control system and the philosophy underlying it.
4. The perceived strategic significance of IS both in relation to the thrust of its applications portfolio and the role played by currently automated systems.

The next subsection discusses alternate methods of defining the control structure.

B. ALTERNATE CONTROL APPROACHES

The establishment of an information services activity as an unallocated cost center--a free resource to users--is advantageous where the resource being used is small. Accounting for such a cost center requires very low expenditures, and the controversey caused by a system of charging is avoided. On the other hand, significant problems usually exist when the users perceive the resource as free and attempt to make irresponsible uses of it. The unallocated cost center also insulates the computer installation from

external measures of performance and makes possible the hiding of operational inefficiencies. Although many organizations start with an unallocated cost center approach, they often evolve to some other form such as the approach of using memos to inform users of what their charges would have been if a chargeback system were being used. Unfortunately, however, a memo about a charge does not have the bite of the actual assignment of the charge. [Ref. 19]

The approach of establishing the information services activity as an allocated cost center has the immediate virtue of helping to make user requests more realistic. While it opens up a debate as to what cost is, it avoids the controversey about whether an internal service department should be perceived as a profit-making entity. Inevitably, however, the allocated cost center introduces a series of complexities and frictions since such a system necessarily has arbitrary elements in it. Full cost charges of a central computer installation can inappropriately stimulate the desires of the users to purchase mini/microcomputers. Allocations could be less than full cost, depending on the organization's overall management control philosophy. [Ref. 20]

The chargeback process has led to a number of unsatisfactory consequences from the users' perspective in the majority of companies:

1. Charges are unintelligible and unpredictable.
2. Charges are highly unstable.
3. Charges tend to be artificially high in relation to incremental costs
4. Efficiency variables are directly assigned to ultimate users.
5. Administration of the chargeback system is frequently very expensive.

The system is based on passing all costs of the activity to customers. The charge for operations costs is based on a complex formula related to the use of the computer by the application. The user can not predict or control these charges because the "equitable distribution" is dependent upon what other applications happen to be run during the month. To be effective, an information systems operations chargeback system must be simple. A second desirable characteristic is that the chargeback system should be perceived as being fair and reasonable. A third desirable characteristic of a chargeback system is that it should separate information systems efficiency-related issues from user utilization of the system. Information Systems should be held responsible for its inefficiencies. Clearly, closing at month- or year-end any over- or under-absorbed cost variances to the user usually accomplishes no useful purpose. [Ref. 21]

The issues involved in charging for information systems maintenance and systems development are fundamentally different from those of operations. A professional contract should be prepared for such expenditures as though it were a relationship with an outside software company.

The establishment of the informaton services activity as a profit center is a third method of management control. This approach puts pressures on the information systems function to hold costs down by stressing efficiency and to market itself aggressively inside the organization. Establishing information systems as a profit center, however, has problems. Because of geography, shared data files, and privacy and security reasons, many users can not go outside. In the short run, the profit center approach leads to higher user costs because a "profit" figure is added to the user costs. A deceptively intriguing approach on the surface. underneath it has many pitfalls. [Ref. 22]

The investment center approach is similar to the profit center approach. The critical difference is that the information systems function is made fully responsible for the assets employed and is forced to make appropriate trade-offs of investment versus additional profits. This produces strong motivations to delay capacity expansion and risk serious erosion in service provided. Another problem is that of focusing only on hardware as an asset and not considering the software. A stand alone investment center can be perceived as being fully organizationally neutral. When set up as a profit, or investment center, the transfer price becomes a critical issue. The strengths and weaknesses of transfer pricing for the information systems function are very similar to those found in transfer pricing in general. With cost-based pricing, the profit center and cost center are similar since profits can only be earned on internal sales by generating positive efficiency variances.

C. THE NAVY'S ADP CHARGEBACK TEST

Before the creation of NAVDAC, the Data Processing Service Centers (DPSCs) provided ADP support on a no-charge basis. To realize "the performance and economic benefits attainable" from a NARDAC, an ADP chargeback test was instituted, in April 1978, at NARDAC San Diego. During the initial phase, statistics were gathered on usage of the NARDAC's resources by its customers. At the beginning of the second phase, the customers were given funds based on the utilization statistics gathered during the first phase. These funds were to be used to reimburse the NARDAC for ADP support.

Permission to deviate from the Resources Management System was granted by the Comptroller of the Navy so that indirect costs could be passed on to customers excluding the

overhead items of administration, electricity, and maintenance of real property. The test algorithm allowed the NARDAC to charge premiums or grant discounts based on the customer's job priority and shift during which the job was run. These premiums and discounts were based on a matrix of percentages of full cost incorporating both requested turnaround time and the requested shift. Such flexible pricing allowed the customer to weigh the importance of his job against the amount of money he was willing to pay. Because of a legal opinion of the Head, Budget Policy Branch, NAVCOMPT, all percentages in the matrix were to be set to 100. The resulting single charge nullified the most important feature of the test. The opinion was that NAVCOMPT would support a chargeback system which allocated all actual costs directly associated with the operation of the computer facility. The overhead items previously mentioned were to be excluded. The charge was to be based upon the cost of providing the service, not upon the economic value of the services. Neither variable prices nor shift differentials were allowable.

D. MANAGEMENT CONTROL AND BUDGETING

The foundation of the information services management control process is the budgeting system. Its first objective is to provide a mechanism for appropriately allocating scarce financial resources. The budgeting process ensures fine-tuning in relation to staffing, hardware, and resource levels takes place. A second important objective of budgeting is to set the specific goals and possible short-term achievements of the information systems activity. Finally, the budget establishes a framework around which an early warning system for negative deviations can be built. Without a budget, deviations in a deteriorating cost

situation may not be detected in time for corrective action. Effective monitoring of financial performance, however, requires a variety of tools, most of which are common to other settings. These normally include a series of reports which highlight actual performance versus plan with variances. Nonfinancial controls are also important in assuring management that day-to-day operations are on target. These include user surveys, reports which monitor staff turnover trends, and reports on development projects. The type of data needed varies widely from organization to organization.

V. NATURE AND ROLE OF OPERATIONAL AUDITING

A. INTRODUCTION

Auditing today differs considerably from what it was centuries ago. In fact, it is also different from what was practiced in the early twentieth century. Whereas the purpose of accounts examination used to be to detect fraud and certify the accuracy of records, the primary purpose now is to express opinions on the fairness of presentation of the financial statements. The purpose of auditing the performance of management used to be to ensure compliance with laws, policies, and regulations. The primary purpose now, however is to improve managerial performance and to determine whether an organization, activity or program has been managed economically, efficiently, or effectively.

Operational auditing is the term used in this thesis in reference to auditing involving work other than financial statement examinations to evaluate the efficiency and economy of a given operation. Such an audit is often called a management audit in the auditing literature.

Because there is a lack of standard terminology concerning the types of audits, the principal forms of government auditing are described below. [Ref. 23].

1. Financial and compliance--determines (a) whether the financial statements of an audited entity present fairly the financial position and results of financial operations in accordance with generally accepted accounting principles and (b) whether the entity has complied with laws and regulations that may have a material effect upon the financial statements.

2. Economy and efficiency--determines (a) whether the entity is managing and utilizing its resources (such as personnel, property, space) economically and efficiently, (b) the causes of inefficiencies or uneconomical practices, and (c) whether the entity has complied with laws and regulations concerning matters of economy and efficiency.

3. Program results--determines (a) whether the desired results or benefits established by the legislature or other authorizing body are being achieved and (b) whether the agency has considered alternatives that might yield desired results at a lower cost.

An audit may be either one of these types or a combination of any of them. A comprehensive audit includes all of them. The operational audit is a subset of an expanded scope or comprehensive audit whenever such broad audit work is required. This subset is also refered to as an economy and efficiency audit.

Operational auditing is planning for, obtaining, and evaluating sufficient relevant evidence, by an independent auditor, to determine whether an entity's management or employees have carried out appropriate laws, regulations, policies, procedures, or other management standards for properly using its resources in an efficient and economical manner. From the evidence on the audit objective, the auditor comes to a conclusion and reports to a third party, with sufficient evidence in the report to convince the third party that the conclusion is accurate, and with a recommendation for the possible correction of any deficiencies.

Accountability and attest are words often found in auditing literature and sometimes are used to mean the same thing. They are related, but they are not the same. Persons in organizations are accountable and report to some outside or higher level of authority. When reliability and acceptability are required of the accountable party, an independent person attests to the information through an audit. The one who receives the audit report may be a higher-level manager within the same organization, the board of directors, the stockholders, the Congress, the public--any individual or group to whom the management or employees of an organization are accountable.

Operational auditing includes all internal operations of an organization accountable to some higher level. It includes operations for accounting, purchasing, personnel, research or any other activity conducted by the organization. Operational auditing attempts to determine for the accountable entity the best use of manpower, material, machinery, and information.

Auditors of management activities in government must follow the 1981 revision of Standards for Audit of Governmental Organizations, Programs, Activities, and Functions by the Comptroller General of the United Staes. These Standards, known as the "yellow book", have been developed in cooperation with other federal, state, and local auditing orgarizations, as well as the American Institute of Certified Public Accountants. These standards include a detail discussion of the following items:

1. Scope of Audit Work
2. General Standards
3. Examination and Evaluation (Field Work) and Reporting Standards for Financial and Compliance Audits
4. Examination and Evaluation Standards for Economy and Efficiency Audits and Program Results Audits
5. Reporting Standards for Economy and Efficiency Audits and Program Results Audits

Conclusions depend upon the evidence obtained on the audit objective and are based on three common elements:

1. An appropriate standard
2. The actions of individuals or organizations that either did or did not follow the standard
3. The results brought about by the actions of organizations or individuals following, or not following, the standard.

Although operational auditing is not a new technique, it is a subject of increasing interest. The operational audit extends traditional audit approaches and techniques to examine policy, procedure and practice in industrial and governmental operations. The organizational structure and administrative controls are examined with the purpose of determining where policies and operating controls vary from those essential to the success of the industry or agency.

More specifically, the operational auditor looks for: [Ref. 24]

1. The existence of those general policies which determine the organization requirements--the functions and activities essential to the conduct of the business or government agency.
2. Indications that people have been designated to perform each of these functions and that the scope of their action and power of decision is both defined and understood.
3. Predetermined goals or planned accomplishments for each control area, including standards, estimates, budgets, forecasts or other criteria to serve as yardsticks for comparison and evaluation.
4. An efficient accounting system accumulates information following the functional organization lines and affords comparison between actual and planned results.
5. A meaningful system of management information that provides essential and timely decision-making data to all three levels of management--top, middle and supervisory. It should communicate current results as well as future plans.
6. Control department statistics and financial trends over a period of time that may indicate a deterioration in the effectiveness of controllable activities.
7. Good communications throughout the whole system of administrative control and evidence that its purpose is being achieved. The object is to determine and transmit what currently should be done and, in the light of later developments, reappraise and communicate the planned course of corrective action to be taken in the future.

Some of the benefits that can be gained from an operational audit include: [Ref. 25]

1. An objective professional review of the complete operations.

2. A substantiated inventory of weaknesses and unfavorable trends with some idea of the impact of these deficiencies on revenues and costs.

3. An opportunity to evaluate present conditions, set targets for corrective action, commit financial and personnel resources and assign responsibility for accomplishment.

4. Creation of an atmosphere for improvement and constructive thinking at all management levels.

Operational auditing serves the needs of managers to be objectively informed about conditions in the units under their control. Managers need a means for detecting problems and opportunities for improvement. Operational auditing is a specialized management tool with a separate role from established management information sources. Its purpose is to create confidence that things are going well or to discover problems or opportunities for improvements on the basis of investigation.

A key feature of operational auditing is that it is based on evidence--not personal opinion unsupported by factual evidence. Judgement is an essential part of the final results, but its value comes only after facts have been gathered and compared with standards.

An operational audit is not designed to evaluate people nor can it be expected to provide specific solutions to any particular problem or weakness. On the other hand, operational auditors should make recommendations, based upon their experience, for corrective action. It must be made clear, however, that the recommendations are strictly proposals and such comments are to be acted upon or not acted upon only as management chooses.

The auditor will encounter some situations in which no definite recommendation may be possible--either because of a

lack of qualifying experience or the facts may not permit a specific recommendation. Sometimes the most effective solutions require analysis and research into alternative courses of action.

Table I presents some of the major characterics of financial and operational auditing.

B. EVOLUTION OF INTERNAL AUDITING

During its early history, internal auditing was used primarily tc detect carelessness or other irregularities on the part of bookkeepers and others charged with the duty of recording transactions. If internal auditing had not grown with the change in character of business, it would nct be of value to management tcday. It was recognized near the end of the nineteenth century that internal auditing could serve broader purposes than mere checks of accuracy of accounting and statistical data. Thus the profession began to develop in a direction which has led to its now being recognized as one of the outstanding branches of management contrcl. [Ref. 26]

Internal auditing refers to a series of processes and techniques through which an organization's own employees ascertain for the management, by means of first-hand, on-the-jcb cbservaticn, whether (a) established management controls are adequate and effectively maintained; (b) records and reports--financial, accounting, and otherwise--reflect actual operations and results accurately and promptly; and (c) each division, department or other unit is carrying out the plans, policies, and procedures for which it is responsible. [Ref. 27]

The internal auditor's work involves constant surveillance of such functions as policies; accounting and operating procedures; systems of internal control; care,

TABLE I

Characteristics of Auditing Types

Financial Auditing	Evaluates financial controls and transactions to express an opinion on financial statements as they disclose or do not disclose a true and fair view
	Requires judgement
	Measures against auditing standards and procedures
	A restrospective viewpoint
	Employs generally accepted accounting principles
	Audit independence essential
	Opinion for outsiders and management
	Performed at least annually
Operational Auditing	Evaluates efficiency of use of resources, reviews internal management systems and structure. Deals with all measurable aspects of the organization.
	Defines problems and opportunities for improvement
	Requires judgement
	Based on evidence rather than opinion
	Management orientated
	Present and future operations
	Employs standards of the organization or industry for evaluating management performance
	Audit is independent
	Does not render opinions
	Periodically performed but with indefinite timing

protection, storage, and destruction of records; care and storage of the organizations valuables; reliability of books of record and accounting and statistical reports; and compliance with all laws and regulations.

The internal auditor must have facts as the basis of any report. These facts are obtained by a detail analysis of the situation. After reviewing the facts, the auditor must appraise them, make judgements on them using his knowledge of policies and objectives, and make recommendations for solving any problems found. Since the auditor has no authority to implement solutions, he must convince management to do so.

There is increasing interest in operational auditing on the part of internal auditors as well as by accountants in public practice. The development of internal operational auditing varies widely between organizations because of company size, size of audit staff, and degree of management acceptance. There is a need to get the concept of operational auditing across to the operating personnel at all levels. This is important because a lack of understanding or an unwillingness to give the recommendations fair consideration makes the audit effors worthless. [Ref. 28]

An operational audit provides a service to the executive management by providing impartial appraisals of the performances of operating groups to the extent of the auditors qualifications to render opinions. Efforts to help management to do a better job through aiding the understanding of the economic factors in their decisions helps the organization as a whole. The objective of the operational audit is to see that management has at hand all the tools available to help in deciding which are most profitable alternatives. This may involve evaluating information flowing in to top management as well as the way it is handled by staff groups. Evaluating how objectives are being met must be done along with how those objectives were set in the first place.

C. ROLE OF AN OPERATIONAL AUDITOR

The role of the operational auditor is not a simple one. The ability to correctly identify operating problems and explain them to senior management often requires a high order of skill.

An auditor must get the willing cooperation of the people being audited. They must be convinced that the audit's purpose is to help them. A way to begin is by sitting down with the manager or supervisor of the facility that is to be audited. An explanation of what action is planned and what accomplishment is expected should be made. The auditor should make an effort to learn what problems the people being audited might want to have studied. More problems will be discovered during the audit if leading questions are asked to get people talking about their jobs.

The auditor must take the time necessary to do the job thoroughly. When time is limited, the activity should be divided into smaller operations to allow the auditor to be thorough with those that are audited. The auditor must be aware of the dangers of not understanding an operation well. Something which, on the surface, seems wrong may be all right in light of the facts. Conversely, something may be basically wrong that initially seems acceptable. When it is suspected that something is wrong, a recommended practice is to discuss the finding first with the person most directly concerned before approaching higher levels of supervision. Another suggustion is to try to recommend a solution to any problem discussed. After all, if a situation is thought to be wrong, there must be some associated idea of what is right.

It is not uncommon to finish an operational audit and still feel that there were other things that should have been done. At the beginning of the audit, auditors spend

the necessary time tc indoctrinate themselves. A lot of time is spent reviewing specific activities before they are understood well enough to know if suggestions are to be made. As an audit is completed, the audit program is revised to incorporate new steps deemed necessary. These revisions are essential to ensure that what is accomplished is what should be accomplished. No matter how advanced or sophisticated a particular brand of operational auditing may be, there is rocm fcr improvement. A failure to plan and strive ror that improvement is a failure to properly carry out the duties as auditors.

D. PLANNING AN OPERATIONAL AUDIT

The output of an cperational audit is either a report or a carefully structured briefing. This output must include all cf the essentials about an auditor's findings. An auditor must think about the report during the planning stage, plan what will go into the report and do audit work that will get the necessary information for the report if an efficient cperational audit is to be done.

> Planning is an impcrtant part of every management undertaking, and is equally important in operational auditing. Thinking what needs to be done, setting it out in a plan, and then following that plan to conclusion is the best way to complete a job satisfactorily in the least possible time. To audit without a plan can result in a lot cf false starts and wasted effort. Consequently, auditors should have a well thought-out plan rcr every assignment. [Ref. 29]

This planning of the report, however, is begun after the auditor has observed conditions where it appears that costs can be reduced or results improved. The observed condition represents the basic premise around which a finding is built. Thus, it shculd be the focal point for the development cf plans for conducting the audit and collecting the necessary irformation. [Ref. 30]

Preliminary survey work is usually needed for effective operational auditing planning. The extent of such preliminary work depends on how familiar the auditors are with the activity or function being reviewed and whether an area for detailed audit has been identified. During the survey the following actions occur: [Ref. 31]

1. The envisioned finding is identified and clearly defined.
2. Sources of information are identified for use in developing the audit program report.
3. Audit techniques for further development of the envisioned finding are tested.
4. Staffing requirements and the scope of audit work, including audit sites, are considered.

Several factors need to be considered when deciding the scope of the audit. One is whether the projects or transactions being audited are intended to represent a statistical sample so that audit findings can be projected to an entire program. The scope of work might also be influenced by available resources in terms of staff and dollars, and by the time constraints. The objective is to do only what is necessary to clearly show any possible bad effect and to develop a convincing case. Consideration should also be given to making pilot studies before embarking on a detailed audit. The pilot study at one or more locations would provide additional knowledge of operating procedures and test the proposed audit techniques.

There are no step-by-step procedures for doing an operational audit. There are, however, certain things that need to be done. While the approach is not as uniform as in a financial audit, it should at least be systematic. The planning should culminate in an audit program. Each program must be tailored to fit each audit, yet certain elements should be always present. The program should briefly

summarize the areas tc be audited and make a general statement as to how the required information will be obtained. It should also state the expected completion date.

Because development of a finding is frequently an evolutionary prccess, audit programs should be periodically updated as work progresses. If conditions or findings are not as anticipated, the plan must be revised or the audit discontinued. Any changes to audit scope should be make a part of the program. Economy and efficiency audits are the cnes where plans are most likely to change as the audit progresses, so the planning of such audits must be flexible.

For economy and efficiency audits, the goal of the organizatien to be examined is whether certain functions can be performed at less cost without degrading the end result of the work. For example, suppose that an auditor is given the assignment of reviewing the maintenance function of an airline to see if the cost can be reduced without in any way jeopardizing safety or degrading passenger service. A further supposition is that the airline has a huge warehouse full of aircraft tires. Inquiry shows that there are enough tires on hand to last the airline for five years at the current rate of consumption. Now the auditors work must be planned. A finding that the airline is overstocking tires and should reduce its inventory will probably be visualized. The audit plan shculd be similar to the follcwing illustration: [Ref. 32]

1.	Authority	Review delegations of authority to the maintenance department to see what authority they have to buy tires, and whether they have exceeded their authority.
2.	Goal	Determine what the goal of the maintenance unit is with regard to maintenance of tires. (It probably is to provide the tires needed to keep aircraft supplied with new tires whenever needed without investing any more mcney than necessary in tire inventory).

3.	Condition	This is what the auditor observed in the survey. The airline appears to have far more tires than it needs--but this must be checked out. The auditor needs to make inquiries to find out how the airline acquired these tires and why. A decision will then have to be made regarding whether there was a reasonable basis for doing so.
4.	Effect	The auditor will want to compute how much can be saved by reducing the stock of tires to a reasonable level. This will probably include obtaining some criterion for determining what a reasonable level is. There might be a plan to see what other airlines use as a basis for stocking tires to get a criterion. As an alternative, a check could be made to see how long it takes to reorder tires and base the stocking level criteria on what quantity is needed to provide stock between reasonable reorder periods. For instance, it might be concluded that a three-months supply of tires plus a reasonable safety level is all that is needed to meet the maintenance department's goals and it might therefore be suggested that quantity of stock is the criterion for the inventory level.
5.	Procedures	The auditor will want to find out what procedures have been established to control the quantity of tires purchased. Such procedures should be designed to achieve the goal that the maintenance department has--presumably the procedures should require some method of determining that stocks on hand do not exceed the minimum necessary to keep operating aircraft supplied with new tires as needed.
6.	Cause	The auditors work should look into what happened that resulted in the undesirable condition. . . . 85% of the time, it will be found that sound procedures exist but they are not followed. In some cases, procedures are improperly conceived and, if followed, will not produce the results intended by the goals established for the organization.

While the above outlines the planning of such an audit, the work would not be done in that order. Item 3 would be performed first. Next, the steps needed to get information for items 1 and 2 would be performed. This is practical since this work takes relatively little time and the

information obtained from these steps can often explain away the condition found and indicate that everything is all right. Next, the auditor must find out what the procedures are for controlling tire inventories and determine whether there is significant effect. This is usually the time-consuming part of the work but, if there is not a significant effect, there is not much use going any further. Item 6 (cause of the problem) would follow if the effect is determined to be significant.

As mentioned previously, auditors will frequently discover in pursuing an envisioned finding that the condition is not what was initially observed. When this happens, the audit program will generally need to be revised. To illustrate, suppose that the auditor learned that the company had recently acquired another airline and had also been authorized to add several more flights. Further suppose that in checking the requirements that many of the tires had been purchased (1) to cover the related expected increase in tire use, and (2) to provide an initial inventory for a new plane that was being put into service. Given these new requirements the tire supply may be justified. If this is the case, further audit work on this would not be warranted.

If the auditors were very inquisitive and began wondering why all new tires were used and none were recapped, and they knew that recapping is common practice in the airline industry, they might visualize that the airline could save considerable money by recapping tires if it could be done without jeopardizing safety. This new picture of the finding requires a revision of the audit plan. The revised plan should be something like the following example. [Ref. 33]

1. Authority — Review the delegations of authority to see what responsibility the

		maintenance department has been given for recapping tires and whether conditions may have been spelled out for recapping.
2.	Goal	Determine what goal, if any, the maintenance unit has. If it is necessary, obtain evidence to establish an asserted goal. On the basis of information obtained from other airlines, the asserted goal might be to "use recapped tires as often as the casings permit."
3.	Condition	It appears the airline could use recapped tires, but the auditors will need to assure that it can be done safely. This will require contacting other airline companies to get information on their experience, the extent they use recapped tires, and their criteria for recapping.
4.	Effect	The auditors will want to compute how much money can be saved by using recapped tires. They will need to obtain information on the price of new tires versus the costs associated with recapping. The auditors will also need to obtain information--from other airlines--to determine the average number of times a tire can be recapped.
5.	Procedures	The auditors will want to find out what, if any, procedures the maintenance department has for recapping tires. These procedures should provide criteria for determining how often and under what conditions tires can be safely recapped.
6.	Cause	The auditors' work should be sufficiently extensive to determine why this condition has resulted. In this case it would appear to result from a lack of procedures for recapping tires.

The audit steps and information requirements of this finding differ significantly from the initial audit plan. This example also illustrates the difficulties auditors encounter in doing operational audits. Even with the best planning, false starts often cannot be totally eliminated.

Another planning consideration is the engagement letter. The auditor often must start his engagement with a proposal. After planning and preparing the proposal letter, it becomes

the engagement letter when signed by the client. The form and structure of this letter are critical. The introduction sets the tone for the entire letter. It should be formal and forthright. Specifics included in the opening paragraph are the date of the visit, the subject of the study and the names of all supervisory personnel encountered during the preliminary survey. The statement of the engagements basic objectives is probably the most critical section. The objectives should be stated simply and concisely in terms of the clients definition of the problem or opportunity. The approach should be a clear and specific statement of the work plan. It should omit nonessential details. Unless the anticipated benefits are stated clearly and confidently the client might infer that there are doubts in the auditors mind. Frequently in proposals to government agencies there is a section presenting the professional qualifications of the auditors. The conclusion should end in a positive vein [Ref. 34]. This discussion pertains to management services but will apply equally well to proposals and engagement letters for operational audits. Public accountants require an engagement letter for approval to continue the audit beyond the preliminary survey and testing of management and internal control. In most government audit agencies, since the law requires that examinations be made, the approval that must be obtained for continuing the audit is from a higher-level authority in the audit agency.

VI. PHASES OF THE AUDIT FUNCTION

A. INTRODUCTION

To be successful an audit must be conducted within a sound conceptual framework with flexible procedures. Such an audit requires analytical ability, ingenuity, and systematic procedures. Each operational audit is unique. There is no common approach and the factors to be considered will vary as much as the approach. Some elements that suggest a starting place are these: goals and objectives, plans, organization, operations, controls, systems and procedures, staffing, facilities, reports, policies, and communications.

Although the sources of information that are available to an operational auditor depend upon the auditors skill, experience and training, some sources are common. The people in the unit being audited are the prime source. A well-conducted interview is often the most efficient tool available.

Internal documentation can also be a major source of information. Organization manuals, organization charts, staff memos, policy manuals, training manuals, and advertising brochures are some of the documents that may be useful in addition to the financial, production, cost and budget ones. The auditor should start the accumulation of documents early in the assignment.

Direct observation is another productive source of information. By consciously observing, the auditor becomes aware of problems that are not reflected in data. Observation is also a source of specific examples that can be used to illustrate general conclusions.

According to Lindberg, each audit assignment has the following phases: [Ref. 35]

1. Definition and organization. The first step in an operations audit is to identify the areas and scope of the study.

2. Preparation. The next step is for the auditor to become familiar with corporate plans, policies, and organization as they relate to the unit or area to be reviewed and to acquaint himself with relevant industry information.

3. Initial survey. The auditor should become oriented in the field within which work is to be done through discussions with key people there. At this stage the auditor samples aspects of the work and the environment of the field of inquiry.

4. Research. After becoming familiar with the field of inquiry, the auditor systematically uncovers the facts about the operations, assignments of responsibility, and plans and management of the area. This stage requires being on guard against attempting to dig out all the facts. Since it is probably impossible to get all of them, the auditor should concentrate on getting the key facts and those that are readily available. They will suffice for the analysis.

5. Analysis. After gathering the key facts and enough additional information to justify the formation of conclusions, the auditor is in a position to analyze and to decide whether the results of analysis indicate true opportunities for the making of improvements.

6. Reporting. At this stage the auditor sums up the findings in writing and takes care to define the uncovered problems as meaningfully as possible in specifics and costs. Although report preparation is customarily regarded as the final step, the auditor will be well advised to start it on the first day; the surest way to drag it out is to wait until the end of the study. It is also beneficial to discuss findings with the manager of the auditing department before submitting the report to a higher level.

7. Justification. This is the last step in a study, often the most critical. At this point such challenges as have arisen to the accuracy or worth of the findings are countered orally by the operations auditor, usually in executive meeting.

To reach the audit objective the auditor must include all of the above steps which can also be characterized as:

1. The preliminary survey
2. The review of management control

3. The detailed examination
4. The report development

These four phases are comparable to the five steps given by the American Institute of Certified Public Accountants for conducting performance evaluations:

1. Ascertaining the pertinent facts and circumstances
2. Seeking and identifying objectives
3. Defining problem areas or opportunities for improvement
4. Evaluating and determining possible improvements
5. Presenting findings and recommendations [Ref. 36]

B. THE PRELIMINARY SURVEY

During the preliminary survey phase, the auditor quickly obtains background and general information on all aspects of the organization being considered for examination. The working knowledge of the entity gained during this phase is not evidence--it is simply descriptive information. It includes historical and operating information as well as legislative information on governmental organizations. Certified Public Accountants (CPA) approach the preliminary survey a litle differently from governmental auditors. They must plan for a request for proposal for the contract for the engagement, as well as prepare for gathering background information. The conclusion of this phase becomes the objective for the next phase. It also becomes the basis for determining how to obtain evidence and how much evidence is needed for the phase that reviews management control.

C. THE REVIEW OF MANAGEMENT CONTROL

One purpose of the second phase is to obtain evidence on the three elements of the tentative audit objective---criteria, cause and effect. Criteria represent the standards for the audit. Causes represent management or employee actions that took place or should have taken place to carry out the appropriate standard. And effects represent the results of the measurement of the causes against the criteria. The term management control as used here includes planning, policy, and procedures determination, as well as the actual practices carried out in managing an organization's affairs. Management control promotes the effective carrying out of assigned responsibility as intended. By obtaining evidence on the tentative audit objective, the auditor determines whether there is a basis for a detailed examination. By determining the competency of the evidence, the auditor can also determine the reliability of the information to be obtained from the management control system.

> Any good management control system follows these steps: setting standards, objectives, goals, or procedures, determining whether the standards, objectives, goals, or procedures have been appropriately carried out; appraising the results of such carrying out; and then, when necessary, taking corrective action. The principle underlying these steps is that no one person should be in complete control of any important part of the operations of the system. [Ref. 37]

The basic approach is to review the specific flow of procedures and practices applied to a specific transaction or item.

D. THE DETAILED EXAMINATION

The detailed examination phase of the audit function is usually thought of as the audit. The prior two phases,

however, determine what is to be done and how it is to be done. Reporting the results of the audit of management's performance concerning efficiency and economy will be discussed in the next section.

The evidence gathered during the detailed examination must be sufficient as well as competent, material, and relevant in order for the auditor to arrive at an acceptable conclusion on the audit objective and then report that conclusion. Interviewing knowledgeable persons generally provides substantial amounts of information that can be used as evidence. The information so obtained may also be used to supplement, explain, interpret, or contradict information obtain by other means.

The emphasis in operational audits in data processing environments is shifting from the evaluation and verification of processing results (e.g. data files, records, reports) to the evaluation and verification of the controls that ensure the continuing accuracy and reliability of processing results. This emphasis is resulting in new audit approaches and techniques. Many of the controls that ensure the accuracy and completeness of data processing results are now automated and can no longer be reviewed and verified through direct observation.

Changing application systems structure presents new problems for auditors. [Ref. 38]

1. Input transactions are being entered for immediate, on-line processing from remote terminal locations in contrast to the single-entry point batch input, typical of earlier years.
2. Applications are being tied together so that a single input transaction performs multiple functions. Transactions are also being generated within an application program and automatically flow into others.

3. Audit trails in hard copy form are being eliminated. For example, detailed lists of input transactions and periodic master data file listings are being replaced by transaction logs on magnetic tape that can be printed if a need arises, and by interrogation of on-line data bases.

Auditing in this environment should include a review of: [Ref. 39]

Manual procedures that have been developed to complement controls internal to computer application programs (e.g., input preparation, input control, error handling, and output balancing and reconcilliation).

Application system controls internal to computer application programs (e.g., data validation, control total verification, batch or transaction balancing and proofing, and error identification and reporting).

Data files and reports produced as a result of computer application processing (e.g., data processing masterfiles, transaction logs, and output reports).

Auditing these areas includes a review of controls to determine their adequacy, tests to verify controls, and tests to verify data (i.e., masterfiles and reports).

E. THE REPORT DEVELOPMENT

All work done in the audit function leads to this phase. The conclusion to the audit objective, which has been developed in the detailed examination phase from evidence gathered in that phase, is converted into a form that an interested third party can accept and understand. There is no standard way for presenting results of an operational audit. There are some basic ideas, however, on ways to present the results.

The "report controls" standard for government economy and efficiency audits and program results audits is presented below. [Ref. 40]

The report shall include:

1. A description of the scope and objectives of the audit.

2. A statement that the audit was made in accordance with generally accepted government auditing standards.

3. A description of material weaknesses found in the internal control system (administrative controls).

4. A statement of positive assurance on those items of compliance tested and negative assurance on those items not tested. This should include significant instances of noncompliance and instances of or indications of fraud, abuse, or illegal acts found during or in connection with the audit. However, fraud, abuse, or illegal acts normally should be covered in a separate report, thus permitting the overall report to be released to the public.

5. Recommendations for actions to improve problem areas noted in the audit and to improve operations. The underlying causes of problems reported should be included to assist in implementing corrective actions.

6. Pertinent views of responsible officials of the organization, program, activity, or function audited concerning the auditors' findings, conclusions, and recommendations. When possible their views should be obtained in writing.

7. A description of noteworthy accomplishments, particularly when management improvements in one area may be applicable elsewhere.

8. A listing of any issues and questions needing further study and consideration.

9. A statement as to whether any pertinent information has been omitted because i is deemed privileged or confidential. The nature of such information should be described, and the law or other basis under which it is withheld should be stated. If a separate report was issued containing this information it should be indicated in the report.

All reportable results should be comparable to the audit results, and should be stated in terms of criteria, causes, and effects. Thus, the auditor will state the criteria in terms of an appropriate standard for the activity, the causes in terms of what were the actual happenings at the time the audit took place as well as what should have been happening and the significance of the results on not carrying out the appropriate standard.

Recommendations are usually brief suggestions by the auditor as to what should be done to bring about improvements in performance. Recommendations are not requirements set by the auditor as to standards that should be followed by the entity. The management of the organization has the responsibility for requiring recommendations to be followed; all the auditor can do is suggest the basis for improvement.

Before preparing a final report, the auditor usually prepares a draft report, which is submitted to the organization concerned with the audit, for their comments in order to be sure that the report is fair, complete, and objective.

Often, the auditor develops and presents a summary or digest of the report to make it easier for the reader to understand the entire report, especially if the report is long.

A useful example of the graphic flow of the phases of the audit function for an operational audit is shown in tables II, III, IV, and V [Ref. 41]

TABLE II

The Preliminary Survey

PHASE CNE

1. Obtain in a relatively short period of time background and general information on organization and management activity being considered for examination.

2. Analyze background and general information to obtain relevant evidence--not necessarily sufficient, material or competent--on one or more elements--criteria, causes, or effects--of a possible audit objective.

3. Assert the other element or elements in order to have a tentative audit objective.

4. Assert alternative criteria and other elements on related management activities to establish possible alternative audit objective.

5. If possible alternative objective is to be considered, obtain relevant evidence, if no evidence has previously been obtained, on one or more elements of the possible audit objective in order to have alternative tentative audit objective.

6. Summarize evidence and assertions on tentative audit objectives.

7. Conclude from relevant evidence and assertions:

   a) that original or alternative tentative audit objective can be used as the objective for the review phase, if relevant, material, and competent evidence can be obtained on all three elements of the tentative objective, and (1) what types of relevant material and competent evidence will be needed to determine the audit objective, and (2) what types and how much evidence will be needed to determine competency of evidence. Proceed to review, or

   b) that tentative objectives cannot be used because evidence would not be available or that conditions do not warrant continuation. Withdraw from engagement.

TABLE III

The Review of Management Control

PHASE TWO

1. Obtain any needed additional background information.
2. Obtain relevant, material, and competent evidence--not necessarily sufficient--on tentative audit objectives by testing management control to determine:
   a) that there could be a reasonable criteria.
   b) that some particular person or group of persons at one or more levels of responsibility could cause an inefficient operation, and
   c) that the effects of the inefficient operation are significant.
3. Obtain evidence from management control system on the competency of evidence that must come from system if additional work is to be done.
4. Determine that evidence could not be obtained on all three elements of the tentative audit objective.
5. Summarize evidence and conclude:
   a) whether the developed tentative audit objective can be a firm objective to be used in the detailed examination phase,
   b) whether evidence that must be obtained would be competent, and
   c) what additional evidence must be obtained and from what source to have sufficient competent, material and relevant evidence to come to a conclusion on the audit objective. Proceed to detailed examination, or
   d) that auditor should withdraw from examination.

TABLE IV

The Detailed Examination

PHASE THREE

1. Obtain any additional background data needed.
2. Obtain sufficient competent, material, and relevant evidence to determine:
   a) the acceptability of the criteria of the audit objective and that any argument against the criteria can be rebutted,
   b) the specific action or lack of action at levels involved in the management activity that caused the effects, and
   c) the significance of the effects.
3. Summarize evidence in terms of criteria, causes, and effects.
4. Conclude from the summarized evidence that the effects in the management activity were significantly inefficient when the actions of employees and management are evaluated against the criteria. Proceed to report development.
5. Conclude that sufficient evidence could not be obtained to determine an appropriate criteria on the management activity, determinable causes, or significant effects or that other conditions warrant that the auditor should withdraw from engagement.

TABLE V

The Report Development

PHASE FOUR

1. Set the scene through background or general information or through scope of audit.
2. Communicate conclusion, stating the significance of the effects caused by not following a proper standard. Sufficient evidence on criteria, causes, and effects should be given with the audit objective for the reader to come to same conclusion as the auditor.
3. State recommendations, usually that the criteria should be followed in the future to obtain best results.

VII. CONSIDERATIONS FOR AN OPERATIONAL AUDIT OF A NARDAC

A. OVERVIEW

An operational audit of a NARDAC can provide a vital check and balance on the organization as it attempts tc meet cost and service goals. The basic purposes of the audit are to ensure that measurable standards for systems development and operaticns functions have been developed; to ensure that these standards are being adhered to by the various departments; to ensure that systems are designed to be easily auditable and that maintenance changes do not create unintended problems; and to act as a catalyst for improving operating efficiency.

The NARDACs are incredibly complex. The governing regulations are intricate and perpetually changing. The pragmatic civil service management tacks new procedures onto the old and maintains the same basic work patterns. The civil servants are a force for continuity in this dynamic operation. In contrast, the military managers are invariably committed to change. When making recommendations for improvements as the result of an operational audit, the auditor must be aware that what can be done in and by a NARDAC is limited by the legal and political framework in which it functions. The lack of administrative continuity increases the need for an effective internal control system.

B. INTERNAL CONTROLS IN FEDERAL GOVERNMENT

In 1950, the Accounting and Auditing Act was passed requiring, among other things, that agency heads establish and maintain effective systems of internal control. Since then, the General Accounting Office (GAO) has issued

numerous publications to guide agencies in establishing and maintaining effective internal control systems. While the need for improved internal controls has continued, development of effective systems has been slow.

In the past decade, numerous situations came to light that dramatically demonstrated the need for controls as the government experienced a rash of illegal, unauthorized, and questionable acts which were characterized as fraud, waste, and abuse. It is generally recognized that good internal controls would have made the commission of such wrongful acts more difficult. Consequently, increased attention is being directed toward strengthening internal controls to help in the restoration of confidence in government and to improve its operations.

The Federal Managers' Financial Integrity Act of 1982 requires renewed focus on the need to strengthen internal controls. The act requires periodic evaluation of agency internal control systems and that the heads of executive agencies report annually on their system status. These evaluations are to be made pursuant to the "Guidelines for the Evaluation and Improvement of and Reporting on Internal Control Systems in the Federal Government," issued by the Office of Management and Budget in December, 1982. The reports are to state whether systems meet the objectives of internal control and conform to standards established by GAO.

Standards for Internal Controls in the Federal Government, issued by GAO, presents the internal control standards to be followed, and covers both the program management as well as the traditional financial management areas. GAO will issue interpretations and revisions to the standards as may become necessary.

The following is GAO's concept of internal controls: [Ref. 42]

The plan of organization and methods and procedures adopted by management to ensure that resource use is consistent with laws, regulations, and policies; that resources are safeguarded against waste, loss, and misuse; and that reliable data are obtained, maintained, and fairly disclosed in reports.

The GAO general internal control standards apply to all aspects of internal controls. Table VI is an outline of the standards: [Ref. 43]

TABLE VI

GAO General Internal Control Standards

1. Reasonable Assurance. Internal Control Systems are to provide reasonable assurance that the objectives of the systems will be accomplished.
2. Supportative attitude. Managers and employees are to maintain and demonstrate a positive and supportive attitude toward internal controls at all times.
3. Competent Personnel. Managers and employees are to have personal and professional integrity and are to maintain a level of competence that allows them to accomplish their assign duties, as well as understand the importance of developing and implementing good internal controls.
4. Control Objectives. Internal control objectives are to be identified or developed for each agency activity and are to be logical, applicable, and reasonably complete.
5. Control Techniques. Internal control techniques are to be effective and efficient in accomplishing their internal control objectives.

It is essential to provide assurance that the internal control objectives will be achieved. These critical techniques are the specific standards outlined in Table VII. [Ref. 44]

TABLE VII

GAO Specific Internal Control Standards

1. Documentation. Internal control systems and all transactions and other significant events are to be clearly documented, and the documentation is to be readily available for examination.

2. Recording of Transactions and Events. Transactions and other significant events are to be promptly and properly classified.

3. Execution of Transactions and Events. Transactions and other significant events are to be authorized and executed only by persons acting within the scope of their authority.

4. Separation of Duties. Key duties and responsibilities in authorizing, processing, recording, and reviewing transactions should be separated among individuals.

5. Supervision. Qualified and continuous supervision is to be provided to ensure that internal control objectives are achieved.

6. Access to and Accountability for Resources. Access to resources and records is to be limited to authorized individuals, and accountability for the custody and use of resources is to be assigned and maintained. Periodic comparison shall be made of the resources with the recorded accountability to determine whether the two agree. The frequency of the comparison shall be a function of the vulnerability of the asset.

Auditors are responsible for following up on audit findings and recommendations to ascertain that resolution has been achieved. Table VIII presents the Audit Resolution Standard. [Ref. 45]

TABLE VIII

GAO Audit Resolution Standard

Prompt Resolution of Audit Findings. Managers are to (1) promptly evaluate findings and recommendations reported by auditors, (2) determine proper actions in response to audit findings and recommendations, and (3) complete, within established time frames, all actions that correct or otherwise resolve the matters brought to management's attention.

C. INTERNAL CONTROLS IN THE DATA PROCESSING ENVIRONMENT

Internal controls in the data processing environment pertain to the processing and recording of an organization's transactions and to resulting management reporting. They are the procedures that ensure the accuracy and completeness of manual and automated transactions, records, and reports, and the avoidance, detection, and correction of errors. They encompass source document origination, authorization, processing, data processing record keeping and reporting, and the use of data processing records and reports in controlling an organization's activities.

The "Data Processing Audit Practices Report," issued by the Institute of Internal Auditors, presents an overview of the elements of internal control in the typical data processing function. These elements are applicable to a NARDAC in addition to general controls needed by any organization. These elements are: [Ref. 46]

Computer application systems, which encompass manual procedures to originate and transmit input transactions to the data processing department; computer application programs that control the processing of transaction

data, record maintenance, and output report preparation; and procedures that guide computer service center personnel in the use of specific computer application programs and the handling of the associated input data and output reports.

Computer service center operations, which encompass the facilities, equipment, personnel, and general procedures that govern computer center operations, as opposed to procedures specific to individual application systems.

Application systems development, which encompasses the personnel and general procedures governing the design, development, testing, and implementation of the manual procedures and computer application programs that make up computer application systems. This element also includes the modification and improvement of existing computer application programs.

The three data processing elements are planned, organized, and managed to achieve various management information system objectives. They are also interdependent. For example, systems development may be constrained by the availability of processing capacity or specialized resources. In contrast, processing capacity may be increased and special features added to accommodate new systems development requirements.

A similar interdependency exists between computer application systems and the computer service center. Poorly designed application programs can degrade overall center operations. Intervention required by center personnel tends to be error prone and to make inefficient use of expensive computer resources. Computer service center operations can have a significant impact upon computer application systems. Poorly or inadequately trained staff are frequent causes of processing problems that affect application systems and their users. Inadequate procedures within the computer service center can cause or allow errors to pass undetected in the preparation, scheduling, and handling of input transactions, data files, and output reports. Such undetected errors can defeat the intent of controls built into computer application programs, at considerable expense in terms of development time and money.

D. THE PERSONNEL SYSTEM

When the Federal staffing process requires several months to routinely fill a position, the process is a disservice to mission accomplishment. The regulations exist to prevent abuse of privileges, but the result is often less flexibility for the responsible manager.

Before action can be taken to hire, transfer, promote, reassign or demote a civilian at a NARDAC (or any Federal government job), a formally established position description (PD), classified in accordance with laws and regulations, must exist for the job. A PD provides information on the principal duties, responsibilities and supervisory relationships of a position. This information is used primarily for classification purposes, but has other functions as well. PD's can help to detect duplication of work or overlapped duties; analyze training needs; and help to determine standards of performance. Because PD's affect so many personnel practices, they are an important source of information for the operational auditor.

A vital part of the Federal staffing process is evaluation of a new employee during the probationary period. Separation of an inadequate employee is more difficult after the probationary period, and the employee could remain on the payroll for many years as a marginal producer. An employee who completes a probationary period can never be required to serve another such period.

E. PRODUCTIVITY CONSIDERATIONS

Before a manager can increase productivity, productivity has to be defined. Performance objectives are tools that are applicable only in settings that demand accountability and that reward performance. One major difference between a NARDAC and a similar organization in private industry is in

the degree by which either would benefit from an operational audit. Much of a NAEDAC's productivity problem may really be a problem of law.

In "Coping with the Employee Turned Institution," Jeffrey Davidson, discusses the phenomenon of the employee in a Federal position who has effectively ceased to function in the position to which hired or promoted. Davidson gives details of how to identify such an employee and what to do about one. [Ref. 47]

> There exists in . . . large organizations at least one employee who has effectively ceased functioning in the role or position for which . . . originally hired, or to which . . . promoted. This type of employee turned institution is acclimated to all the ways of getting through each workday contributing an appearance of being on top of the job.
>
> The personnel, management, and monitoring systems and procedures within federal government leave much to be desired. The possibility that an employee can become an institution within any organization stems from a variety or reasons. One reason is that the employee possesses specific knowledge or skill that the organization cannot readily acquire from other sources. The employee may have developed a particular expertise that, at least periodically, is of vital importance to operations. Frequently, an employee turns "institution" within an organization simply because he or she is <u>allowed to</u>, and no one (not even the supervisor) is cognizant of, or willing to expose, the employee's general lack of dedication and limited effectiveness on the job.
>
> Usually when an employee turns institution the occurrence is due, in part, to a <u>lack of awareness</u> on the part of one key manager or supervisor. That one key person having knowledge of the employee's true work habits and operating procedures, would not allow such a practice to exist. The employee turned institution promotes mediocrity; when confronted with an idea that might be good for the organization but would involve real work, the employee will often respond with idea-killing phrases like "We've tried that before," or, "That never works."
>
> While the employee may make no significant contributions, rest assured that he or she will be well informed of organization policies and procedures, and will do whatever possible to stretch the policies for personal advantage. The employee turned institution can flourish only when otherwise good managers and supervisors refuse to see the true picture. The employee must be stopped cold, before having a chance to:
>
> 1. Lower productivity,
> 2. Demoralize other employees,

3. Unfavorably influence other employees,

4. Tarnish the organization's image to outside parties.

This pheromenon of the employee turned institution occurs frequently throughout the federal government, since it is difficult to remove an employee from a federal position.

F. NARDAC LEAD-ACTIVITY APPROACH

Because ADP technology changes so rapidly and ADP resources are scarce, individual NARDACs have been assigned the lead responsibility in specific aspects of the technology. For example, NARDAC Norfolk has been tasked by NAVDAC with the responsibility of providing client support for the acquisition and use of microcomputers. In response to this tasking, it has developed a Technical Reference Library and Software Exchange Center. It has established a microcomputer user group, and it also performs ongoing hardware/software evaluation programs. This lead activity has alsc prepared reports on the subject of Low-ccst Expandable Microcomputer Systems, also known as the LEMS Project. This lead assignment approach has distinct advantages to the customer activities and the NARDACs. It enables all NARDACs tc keep abreast of the state of the art while avciding costly duplication of effort. Moreover, it fosters standard implementation of enhancements at all NARDAC sites.

The lead assignment of each NARDAC would require special consideration in the desigh of an audit program fcr a particular NARDAC.

G. CONCIUSIONS

Every manager must have a means for readily identifying and accurately defining emerging problems before they beccme institutionalized. The motive for operational auditing is

that it is an efficient source of information about the sophisticated problems facing a manager.

> The manager's task is far more difficult and challenging than the normal tasks of the mathematician, the physicist, or the engineer. In management, many more significant factors must be taken into account. The inter-relationships of the factors are more complex. The systems are of greater scope. The non-linear relationships that control the course of events are more significant. [Ref. 48]

As more authority is delegated it becomes increasingly difficult for top management to keep informed on how well its programs and policies are being carried out. Operational auditing provides information needed by top managers who can not be personally informed about all areas for which they are responsible. Without a means for objectively measuring performance, managers may spend too much time doing the wrong things--things that might make them look good on the surface but which actually are not good for the organization.

VIII. PERFORMING THE AUDIT

A. PURPOSE OF THE AUDIT

The NARDACs became Navy Industrial Fund (NIF) activities at the beginning of fiscal year 1984. NIF activities are required to bill customers, using a stabilized rate, for the ADP services rendered. Commander, Naval Data Automation Command (COMNAVDAC) approves the number and kind of rates to be established. These rates are expected to remain in effect for an entire fiscal year. Any variance between stabilized rate billings and actual costs become profits or losses to the NIF activity and are absorbed by the corpus. The goal, however, is total cost recovery, generating neither profit nor loss. Because all costs are passed on to the customers, efficient and economical operations are a major concern. The customers should not be required to pay for inefficiencies. Thus, an operational audit is critical to the identification of areas in need of improvement.

The NARDACs have been studied for potential contracting out of the services now performed by government civilian and military personnel. Plans are being made for an internal reorganization to allow for government management and monitoring of the operations after the contract has been let. When contracting for services, the government has to specify acceptable standards of operations. An audit would help to define the needed criteria and provide a means to evaluate these criteria that will be applicable to the contractor.

The commanding officer of the NARDAC would be the recepient of the audit report except when the audit has been conducted at the direction or request of COMNAVDAC. In that case, the report would be made to COMNAVDAC.

Effective, efficient, and economical use of the computer resources at a NARDAC requires ongoing coordination among management, computer users, and auditors to bring this powerful tcol intc proper perspective and under close control. Vast amounts of data have been concentrated in a few ccmputer centers. This condition has resulted in virtually total depen.dence upon the computer. To minimize the potential vulnerability for loss associated with this dependence requires a greater degree of audit involvement than previously required. Data processing equipment, software and perscnnel are expensive. These costs and the pctential for loss, destruction, or misuse of these resources must all be considered when reviewing the internal contrcls and security required fcr the Electronic Data Process (EDP) facility.

Unlike auditing in the traditional sense, operational audits concentrate on the utilization of resources, also paying considerable attention to information systems and internal organization and procedures. There is scme overlap, however, of financial audits and operational audits. Bcth, for example, review the systems and procedures of internal ccntrol. Operational auditing also provides detailed reviews of other areas such as space utilization, purchasing practices, hiring practices, and management decision making. Operational auditing provides a means to determine whether employees are giving their best efforts or whether costs can be lowered.

B. PURPCSE OF THE AUDIT GUIDE

The purpose of this guide is to provide uniform instructions and guidance to personnel engaged in auditing EDP facilities at a NARDAC. This audit guide (program) is a result of the increased emphasis being place on management

of and control over the Navy's EDP facilities. The guide is designed to include organization, facility internal controls, maintenance, security, resources and contingency planning, and user billing/chargeout procedures. Audits at a NARDAC may involve only the NARDAC or include reviews at a number of customer activities. The extent of detailed work to be accomplished will depend on the quality and extent of the services provided to customer activities. **The auditor will determine the order and extent of audit coverage necessary for the particular NARDAC being audited.** The audit steps are intended to lead the auditor into the more important aspects of the NARDAC management but are not intended to be restrictive or to serve as a substitute for initiative, imagination, and judgment.

The objectives of EDP facility audits are to:

1. appraise the adequacy, efficiency, and reliability of the EDP facility, including training programs, security, and processing controls;
2. determine the extent and adequacy of application system procedural controls; and
3. Evaluate procedures, standards, and controls over local program development.

The audit guide provides a standardized audit approach. It is, however, only to aid the auditor during the audit process--not to direct every step. The auditor must still rely on experience, intuition, and preliminary results of the audit in determining the full scope of the audit. The objective of this guide is to organize the audit approach, reduce preparation time, and ensure a level of completeness on the audit. This guide is primarily a result of adapting audit programs issued by the Naval Audit Service. (The Naval Audit Service designs audit programs that provide comprehensive guidance for auditing selected functions.) Other guides can be obtained in the following ways: [Ref. 49]

1. From associations such as: American Institute of Certified Public Accountants, The Institute of Internal Auditors, Bank Administration Institute, Canadian Institute of Chartered Accountants.

2. From major certified public accounting firms and chartered accounting firms.

3. From organizations supplying manuals and an updating service such as: Auerbach, Datapro, FAIM.

4. From publications such as Security, Accuracy, and Privacy in Computer Systems by James Martin (Prentice-Hall, 1973) AFIPS Systems Review Manual on Security, AFIPS, Montvale, N. J. (1974); Computer Security, National Computing Centre, (Manchester, U. K.) Guidelines for Automatic Data Processing, Physical Security, and Risk Assessment, National Bureau of Standards (1974).

Audit guides obtained from the above sources can be modified to meet the specific needs of the organization. It is recommended that two or more audit guides for one area be obtained. At that time . . . auditing personnel can combine the questions and approaches on the audit guides with their own knowledge of the organization in that area. This would result in an audit guide meeting the specific needs of the organization. A data processing background is necessary to effectively use this auditing guide. Without this background, the auditor will not comprehend the importance of or meaning behind some of the items in the guide.

C. GENERAL INSTRUCTIONS

In performing an audit, the auditor should proceed as follows:

1. Establish the purpose and scope of the audit.

2. Make necessary modifications to the audit program based on the particular audit objectives.

3. Perform an initial survey, interviewing NARDAC management to obtain background information; to gather documents describing the NARDAC organization, their equipment and applicable Department of Defense, Secretary of the Navy, Chief of Naval Operations, and Commander, Naval Data Automation Command Instructions detailing standards; and to gain an understanding of the NARDAC policies and standards.

4. Conduct a review of management controls. Interview and gather data from NARDAC customers and NARDAC employees.

5. Perform a detailed examination of operations. Analyze the data, making additional examinations and evaluations as required.

6. Write a final report indicating the conclusions drawn from the audit and supporting each conclusion by the finding upon which it is based. Make recommendations for solving the problems found.

This audit guide is organized into three chapters. Each chapter gives detailed steps applicable to three areas of EDP facility operations as follows: [Ref. 50]

1. Computer center controls
   a. organization and management;
   b. input/output procedures;
   c. media library;
   d. operations;
   e. environment and security;
   f. resource and contingency planning;
   g. time accounting and billing;
2. Application system procedural controls
   a. transaction origination;
   b. transaction entry;
   c. data communications;
   d. computer processing;
   e. data storage and retrieval;
   f. output processing;
3. Local programming development controls
   a. requirements approval;
   b. programming management;
   c. acceptance testing;
   d. documentation and interface;
   e. data base administration.

The auditor may add to this program, or omit certain steps from the program to attain the audit objectives. Assistance of computer specialists may be required in application of this guide.

Internal controls are essential to the prevention of fraud or illegal practices. Those audit steps annotated by

the letter M ("M") are to be highlighted and performance of these steps is recommended.

IX. AUDITING THE COMPUTER CENTER

A. ORGANIZATION AND MANAGEMENT

The organization of the computer center is basic; the structure of the organization and the quality of personnel affect management's ability to implement internal controls.

The preliminary survey provides the first set of information about the NARDAC, information needed to direct and execute an audit efficiently. Through a set of interviews with Department Heads and Division Heads, the auditors should obtain background information on the development of the NARDAC, its organizational ties, its purpose, the types of services it provides, the resources available to it, how they are applied, who its customers are, and the bases for its service charges.

As much documentation as possible should be obtained since documentation on policies, procedures, plans and management reports can indicate the efficiency of NARDAC management.

The background information obtained through the interviews and the availability of documentation--or lack of documentation--will allow the auditors to prepare an audit plan that properly addresses itself to the areas that seem to need special attention. Obtain an overview of the historical development of the NARDAC.

The "Navy ADP Reorganization Study Implementation Plan Report" provides a detailed overview of the historical perspective of NARDACs. Obtain documentation of the organization charts, policy statements, job descriptions, personnel listings and descriptions of services. The NARDAC

Organization Manual is an excellent source for some of the necessary information. Indications of the established delegation of responsibilities should be obtained, as well as of the separation of authority, how these are defined, and the controls in force to assure proper adherence.

Lists of assets reflecting the entire complement of facilities and hardware, as well as software, should be obtained, together with supporting layout plans. Supplemental documents for the various functional areas (e.g., standards manuals, operator manuals, user manuals, equipment lists and layouts, facilities plans, user lists) should also be gathered.

Analysis of management's use of performance reporting systems will indicate potential problems. Documentation of planning done for the NARDAC, operational as well as financial, for the short term and long term, should also be requested.

For an overview of the administration of the NARDAC, the organization manual, procedures or directives pertaining to internal as well as external functions should be reviewed. Personnel management will be reflected in the available recruiting and hiring policies, functional descriptions, personnel development plans and training programs, and career path and promotion plans.

1. Identify the mission and operations of the facility to determine the major areas of EDP responsibilities of the activity, including scope of operations and limitations on responsibility and authority.
2. Determine if the facility organization promotes mission accomplishment and provides separation of responsibilities.
3. Examine the latest reports of internal review, inspections, and audits, and evaluate action taken to correct deficiencies.
4. "M" Review the EDP facilities risk assessment. (Refer to Enclosure (3) of OPNAVINST 5239.1 entitled "Automatic Data Processing Risk Assessment" for the definition and scope of an EDP facility risk assessment.)

a. Ensure that all assets have been identified.

b. Evaluate the reasonableness of the identified potential for loss.

c. Ensure that a positive balance of facility controls has been established which equates the incremental cost of including such controls with the risk of loss due to their omission.

5. "M" Determine that the EDP facility has established a formal system of administrative controls which establish tasks, functions, and policies covering the following areas:

a. preinstallation controls which cover feasibility studies and preinstallation planning.

b. organization controls which cover the division of duties both outside and within the EDP divisions, the functions of the data control group, tape library, etc.

c. development controls which cover the planning of new applications, the establishment of standard procedures for system design and programming, authorizations and approvals, testing, controls over initial conversion, and control over subsequent changes.

d. procedures established for control over change to central design agency (CDA) supplied programs.

e. operations controls which cover standard operating instructions, file handling, and protection against accidental destruction.

f. processing controls which cover hardware controls, input and output controls, programmed controls, and provide audit trails.

g. documentation controls which cover problem definition, documentation standards, systems and program documentation, operators's manuals, etc.

h. outside data center controls which cover the commitment and selection of data center services, organizational requirements for data center operations, I/O controls and audit trails, and security for customer data records.

6. "M" Review the EDP facility security plans, policies, and procedures. (OPNAVINST 5239.1, NAVCOMPINST 7000.36; and FIPS PUB 31)

a. Ensure that an EDP security officer has been assigned. This position should be organizationally separate from the EDP operations and have specific responsibilities and authority for implementation and maintenance of facility security.

b. Review established security policies and procedures. Specific responsibilities should be identified for all facility personnel concerning EDP security and periodic security training provided.

c. Evaluate results of periodic security reviews and determine that appropriate actions have been taken to prevent reoccurance of security violations.

d. At activities with remote terminal operations, determine that passwords and terminal access control responsibilities are centralized with EDP security officer. Ensure that procedures are established which require periodic changes of passwords and mandatory changes upon personnel separations.

e. Ensure that at facilities responsible for processing classified data EDP personnel have security clearances equivalent to the classification of data being processed.

f. Ensure that a formal access list indicating the specific conditions under which access to the various EDP areas will be authorized. This should include limited access to the computer and library areas to only personnel with assigned responsibilities in these areas.

g. Review accountability of control procedures and devices used at the facility. Ensure that badges, card keys, cypher books, safe combinations, or similar devices in use are controlled and periodically changed and that these actions are recorded.

7. Ensure that user/customer liaison procedures have been established to provide for not only resolution of input/output problems but to support periodic reports and management reviews. (SECNAVINST 5214.2; SECNAVINST 5210.8a)

8. "M" Verify that EDP support provided to private parties or contractors has been properly approved. (Navy Regulations, Article 0749; and NAVCOMPT Manual, par 075500-1) and that appropriate billing rates are established. (NAVCOMPT Manual, par. 0355881)

B. INPUT/OUTPUT CONTROL AND SCHEDULING

Effective quality assurance/production control ensures the timeliness, accuracy, and overall integrity of work submitted to and emanating from the computer center. This includes scheduling of work and quality control of source data and outbound reports to ensure accuracy and completeness of data received and distributed. (NAVCOMPTINST 7000.36)

9. "M" Review facility procedures for acceptance and scheduling of input data:

   a. Examine logs, records, and schedules of anticipated inputs.

   b. All input data should be scheduled.

   c. Follow up should be provided on late data receipt.

   d. Records should be maintained indicating the date source documents are due in, date received, persons authorized to submit, and persons actually submitting.

   e. Are negative responses required when anticipated data is not to be submitted? How is unscheduled data received?

   f. Do receipt procedures require preliminary verification to ensure that all illegible, incomplete, or otherwise unacceptable source documents are returned to the originator prior to further processing of the document? Unused portions of input coding sheets should be voided by the originator to preclude unauthorized additions.

10. "M" Review facility procedures for transcription and control of input data. Analyze the following:

   a. Input job control procedures should be documented for each job and detailed procedures established to prevent loss, misuse, or improper handling. To ensure complete and accurate receipt and transfer of all input documents, one or more of the following checks should be used for each job:

      (1) Document register;

      (2) Batch control tickets;

      (3) Transmittal slip;

      (4) Beginning and ending document numbers:

      (5) Money amount totals;

      (6) Hash totals.

   b. Source data automation procedures should use key entry system production features to the maximum extent possible for data verification. Rekeying verification should only be used when key entry system production features do not provide sufficient assurance of data accuracy.

   c. Ensure that key entry operating procedures prohibit key entry personnel from altering data on source documents and restrict access to source data automation programs.

d. Ensure that the computer programmers, system analysts, and computer operators do not have access to source documents. Programming jobs which require fast turnaround time should be submitted through normal input procedures with priority handling.

e. Analyze data entry production statistics for effective utilization of personnel and equipment capabilities. Ensure that source data automation back-up support plans are documented and filed both onsite and offsite.

f. Ensure that the input preparation phase is completed in accordance with clearly specified processing schedules. Investigate excessive late deliveries of input data for processing.

11. "M" Review facility procedures for processing output to users. Perform an analysis of the following:

a. Ensure that there is adequate control of rejected original documents to ensure timely distribution to the authorized originator for investigation, correction, and reinput or cancellation.

b. Ensure that authorization listings are maintained for individuals designated to receive output and that these provisions are enforced.

d. Ensure that the data and condition of issuance of input data or other ADP source data distributed for use at other EDP facilities is documented and that authorization is verified before distribution.

e. Ensure that procedures are established to indicate location and specific retention and disposition of original source documents.

C. MEDIA LIBRARY CONTROLS

Data processing management must ensure the continued availability of data stored on various data processing media (primarily magnetic tapes and disks). In addition, some of this data may be especially sensitive or confidential, requiring special custody methods. (NAVCOMPINST 7000.36 and FIPS PUB 31)

12. "M" Review access controls to the media library and the procedures for issuance of media.

a. Ensure that there is a physical separation of the media library from the computer room and that adequate space is provided for storage of tapes, disks, etc. This area should be secured when not staffed.

b. Ensure that access to the media library is limited to specifically authorized personnel and is consistent with the separation of duties between input/output, computer operation, and media library personnel.

c. Identify personnel designated as librarians and ensure that their duties are separate and distinct from other EDP functions. Assess the work schedule of the librarians to ensure that staffing is sufficient to maintain controls over the issuance of media.

13. "M" Review media library inventory procedures.

a. Ensure that the schedules, logs, etc., are maintained indicating when media is issued and is due for return. Evaluate procedures for protection of intransit media. The catalogs or index listings should show the current physical location of all media storage units. Compare this record with job accounting records to check for consistency. Evaluate procedures for follow up on overdue media storage units.

b. Ensure that instructions indicating how and under what circumstances tapes or disks (including blanks) can be checked in or out of the library. This should include listing of authorized personnel and security clearances. Ensure that borrowed media from other locations are documented: (1) Name of requester. (2) Date received. (3) Due date to return. (4) Lending location.

c. Ensure that a complete inventory listing is maintained for each storage location that accounts for all media storage units from receipt of blanks to disposal of used units. The inventory list should include as a minimum: (1) Library location. (2) Reel or serial number. (3) Job or project number. (4) Description of data. (5) Date created. (6) Retention-expiration of retention period. (7) Owner. (8) Issued to and date. (9) Returned date.

d. Ensure that periodic physical inventories are performed and that differences are reconciled and missing media located. Ensure that on hand media stocks are adequate for continuous operation.

e. Assess the adequacy of the physical storage facilities in the main media library and in back-up libraries.

14. Review media storage maintenance procurement and disposal procedures.

a. Evaluate the facility's media unit test, cleaning, reconditioning, and degaussing procedures. Determine the adequacy of procedures established for monitoring and accounting for media storage usage.

b. Ensure that media storage cleaning, reconditioning, and degaussing machines are physically separated from the library area.

c. Unless nonstandard media storage units are justified by the facility, ensure that only standard stock media storage units are procured through standard supply schedules.

d. Evaluate procedures for disposal of used media storage units. Storage units which contained classified or sensitive data should be erased before disposal.

e. Trace the backup and retention systems for the media and ensure that procedures and the compliance thereto are adequate to support EDP processing backup.

D. OPERATION AND MALFUNCTION/PREVENTIVE MAINTENANCE

Effective and efficient processing is facilitated by formally defined procedures for operating personnel. This includes not only production procedures but also procedures for reporting of hardware and systems software malfunctions.

15. Review computer room procedures.

a. Ensure that shift schedules provide for personnel rotation and that all operators are given experience in processing various applications. No one operator should always be responsible for a particular application.

b. Ensure that the duties of computer operators, programmers, or system analysts do not include initiation of transactions into the system and/or changes in the master files. Operators also should not be allowed to utilize the console to handle error routines without prior approval of persons outside the operations unit.

c. Programmers, analysts, and system managers should be denied uncontrolled access to the computer room unless such access is clearly prescribed and consistent with formally assigned duties and responsibilities.

d. Determine that there are formal system operating procedures for each scheduled application and that console logs are reviewed.

16. Evaluate malfunction and maintenance records.

    a. Review malfunction and maintenance records to detect patterns of poor performance and other exceptional characteristics.

    b. Review computer system performance records and schedules to assess the impact of maintenance and reliability on the productivity of the installation.

    c. Review accounting system production run time statistics to determine any positive or negative trends in the length of time required to process specific applications. If times are increasing, review maintenance and operating procedures and statistics to determine why production efficiency is declining rather than improving.

    d. Interview management, vendor, and service personnel concerning their function and their interactions.

    e. Trace the process of detecting, correcting, accounting, and reporting hardware and software failures. (SECNAVINST 5238.1a) Critical points are logging, setting priorities, assigning for resolution, exception reporting for long-lasting troubles, assessing the performance of the vendor, and comparing this instance with prior instances.

17. Obtain a listing of remote terminals, evaluate the justification for the installations and the capabilities available at each terminal relative to file updating and transaction input.

E. ENVIRONMENTAL CONTROLS AND PHYSICAL SECURITY

Data processing facilities are a substantial asset and must be managed to minimize the possibility of loss of capability. This includes physical protection against natural hazards and the control of individuals' use of facilities. (OPNAVINST 5239.1, NAVCOMPTINST 7000.36)

18. "M" Obtain and analyze the floor plan of the facility.

    a. Evaluate the adequacy of the locking devices between facility areas and at entrances and exits (including windows).

    b. Evaluate the construction and materials used in the facility with regard to their fire-resistant qualities. Ensure that storage areas for combustible items, such as stocks of paper,

tapes, etc., are physically separate from the computer room. Computer room stocks of combustible materials should be limited to working stock and stored near fire extinguishers.

c. Review all fire alarm systems and determine how and where the systems may be activated. Determine if the fire alarm sounds locally at the guard stations, or at the police and fire departments. Ensure that heat and smoke detectors are installed.

d. Determine if there is a water detection system. Review the drainage system of the building; and, if necessary, determine that an adequate pumping system is installed or available from the fire department.

e. Ensure that the condition of the facilities' ceiling or roof provides adequate protection from leaks. Examine the overhead area for the presence of any pipes that may result in water damage.

19. Examine the power supply, assessing the appropriateness of back-up equipment to the needs of the facility.

a. Check records of the reliability of the local power supply and the impact of failures on the operation of the facility. Examine the records of recording instrumentation measuring line voltage.

b. Determine if there is a standby power source to support computer operations, emergency lighting, and electrically-operated access controls. Ensure that the standby power system is adequately maintained and periodically tested.

20. Examine provisions for air conditioning for the computer room, input area, and media library.

a. Ensure that the air-conditioning equipment is secure and is dedicated to the production areas. Ensure that proper temperature and humidity is maintained.

b. Determine that air conditioning and heating systems are serviced on a regular schedule. Ensure that backup air conditioning provisions are adequate.

c. Assess the degree of protection provided for air intakes, cooling towers, smoke removal, and exhaust systems.

21. Obtain a listing of remote terminals, and evaluate the security procedures for permanent and portable installations.

a. Inspect the terminals to determine if they are located in appropriately controlled areas. Examine practices from the standpoint of the use of keyboard locking devices, operator IDs and passwords, overprinting of passwords, and related features.

b. Examine the access of terminal users to

assembly-level languages and assess the protection mechanisms that are available.

c. Determine if the use of terminals associated with classified data bases and programs is adequately monitored and supported by data protection techniques.

22. "M" Evaluate the facility physical access controls.

a. Obtain list of personnel who have authorized access to various areas in the facility and assess the necessity of such access. Compare this list with the issue control list of card keys, combinations, etc. that have been issued.

b. Ensure that procedures for issuance of keys, combinations, etc. are adequate.

c. Determine if badges are used for personnel or visitors.

d. Ensure access controls outside of day-shift hours require reporting to notify management of personnel who access the facility. Determine if personnel challenge strangers.

23. Review emergency procedures.

a. Observe that emergency telephone nembers are posted conspicuously.

b. Ensure that emergency power off switches are marked and placed at all emergency exits and are protected from accidental activation.

c. Review fire drill and shut down procedures for adequacy and completeness. Determine if employees know the location of the sprinkler shut-off valve.

d. Ensure that portable fire extinguishers are suitably located throughout the computer area and that personnel are trained in their use. Obtain documentation to verify that fire detection equipment is tested on a regular basis. Ensure that smoking is prohibited in the computer area and the media library.

e. Ensure that exits are adequate, well-marked and kept free of obstructions.

24. Determine if back-up facilities are tested at regular intervals, and if the procedures for the test and the changeover are readily available to personnel.

F. RESOURCE AND CONTINGENCY PLANNING

Management Of the computer center has a continuing responsibility to ensure that efficient and economical

services are provided on a continuing basis. Management must be able to predict changes in workloads and the effect of those changes on resource requirements. A primary responsibility is to maintain suitable contingency control plans covering disaster conditions, either natural or man-made.

25. Review activity budgeting responsibilities and determine the adequacy of fund administration for budget execution.

26. Review controls and procedures for acquiring, reporting and monitoring the utilization of EDP equipment.

    a. Appraise the procedures for determining and evaluating idle and excess property. Examine the most recent Reconciliation of Plant Account for accuracy of reporting. (SECNAVINST 5237.1A)

    b. Appraise the reporting and processing of excess EDP equipment for reutilization or disposal actions. (SECNAVINST 5237.1)

    c. Appraise management procedures to report EDP equipment utilization. (SECNAVINST 5238.1A)

    d. Appraise management procedures to maintain optimum utilization, including the following:

        (1) Determine who is responsible for performance measurement within the data processing organization.

        (2) Determine what methods or techniques the installation uses for evaluating the efficiency of computer operations (hardware and software).

        (3) Review the installation's program for evaluating computer systems performance.

        (4) Evaluate results obtained from performance evaluation.

        (5) Review available performance measurement statistics such as hardware or software monitor output, and system management facility information. Do statistics show under-utilization of any hardware? Of particular concern are the central processing unit (CPU), tape drives, printers, disk drives, and channels.

27. Review facility contingency plans:

    a. Obtain and review risk analysis performed to identify potential threats to the facility. Ensure that contingency plans developed from this risk analysis are consistent with the identified threats and equate cost of implementing the

contingency plans to the potential for loss. (OPNAVINST 5239.1)

b. Review contingency plans to ensure that procedures are established to guide facility activities during natural disasters as well as civil disturbances. Contingency plans should cover both (1) loss or destruction of data and program files and (2) theft of information and delays in computer processing.

c. Ensure that security and operations personnel are periodically briefed on their responsibilities for implementing disaster contingency plans.

28. Review facility backup support agreements:

a. Ensure that backup support agreements provide for not only processing of critical applications but also for input data transcription services.

b. Ensure that support sites have the capacity or can arrange to accommodate the added backup support by discontinuing their nonessential processing.

c. Ensure that detailed operating procedures, instructions, etc. are stored with back up media at a remote site from the facility which can be transferred to the backup facility if necessary to resume EDP processing.

d. Ensure that the backup processing plan has been tested and problems identified resolved.

G. TIME ACCOUNTING AND BILLING PROCEDURES

Management has a responsibility to ensure that operating costs of the computer center are equitably distributed among reimbursable users. Equitable distribution of cost requires that an adequate acccunting system provide maintenance of records and documentation for both financial and nonfinancial data. Documentation of recorded CPU time and storage cost plus material and labor usage must afford an adequate basis for billing and provide a logical audit trail.

29. Review EDP acccunting procedures.

a. Ensure that billing algorithms, statements, and rerun cost allocation procedures provide for identification of responsible customer.

b. Ensure unique supplies and other quantifiable

direct cost, such as commercial data transcription services, are identified and supported.

c. For nongovernment users, private parties, ensure that the greater of either the activity computed cost or the local commercial rate is billed. (NAVCOMPT Manual, par. 035881)

d. Ensure that the billings are supported by detail billing analysis for each customer.

30. Review activity billing procedures and analyze the following:

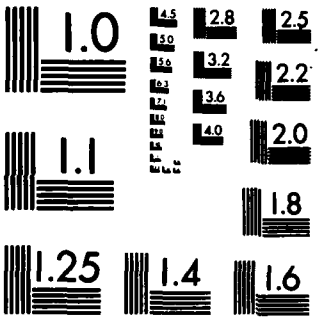
a. Determine that there are intra/inter services support agreements between the computer center and reimbursable users.

b. Examine consistency between billings and the job accounting system.

c. Examine procedures to arbitrate billing disputes between users and the center.

AD-A145 785 EVALUATION OF MANAGEMENT SYSTEMS PERFORMANCE AT NAVY REGIONAL DATA AUTOMATION CENTERS(U) NAVAL POSTGRADUATE SCHOOL MONTEREY CA G J SCOTT MAR 84 2/2

UNCLASSIFIED F/G 5/1 NL



X. EXAMINING APPLICATION SYSTEM PROCEDURAL CONTROLS

A. INTRODUCTION

Application system program procedural controls have replaced many of the more conventional internal controls develcped for manual systems. To ensure that internal controls are valid and effective, a comprehensive approach is necessary. Not only must procedural requirements for all operatonal system applications be reviewed, but the application ccntrols for locally developed and operated applications must also be validated. The scope of the facility audit of application system controls should include a review of the majcr contrcl procedures of the CDA application systems and local applications in operation at the facility for which the facility has control responsibility. This includes comparison of application controls, documentaticn, interface with facility unique applications (and their controls), and review of CDA required processing procedures with activity operations. Software internal control reviews of specific applications are beyond the scope of this audit program.

B. TRANSACTION ORIGINATION

Effective transaction control requires that source data be captured as soon and as close to the point of origination as possible. Procedures must be established to contrcl and ensure the accuracy and completeness of each transaction from originator and subsequent transcription entry into transaction edit routines.

1. Review selected application systems and evaluate manual transaction origination procedures.

a. Ensure that control documentation describes how and under what circumstances transactions arise, who is responsible for recording, encoding, and initiating, and how it is processed.

b. Select a sample of transactions from various applications and trace back to the corresponding source documents, verify authorizing signatures. Ensure that actual processing procedures were as described in the control documentation.

c. For centrally designed systems, compare processing procedures and practices to CDA system specifications. Ensure that transaction origination practices are consistent with system requirements.

2. Review interactive terminal application system input control procedures.

a. Ensure that control procedures for terminal operations require review and certification of input transactions by other than the terminal operators.

b. Ensure that controls have been established requiring passwords and other processing controls.

C. TRANSACTION DATA ENTRY

Effective use of transaction data entry controls can verify prior to application processing that data transcribed is consistent with specified limits. Various methods can be employed to edit transactions such as batch and check totals, alpha and numeric field limits, etc.

3. Review selected application systems and determine what types of edit checks are used. Ensure that prescribed procedures are consistent with facility operating procedures.

4. Trace a selection of transactions through this stage of the application system to evaluate the effectiveness of the transaction data entry controls.

D. DATA COMMUNICATIONS

The integrity of data is dependent upon processing controls and systems operating procedures' ability to compensate for momentary or major commercial network

failures. In addition, communication controls are required to ensure that only authorized users have access to system application through the communications network.

5. Review operating and application system communications controls. Ensure that the documentation is consistent with facility operating procedures.

6. Review communications Preventive Maintenance and Failure Reports. Records of reported failures, emergency, and preventive maintenance actions should be examined to assess promptness, thoroughness, and general quality of maintenance support.

7. Review Recovery Logs or other files prepared for use in recovery/restart processes. Review lost or garbled data error message accountability.

8. If the system under audit possesses an integrated test facility (ITF), this should be used to validate error routines.

E. OUTPUT PROCESSING

Effective utilization of output products requires controlled, timely distribution to both originators for data confirmation and to users for action.

9. Ensure that procedures are adequate to support user requirements.

   a. Trace selected individual output products from printing to user receipt and usage.

   b. Verify facility procedures in processing and correcting erroneous output.

10. Review formal output procedures.

    a. Ensure that procedures provide sufficient control to prevent unauthorized access to outputs and that these procedures are followed by facility and user personnel.

    b. Ensure that allocation of responsibilities within and between the computer center and its user/customers provides for effective control and liaison.

XI. AUDITING LOCAL PROGRAMMING MAINTENANCE AND DEVELOPMENT

A. REQUIREMENTS APPROVAL

Facility local programming for support or new programs is contingent upon the amount of effort provided to centrally designed and maintained programs and program changes. Local program effort is usually very limited and as such, user requirements must be documented and reviewed to ensure that the maximum benefits can be obtained.

1. Review procedures for accepting user/customer requirements for new or modified programs.
   a. Determine that the user requirements have been carefully and thoroughly documented.
   b. Review estimating procedures for programming requirements. For systems requiring cost-benefit analyses, ensure that hardware requirements were determined and considered in the analyses.
   c. Review reporting procedures for proposed programming effort. Are users provided with guidance on existing output or other methods of satisfying their requirements?
2. Review acceptance procedures.
   a. Ensure that jobs accepted are formally approved within the computer center.
   b. Review procedures for establishing programming priorities and subsequent scheduling.
   c. Review programming workload: Ensure that contractor programming support has been considered if backlog situations are a continuing problem for valid requirements.

B. PROGRAMMING MANAGEMENT

Project management techniques can be used for program changes and development to provide a formalized means of measuring progress through the use of periodic status reports. (OPNAVINST 5231.1)

3. Verify that a suitable management structure exists for program development.

   a. Examine status reporting provisions. Determine the need and the availability of specialized reporting techniques such as PERT or reporting approaches such as Gantt charts. The auditor should be able to easily determine the status of all CDA and local development projects.

   b. Analyze reporting procedures for programming progress. How well do original programming estimates compare to project and budgets and actual expenditures?

   c. Examine the dissemination of status reports and other project information to interested parties both inside and outside the data processing group.

   d. In projects that are completed or nearing completion, ensure that feedback mechanisms will ensure that lessons learned are taken into account in future development projects.

4. Review programming methods for the following:

   a. Review user and operational documentation for compliance with standards. (SECNAVINST 5233.1A; DCDINST 4120.17M)

   b. Ensure that the conversion plan provides for program implementation without interruption of data processing services to the users.

   c. Determine if an adequate test plan is developed and followed to validate each new system. Review the adequacy of test results.

   d. Does the facility use a structured programming approach to program development?

5. Determine the degree of independence exercised by the group charged with acceptance testing of new application systems.

6. Evaluate the completeness and comprehensiveness of test planning and test specifications used by the acceptance testers.

7. Evaluate the thoroughness of the acceptance testing.

8. Review procedures to resolve discrepancies reported by acceptance testing.

9. Evaluate the degree to which users participate in the planning, conduct, and evaluation of acceptance testing.

C. CHANGE CONTROL

Formalized procedures for modifying operatonal application systems must require written approvals and supporting documentation. Controls in this area should focus on preventing unauthorized, erroneous, or accidental changes from being introduced into previously tested and accepted computer programs. (NAVCOMPINST 7000.36)

10. Ensure that procedures requiring formal, written requests for changes have been established.

11. Determine what mechanisms are used for review of proposed changes and how effectively these mechanisms are used. For example, is there a change control committee that is responsible for deciding priorities and allocation of resources to changes?

12. Determine if there are restrictions on the number and /or type of persons who can make changes.

13. Determine if independent means are used to report the existence of program changes. For example, some installations have automated the systems management facility of the computer operating system to prepare reports on all changes to libraries.

14. Examine the processes associated with "quick fixes" to ensure that these fixes are controlled adequately.

15. Determine if there are controls on the number of times changes can be made during a given time period or on the frequency of changes to any given program.

16. Ascertain whether any special programs are used to control access to libraries of source programs.

D. DOCUMENTATION AND INTERFACE

Documentation is the process of describing on paper the functions that each application system performs, how they are performed, how the functions are to be used and how the application interfaces with the total system. (SECNAVINST 5233.1A; NAVCOMPINST 7000.3C)

17. Ensure that documentation describes the flow of data within the application system.

18. Ensure that documentation describes how programs implement controls.

19. Ensure that documentation specifies how programs are to be operated, how they are to be backed up, and how recovery procedures are conducted.

20. Review documentation and ensure that it is being properly maintained and is updated.

21. Evaluate all user documentation and review for clarity and usability.

E. DATA BASE MANAGEMENT AND CONTROL

Data base management and administration have a significant impact on the efficiency, accuracy and effectiveness of an EDP facility, especially in the area of computer processing. Proper documentation of operating procedures, applications programs and procedures, and accurate cataloguing and maintenance of changes to data base files, discs, tapes, data dictionary, etc. are critical in ensuring control over the data base and the processing accuracy of the facility's applications. There are several major areas of control and associated safeguards that must be reviewed during the facility audit. These include: (1) data base control, access and physical security; (2) data base maintenance and data base library controls; (3) user and technical staff training; (4) data base/facility operations interfaces; (5) systems development and testing; and (6) systems, programming and procedures documentation.

These functions are appropriately the responsibility of the Data Base Manager (DBM). All data base systems need at least one position of authority to enforce data base policy and procedures. Related elements of these areas will have been review during other sections of the facility audit. The administration of the data base has a major impact on the overall operations of the facility, any potential overlaps are worth reviewing to thoroughly evaluate the interfaces between data base and other facility activities.

22. Data Base Control, Access and Physical Security:

a. Review the organization structure to determine if the DBM function is effectively segregated from the rest of the organization, especially the system development, user and operations functions. The DBM function requires independence to be effective in data base control.

b. Review the facility's operation's access controls to ensure that the DBM does not have direct access to the computer operations center. The DBM should not be allowed to operate the facility's computer equipment.

c. Select a major customer for review of its input controls. Review its written procedures for input controls to ensure they maintain data base security by keeping unauthorized users out of the data base and also control authorized users access to and use of the data ase. Types of controls over users include separation of duties for document preparation and data entry, written authorization for data entry, passwords for system entry, system logs to document system usage, etc. These controls should also require that the DBM must receive user department approval prior to entering transactions into the system.

d. Review the DBM's control over inputs to the data base. The DBM has responsibility for all inputs, and should be reviewing the data entered for quality, organization (to ensure that it complies with existing data base formats), integrity and level of security required.

e. Review the system of checks and balances over changes to the data base. While the DBM is responsible for reviewing, approving and auditing changes to the data base, facility procedures should call for another authorized signature (director of data processing, facility system development committee, etc.) prior to the DBM making changes to the data base.

f. Review the data base file controls to ensure they restrict access to and provide complete security for classified material in accordance with OPNAVINST 5510.1F, Department of the Navy Information Security Program Regulation. Relate these controls to the security descriptions in the data base dictionary, select (if you have the appropriate security clearance) a random sample of classified data elements, and review access to and control over these elements.

g. Review the physical security of the data base, including location in the facility, access controls and logs, etc. The DBM is responsible for the physical security of the data base, and should have written procedures on file governing security of the data base. The DBM must be consulted by the facility security manager before any changes are made to the facility that affect access to and security of the data base as the DBM is responsible for the overall security of the data base.

i. Review the DBM's written procedures for recovery and verification of the data base in the event of partial or complete destruction, security violation, or other compromise of the data base.

Interview the facility security manager and DBM to evaluate their responses to such data base compromise or destruction possibilities as theft, classified material violations, unauthorized changes to data base programs or the data base dictionary, modifications to data base application's programs, unauthorized use of system or vendor utility programs to access the data base, etc. Classified material violations should be investigated. (OPNAVINST 5510.1F)

j. Review the facility risk assessment (OPNAVINST 5239.1).

Determine if the security measures and controls selected and instituted by the facility are appropriate and adequate to ensure control over the data base. Review the specific controls, including use of passwords, locatewords, photographic ID cards for access to the data base storage area, restriction of access to computer operations personnel only, maintenance of a directory of access privileges and related security clearances and security profiles for all personnel authorized access to the data base, authorization tables for access to specific programs, file records, control documentation, etc.

k. Review systems analyst, programmer and operators' access to the data base and determine if appropriate controls exist to ensure data base security and integrity. Specific items to be reviewed include:

(1) computer console logs and data base access logs

(2) DBM control over access to the data base library

(3) other physical access controls over database related software

(4) the software controls over the access to the database via utility programs, online networks, etc.

(5) input/output (I/O) device control and access

(6) programming and user documentation governing access to the data base

(7) DBM control over all vendor-supplied utility programs

(8) controls over other programs relating to the data base to ensure only authorized personnel can use the programs

(9) procedures for systems analyst/programmer changes to data base programs

(10) control over access to the master terminal

for for entry of changes to system utility commands and other database-related access changes

(11) access controls in force when purging, reorganizing or compressing a data base

23. Data Base Maintenance and Data Base Library Controls

a. Review the facility's job descriptions to ensure that the DBM has complete responsibility for data base maintenance and the data base library.

b. Review the DBM's control over the contents of, changes to, and distribution of the data dictionary, the procedures for reviewing and updating the data dictionary, and the quality of the definitions in the data dictionary. The data dictionary should include data definitions as well as information on the audit and/or management trails in the system. The data dictionary is actually the audit trail for the data base in that it identifies the nature and organization of data in the data base, the program/data relationships for the facility's applications, and is a tool for validation, edit and control of the data in the data base. The DBM should be restricting access to the data dictionary by providing safe storage and tight physical control over the available copies.

c. Review the log of changes made to materials held in the data base library. The changes should be subjected to a quality control review by the DBM as well as by another independent authority, such as the director of data processing, system development committee, etc., and should have received signature authorization prior to entry into the data base. Determine if a software program exists to periodically scan the data base and identify if any unauthorized changes have been made.

d. Review the DBM's data base log to determine if it accurately records such information as:

(1) data additions, deletions and changes

(2) the user, programmer or system analyst originating the additions, changes and deletions

(3) the reasons for the update, revisions, reorganizations or compressions of the data base

(4) the utilization of the data base by specific users as well as by application, including utility programs

(5) classified material or other data base security violations

24. User and Technical Staff Training

a. Review the facility's training records or individual personnel files to ensure that both user and technical staff personnel have training in:

(1) proper use of the data base

(2) data base security, including instruction in the handling of classified material as required by OPNAVINST 5510.1F

b. Review the training schedule and lesson plans employed by the facility security officer and DBM to determine the frequency and quality of the instruction provided to facility personnel in data base management and classified material control.

25. Data Base/Facility Operation's Interfaces

a. Review the controls over the operating environment of the data base such as operations scheduling, monitoring, data base recovery, user access, etc. The DBM should be responsible for controlling the data base operating environment, authorizing any changes to operations impacting data base usage, and coordinating with users and application programmers regarding usage, storage, extraction and retrieval of data in the data base.

b. Review the preparation of the facilty's operating logs as well as usage reports generated from the logs. The DBM should be generating data base usage statistics, data base modification reports, data utility program usage data, etc. for review by the director of data processing and other EDP management personnel.

c. Review the facility's JCL for batch-oriented applications of special interest to the audit team to establish the level of control over data base access provided by the JCL. The EDP auditor should insure that individual jobs can only access specifically identified files or sets of files in a data base. This control also applies to online systems in that specific applications and individual transactions processed via these applications should access only specific segments of the data base. Test sample transactions to determine the integrity of the jcl/online system data base access controls by attempting to access unrelated files or segments of the data base.

26. Systems Development and Testing

a. Review the facility's written procedures governing systems development and testing of new applications to determine if the DBM participates in the system development and testing process. The DBM should review and approve all modifications to software which affects the data base. This is especially critical in the areas of financial applications and classified material control, and relates to both inhouse and vendor-prepared modifications.

b. Review the system development and testing procedures to determine if the facility's internal review staff participates in the process or reviews new applications prior to their approval for use in the facility. The internal review staff should participate in the data base

and application system development and change process to ensure that adequate controls are being built into the data base and new applications software.

c. Review the facility's unit and system testing standards. These standards should be formalized into written procedures, and compliance with these procedures should be documented and retained for all new system development activities. The standards should set criteria for preparing test data base, accompanying manual ledgers with anticipated results to check the accuracy of program algorithms, and documentation modifications to applications being tested to provide an audit trail for system development audits.

d. Review the approaches to development of and access to test data base. While all test data bases and program test documentation should be maintained in the data dictionary, the DBM should be restricting access to the test data base and documentation, and should ensure that applications development staff controls the sample test data used to evaluate new applications during the system testing process. The DBM should also be testing all modifications to software affecting the data base prior to acceptance and usage by customers.

e. Review the testing program at a detailed level. Specific areas to be thoroughly evaluated and steps to be followed include:

(1) Review the testing procedures to ensure that data base backup and recovery procedures for new applications are tested prior to testing the entire application to guard against loss of the test data base.

(2) Ensure that only test data bases are used for applications testing. The facility should never allow live data bases to be used for testing purposes. Various types of test data bases include unit test data bases used by applicationdevelopment staff to debug programs, and benchmark test data bases used to test program revisions when previous testing indicates that modifications are required.

(3) Ensure that data base users have participated in testing of all applications affecting the data bases relating to their applications. User confidence in both the data base and applications software is critical to effective control and use of new applicatcns, and user participation in the testing process in invaluable in establishing user confidence. User feedback to applications development staff is also valuable in development of program modifications.

27. Systems, Programming and Procedures Documentation

a. Review the job description of the DBM to ensure the DBM is responsible for all systems, programming and procedures documentation relating to the data base.

b. Review the written documentation standards to ensure they establish specific criteria for evaluation of all documentation affecting the data base. All documentation relating to the data base should be thoroughly reviewed and approved by the DBM prior to program implementation.

c. Review the operating instructions and procedures manuals for all applications programs accessing the data base to ensure that backup and recovery procedures are thoroughly documented.

d. Review the systems, programming and procedures documentation to ensure that database-related documentation is cross-referenced in the documentation and consistent in its approach to data base access, control and usage.

XII. SUMMARY AND CONCLUSION

Operational auditing is not a new concept or practice. Operational audits have been conducted for many years by internal auditors in industry as well as government.

Various names have been given to audits which involve more than the traditional financial audit. Some of the more popular ones are **comprehensive auditing, effectiveness auditing, systems auditing, and operational auditing.** This paper has dealt only with operational auditing. As used here, an operational audit is an examination of policies, practices, procedures, and controls used to find out what areas may be improved. Operational auditing extends well beyond financial audits, which are concerned with the receipt, control and disbursements of funds. It includes an evaluation of the utilization and control of nonfinancial resources such as property, equipment, personnel, and supplies. Thus, there is a substantial amount of literature available for those who wish to study it in greater depth.

A NARDAC is a high technology and fast changing organization. It covers the development, maintenance and operation of all information services technologies including the acceptance testing of software developed externally. It needs inplace, ongoing evaluation. The commanding officer of a NARDAC can gain valuable assistance from a constructive operational audit. In general, managers of NARDACs can not conduct such in-depth reviews of their own operations though an internal operational audit group is possible. Several issues are important in the evaluation of performance at a NARDAC: Who sets the standards? Who plays what role in planning for the future? and Who makes basic policy affecting both the NARDACs and the customers of NARDACs?

Because the NARDACs have Navy wide responsibility for non-tactical ADP, some of the issues must be resolved by senior Navy management--they can not be delegated to lower levels.

The NARDAC is an organization whose scope of technologies to be coordinated has expanded tremendously as computers, telecommunications and office automation have merged together, and whose product offerings are extending into new customer areas. The complexity of implementing projects, the magnitude of work to be done, and the limited human resources have forced the NARDAC away from being primarily a production oriented organization to one where a significant percentage of its work is concerned with coordinating the acquisition of outside services for use by its customers.

Measuring performance at a NARDAC by operational auditing provides a consistent methodology and basically uniform technique that can be used to adequately assess performance in the seven NARDACs. The auditor, however, must tailor the audit engagement by selecting those steps that are appropriate to the particular NARDAC, the interests of the audit client, and the relationship between data availability and audit resources. This selection is the key to the success of the audit effort. An overriding consideration in making the selection is the evidence standard, promulgated by the U. S. General Accounting Office, which states: [Ref. 51]

> Sufficient, competent, and relevant evidence is to be obtained to afford a reasonable basis for the auditors' judgements and conclusions regarding the organization, program, activity or function under audit. A written record of the auditors' work shall be retained in the form of working papers.

It is the rare case where the operational auditor can isolate the ideal single measure or standard to evaluate

performance. Yet, operational auditing can provide needed data for improvement.

The focus on productivity improvement as the measure of a NARDAC's value requires an instrument for measuring productivity. Usually, productivity relates to people-based activities, and an operational audit is an ideal tool for seeing that management has at hand the necessary information for decisionmaking. Operational auditing involves not only ascertaining how objectives are being met, but also evaluating the way the objectives were set in the first place. Although performance criteria may be applied objectively, it must be recognized that subjectivity enters into the selection of these criteria.

A NARDAC is required to recover all of its costs. The policies, as a Nif activity, are geared toward cost liquidation. The establishment of appropriate prices is a complex issue. An appropriate resolution is critical to establishing and maintaining a realistic relationship between NARDACs and their customers. NARDACs must continually search for ways to deliver new products in more efficient ways.

The previous chapters presented a series of frameworks for examining the NARDACs and their function of information services management. In sum the paper specifies the details as to how an information services operational audit should be conducted. The NARDAC was treated as a stand-alone business within the Navy. This permitted the development of the concepts of control for information services. Issues of internal accounting control within the NARDAC was not covered as they do not have a direct impact on the interface between the NARDAC and its customers.

The following overview of operational auditing is a brief summary of the various phases and steps involved in conducting an operational audit: [Ref. 52]

At the beginning the auditor has no idea where to go or what to do. The first step involves determining the total (universe).

> Obtains general knowledge of total responsibilities. Leads to total areas that can be audited.

The auditor finds there are many areas from which to choose. An area is selected.

> Background and general information on areas leads auditor to select a specific area to be audited.

The auditor selects an area from the universe of areas; then does a preliminary survey.

> Background and general information from area leads auditor to tentative audit objective by some evidence and assertions. Possible alternative tentative objectives considered.

The objective of a specific activity is determined--very tentative. Also tentative alternatives are determined. A review and test of management control is made.

> Tests of management control give auditor evidence to support firm objective.

A possible tentative report could be prepared at this time. Also a program for the detailed examination is prepared if audit is to continue.

The auditor selects firm audit objectives; gathers sufficient, relevant, material, and competent evidence on audit objective to come to a conclusion on that objective. The detailed examination is done.

> Obtains sufficient, relevant, material, and competent evidence to support the conclusion on the audit objective, including any evidence obtained in prior phases.

A summary of evidence in working papers is made, sufficient to support conclusions on the objectives.

Summarizes all evidence in working papers on the objective in order have a workable amount for the report, and to support the auditors' conclusions.

From summarized evidence, the auditor prepares the report, including conclusions and recommendations. The report is the final product of the audit.

Uses summarized evidence to support conclusion and recommendations.

APPENDIX A

DEFINITIONS OF SPECIAL TERMS

ACCEPTANCE TESTING: a process in which persons not responsible for program implementation are charged with checking the application system before it becomes operational. This approach is intended to foster objectivity in evaluation of the performance of the program and to test, in parallel, both the application system itself and its documentation.

ACCESS METHOD: a procedure by which a program obtains data from a mass storage file. The common access method for tape files is sequention. There are several access methods for disk files that vary from sequential to truly random access.

AUDITABILITY: features and characteristics of an information system, either computer-based or manual, that allow verification of the adequacy and effectiveness of controls and verification of the accuracy and completeness of data processing results.

AUDIT SOFTWARE: a set of programs which assist auditors in performing tests on computer data files. The end product is usually a report analyzing the data in a format designed by the auditor to accomplish the desired audit objective.

AUDIT TRAIL: files, indexes, reports and references that allow specific transactions to be traced back to their source or forward to their final recording in the accounts. It also is referred to as a management trail since it allows management to determine propriety of processing and to follow up on errors.

BATCH CONTROLS: a control procedure used to assure the conversion or processing of groups of data completely and accurately. For example, when a card file is processed, the last card may have totals (sometimes referred to as hash or control totals) of account numbers and amounts. As the computer processes this file, it adds up the account numbers and amounts and compares their sums to the numbers on the last card. If they do not agree, an error message is printed and processing suspended until the error is found and corrected.

BATCH PROCESSING SYSTEM: a system for collecting and processing data in groups (batches). Many applications in business are of this type.

CPU: Centeral Processing Unit. This is the principal part of a computer system. It is the CPU which contains the operating system (the "brain" of the computer) and performs the processing. The CPU contains the circuitry for the arithmetic and logic functions included in the computer design. A variable amount of "main memory" is also associated with the CPU. Only data and programs contained in "main memory" can be processed by the logic and arithmetic functions of the computer.

COMPUTER APPLICATION SYSTEM: a computer-based information system that includes both manual and computerized procedures for source transaction origination, data processing and record keeping, and report preparation.

DATA BASE: a collection of data which is organized in such a way that allows a data item to be available to different users within an organization. Rather than having separate files for each application, all files for all applications are merged into one "total" file or data base. It is frequently associated with data base management systems which rely on such a file structure.

DATA TRANSMISSION (DATA COMMUNICATION): the sending of data from one location to another location. Typically, information is sent over telephone wires from outlying terminals to the central processor. Typical controls which assure the completeness and accuracy of such transmission are character counts, message counts and dual transmissions. Data security is an important internal control consideration in systems which use data transmission since data and programs are more susceptible to accuss by unauthorized persons.

DISK PACK: a device for storing computer created data files. Although their capacities vary significantly, a typical disk pack can store millions of characters. Some disk packs are portable. This allows more than one disk pack to be placed on a disk drive, the device the computer uses to read and write from a disk pack. Because of the portability of some disk packs, good internal control requires that they be properly safeguarded.

DISTRIBUTED PROCESSING: a decentralized approach to information processing. A distributed system is an aggregation of information systems (intelligent terminals or minicomputers) arranged as relatively independent subsystems that are tied together through a central computer via communication networks.

DOCUMENTATION: a means for understanding the purpose of a program and communicating the program details to a reader.

DOCUMENTATION STANDARDS: a established acceptable level of documentation. All program and system documentation should be measured against this standard, and procedures should be established for bringing inadequate documentation to an acceptable level.

EDIT: a control technique which determines if data is inaccurate, incomplete, unreasonable or fails to meet established criteria. This procedure can be be done manually before processing or by the computer at the beginning or at subsequent stages in regular processing. This may be the sole purpose of certain programs (commonly called edit programs) within an application. Common edits are: edits for reasonableness or limit tests, such as determining if hours reported for a weekly wage earner are in excess of 60 hours; missing data tests, such as no employee or part number; and illegal character tests, such as an alpha character (letter) in a numeric field.

ERROR CORRECTION PROCEDURES: the method by which errors detected by input, program and processing, and output controls of the computer system are corrected and resubmitted for processing. Unless the corrections or errors are subjected to the same controls as new input data, an otherwise strong system of internal accounting control could be ineffective. In general, computer operators and control clerks should never correct errors committed by a user.

FILE: a complete set of related logical records.

FILE CONTROL: a system of protection and back-up provisions which help assure that data files will not be harmed or manipulated intentionally or accidentally. Examples of file controls are the son-father-grandfather system of back-up, retention dates on header labels, fireproof storage vaults, off-premise storage, temperature and humidity controls, restricted access and file protection rings.

FLOWCHART: a diagram which shows the logic of a program (the way in which a record is processed) or shows the sequence in which programs are processed and files are used or created. Flowcharts of the first type are called program flowcharts, logic diagrams or logic charts; the latter type are called system flowcharts.

GRANDFATHER-FATHER-SON. a system for backing up magnetic media files where previous master files and transaction files are kept to reconstruct the current master file if necessary. The current master file (the son) is a product of processing the last transaction file with the next to last master file (the father) which itself is the product of the next to last transaction file and the second oldest master file (the grandfather).

INTERNAL CONTROL: (administrative control and accounting control) administrative control includes, but is not limited to, the plan of organization and the procedures and records that are concerned with the decision processes leading to management's authorization of transactions. Such authorization is a management function directly associated with the responsibility for achieving the objectives of the organization and is the starting point for establishing accounting control of transactions.

INPUT CONTROLS controls designed to insure that data going into the EDP system is authorized, accurate, and complete. This is where most errors are generally made, and therefore, the controls should be designed to be effective as possible.

MASS STORAGE FILES: storage devices, usually on tapes or disks, which permit the storage of very large volumes of data.

MASTER FILE: an organized data file which provides the primary basis of current information for accounts or other types of files, such as name and address files. Master files are updated periodically by other data files (called transaction files) which include all changes to the file since the last updating run. The combination of old master files and transaction files provide the back-up for the current master file.

OPERATING LOGS: written records of all functions performed by the computer system, including the jobs processed, the start time, the stop time, the condition of the termination of the job (normal or abnormal) and operator actions taken. Operating logs can be completed by the operator, by the computer through the console typewriter or by both.

OPERATING SYSTEM: a group of programs that control all resources attached to the CPU, manage application programs in process and provide other supporting functions.

OPERATOR: the person with the responsibility of running jobs on the computer, who generally processes the jobs according to a prearranged schedule and handles all of the equipment including putting card program decks into the card reader and mounting tapes and disks on drives.

OPERATOR INSTRUCTIONS: written procedures that operators follow to run a job. These instructions cover mounting and dismounting tapes, changing paper, setting dials and switches, and responding through the console typewriter. In general, these instructions include all items necessary for setting up, processing and completing a job.

PREVENTIVE MAINTENANCE: the process of keeping computer equipment in acceptable working condition as opposed to correcting after malfunctions occur. Owners or lessors of computer equipment generally enter into equipment servicing contracts with the manufacturer. In addition to providing for service when equipment breaks down, these contracts call for cleaning and testing equipment on a periodic basis, usually weekly.

PROGRAM CODING SHEETS: worksheets used for writing programs. These forms are designed for ease in keypunching and for adherence to conventions established for programming language.

PROGRAM LISTING: a sequential listing of all the statements of a computer program. In general, program listings should not be available to computer operators since this would violate the principle of segregation of duties.

PROGRAM REVISIONS: changes to a computer program. Good internal control calls for adhering to established documentation standards whenever a program is changed. A record of the review and approval of these revisions should be kept.

PROGRAM TESTING PROCEDURES: the established method for testing new programs or changes to existing programs. Test data, sometimes called test decks, should be designed to thoroughly test all logic paths within the program. Valid as well as invalid data should be used to test the program. Once the test data is created, it should be retained to document this testing of the program and to be available for testing program revisions.

RESTART: the capability to continue processing a file after the program stops at an interim point for some reason. Many programs can take a relatively long time to process a file, primarily because of the volume of data on the file itself. On occasion processing will be halted abnormally. If it were necessary to begin all programs at the beginning each time, hours of processing could be lost. Restart capabilities therefore can be important from an efficiency point of view.

RETENTION DATE: a date placed upon the label of a tape or disk which tells the computer, operator or librarian how long the file is to be kept. If the retention date has not passed, the file should not be updated or discarded (scratched).

RUN: a description of the processing of a job by the computer
the printed output related to the processing of a job.

RUN BOOKS: a potentially ambiguous term. In some installations they refer to operators' manuals which are used to process jobs. In other installations they refer to manuals which contain all documentation for a application. The difference is important, since if operators have access to run books and they contain all information on an application, good principles of internal controls are violated.

SCRATCH: a description of a tape or disk which is ready to accept new data; the process of making a take or disk ready to accept new data.

SEQUENCE CHECKING: an editing procedure that compares the control number in a sequential file with the previous control number. It it is not greater than or equal to the previous number, the program notes that a sequence error has occurred.

SERVICE CENTER: an organization which provides data processing and other closely related services to other organizations.

SOFTWARE: a computer programs.

SOURCE DOCUMENTS: the beginning point for data entering the computer system. These documents originate in user departments and may be in the form of time cards, purchase requisitions, etc. After the data are entered into the computer system, these documents should be stored or returned to the customer.

STRUCTURED PROGRAMMING: the group of techniques that provide specific guidelines to programmers on how they may use programming languages and how elements of programs fit together to form an application system. These techniques were initially developed with the intent of providing more controllable and usable programs. They also offer, as a fringe benefit, improved auditability of programs produced under these techniques. The techniques falling under this heading are as follows:

Chief Programmer Team Organization. This technique is based on the establishment of a small, integrated team headed by a chief programmer and supported by two or three analysts and programmers and a librarian. Use of this approach has proved effective in many instances.

Top-down Design. This technique consists of designing program logic by specifying the highest level functions first and then proceeding downward to greater and greater detail. Use of this approach tends to organize programs more simply and effectively.

Modularization. This technique focuses on careful segmentation of programs into common and generally useful modules to ensure simplicity and minimum redundancy.

Structured Coding. This approach uses a collection of conventions for syntax and program format to ensure that the programs are more easily understood are less likely to contain errors.

Walk-through. A planned review of system specifications and coding by peers of the developers. This approach has been effective in minimizing built-in errors.

Top-down Testing. Skeleton control modules are tested first and then progresses down the module structure to finally test the entire system.

(The auditor should focus on determining the presence or absence of the above or related techniques and the effectiveness of their use. Evidence of the use of these techniques can be considered a positive sign even though the auditor may be unable to fully appreciate and understand the mechanics of the techniques.)

SYSTEM ANALYSIS: process of studying systems to determine if changes should be made and if so, how they should be carried out.

SYSTEM DEVELOPMENT: designing, testing and implementing new systems.

TIME SHARING: a method of data processing which provides extensive data processing capability on a basis that would not be practical or economically feasible if maintained individually by each user. Generally a wide range of computerized applications are offered simultaneously for many users. These users in effect "share" the CPU.

TRANSACTION FILE: record of all changes to a master file since the last master file updating run.

UTILITY PROGRAMS: programs provided by manufacturers to assist an installation in the functioning of its data processing. Examples of such programs are sorts, merges, and DITTO (a program which, among other things, allows for dumping or copying a file).

LIST OF REFERENCES

1. O'Brien, J. A., Computers in Business Management: An Introduction, Third Edition, Richard D. Irwin, Inc., Homewood, Illinois, 1982, p. 551.

2. Ibid.

3. Parish, R. J., The Navy Industrial Fund And Its Applicability to the Naval Data Automation Command, M.S. Thesis, Naval Postgraduate School, Monterey, California, 1980, p. 63.

4. Ibid., pp. 76-81.

5. Ibid.

6. Ibid., pp. 78-79.

7. Office of the Navy Comptroller, Introduction to the Navy Industrial Fund, U. S. Government Printing Office, 1982, p. 13.

8. Ibid.

9. Ibid.

10. "Navy Industrial Fund, Module H," Practical Comptrollership Course, Text, Naval Postgraduate School, Monterey, California, p. H-6, Revised 1983.

11. Office of the Navy Comptroller, Introduction to the Navy Industrial Fund, U. S. Government Printing Office, 1982, p. 14.

12. Mellon, S. F., Knowing NIF, Text, Naval School, Civil Engineer Corps Officers, Port Hueneme, California, 1970, p. v.

13. "Navy Industrial Fund, Module H," Practical Comptrollership Course, Text, Naval Postgraduate School, Monterey, California, p. H-18, Revised 1983.

14. "Budget Execution, Module D," Practical Comptrollership Course, Text, Naval Postgraduate School, Monterey, California, p. D-31, 1982.

15. "The Navy Stock Fund, Module G," Practical Comptrollership Course, Text, Naval Postgraduate School, Monterey, California, p. G-3, 1982.

16. Office of the Navy Comptroller, Financial Management of Resources, U. S. Department of the Navy, NAVSO, P-3006-1.

17. Cash, J. I., Jr., F. W. McFarlan, J. L. McKenney, Corporate Information Systems Management: Text and Cases, Richard D. Irwin, Inc., Homewood, Illinois, 1983, p. 254.

18. Ibid., pp. 254-255.

19. Ibid., p. 260.

20. Ibid., p. 261.

21. Ibid., pp. 262-265.

22. Ibid.

23. U. S. General Accounting Office, Standards for Audit of Governmental Organizations, Programs, Activities and Functions, U. S. Government Printing Office, Revised 1981.

24. Morin, D. B. J., "The Operatonal Audit," International Journal of Government Auditing, January 1974, pp. 2-3.

25. Ibid.

26. Lamperti, F. A., J. B. Thurston, Internal Auditing for Management, Prentice-Hall, Inc., Englewood Cliffs, N. J., 1953.

27. Ibid.

28. Miller, F. J., Jr., "Operational Auditing--Where Do We Go From Here?," The Internal Auditor, pp. 16-21, December 1978.

29. Scantlebury, D. L., "Planning an Operational Audit," The Government Accountants Journal, pp. 18-21, Fall 1976.

30. Ibid.

31. Ibid.

32. Ibid.

33. Ibid.

34. Mitchell, J. R., "The MAS Proposal Letter," The Journal of Acccuntancy, June 1975, pp. 38-45.

35. Lindberg, R. A., T. Cchn, Operatons Auditing, American Management Asscciation, Inc., New York, 1972, pp. 34-35.

36. American Institute of Certified Public Acccuntants, Management Advisory Services, Guideline Series Number 6, "Guidelines for CPA Participation in Government Audit Engagements to Evaluate Economy, Efficiency, and Program Results," New York, 1977, p. 19.

37. Herbert, L., Auditing the Performance of Management, Lifetime Learning Publications, Belmont, California, 1979, pp. 35-36.

38. Standford Research Institute, Systems Suditability and Contrcl Study, Data Processing Audit Practices Report, Institute of Internal Auditors, Inc., Altamonte Springs, Florida, 1977, pp. 36-37.

39. Ibid.

40. U. S. General Accounting Office, Standards fcr Audit of Governmental Organizations, Programs, Activities, and Functions, U. S. Government Printing Office, Revised 1981, pp. 49-50.

41. Herbert, L., Auditing the Performance of Management, Lifetime Learning Publications, Belmont, California, 1979, pp. 38-39.

42. U. S. General Accounting Office, Standards for Internal Contrcls in the Federal Government, U. S. Government Printing Office, 1983, pp. 1-11.

43. Ibid.

44. Ibid.

45. Ibid.

46. Stanford Research Institute, Systems Auditability and Contrcl Study, Data Processing Audit Practices Report, Institute of Internal Auditors, Inc., Altamonte Springs, Florida, 1977, pp. 22-23.

47. Davidison, J., "Coping with the Employee Turned Institution," Management, Winter 1981, pp. 14-16.

48. Forrester, J., Industrial Dynamics, Cambridge, Mass., The M. I. T. Press, 1961, p. 1.

49. Stanford Research Institute, Systems Auditability and Control Study, Data Processing Audit Practices Report, Institute of Internal Auditors, Inc., Altamonte Springs, Florida, 1977, p. 179.

50. Office of the Auditor General of the Navy, "Audit Program No. 19A--EDP Facility Audits, (Basic, June 1979)," Naval Audit Service Headquarters, Falls Chuch, VA.

51. U. S. General Accounting Office, Standards for Audit of Governmental Organizations, Programs, Activities and Functions, U. S. Government Printing Office, Revised 1981.

52. Herbert, L., Auditing the Performance of Management, Lifetime Learning Publications, Belmont, California, 1979, pp. 2-3.

BIBLIOGRAPHY

Canadian Institute of Chartered Accountants, Computer Control Guidelines, CICA, Toronto 5, Canada, 1970.

Davis, Gordon B., Auditing and EDP, American Institute of Certified Public Accountants, Inc., New York, 1968.

Fitzgerald, Jerry, Internal Controls for Computerized Systems, E. M. Underwood, San Leandro, California, 1978.

Hodges, S. E., "A 'Listening' Approach To Operational Auditing," The Internal Auditor, December 1978, pp. 53-55.

Knighton, L. T., "A Practical Audit Approach," The Internal Auditor, June 1977, pp. 40-47.

Peat, Marwick, Mitchell and Company, Audit Manual, Section 6000, Audits of Electronic Data Processing Systems, Peat, Marwick, Mitchell and Company, New York, 1976.

Pomeranz, F., A. J. Cancellieri, J. B. Stevens, J. L. Savage, Auditing in the Public Sector, Warren, Gorham & Lamont, New York, 1976. Santocki, J., "Meaning and Scope Of Management Audit," Accounting and Business Research, Winter 1976, pp. 64-69.

Staats, E. B., "Government Auditing--Yesterday, Today, and Tomorrow," The Government Accountants Journal, Fall 1976, pp. 2-7.

INITIAL DISTRIBUTION LIST

		No. Copies
1.	Defense Technical Information Center Cameron Station Alexandria, Virginia 22314	2
2.	Library, Code 0142 Naval Postgraduate School Monterey, California 93943	2
3.	Professor Carl R. Jones, Code 54Js Department of Administrative Science Naval Postgraduate School Monterey, California 93943	1
4.	Professor Joseph G. San Miguel, Code 54Zp Department of Administrative Science Naval Postgraduate School Monterey, California 93943	1
5.	Lieutenant Commander Gloria C. Scott, USN Atlantic Command Operations Support Facility Norfolk, Virginia 23511	1
6.	Officer in Charge Naval Data Automation Facility U. S. Naval Air Station Lemoore, California 93245	1
7.	Computer Technology Curricular Office Naval Postgraduate School Code 37 Monterey, California 93943	1

END

FILMED

10-84

DTIC