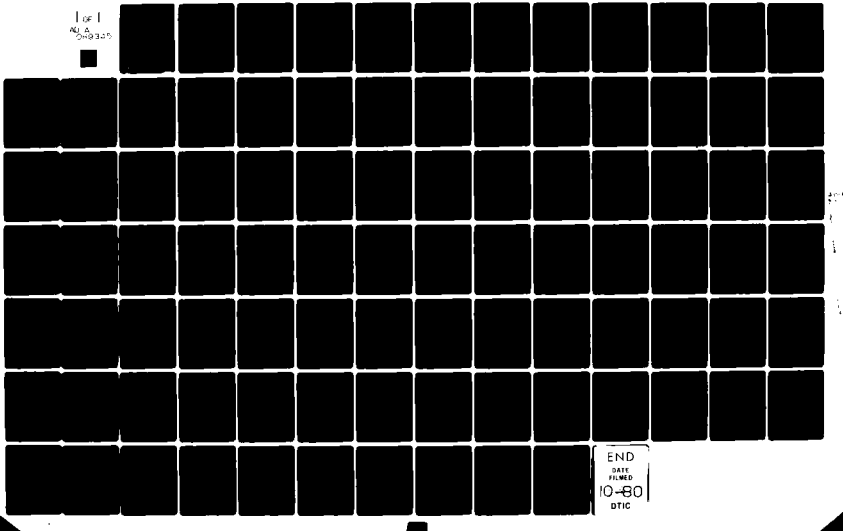
AD-A089 345 SYSTEM DEVELOPMENT CORP MCLEAN VA F/G 15/5
AUDITING STUDY REPORT.(U)
AUG 80 B KING N000173-78-C-0455
UNCLASSIFIED SDC-TM-WD-7999/400/01 NL



LEVEL II

TM-WD-7999/400/01
FINAL

AUDITING STUDY REPORT

AUGUST 29, 1980

TM-WD-7999/400/01
FINAL

AUDITING STUDY REPORT

BROADUS KING

AUGUST 29, 1980

EXECUTIVE SUMMARY

The purpose of this study was to review the state-of-the-art of auditing and control techniques applied to computerized information systems, particularly large-scale logistics information systems, and to present the findings as a basis for planning and organizing a research and development effort covering real-time software auditing and conventional process auditing of logistics information systems.

The basic problem motivating this study is undue depletion of government assets caused by gross inefficiencies resulting from erroneous computerized recordkeeping, by assets being misappropriated through possible misuse of the computer, or by some combination of the two. The erroneous processing results may be caused by a combination of varied deficiencies, including incorrect input processing and latent computer program faults. The objective of the auditing techniques under discussion in this report is to determine, on an ongoing basis, whether system controls are operating effectively to detect, deter, prevent or correct erroneous processing results -- whether from hardware failure, software deficiencies, inadvertent error, or intentional misuse.

The approach followed in conducting the study was to explore the problem from an overall viewpoint before concentrating on computer control and auditing techniques. This was deemed necessary to provide an adequate perspective for evaluating the worth to a comprehensive control program of any techniques considered for a research and development effort. The approach is consistent with that used in all the literature reviewed, including Office of Management and Budget (OMB) Circular A-71.

FINDINGS

Major findings of the study included the following points:

- Inadvertent errors, program deficiencies, and fraud are all areas of concern and when considered together, as they should be, constitute one of the major, if not the major, problems in information processing today. Although the greatest sources of computer losses are the result of innocent errors and omissions, the same basic controls are applied to protect against program deficiencies and fraud.

- The auditing and computer security communities were unanimous in their contention that the most effective approach to solving computer control and audit problems requires use of systems engineering methodology. All aspects of the problem must be considered as an entity and an integrated control program developed. Major elements of such a program are:

  - Management participation.
  - Risk analysis.
  - System of controls.
  - Adequate audit program.

- Several techniques for risk analysis and evaluation of controls have been developed. All have varying strengths and weaknesses in various environments. Enhancements could be made to tailor a combination approach to the logistics problem.

- Knowledge of the nature and extent of problems likely to occur at an installation or with a system is required to perform an adequate

risk analysis and select the most cost-effective set of controls for a system. The nature and particularly the extent of the problems in the Navy Supply environment have not been clearly defined.

- Advanced on-line systems may require changes to permit enhancement in the conventional control areas of input batch control, access control, file balancing controls, editing and validating controls, input to output controls, and document controls.

- Generalized audit procedures for gathering evidence are the same regardless of the type of system. However, the environment influences techniques that can be used to carry out a procedure. The increased capability of equipment has made real-time software auditing more of a practical possibility. Several real-time software auditing techniques show promise, but all require additional work to overcome existing drawbacks.

CONCLUSIONS

Computer control and audit is the essence of management control in any modern organization of any size. The consequences of lack of control in daily operations can be more devastating than some catastrophe such as a fire. Security, in the sense of protection from hazards and perpetrators of fraud, sabotage, etc., is a part of the overall problem, but far from the only problem or even the most significant part of the problem. Not only is the reliability of the records maintained and the outputs produced vitally important to the organization but the degree of operational effort (i.e. cost) required to achieve acceptable quality is of major importance. Therefore, the control and audit problem should rank near the top of management concerns.

The problem of computer control and audit is almost certainly serious enough to warrant a research and development effort to find generalized aids to assist in its solution. However, the exact nature and extent of the Navy Supply problem needs to be probed further to determine which aspect of the problem offers the most potential for gain. If the assumption is valid that the quality of inventory records adds or detracts from the quality of service provided to the Fleet and can actually affect Fleet readiness, then support emanating from the highest echelons of commands should be forthcoming.

Several components of an overall computer control and audit program would benefit from a research and development effort. There are risk analysis and control evaluation techniques developed in recent years that can be enhanced and tailored for logistics systems. There are control problems, handled in a more or less standard fashion in conventional systems, that require reanalysis and the development of generalized techniques for an interactive environment. Real-time software auditing techniques require considerably more development to make them a useful tool in a modern logistics system environment. Standards are needed for design and development.

In summary, with appropriate management support, a needed research and development effort concerning computer control and auditing problems can be formulated.

RECOMMENDATIONS

Detailed analysis of state-of-the-art activities discussed at length in the full report led to the recommendation of the following activities as offering the most potential for benefit from research and development efforts.

Risk Analysis/Control Evaluation Technique Development

The purpose of this effort would be to develop control evaluation and risk assessment techniques specifically designed for logistics systems. The first

step in the process would be a study to determine the exact nature and extent of NAVSUP's computer control and audit problem. By accumulating statistics on items such as the number of inventory adjustments, the number of reversal transactions, number of vendor complaints, number of user complaints, plus interviews with appropriate personnel, an opinion would be formulated as to the reliability of the records, the trend of the reliability, causes for any change, and impact of the reliability on overall performance.

This information would be used as the basis for determining causes of exposure and estimating exposure in risk analysis and control evaluation procedures. The various techniques of quantification and rating used by existing approaches such as those described in Section 3 would be analyzed, and the most appropriate chosen for logistics systems. In this manner, a new technique combining the features of other approaches that are most suitable to logistics systems would be developed.

Real-Time Software Auditing - Language Processor

This effort would be divided into two parts: requirements analysis and conceptual design, and design and development of an auditing language processor. The requirements analysis phase would involve determining the capabilities that such a language processor should possess. This would be based on an analysis of existing auditing language processing packages and a determination of their advantages and shortcomings. During this phase, a determination would be made as to whether an existing processor would be satisfactory, whether modification would be required, or whether an entirely new version would be required. Equipment required to run the language processor would be considered.

The second phase, assuming it were required, would be the design and development of the approved conceptual design.

Real-Time Software Auditing - Integrated Test Facility (ITF)

The ITF has drawbacks, as discussed in Section 4 of this report, in that it may modify live records with fictitious data. This research effort would be devoted to finding a generalized way to eliminate the effects of ITF processing automatically, without modifying the application programs, and without utilizing an undue amount of mainframe computer time.

Real-Time Software Auditing - On-Line Monitor

This effort would involve developing a concept of selectively auditing the application of input controls, particularly identification, authorization and approval procedures, in a real-time on-line mode.

Controls - Generalized Techniques for Interactive Systems

Interactive systems require different approaches than batch systems to prevent input errors, lost transactions, duplicate transactions, etc. Techniques are suggested in Section 3. The effort would be to study this problem in depth and to develop techniques, including generalized software frameworks which could be incorporated in on-line logistics systems.

TABLE OF CONTENTS

TABLE OF CONTENTS (Cont'd)

LIST OF FIGURES

1. INTRODUCTION

This section describes the purpose of the study, the problem addressed, the approach used in conducting the study, and the scope of the study.

1.1 PURPOSE

The purpose of this study was to review the state-of-the-art of auditing and control techniques applied to computerized information systems, particularly large-scale logistics information systems, and to present the findings as the basis for planning and organizing a research and development effort covering real-time software auditing and conventional process auditing within logistics information systems. The objective of the auditing program would be to determine, on an ongoing basis, whether system controls are operating effectively to detect, deter, prevent or correct erroneous processing results -- whether from hardware failure, software deficiencies, inadvertent error, or intentional misuse.

Specifically, in this effort, a survey was conducted to identify technical developments that might be directly applied, or might be adaptable, to real-time software and/or conventional process auditing. The developments were evaluated with respect to their applicability, either in their current state or with further development, to logistics information systems.

1.2 THE PROBLEM

The basic problem motivating this study is undue depletion of government assets caused by gross inefficiencies resulting from erroneous recordkeeping, by assets being misappropriated, or by some combination of the two.

There are varying perceptions of the extent of the problem, its causes, and the means to control it. The statement of work for this effort identifies

software deficiencies and misuse of computer mechanisms as primary causes that can possibly be eliminated or controlled through real-time software auditing and/or conventional process auditing.

The terms real-time software auditing and conventional process auditing connote different things to different people. Because the word audit is used in referring to so many different types of reviews, we have established definitions specifically applicable to this report, to avoid confusing the reader. Discussion of the subject involves other terms such as security, controls, software, etc., for which definitions also are not exact. Therefore, the remainder of Section 1.2 contains definitions of terms used in this report, followed by subsections discussing various perceptions of the ADP auditing problem.

1.2.1 Definitions

1.2.1.1 Audit

The word audit, when used in its broadest sense, means any thorough examination and evaluation of a problem; qualifiers are needed to convey a more definitive meaning to the reader. Thus, there are management audits, operational audits, performance audits, security audits, financial audits, etc. The term is most commonly used in reference to financial statements, for which the audit consists of a searching investigation of the accounting records and other evidence supporting the financial statements. By studying and evaluating an organization's system of internal controls (including tests of compliance and tests of effectiveness), inspecting documents, observing assets, making inquiries within and outside the organization, and other auditing procedures, auditors gather the evidence needed to determine whether the records provide a fair and reasonably complete picture of the organization's financial position and its activities during the period being audited.

Closely related to this standard accounting definition of audit is the definition of "Computer Security Audit" used by the National Bureau of Standards in its Second Invitational Workshop on Audit and Evaluation of Computer Security (see Appendix A):

> A computer security audit is defined as an independent evaluation of the controls employed to ensure:
>
> - the accuracy and reliability of the data maintained on or generated by an automated data processing system,
> - the appropriate protection of an organization's information assets (including hardware, software, and data) from all significant anticipated threats or hazards,
> - the operational reliability and performance assurance of all components of the automated data processing system.

Thus, interpreting the two definitions, the computer security audit is a subset of the broader financial audit and should be a part of any financial audit where computer processing is involved.

Operational auditing differs from financial auditing only in its objective: it is directed at deficiencies that cause excessive costs, erroneous management decisions, competitive disadvantage, etc., rather than being directed at determining the fairness of financial statements.

The deficiencies imply a need for certain audit procedures, especially the evaluation of controls. The audit procedures used will be derivatives of the corresponding controls used to detect, deter, and prevent error and fraud. Tests to validate results, to evaluate the effectiveness of controls, and to determine the extent of compliance with controls are significant, but are far from the only procedures implied by the term audit.

Based on the preceding discussion, the following definitions have been applied in this report:

- o Auditing is the examination and evaluation of a system of records (inventory records, purchasing records, etc.) and any supporting evidence, including the procedures for maintaining and controlling data in the records, to determine whether the records provide a reasonably accurate and complete picture of a function's status (inventory status, financial status, etc.) and its activities during the period being audited.

- o Real-time software auditing is the monitoring, as processing occurs, of internal controls in a computerized system to verify that they are being carried out, as designed, to reduce the risk of erroneous processing and/or fraudulent activities resulting in loss.

- o Conventional process auditing is the selective examination, testing, and evaluation of processing results to obtain evidence supporting conclusions as to the reliability of the overall results.

- o Financial auditing is auditing to determine whether an organization's financial statements fairly present the organization's financial status and activities during the period being audited.

- o Operational auditing is auditing to determine whether an organization's operations are being conducted efficiently, to aid management in achieving the most efficient administration of the business.

1.2.1.2 Loss-related Terms

Definitions of loss-related terms, as used herein, are:

- o Exposure is the effect of a cause (stated in dollars) multiplied by the probable frequency of its occurrence. For example, assume that 1,000,000 tax refund checks of $200 each were to be issued. Also assume that the probability of issuing duplicate checks is 1 in 5,000. The exposure would be $200 x 1,000,000 x 1/5000, or $40,000.

- o Causes of exposure are the occurrences of events which create the possibility of a loss. For example, failure to process a transaction representing the receipt of material creates the possibility of loss from excessive costs of ordering material on a priority basis when in fact it is already on hand.

1.2.1.3 Controls

As inferred from the auditing definitions in Section 1.2.1.1, controls are almost inseparable from auditing. In a system of any size, controls must be relied upon to minimize the risk of loss from errors and fraud. Controls are procedures designed to reduce the causes of exposure to loss. They may be both external to computer software (operating independently or in conjunction with the software) and internal to the software (supporting an external control or operating independently of external activities). There are several categories of controls, defined as follows:

- o Preventive controls are designed to prevent a cause of exposure to loss from happening. A preventive control acts as a guide to ensure that things happen as they should. Historically in

ADP systems such controls usually are not foolproof; they often allow a significant percentage of violations.

- o Access controls are a very significant type of preventive control designed to limit who may use the computer to perform certain functions or have access to certain data within the computer.

- o Detection controls are designed to detect the fact that a cause of exposure has occurred. They do not prevent a cause of exposure from happening but instead trigger an alarm after it has happened.

- o Corrective controls are designed to correct the effects of a cause of exposure after it has been detected. Maintenance and follow-up of a suspense file of error transactions is an example of a corrective control.

1.2.1.4 Software

- o Application software is that portion of a system of computer programs which causes the computer hardware and/or system software to perform the functions specific to the application being processed.

- o System software is that portion of a system of computer programs which controls and supports the operation of the hardware and the application software.

- o Generalized software is a computer program(s) that performs a number of given functions which can be applied to the solution of specific problems through the use of parameters describing the data to be processed.

1.2.2 Navy Supply Perception of the Problem

Our understanding of how the Navy Supply organizations perceive the problem is derived primarily from the task statement of work and from discussions with the contract monitor. Supplementing these sources of information were meetings with a supply systems specialist at NAVSUP and the Computer Security Officer at the Naval Supply Center, Norfolk, Virginia.

1.2.2.1 Description of the Problem

The Navy Supply organizations believe that they are experiencing significant losses due to inefficient operations caused by erroneous inventory records and misappropriation of Navy property. The exposure resulting from erroneous recordkeeping can be significant not only in terms of dollars lost because of excessive costs, but, if severe enough, its adverse impact on the readiness of the Fleet. For example, if the records indicate that critical parts are in stock, but they are not there when called for, consequences are easy to imagine and become increasingly severe as the frequency of occurrence goes up.

Losses from computer-related theft are also thought to be significant. One specific instance that was cited involved the theft of flight jackets, and another involved the hauling off of material in the trunk of an automobile. These thefts were facilitated by the expeditious order handling provided through computer terminals.

No data was available to this study to indicate the extent of losses actually incurred from these exposures or the specific sources. But it appears obvious that the losses can be staggering particularly from erroneous recordkeeping, if not controlled.

1.2.2.2 Causes of the Problem

Navy Supply believes that software deficiencies are a major cause of erroneous records. The task statement of work declares:

> . . . the basic assumption of this research task is that such imperfections (i.e. software deficiencies) exist in production systems and do cause considerable damage . . . their incidence increases each time new modules or modifications are placed in production status.

Navy Supply also indicated that erroneous input, traditionally the major cause of erroneous records, is a problem. As indicated in Section 1.2.2.1, theft is also perceived as a significant problem. However, the extent to which theft occurs because of circumventing external controls as opposed to misusing the computer is a matter for speculation at this point because we were not able to gather specific data in this area for the study, even though several interviews were conducted.

Circumventing access controls for computer terminals in warehouses is known to occur. Sometimes terminals are signed on first thing in the morning and remain on-line for the remainder of the day, available for possible unauthorized use. The potential exposure can range from inadvertent erroneous input to intentional misuse for personal gain. Actual consequences are unknown.

1.2.2.3 Approaches to Solutions to the Problem

The statement of work indicates that Navy Supply believes solutions to the problem lie in real-time software auditing and conventional process auditing.

Per interviews, the concept of real-time software auditing is perceived only as a possible long-range solution to the Navy's problem for two reasons:

a) First, it would probably require substantial modification to the existing software, and this is considered impractical under existing conditions.

b) Second, the concept requires an unknown amount of research and development activity before becoming viable in such a large and complex environment.

Another approach perceived by the user as a long-range solution is the inclusion of specific control and audit requirements in the design specification for all new systems and system modules. Specific guidelines would have to be developed and training provided for functional and system designers.

Conventional process auditing may, on the other hand, be able to offer short-range assistance through generalized auditing software which would not necessarily have to run on the same computer as the application being audited, and therefore would not have to consume vital system resources which are already fully committed.

1.2.3 General Perception of the Problem

The community providing a general perception of the problem comprises individuals who are auditors and computer specialists representing such organizations as the Institute of Internal Auditors, the American Institute of Certified Public Accountants, the National Bureau of Standards, major accounting firms, major software houses, and major industrial firms (see Appendix A). There was a remarkable degree of concurrence among this community as to the nature of the problem, its causes, and approaches to a solution. These topics are discussed in the following paragraphs.

1.2.3.1 Description of the Problem

The computer auditing and security community believes that the potential for losses stemming from computerized information systems is enormous. Computerized information systems have characteristics which increase the potential for catastrophic losses, whether the exposure is caused by intentional misuse of the computer, a natural disaster such as a flood, or inadvertent errors. The tremendous concentrations of data in one physical location tend to create possibilities for large-scale disasters, with corresponding losses. One undetected program deficiency could create errors in thousands of records before it became known. The cost of making corrections could be enormous. Creating fictitious transactions is easier for an informed embezzler to hide. Case histories of such events are included in much of the literature.

1.2.3.2 Causes of the Problem

The community agrees that the majority of the losses that actually occur arise from inadvertent errors. Quoting from Mair, Wood and Davis' "Computer Control and Audit" (see Appendix A):

> While they are serious threats catastrophe and organizational amnesia (lack of information) are still not the primary concern with modern computer systems. . . . BASED ON OUR EXPERIENCE, THE GREATEST SOURCES OF COMPUTER LOSSES ARE INNOCENT ERRORS AND OMISSIONS. Errors and omissions in input may be the source of millions of dollars of losses.

Kraus and MacGahan state in their book "Computer Fraud and Countermeasures" (Appendix A):

> Errors are far more common and costly than computer fraud. For every fraudulent transaction, there are perhaps 100 errors that result in losses. Sound administrative practices and control cut down on errors, aid in detecting them before they cause serious losses and also serve as fraud countermeasures.

Program deficiencies are a major source of erroneous data, and the errors from this source are the most costly to rectify. Not only are there the costs of researching the problem and making the correcting program modifications, but research is required to discover how many times the error was made before this deficiency was detected, how many records are incorrect because of it, and what procedure can be developed to effect the correction. On top of all these costs, there will probably also be significant costs involved in actually making the corrections to the data. For example, it is not inconceivable that program deficiencies could so degrade the reliability of an inventory file that a complete physical inventory would be necessary to reestablish integrity.

Another area that causes a great deal of concern is unauthorized modification of programs to provide personal gains. The concern arises because:

- Some program modification schemes are untraceable.
- All program modification schemes are difficult to detect.
- Motivation for perpetrators is great because a single blitz can effect large benefits rapidly, with little chance of detection or prosecution.

In summary, the auditing and security community believes that inadvertent errors, program deficiencies, and fraud are all areas for concern and, when considered together, as they should be, constitute one of the major, if not the major, problems in information processing today.

1.2.3.3 Approaches to Solution to the Problem

People in the auditing and security community are consistent in advocating that this problem be dealt with as a whole, using a systems approach.

The systems approach requires identification of exposures, the causes of these exposures, and the various means of controlling or eliminating the causes. Internal computer processing controls need to be considered with respect to their relative contribution and cost, when compared to controls in other areas which may accomplish all or part of the desired result for less cost. One classification of control areas includes:

- o General organizational controls.
- o Input controls.
- o Data communication controls.
- o Computer processing controls.
- o Output controls.
- o On-line terminal/distributed systems controls.
- o Physical controls.
- o Data base controls.
- o System software controls.

Auditing, as management's monitor and evaluator, must review the effectiveness of this entire system of controls. To be most effective, the review and evaluation should begin at the design and development stage in the system life cycle, because it is very costly to attempt to retrofit controls.

In summary, the approach generally advocated is a systems approach in which management is involved in setting policy and assigning responsibility for a control (security) program that includes:

- o Analysis of requirements (risk analysis).

- o Design and development of a system of controls as a part of overall system design and development.

- o Administration of the control (security) program.
- o Ongoing audit of the entire program, including risk analysis, development, and operations.

1.3 APPROACH AND SCOPE

The approach followed in conducting the study was to explore the problem from an overall viewpoint before concentrating on computer control and auditing techniques. This was deemed necessary to provide an adequate perspective for evaluating the worth to a comprehensive control program of any techniques considered for a research and development effort. The approach is consistent with that used in all the literature summarized in connection with this study, including Federal Information Processing Publication #65 and OMB Circular A-71.

The original work plan called for the study to be conducted in four steps:

- o Determine user's perception of the problem.
- o Conduct research, classify articles, and resources.
- o Summarize findings.
- o Prepare conclusions and recommendations.

The first step was not carried out to the extent and depth anticipated because many of the key users at NSC Norfolk, Mechanicsburg, and Charleston were not available for interview in the time frame of this study. However, interviews were held with the contract monitor, with a supply specialist at NAVSUP, and with the Computer Security Officer at Norfolk. The results of the interviews are summarized in Section 1.2.2, Navy Supply Perception of the Problem.

The literature survey covered recent publications by members of the auditing and security community. Authors represented viewpoints from the following groups:

- o American Institute of Certified Public Accountants.
- o The Institute of Internal Auditors.
- o Institute for Computer Sciences and Technology, National Bureau of Standards.
- o National accounting firms.
- o National software firms.
- o Universities.
- o Large industrial firms.
- o The General Accounting Office.
- o Government agencies (as computer users).

Appendix A contains brief abstracts of the publications considered most relevant to the study.

The common elements among the articles were identified and the information collected was summarized for analysis and presentation in this report, along with conclusions reached and recommendations of areas for further study.

Analysis of the problem (discussed in Section 1.2) immediately resulted in consideration of the areas of management participation, risk analysis, and

the systems engineering approach, as well as control and auditing techniques. Section 2, State-of-the-Art, therefore discusses the broader aspects of the problem, with specifics on management participation and risk analysis. Section 3 presents specific control techniques, and Section 4 describes auditing techniques and tools. Section 5 contains findings, conclusions, and recommendations.

2. STATE-OF-THE-ART

This section presents the findings of the study relative to the state-of-the-art in computer control and audit. The section includes an overview and subsections on management responsibilities, risk analysis, and control and auditing.

2.1 OVERVIEW

The advent of computers has brought about great change in the way business and government handle their assets. The way transactions and recordkeeping have changed has made many cherished accounting and auditing controls obsolete. Electronic systems are performing more and more operations without a piece of paper to support each step. Electronic Funds Transfer Systems (EFTS) are probably at the forefront of this technology. Rigorous systems of control have to be developed for such systems, and a subset of the computer science and auditing communities has formed to deal with the problem.

The technology that is evolving is based on the recognition of certain characteristics of the problem, namely:

- The problem has many facets which pervade all members of an organization: line, accounting, data processing, personnel, communications, etc.

- The potential losses could be so devastating that the problem requires significant top-management attention, even though the probability of occurrence appears slight.

- Inadvertent errors, particularly on input, are one aspect of the overall problem and are not just the concern of the data-entry department.

- A system of controls that neutralizes inadvertent errors can also reduce threats from program deficiencies and fraud.

- A cause of exposure (threat) often can be neutralized by the addition of any one of a number of controls, either manual or computerized.

- Because various threats create varying degrees of exposure, and because there is a choice of controls to neutralize the threats, a risk analysis is required to determine how to best minimize the risk, using available financial and technical resources.

- The quantity of data being dealt with is so great that the computer must be used to assist in executing control procedures and in auditing.

- The number of computerized records maintained and the volume of transactions processed is so great that it is impractical, if not impossible, for auditors to verify the correctness of every record or account. The auditor must rely on his evaluation of the system of controls to formulate his opinions as to the reliability of the records.

The system approach to solving the information system control problem considers all of the aforementioned characteristics of the problem, with the goal of providing an adequate integrated solution at a minimal cost. There are four major components to the approach:

- Top-management participation.
- Risk analysis.
- System of controls.
- Continual audit.

Management must understand the problem so that they support and rely upon the system. Risk analysis is necessary to coordinate controls and evaluate cost-versus-benefit tradeoffs. The design of the system of controls must meet the requirements that fall out of the risk analysis. A continual audit must be conducted on operational systems to verify that the system of controls is in place and operating effectively. Each of these aspects is discussed in more detail in subsequent portions of this section.

2.2 MANAGEMENT RESPONSIBILITIES AND PARTICIPATION

A paper titled "Managerial and Organizational Vulnerabilities and Controls - Staff Level," prepared as part of the proceedings of the NBS International Workshop on Audit and Evaluation of Computer Security (Appendix A), provides an excellent overview of top management's responsibilities relative to computer control and audit. The paper is the work of a panel session consisting of the following persons:

D. L. Scantlebury, Division Director at the U. S. General Accounting Office.

Robert Blake, Chief of Division, Institute for Computer Sciences, National Bureau of Standards.

Howard Davis, Director, Office of Audits, General Services Administration.

David Harris, Partner, Lilly & Harris, CPA.

Bryan Mitchell, Assistant Inspector General, Department of Health, Education, and Welfare.

Frank Sato, Deputy Assistant Secretary of Defense (Audit).

Joseph Sickon, Director of Audit, Department of Commerce.

The view expressed by this panel is that top management in the more progressive organizations will understand the nature of the problem and the requirement for a coordinated system of controls. They will assume responsibilities in four major areas:

- o Establishing an organizational structure supportive of a coordinated system of controls.
- o Establishing policy and control standards which promote secure, well-controlled systems.
- o Allocating adequate resources to provide a system of controls and to periodically audit or test these controls.
- o Requiring periodic reports on the effectiveness of controls.

2.2.1 Organizational Structures

The key elements of an organizational structure which promotes computer control are:

- o Designation of a senior official as responsible for the program.
- o Establishment of a committee of senior managers (not delegates) from all organizational components to effect coordination of the program.
- o Requirement for an adequate level of auditing and assignment of responsibility thereof.

- o Identification of those positions in the organization that require personnel who have a security clearance, and assignment of responsibility for the required screening of the personnel.

The auditing responsibilities are of special interest and importance to this study. To be effective, any auditing techniques used must be part of a program mandated by and vigorously supported and enforced by top management. The charter must include evaluation of the system of controls at critical stages in the development of new systems, as well as testing of operational systems to determine whether prescribed controls are in place and functioning effectively.

2.2.2 Policy and Control Standards

Top management must determine the overall level of security required for the organization, and establish policies and standards which will promote this level of security on a consistent basis throughout the organization. For example, it would make little sense to encrypt data transmissions if there is uncontrolled access to the transmitting terminals.

To arrive at the level of security required for the organization, top management should require that an analytical assessment of the exposures be prepared for their review. Certain of the inputs to the study require subjective evaluations of various characteristics of the organization's operations. For example, what would be the consequences of being out of stock for 60 days on 20% of highly specialized electronic components? Top management must not only commission the "risk analysis" but must ensure participation of those most qualified to provide needed input to the analysis.

Formal standards providing guidelines for the protection of the integrity of data should be published by the organization. "The Auditor's Study and Evaluation of Internal Control in EDP Systems," published by the AICPA

(Appendix A), includes 19 standards that would require little or no modification for most organizations.

2.2.3 Allocation of Resources and Reporting

Top management must allocate the funds and people to enable the computer control and audit program to be implemented as described in the preceding paragraphs. Periodic reports on the effectiveness of the system of controls must be required as top management's method of monitoring the program.

2.3 RISK ANALYSIS, EXPOSURE, AND CONTROL EVALUATION

In recent years, as the significance of computer control and audit has increased, more analytical approaches to evaluating exposure and determining the level of control required have evolved. As defined by the Institute for Computer Sciences and Technology of the National Bureau of Standards (Appendix A), risk analysis is:

> An analysis of an organization's information resources, its existing controls, and its remaining organization and computer system vulnerabilities. It combines the loss potential for each resource or combination of resources with an estimated rate of occurrence to establish a potential level of damage in dollars or other assets.

Techniques of varying degree of sophistication have been developed for the purpose of risk analysis. Regardless of the technique used to arrive at the exposure, top management must decide whether they can tolerate such a level of exposure. If the exposure is too great, an analysis must be conducted to determine ways to reduce it and at a minimized cost. This will probably involve adding additional controls which reduce or eliminate causes of exposure and thereby reduce the overall level of exposure. The cost of implementing such controls must be weighed against the reduced

level of exposure. In most cases there will be several possible solutions to the problem, and top management should be provided with the information necessary to determine the most cost-effective solution.

Some of the techniques in use for risk analysis and/or evaluation of exposure and control are briefly described in the following paragraphs.

2.3.1 Risk Analysis - System Development Corporation (SDC)

SDC has developed advanced risk assessment methodologies for the Navy and the Social Security Administration. These methodologies provide all of the information required by the present government standard, FIPS PUB 65. The SDC methodologies contain a number of features not found elsewhere. These features are discussed later in this section; two of the more important innovations are the ability to relate threats to vulnerabilities and a means for valuing and assessing the exposure of special assets such as inventory records or classified information.

Risk assessment is an organized examination of the events and conditions that could harm a ADP system. The result of a risk assessment is an indication of the degree of exposure or risk of the assets to various threats. The risk assessment can be conducted at varying levels of detail (system or subsystem level, for example) and may be targeted at an existing or planned installation.

The general risk assessment methodology that SDC uses performs the following:

- Identifies conditions or potential events that threaten harm to the ADP system and evaluates the seriousness of these threats.

- Identifies and evaluates conditions within the ADP system that could allow the ADP system and the data it maintains and reports upon to be damaged or degraded.

- Identifies and evaluates the properties and importance of the assets, including data in the ADP system.

- Estimates the Annual Loss Expectancy (ALE) of the ADP system due to the realization of threats.

- Estimates the level of exposure or risk for classified, sensitive, or mission-essential assets.

- Identifies the most dangerous or costly weaknesses of the ADP system and recommends means to remedy them.

SDC's risk assessment methodology consists of six major activities. These activities can be conducted by a single individual or, preferably, by teams, depending upon the level of resources available. The six activities in the risk assessment methodology are the following, which are illustrated in Figure 2-1:

- Threat Evaluation. Identify the threats (causes of exposure such as failure to enter a receipt) to the ADP system and the frequency of occurrences.

- Vulnerability Evaluation. Identify and evaluate the weaknesses of the ADP system.

- Asset Evaluation. Identify the assets of the ADP system and assign a value based upon possible impact.

- Threat/Vulnerability Merger. Estimate the frequency of successful attacks against an ADP system -- how often threats succeed in exploiting a vulnerability.

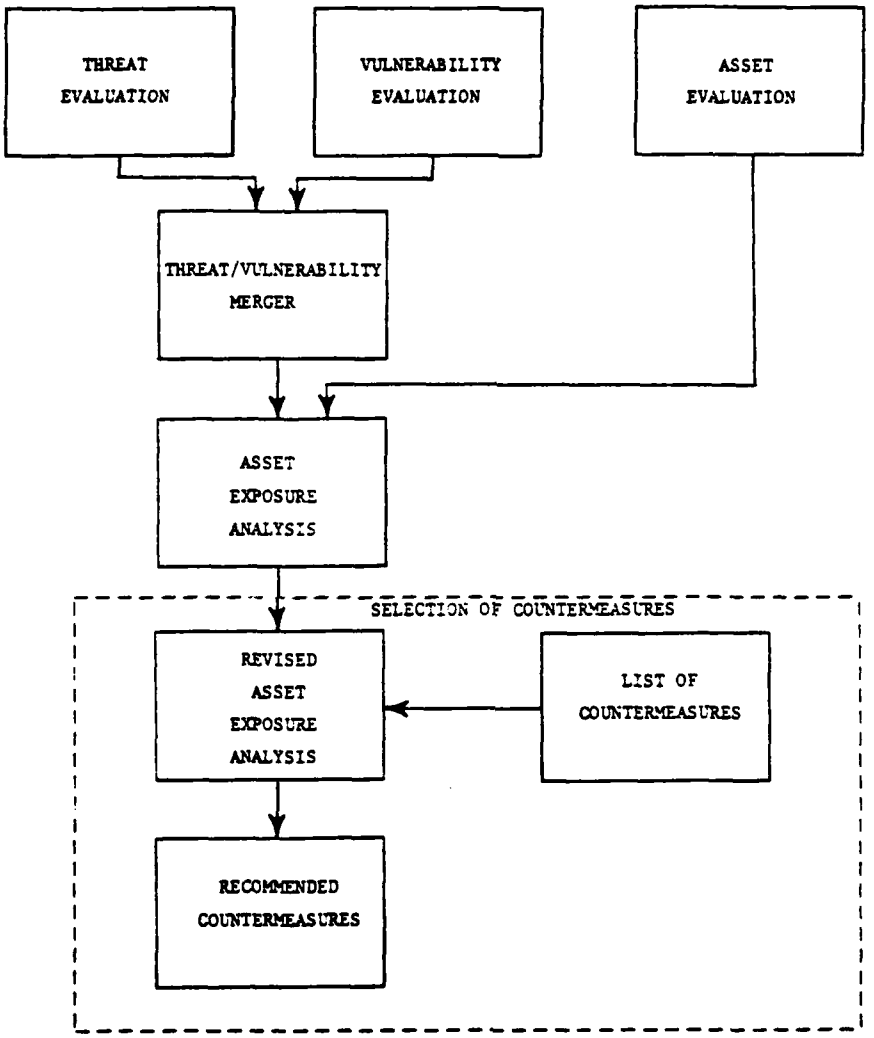


Figure 2-1.
Major Activities in Risk Assessment Methodology

- o Asset Exposure Analysis. Quantify the effects of successful attacks against the assets of an ADP system.

- o Selection of Countermeasures. Select countermeasures that will reduce the asset exposure.

This methodology can be readily adapted to the NAVSUP environment to arrive at an assessment of the current degree of exposure, to assist in the design of a system of controls for any new systems or subsystems, or both.

2.3.2 Evaluation of Controls - Touche Ross & Co.

Touche Ross & Co. is one of the large national public accounting firms. Mssrs. Mair, Wood, and Davis of that firm wrote a book, "Computer Control and Audit", in which they included a standard procedure used by Touche Ross to evaluate controls in computer systems. The procedure uses a matrix approach to relate controls, causes of exposure, and exposure level. The strength of controls and probability of exposure are rated numerically. Figure 2-2 is an example of one column of a matrix and Figure 2-3 is the standard table (matrix) used for evaluating application controls. Considerable judgment must be applied, when analyzing the data in the matrix, to form an opinion as to the quality of control, the likelihood of each cause of exposure occurring, the probable exposure if it does occur, and finally the resulting exposure. This result may be used in further analysis to determine what the overall level of exposure should be, what controls should be strengthened, what controls should be specified for a new system, etc.

The strength of this approach is that it provides a structured, standardized methodology by which relatively inexperienced personnel can learn the technique and perform much of the time-consuming detail work and present it to a

CONTROL EVALUATION TABLE

CONTROLS	CAUSES OF EXPOSURE: Lose a Check	KEY TO STRENGTH OF CONTROLS
Training	1	
Secure custody	2	3 – Very reliable
Prenumbered form	3	2 – Moderately reliable
Endorsement	1	1 – Useful but not reliable
Transmittal document	2	Blank – No significant use
Amount control total	3	
Document control count	3	
Reconciliation	3	
Discrepancy reports	2	
		EXPOSURES
KEY TO MAGNITUDE OF EXPOSURE	3	Erroneous record keeping
		Unacceptable accounting
3 – Virtually certain	1	Business interruption
2 – Probable		Erroneous management decisions
1 – Possible but unlikely		Fraud and embezzlement
Blank – Very unlikely		Statutory sanctions
	2	Excessive costs
	3	Loss or destruction of assets
	2	Competitive disadvantage

(From "Computer Control and Audit," Institute of Internal Auditors.)

Figure 2-2.

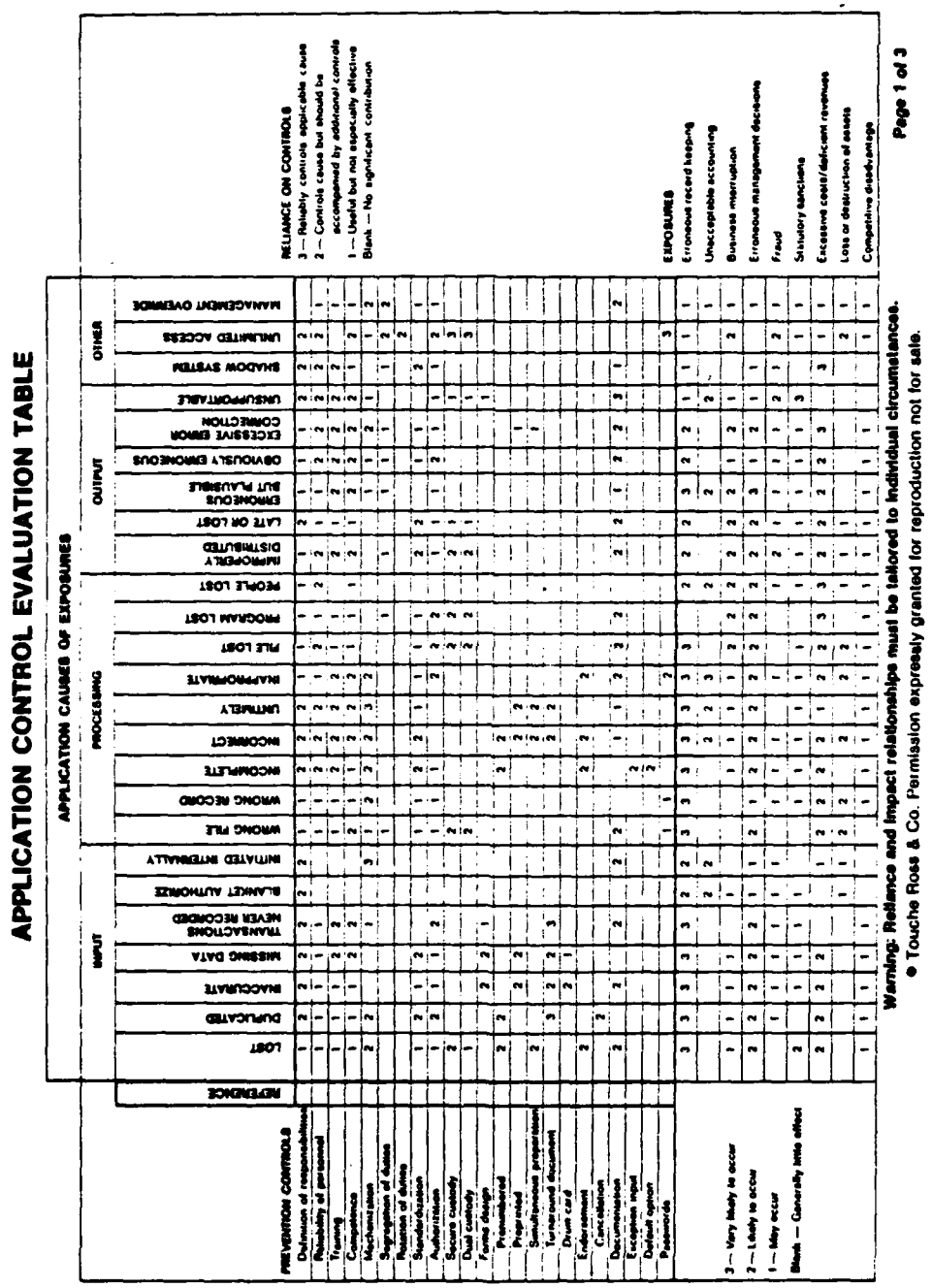

APPLICATION CONTROL EVALUATION TABLE
APPLICATION CAUSES OF EXPOSURES
INPUT
PROCESSING
OUTPUT
OTHER
PREVENTION CONTROLS
REFERENCE
LOST
DUPLICATED
INACCURATE
MISSING DATA
TRANSACTIONS NEVER RECORDED
BLANKET AUTHORIZE
INITIATED INTENTIONALLY
WRONG FILE
WRONG RECORD
INCOMPLETE
INCORRECT
UNTIMELY
INAPPROPRIATE
FILE LOST
PROGRAM LOST
PEOPLE LOST
IMPROPERLY DISTRIBUTED
LATE OR LOST
ERRONEOUS BUT PLAUSIBLE
OBVIOUSLY ERRONEOUS
EXCESSIVE ERROR CORRECTION
UNSUPPORTABLE
SHADOW SYSTEM
UNLIMITED ACCESS
MANAGEMENT OVERRIDE
RELIANCE ON CONTROLS
3 — Reliably controls applicable cause
2 — Controls cause but should be accompanied by additional controls
1 — Useful but not especially effective
Blank — No significant contribution
EXPOSURES
Erroneous record keeping
Unacceptable accounting
Business interruption
Erroneous management decisions
Fraud
Statutory sanctions
Excessive costs/deficient revenues
Loss or destruction of assets
Competitive disadvantage
Definition of responsibilities
Reliability of personnel
Training
Competence
Supervision
Segregation of duties
Rotation of duties
Standardization
Authorization
Secure custody
Dual custody
Forms design
Prenumbered
Preprinted
Simultaneous preparation
Turnaround document
Drum card
Endorsement
Cancellation
Documentation
Exception report
Default option
Passwords
3 — Very likely to occur
2 — Likely to occur
1 — May occur
Blank — Generally into effect
Page 1 of 3
Warning: Reliance and impact relationships must be tailored to individual circumstances.
© Touche Ross & Co. Permission expressly granted for reproduction not for sale.

Figure 2-3.

APPLICATION CONTROL EVALUATION TABLE

DETECTION CONTROLS	REFERENCE	INPUT: LOST	INPUT: DUPLICATED	INPUT: INACCURATE	INPUT: MISSING DATA	INPUT: NEVER RECORDED	INPUT: BLANKET AUTHORIZE	INPUT: INITIATED INTERNALLY	PROCESSING: WRONG FILE	PROCESSING: WRONG RECORD	PROCESSING: INCOMPLETE	PROCESSING: INCORRECT	PROCESSING: UNTIMELY	PROCESSING: INAPPROPRIATE	PROCESSING: FILE LOST	PROCESSING: PROGRAM LOST	PROCESSING: PEOPLE LOST	OUTPUT: IMPROPERLY DISTRIBUTED	OUTPUT: LATE OR LOST	OUTPUT: ERRONEOUS BUT PLAUSIBLE	OUTPUT: OBVIOUSLY ERRONEOUS	OUTPUT: EXCESSIVE ERROR CORRECTION	OUTPUT: UNSUPPORTABLE	OTHER: SHADOW SYSTEM	OTHER: UNLIMITED ACCESS	OTHER: MANAGEMENT OVERRIDE
Anticipation		3				3					3		1		2	2	2	3	3							
Transmittal document		2	2	2							2							2								
Batch serial numbers		3	3						2						3											
Control register		2	2	2					2		2				2											
Amount control totals		3	3	2					3		3	2														
Document control count		3	3						3			1														
Line control count		3	3						2		2	1														
Hash totals		3	3	2					3		2	1														
Batch totals		3	3	2					3		2	2														
Batch balancing		3	3	2					3		2	2														
Visual verification			1	1	2				2	1	1	1		1				2			3					
Sequence check		2	2	1		2			2	2	2	2			1											
Overflow check				2					2	2	2	2		2												
Format check				2					2	2																
Completeness check					2				2	2	2	2	1	2						1	2					
Check digit				3					2																	
Reasonableness		1	2	2	2			2	2	2	2	2	1	2							2					1
Limit check				2				2	1			2									2					
Validity check				2					2																	
Readback		2		3	2									2							2					
Dating			1			2			2				2	2	2								1			
Expiration			2			2			2					2	1											
Keystroke verification				2	2																					
Approval			1	2	2		2		2		1	2	1	2							3		3	2	3	1
Run to-run totals									3		3	2			3						3					
IMPACT OF CAUSES		3	3	3	3	3	2	2	3	3	3	3	3	3	3		2	2	2	3	2	2	1	1	1	1
							2	2				2	2	3			2			2			2			1
3 — Very likely to occur		1	1	1	1		1				1	1	1	1	2	2	2	2	2	2	1	2	1		2	1
2 — Likely to occur		2	2	2	2	2	1	1	2	1	2	2	2	2	2	2	2	2	2	3	1	2	1	1		1
1 — May occur			1	1	1	1	1	1		1	1	1		1			1	2	1	1	1	1	2	1	2	1
Blank — Generally little effect		2		1	1	1	1			1	1	1	1	1	1		1	1	1	1	1	1	3		1	1
		2	2	2	2			1	2	2	2	2	1	2	2	3	3	2	2	2	2	3		3	1	1
							1	1	2	2		2		2	2		1	1	1		1	1			2	1
		1	1	1	1	1				1	1	1	1	1	1	1	1	1	1	1	1	1			1	1

RELIANCE ON CONTROLS
3 — Reliably controls applicable cause
2 — Controls cause but should be accompanied by additional controls
1 — Useful but not especially effective
Blank — No significant contribution

EXPOSURES
Erroneous record keeping
Unacceptable accounting
Business interruption
Erroneous management decisions
Fraud
Statutory sanctions
Excessive costs/deficient revenues
Loss or destruction of assets
Competitive disadvantage

Warning: Reliance and impact relationships must be tailored to individual circumstances.

Page 2 of 3

Figure 2-3.

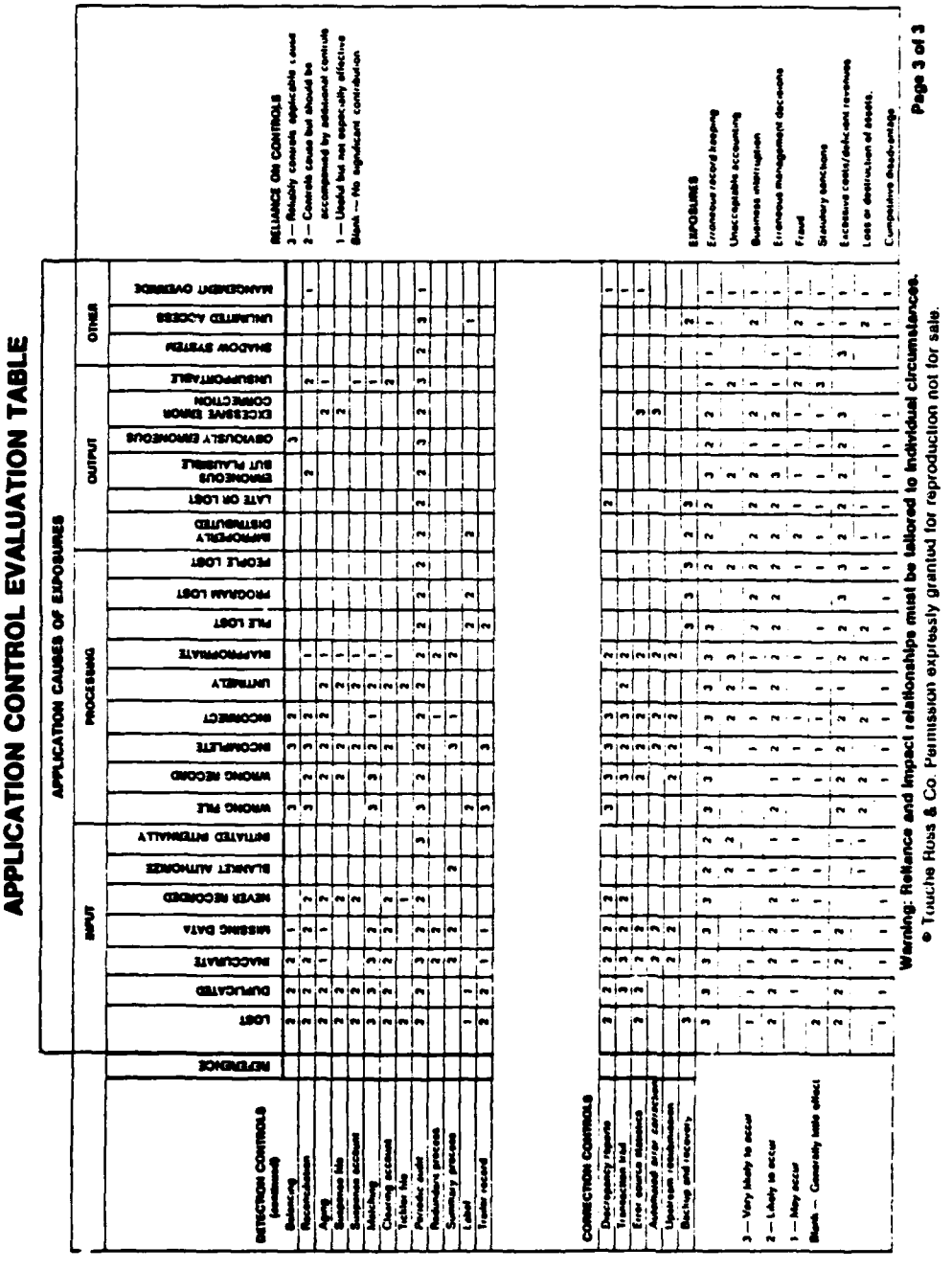


Figure 2-3.

more experienced person for review, evaluation, and formulation of judgments. The incorporation of weighting factors adds a valuable dimension to the techniques. The possible shortcomings include a lack of specificity in identifying controls and a need for updating to keep pace with the changes in concepts of system architecture now emerging (communications-based, distributed systems, on-line systems using a DBMS, etc.). It could be applied in the NAVSUP environment with little modification.

2.3.3 Control Matrix Approach - Dr. Jerry Fitzgerald (Appendix A)

This technique uses a matrix approach to correlate resources to be protected from loss with causes which expose these assets to possible loss. Controls to neutralize these causes are recorded in the appropriate cells in the matrix. The approach divides the computer system into nine components and has a unique matrix for each component. More than 650 controls have been identified.

This technique provides a very thorough approach to performing one of the first steps in a risk analysis. It provides in-depth criteria to assist in evaluating an existing system of controls, in suggesting controls which might be added to reduce exposure, in selecting controls for incorporation in a new system, etc. The technique could be applied in the NAVSUP environment for any of the aforementioned purposes. It could possibly be used as a basis for updating and expanding the Touche Ross Technique.

2.3.4 Security Profile Evaluation - Security and Reliability in Electronic Systems for Payment (Appendix A)

This technique categorizes assets and resources to be protected in 7 major and 9 minor groups, and considers controls for each of the 16 groups from 3 aspects: access, reliability and contingency plans, and accountability.

There is a list of 354 questions, each implying the requirement for a different control. The author has identified each of the questions that apply to each of the 3 aspects under each of the 16 groups. Any one question may appear multiple times. The analyst then determines the answer to each question, rating the control representing his reply as very strong, good, acceptable, questionable, or critically deficient. Figure 2-4 is a sample of the form used for rating the responses (Appendix A, "Security and Reliability in Electronic Systems for Payment").

An advantage of this technique is that it combines much of the detail on controls, as provided in Dr. Fitzgerald's approach, with a reasonable approach for arriving at a quantitative evaluation. As currently structured, it is tailored for Electronic Funds Transfer Systems but could be readily modified for logistics systems.

2.4 CONTROL AND AUDITING

One of the generally accepted auditing standards with which CPAs must comply is:

> There is [must be] a proper study and evaluation of the existing internal control as a basis for reliance thereon and for the determination of the resultant extent of the tests to which auditing procedures are to be restricted.*

This standard applied even before the explosive growth of computerized information processing; it recognizes that examination of every business transaction is often impractical and unnecessary. It seems readily apparent that, in determining the reliability of output from a computerized information system, the auditor must rely on his or her evaluation of the system of controls employed -- external to, in conjunction with, and internal to the

*Meigs, Larsen and Meigs, "Principles of Auditing," Richard D. Irwin, Inc., Homewood, Illinois, 1977, p. 21.

Figure 2-4.
Security and Reliability Profile

computer. It is impossible to verify every account balance and every transaction affecting accounts in the period under audit. Therefore, it is the system of controls that is more often being examined in an audit, not the results of processing. Auditing techniques must change with the control techniques being employed. The control techniques change as information processing technology advances.

Information system architecture has evolved from card-sequential batch to tape-sequential batch, to random-access batch to transaction-driven random access, to a time-sharing environment with data base management systems, to distributed systems. With each shift, the control problem became more complex. Control technology appears to be lagging behind the new system approaches. One reason may be that many of the controls are application-specific and do not lend themselves to generalized solutions. Another reason may be a general lack of awareness of the problem, which has resulted in lack of pressure for a solution. Despite the above reasons, there are areas which have received some attention. Executive systems, transaction processors, and data base management systems advertise security features to control access and protect data. The trend is towards concentrating controls in generalized software to the maximum extent possible. Controls over the operating versions of computer programs and electronically stored data are unique to the computer era. Generalized software is available to assist in this area. Control techniques are discussed in Section 3.

As information systems architecture has become more complex and the generalized system software used with these systems has become highly sophisticated, the auditing task has become equally complex. How does an auditor, trained as an accountant, verify the claim of a DBMS vendor that "Our DBMS will not allow an unauthorized user to access your data base"? He must call in a highly specialized and highly qualified computer scientist to conduct an evaluation for him (or rely on a prior evaluation by

such a person). Many in the field believe that a security certification provided by independent specialists, in accordance with an industry-accepted standard, would be an extremely valuable asset to the auditing profession.

One concept that has universal appeal is real-time software auditing, i.e., using the computer to audit as the processing is occurring. In this paper, we define auditing as an independent review of control processes to formulate an opinion as to the reliability of overall processing. The concept will be further explored in Section 4.

Conventional process auditing is relying more and more on computers to analyze data and conduct tests. The most advanced techniques employ generalized report writer software with special auditing features. This technique is also discussed in more detail in Section 4.

The auditing and security communities believe that auditors must begin their evaluation of control during the design and development phase of the system. Retrofitting of controls is almost always an extremely costly and problematic process. Hence, the scope of the auditor's activities is increased significantly, that is, from system design and development through the total systems life cycle.

3. CONTROL TECHNIQUES

Control is anything that tends to cause the reduction of exposures. The effect that computers have on controls are:

- o Eliminating the need for some, by eliminating the cause of exposure.
- o Creating the need for some new controls, by creating new causes of exposure.
- o Increasing or decreasing the effectiveness of different types of controls.

As computerized information system architecture changes, the type of controls used must shift to meet the new challenge; but the objective of the controls -- to reduce exposure -- remains unchanged.

Various authors have classified controls in a number of different ways. Figure 3-1 is a table showing the classification adopted by four authors. Under these classifications, hundreds of individual controls -- some manual and some computerized -- can be and have been identified. Dr. Fitzgerald, for example, has listed over 650 in his book. The AFIPS Security System Review Manual lists review questions which imply over 800 individual controls. Because most causes of exposure can be neutralized by more than one control, far from every control is needed in every system. Using the system engineering approach to select the controls required and to integrate them into a coordinated system of controls, is the approach being used by more sophisticated designers, especially those developing large, complex, communications-based and/or distributed systems.

Other advanced techniques apply to individual controls or small groups of controls incorporated into systems.

Finally, there are special control problems in controlling the operating versions of programs (systems) and electronically stored data. Techniques for these purposes are continually being improved.

A	B	C	D
General organizational Input Data communications Program/computer processing On-line terminal/distributed systems Physical security Data base System software	Applications Development Operational	Physical Design Operational Administrative - Auditing - Personnel - Legal	Managerial - Policy and standards - Development - Audit Technical - Terminals - Communications - Processors and systems software - Applications - Data base

A - From "Internal Control for Computerized Systems," Fitzgerald.
B - From "Computer Control & Audit," Mair, Wood, Davis.
C - From "Security and Reliability in Electronic Systems," Bank for International Settlements.
D - From "Audit and Evaluation of Computer Security II," National Bureau of Standards.

Figure 3-1.
Classification of Controls

The remainder of this section discusses techniques in three areas:

- o Systems engineering -- overall methodology.
- o Selected application control techniques.
- o Selected administrative control techniques.

3.1 SYSTEMS ENGINEERING -- OVERALL METHODOLOGY

The overall systems approach was discussed in considerable detail in Section 2 of this report. Briefly, the approach consists of four components:

- o Top-management participation to support the effort and to provide coordination between all of the organizational components involved.
- o Risk analysis to determine what the control requirements are in light of the estimated exposures.
- o System of control to cost-effectively reduce the exposure to an acceptable level.
- o Continual audit to ensure that the controls are in place and operating effectively.

In this section, we are concerned with the methodology for selecting the specific control techniques that will meet the control requirements determined in the risk analysis step. Not only may one control be effective against several causes of exposure, but one technique may incorporate multiple controls. For example, control totals on amounts detect lost transactions, duplicate transactions, and errors in amount -- all causes of exposure. The technique of upfront, interactive input not only develops control totals at the entry to computer control, but can perform numerous other control functions such as edit and validation of input data, access control through password checks, verification of transaction identification

by providing read-back of key information, prompting the user in entering the data, etc. At the other extreme is the technique of transmitting the source documents to a central point for conversion to machine-readable media. Control totals can still be developed and the exposure reduced to some degree. There are many variations between the two extremes. The analyst must weigh the overall reduction in exposure with the overall cost of the most promising alternatives, and select the best solution to the problem. From the above example, it is also readily apparent that design of the controls is intimately interwoven with the design of the overall system architecture, and cannot be easily retrofitted.

The analysis of which exposures must be eliminated or significantly reduced, and the possible controls for accomplishing the reduction, should have been performed in the risk analysis step. Possible techniques for implementing the controls in the proposed system environment must now be identified and evaluated. The techniques selected must be integrated into the design as an integral part of the system. It should be noted that auditing is an overall control, and that maintenance of records of activity (audit trails) must be designed into the system so that it can be audited.

Thus the essence of systems engineering methodology, as applied to the control problem, is that all elements of the system -- application requirements, performance requirements, control requirements, auditing requirements, etc. -- must be considered as an entity throughout all stages of design and development.

3.2 APPLICATION CONTROL TECHNIQUES

Use of communications-based systems, with data being input from numerous widely dispersed terminals for financial, inventory, personnel, and other business type applications, has made control more difficult in some areas and offered opportunity for more effective control in other areas. The

changes in control techniques to meet this challenge are discussed in relation to six categories of controls applied in most conventional business type systems. It is possible to implement many of these new control techniques by designing and developing a generalized framework which can be made application-specific through the use of parameters, tables of criteria, etc. The susceptibility of each technique to this approach is indicated in the presentations that follow. The six controls are:

- o Batch balancing.
- o Authorization and approval.
- o File balancing.
- o Editing and validating.
- o Input-to-output control.
- o Document control.

3.2.1 Batch Balancing

Batch totals are used to ensure that no transactions are lost, that none are processed twice, and that the dollar amounts are entered correctly. If the degree of control offered by other on-line techniques is not considered satisfactory, an on-line-batch totaling technique can be used. This technique involves making after-the-fact batches by establishing some time criteria to define a batch (e.g., all transactions processed through any one terminal between 8 a.m. and 4 p.m. constitute a batch). The computer maintains totals by terminal as transactions are entered. At the end of the batch period, a supervisor (not the operator) manually determines the batch total and invokes a balancing routine via the terminal by entering the total developed externally. If this does not match the internal total, the supervisor is so notified and a listing of the accepted transactions is retransmitted to the terminal. The reconciliation process takes place and, if a previously accepted transaction is found to be in error, a reversing transaction and a reentry of the correct transaction occurs. From a design and development viewpoint,

batch balancing is a far more complicated process in an interactive, transaction-driven environment than in a more conventional batch environment. When transactions are entered as events occur, conventional batches do not exist. The internal bookkeeping required to execute this process is far more extensive than for conventional batch balancing.

It is possible to design and develop a generalized routine that will accomplish most of the complex housekeeping, with parameters being entered to specify application-dependent items such as the field(s) to be totaled. It would constitute a major modification to retrofit this capability into an already operating system.

3.2.2 Authorization and Approval

In a batch environment, policies regarding access to the computer are enforced by people, with little or no computer verification beyond a log of jobs run. Approvals, especially those requiring verification of identity, are primarily external. The computer is used to check that individual transactions comply with certain organizational policies (e.g., no shipment over $1,000 before receiving payment).

An on-line terminal environment makes control of authorization and approval policies more difficult. A great deal of effort is going into research to find more effective and practical solutions to this problem. At present, most software solutions (hardware solutions are covered under a separate report) involve the use of passwords to gain access to the computer, to access specific data, or to invoke certain functions. Basic capabilities are provided in vendor system software; the analyst must determine whether more restrictive and/or more secure measures are required.

Three topics--system access, data base access and protection, and authorization profiles--are discussed in the following paragraphs.

- o System access. The ability to control system access through the use of passwords is usually included in the vendor-supplied operating system. Some of these controls provide for different levels of security and some include validating the correlation of passwords with such criteria as geographic location, terminal identification, time of day, etc. Several proprietary software packages on the market provide for a much finer granularity of access control than the operating systems. They operate in an IBM 360/370 environment and therefore are not directly applicable to NAVSUP's systems. It is feasible to build such a package for NAVSUP computers if the requirement for additional control exists.

- o Data access and protection. Data Base Management Systems (DBMS) usually include a number of control features that may or may not be applied at the user's discretion. For example, access may be restricted by individual, by program, by transaction type, or by a combination thereof. Access may be denied to all data, a certain type of data, or even to certain data elements. Access may be restricted to read only, with updating capability denied. Obviously, these control features apply only to the data under control of the DBMS.

- o Authorization profiles. This technique is increasing in comprehensiveness because the power of hardware is increasing. The additional capability is needed because of the expanded use of on-line terminals in numerous types of information systems. The technique involves checking a large number of related factors to determine whether a particular function is authorized. For example, a particular transaction might be restricted to certain individuals assigned to specific terminals at specific times of

the day (e.g., a transfer of funds of over $5,000 can only be initiated by A, B, or C using the Treasurer's terminal between 2 and 3 p.m.). Profiles may be developed in various ways, as the requirements of the application dictate. For example, they may be by individual, by organization, by terminal, or by transaction type.

3.2.3 File Balancing

A control frequently used in a conventional batch environment involves maintaining totals on key fields in files, predicting the effect of transactions processed on these fields, and comparing the predicted total with the actual total computed after processing is complete. Totals between files that have a relationship are also checked to make sure that the correct relationship exists (e.g., productive hours in the payroll file must equal project hours in the labor distribution file). With on-line systems, implementation of this control is far more complex. The point in time to check the integrity of the data bases must be established, be it once a day, twice a day, once a month, or whatever. Transactions from all sources -- terminals, interfacing systems, remote batch, etc. -- must funnel through the prediction routine to accumulate the effect of changes, including additions to and deletions from the file. At the established time, the actual total is computed and compared with the predicted; to accomplish this, either the processing of transactions must be suspended or a copy of the file set aside for this purpose.

Application systems using a DBMS may have some degree of this type of control provided by the DBMS. The nature of most DBMSs is such that the need to balance items between files is reduced because the concept is to store an item once and use it for multiple purposes. The DBMS may also provide some equivalent of overall file balancing, but probably by record count rather than dollar total. Whether or not a DBMS is used, the designer must evaluate the extent of file controls required and provide for them in the application design.

It would be possible to build a generalized framework to provide this function, with specific file characteristics and definition of total fields being entered as parameters.

3.2.4 Editing and Validating

Editing and validating are essential and significant parts of every computerized business information system. The processes consist of comprehensive checks on the characteristics of the data entering the system, relationships between the elements within a transaction, and relationships between the elements in a transaction and data already stored in the system. The obvious purpose is to prevent erroneous data from being processed by the system, thereby degrading the quality of the records being maintained. In an interactive environment, editing and validating procedures are being enhanced to provide more effective preventive and detection controls. A discussion of new innovations in this area follows:

- Interactive Editing and Validating. This technique is becoming more practical, as the cost of terminals with microprocessors decreases and capabilities increase. The terminals are located at or close to the source of the transaction, so that the data recording the event is captured as soon as possible after the event. (There are special-purpose devices, such as scanners used in supermarkets, that capture data as a part of completing the transaction.) The data is edited and validated as the operator enters it, and errors detected are pointed out immediately.

  A transaction is usually not accepted until it is errorless. Because of proximity to the event in both time and location, research for error correction is easier and more timely. In many applications, failure of one transaction to process creates errors in later transactions that would otherwise be valid. Thus, the timely correction of errors also helps to reduce the overall error rate. This technique

uses a large number of specific controls the designers must select. It actually involves designing an input methodology for the system, which can range in complexity from a rather straightforward approach, using an intelligent terminal that can check element attributes, to a very sophisticated system making extensive relational checks. The technique can be used with both batch and on-line transaction-driven systems.

- o Input Prompting. This technique is almost always used, to some extent, with the editing and validating techniques described above. Prompting in large-volume operations usually consists of presenting a form on the CRT screen, with a cursor indicating the next position in which data is to be entered. Screens are selected by making choices from a "menu", by responses to computer-generated questions, and automatically, based on data entered in a previous screen. Properly designed, this is a very effective preventive control technique.

- o CRT Turnaround Document -- Exception Input Technique. In the conventional sense, a turnaround document is one generated by the computer for subsequent reentry, with some additional information added (e.g., a utility bill for which amount paid is added). An exception input is an entry made only when there is a variance from some standard (e.g., enter hours only when more or less than 40). Expanded use of terminals that can access stored information has made it practical to combine these techniques with an interactive input terminal operation, to achieve accuracy and efficiency. The turnaround "documents" are electronically stored. At the appropriate time for entry (e.g., the operator has the time and attendance data ready to be entered), the turnaround documents are called from memory and displayed on the

CRT screen. The document, as presented, contains all of the standard entries. The operator must make a positive indication to accept the standard or to make changes required. If changes are made, editing and validating are performed. This technique tends to ensure completeness (i.e., no lost transactions) and to improve the quality of data, while increasing efficiency because fewer entries have to be made.

For the most part, the above techiques are application-specific. However, computer scientists have developed interpretive languages to make the programming of this type of control an easier task for application specialists. Some microprocessor-based terminals have such editing and validating languages.

3.2.5 Input to Output Controls

This control technique is designed to detect the omission, duplication, or misapplication of a transaction during computer processing. Such errors are most likely to occur because of a program deficiency in the recovery routine. The problem is compounded in an interactive system because there are so many sources for transactions and so many stages in the processing of a transaction. The recovery routine must ensure that each transaction input source restarts from the proper stage. Capabilities to save the necessary data and effect the recovery are usually part of vendor-supplied system software. The technique of input-to-output control is intended to detect any errors that occurred in the process.

The technique is similar to batch balancing and file balancing, in that it must deal with a specific group of input transactions and the corresponding set of outputs; therefore, it involves the same batch determination problems as the other techniques. The input tables can be designed to be the same as the input batch totals, so that the control system is integrated. The system must be designed so that all of the inputs in the batch are completely processed before the output totals are computed. Dollars or quantities input to the system must be reflected in outputs from the system. Differences must be identified and legitimately reconciled or noted as errors (e.g., requests for shipment, 100; shipped, 80; backordered, 15; to error suspense file, 5; hence all accounted for); to be most effective, the routine should operate by input source, so that processing errors can be more easily tracked down and corrected.

This procedure can become relatively complex. However, a generalized framework could be developed with application specifics being entered by parameter.

3.2.6 Document Control

Sequential numbering of documents, often by preprinting the numbers on the documents, is a proven technique of document control. When the documents are prepared by computer, the sequential numbers are often generated by the computer. Applications often contain software to check that all documents in a series are processed and only once. Reports are printed listing missing or duplicated numbers. The same procedure can be applied in a terminal environment, but the problem is compounded by possible dispersion of documents to so many different physical locations. In this type of environment, sequential transaction numbers are internally generated. This is usually included in the input batch balancing procedures.

3.3 ADMINISTRATIVE CONTROLS

Administrative controls are equally important in batch or interactive terminal environments. However, because on-line systems are usually much larger and have more complex software, certain administrative controls affecting the quality of the software are included in this paper. Four areas--program and data administration, program maintenance, program development, and auditing--are discussed in the following paragraphs.

3.3.1 Program and Data Administration

The importance of control over access to and use of operational programs and data cannot be overemphasized. In an on-line environment without controls, any programmer, at any terminal, authorized or not, would have the capability to call up a program, modify it or execute it, return it to the library, or destroy it. The potential consequences are so catastrophic that all installations have some degree of control. The issues are how much control is required and how it should be achieved.

Our contention is that the most significant single cause of program deficiences resulting in loss of integrity of the data base occurs as a result of situations where programmers are allowed to directly access operational program libraries to fix a "bug" under crisis conditions. No independent or controlled test is made of the modified program to determine if the change had any undesirable effect on the system. The program is run, the data base is changed, and some time later a flaw is discovered. The data base is rarely completely repaired. To avoid this type of situation, the most advanced installations follow rules similar to the following:

- Restrict ability to add, replace, or modify programs in the operational library to a very small group of highly responsible personnel (e.g., two senior people from Quality Control).

- o Require satisfactory acceptance test before adding a program or modification to the operational library.

- o Restrict ability to invoke operational programs to specific individuals on the operating staff.

- o Restrict the ability to update operational data to specific operational programs.

- o Enforce all of the above through rigid administration control techniques.

3.3.2 Program Maintenance

Program maintenance procedures are of equal importance to program administration. Large systems are continually being modified to incorporate changes in requirements, to enhance operating capabilities, or to correct program deficiencies. Every aspect of this process must be controlled, if system integrity is to be maintained. Proposed changes must be thoroughly evaluated and alternative solutions considered before proceeding with implementation. The effect of a change or a series of changes on the overall performance must be thoroughly analyzed to avoid creating latent defects that defeat or detract from the benefits of the change. Once the changes have been incorporated in coding, the system, not just the changed program, must be tested to determine if there are any undesirable side effects from the change. Even after the new version of the system checks out, it cannot be released to the program library until coordinated with other possible installation requirements such as retraining of terminal operators, modification of the data base, installation of new hardware component, etc.

In large systems, several versions of the system will probably be under development at any one point in time. The task of coordinating and

monitoring all of these activities is referred to as configuration management by engineering-oriented people and as change control by most others. At any rate, it includes a significant bookkeeping task. Some very large installations have automated the task. SDC has applied configuration management techniques to a large variety of software projects, ranging from very large command and control systems to moderately sized business information systems. Technical memoranda prescribing procedures for a number of different projects are available as models for establishing a system for an installation.

3.3.3 Auditing

Auditing is the most comprehensive and powerful of all controls. However, it can be relatively expensive and will not be effective if other controls are deficient, particularly if top management does not ensure corrective action by line managers.

Auditing may be performed by external auditors, internal auditors, or by the operating divisions and departments. The principal advantages of external auditors are their independence of the organization being audited and their broader range of experience gained from working with many clients. GAO is operating in the role of external auditor when they audit an agency in the Executive Branch of the U. S. Government. They report to no one, including the President, in the Executive Branch. Disadvantages of external auditors are their cost and limitations, because of cost and time, on the scope of their efforts. If an organization can afford to keep a large group of external auditors around on a continual basis for a variety of auditing purposes, the organization is, in effect, hiring an internal auditing group.

Internal auditors are employees of the organization being audited, but are independent of everyone in the organization except top management. Their

objective is to aid management in achieving the most efficient administration of the business. The advantages of internal auditors are the continuity they provide, their familiarity with the organization's operations, and their immediate availability for a wide variety of auditing assignments as needs dictate. Possible disadvantages include reluctance to prepare a report critical of their top management (or of particular operations because of their personal identification with the operations).

An operating department, particularly the data processing department, may feel the need to audit its own work. Data processing departments often establish a quality control group for this purpose. Such a group can be very effective in monitoring day-to-day operations and in suggesting ways to improve these operations.

Establishment of an operational quality control group in no way precludes the need for an internal auditing group, nor does an internal auditing group preclude the need for an external auditor. The most effective control consists of the proper mix of all three.

4. AUDITING TECHNIQUES AND TOOLS

Auditing techniques involve a variety of procedures to gather evidence to support an opinion as to the fairness of financial statements, the quality of business records, or the efficiency of operations. The general techniques include evaluation of an organization's system of internal control (including tests of compliance and tests of effectiveness), observation or count of assets, inspection of documents--particularly those prepared outside of the organization--making inquiries within and outside the organization, obtaining an expert opinion, and applying other auditing procedures.

The general procedures that an auditor uses to gather evidence remain the same whether the audit is of a manual system, a computerized batch system, or a sophisticated on-line system. The emphasis or degree to which the various procedures are used is vastly different however. In auditing a moderate-size manual system, the auditor may spend little time evaluating internal controls; most of the effort will be in substantive testing of results. In auditing computerized systems, the opposite approach is probably more practical and effective.

This section is concerned with computerized techniques which support any of the general evidence-gathering techniques mentioned above and their potential applicability to the NAVSUP environment. Other techniques of special interest are also presented.

This report is concerned with very large computerized logistics information systems. Therefore, the auditing techniques discussed are for the most part applicable to the evaluation of internal controls, but some, depending on the extent of their use, may be used for substantive testing or even as a processing control.

4.1 COMPUTERIZED TECHNIQUES

The logistics systems of concern are very large communications-based systems with on-line activity and widely dispersed terminals. The volumes of data being processed are very large and it would be extremely difficult to develop an auditing plan without considering the use of a computer. In fact, because of a shortage of resources, the more automated the procedure the better. Of particular interest are any real-time software auditing techniques that are in use or show promise. New or enhanced techniques supporting the more conventional post-processing auditing approach are also of interest, and both approaches are discussed in the following paragraphs.

4.1.1 Real-Time Software Auditing Techniques

Real-time software auditing is defined in this paper as the monitoring, as processing occurs, of internal controls in a computerized system. Monitoring of internal controls is the equivalent of what the auditing profession calls compliance testing. There are two types of compliance tests:

- o Transaction tests which trace a sample of transactions through the system to determine whether controls are being applied as designed.

- o Functional tests which test a particular control to determine its effectiveness.

The techniques discussed in the balance of this subsection apply to one or the other or both of these types of tests.

4.1.1.1 Integrated Test Facility (ITF)

ITF involves establishing "dummy" records or a "dummy" entity which is integrated in the live data base. As the system is operating, fictitious transactions which affect the "dummy" records are entered along with the

actual transactions being processed. The operational program processes the fictitious transactions in the same manner and intermixed with actual transactions.

With the ITF the auditor can design numerous tests to meet a wide variety of objectives. The tests would primarily be transaction tests to detect program deficiencies.

One purpose for which the facility could be used is to determine the impact of program modifications on the overall system and to detect any unplanned change in the performance of the system. For this purpose a standard set of test transactions would be developed. The transactions would be run every day (or every time the system was run) and the results automatically compared with the standard expected results. Any differences would indicate a change in the performance of the system and would require evaluation of the extent and consequences of the differences and investigation to determine the causes. This technique would be useful to internal auditors and to a data processing quality control group.

The technique could also be used to further test specific controls or groups of controls, where there are indications of trouble. More extensive sets of transactions designed to probe the specific areas would be developed and run.

The ITF technique has two major drawbacks. First, the effect of the dummy transactions must be neutralized. Goods cannot be shipped, orders cannot be placed, checks cannot be issued, etc. because of fictitious transactions. If the test is to be worth the effort, all aspects of the system must be tested using the operating program <u>without</u> modification. If the programs are modified to process the test transactions differently, then the test is no longer valid. Thus the effects must be removed after the processing has been completed, including the production of any outputs.

The second problem involves processing tests in an environment where live data bases exist. Test transactions are designed to probe for flaws, and it is impossible to predict what will occur when a flaw occurs. Thus, there is the possibility that live records will be erroneously changed or destroyed.

The alternative to this facility is a rigorously enforced, comprehensive system testing policy where all programs and program modifications must pass an acceptance test before the program/program revision is included in the operational library. The same or even more exhaustive tests would be run by the systems test group but not in an environment with the live data base. The advantage of the system test approach is that live data is not exposed to the vagaries of some latent defect. The disadvantage is that it may require more resources than are available.

Some reasonable amount of system testing of program modifications is essential if any degree of system integrity is to be preserved. Use of the ITF to supplement this and to provide auditors a means of assessing the adequacy of the system testing makes a powerful combination of controls.

Thus, efforts to develop a practical way to minimize the problems associated with the ITF (i.e., removal of effects and possible impacts on live files) could result in a valuable tool being available to auditors.

4.1.1.2 Parallel Simulation

Parallel simulation consists of the programming of a separate application system that performs the same functions as the application system being audited. The parallel simulation need not reproduce the application system in full. The auditor selects data and functions on the basis of their audit significance (relationship to materiality). Furthermore, simulated applications can be programmed using a general-purpose auditing language because

operating efficiency, sophisticated controls, recovery procedures, etc. are not major considerations. Thus, because only a reasonable subset of all functions need be programmed, because programming aids to increase programming productivity can be used, and because only a sample of the overall volume need be processed, parallel simulation is more practical than the name might imply.

The important characteristic of parallel simulation as an audit tool is that independent processing of relevant data takes place. The processing does not have to occur on the same computer as the actual live processing, so it can be done in a manner which in no way interferes with normal operations.

The parallel simulation technique can be used by auditors to meet a number of objectives, primarily related to functional testing. One method of testing the effectiveness of controls is to test the quality of the output. If the output is correct, then the assumption is that the control(s) worked. This method can be used for certain controls.

If there is an extremely critical element in the application, the technique can be used as an operating control. The simulation would process the critical data in parallel with the operating programs, and results would be compared at the end of an operating period. If there is a discrepancy in the results, immediate corrective action can be initiated.

The technique can also be utilized by the system test and quality control teams in predicting the results of their tests. With large, complex systems, the task of predetermining results for a large test is almost impossible without computerized assistance. The simulation can provide this assistance.

The software tool required to implement this technique is a high-order-language processor similar to some of the general-purpose audit programs currently available. The major objective in the design of the language is ease of programming. A non-EDP person such as an auditor should be able to become reasonably proficient at developing simulation programs after several days of training and a week or two of practice.

The packages currently available are primarily for IBM 360/370 configurations. Most are designed following a report generator concept where data is extracted from files and manipulated to produce reports. Simulation of updating is possible but somewhat limited, and not as straightforward a programming task as for reports. No existing general-purpose audit software language allows the submission and processing of inputs via an on-line device. Access to records stored under data base management systems is an issue which needs to be addressed.

4.1.1.3 On-line (Security) Monitoring

A concept that has considerable appeal in the intelligence community is an on-line monitoring station to assist the ADP System Security Officer (SSO) with those monitoring functions for which he or she is responsible. In the most simplified of terms, the function of the station is to monitor computer activity to detect actual and/or attempted security violations, report them in real-time to the SSO's terminal, and provide the SSO with the capability to initiate a countermeasure(s) such as locking out a terminal or even, in the extreme, shutting down the computer.

A test of this concept was initiated (by the WWMCCS ADP Directorate) by beginning the development process for a prototype station. One of the original concepts in the Feasibility Analysis was that a microprocessor-based hardware system be used, and that little or no additional workload be placed on the mainframe.

The project was abandoned after the design review stage for several reasons, including the fact that microprocessor equipment was not proposed and it was necessary under the approach to place significant additional workload on the host (mainframe) computer. Furthermore, addditional study of the problem indicated that the original requirements included functions of little value or of no concern to the SSO. Also, the SSO would have been presented with raw data for his or her analysis, rather than an indication of a problem deducted from computerized analysis.

The concept of real-time monitoring without interfering with the host computer is being successfully applied, using microprocessors, in computer performance monitoring and communications monitoring applications. The technology appears to be there, if there is a requirement of this nature in logistic systems. However, there are valuable lessons to be learned from the WWMCCS experience, not the least of which is to be sure not to overstate the requirements because of technical enthusiasm.

A variation on the monitoring concept which might have applicability in the logistics environment is to use the monitoring computer as an on-line enforcer of certain controls. For example, assume that only certain employees are authorized to enter requisitions for certain material, and that an identity check is to be made on the requisitioner before entering his request. The monitoring station could detect when such requisitions were being entered, randomly select some for audit, and request additional information from the sending terminal that would indicate whether controls such as the identity check were being followed. The knowledge that such monitoring was occurring would tend to increase compliance with the control procedures. However, such a technique may be considerably in excess of that required for the situations with which this study is concerned. A detailed analysis of the problem is required to determine its exact nature, extent, and cause.

4.1.2 Conventional Processing Auditing Techniques

The amount of data that an auditor has to deal with when auditing computerized information systems is so great that computerized assistance is a necessity. The auditing procedures where computerized assistance is most helpful involve compliance testing and substantive testing. The software aid that the auditor requires for this task is a general-purpose audit program. This is a slightly less sophisticated version of the auditing language required for the parallel simulation approach discussed in paragraph 4.1.1.2. There are a number of packages on the market. It is beyond the scope of this report to perform a comparative evaluation of the packages, but Appendix B, extracted from Computer Fraud and Countermeasures by Kraus and MacGahan, lists the attributes of fifteen packages.

The more important capabilities to include in such a package are:

- Ability to access a variety of file structures, including DBMS structures on various media (e.g., tape and disk).
- Ability to handle a variety of data such as character, packed decimal, and binary.
- Ability to perform basic arithmetic operations.
- Ability to perform the logic function incorporated in Boolean algebra.
- Ability to sort, merge, and consolidate records.
- Ability to compare and update multiple files.
- Ability to format reports.

Generalized report-generation packages have most of these capabilities to one degree or another. In fact, many audit programs are based on report generation, with specialized auditing routines (e.g., random-number generators, and statistical routines) added. The requirement of NAVSUP auditors for such a package has not been evaluated as a part of this study.

4.2 OTHER (NON COMPUTERIZED) TECHNIQUES

Although it has been mentioned at several points throughout this report, the systems approach to establishing a control and audit program is important enough to warrant further emphasis. Auditing is an integral part of the systems approach. Of necessity, auditing's role must emphasize evaluation of the system of controls. This evalution must start with a review of the requirements specifications and continue with review throughout the life cycle of the systems.

Analytical techniques for evaluating the system of controls have been developed. These techniques, which are briefly described in paragraph 2.3.1, are particularly applicable during the design and development phases of the system life cycle. These techniques are relatively new and could possibly be refined and tailored to be more suited for logistics information systems.

5. FINDINGS, CONCLUSIONS, AND RECOMMENDATIONS

This section presents the findings, conclusions, and recommendations resulting from this study.

5.1 FINDINGS

The study resulted in a number of findings which are presented in summarized form in this section and in detail in Sections 1 through 4. The findings were:

a) The Navy believes that it is experiencing significant losses due to inefficient operations caused by erroneous inventory records and misappropriation of Navy property. The erroneous records may be caused by undetected program deficiencies as well as by incorrect or omitted input transactions.

b) The auditing and computer security communities believe that inadvertent errors, program deficiencies, and fraud are all areas of concern and, when considered together, as they should be, constitute one of the major, if not the major, problems in information processing today.

c) The auditing and computer security communities hold that THE GREATEST SOURCES OF COMPUTER LOSSES ARE THE RESULT OF INNOCENT ERRORS AND OMISSIONS.

d) The study supports the contention that basically the same controls are applied to protect against inadvertent error, program deficiencies, and intentional misuse (fraud).

e) Auditing cannot be considered independently of controls because, in large systems, evaluation of controls is the only practical way that auditors have of evaluating the reliability of results.

f) The auditing and computer security communities were unanimous in their contention that the most effective approach to solving computer control and audit problems requires use of systems engineering methodology. All aspects of the problem must be considered as a whole and an integrated control program developed. Major elements of such a program are:

- o Management participation.
- o Risk analysis.
- o System of controls.
- o Adequate audit program.

g) An assessment of risk is required to select the appropriate degree of controls for any given system. Because various threats create varying degrees of exposure, and because there is a choice of controls to neutralize the threats, a risk analysis is required to determine how to minimize the risk within the financial and technical resources available.

h) Several techniques for risk analysis and evaluation of controls have been developed. All have varying strengths and weaknesses in various environments. Enhancements could be made to tailor a combination approach to the logistics problem.

i) Knowledge of the nature and extent of problems likely to occur at an installation or with a system is required to perform an adequate risk analysis. The nature and particularly the extent of the problems in the NAVSUP environment have not been clearly defined.

j) The auditing and computer security communities were unanimous in their contention that auditing has a role in the design and

development of systems. Practical procedures for evaluating controls require auditors to evaluate at every stage of development, from requirements specifications on. Retrofitting of controls is costly and often ineffective.

k) The architecture of the system influences the design of the system of controls. The architecture may eliminate the need for some controls and add the requirement for others. Increased capability and cost-effectiveness of equipment in systems using remote terminals have expanded possibilities for improving input control techniques while adding data transmission concerns.

l) Some general controls such as access controls are provided by vendor system software, but they may have to be enhanced for specific applications. In any event, there are always significant controls that are application dependent (e.g., editing and validating controls).

m) Advanced on-line systems may require changes or permit enhancement in the conventional control areas of input batch control, access control, file balancing controls, editing and validating controls, input to output controls, and document controls.

n) Generalized audit procedures for gathering evidence are the same regardless of the type of system. However, the environment influences techniques that can be used to carry out a procedure. The increased capability of equipment has made real-time software auditing more of a practical possibility.

o) Several real-time software auditing techniques show promise, but all require additional work to overcome existing drawbacks.

5.2 CONCLUSIONS

Computer control and audit is the essence of management control in any modern organization of any size. The consequences of lack of control in daily operations can be more devastating than some catastrophe such as a fire. Security, in the sense of protection from hazards and perpetrators of fraud, sabatoge, etc., is a part of the overall problem, but far from the only problem or even the most significant part of the problem. Reliability of the records maintained and the outputs produced are usually vitally important to the organization and, therefore, the problem should rank near the top of management concerns.

The problem of computer control and audit is almost certainly serious enough to warrant a research and development effort to find generalized aids to assist in its solution. However, the exact nature and extent of the NAVSUP problem needs to be probed further to determine which aspect of the problem offers the most potential for gain. If the assumption is valid that the quality of inventory records adds or detracts from the quality of service provided to the Fleet and can actually affect Fleet readiness, then support emanating from the highest echelons of commands should be forthcoming.

Several components of an overall computer control and audit program would benefit from a research and development effort. There are risk analysis and control evaluation techniques developed in recent years that can be enhanced and tailored for logistics systems. There are control problems, handled in a more or less standard fashion in conventional systems, that require reanalysis and the development of generalized techniques for an interactive environment. Real-time software auditing techniques require considerably more development to make them a useful tool in a modern logistics system environment. Standards are needed for design and development.

In summary, with appropriate management support, a needed research and development effort concerning computer control and auditing problems can be formulated.

5.3 RECOMMENDATIONS

The following activities are considered to offer the most potential for benefit from research and development efforts.

5.3.1 Risk Analysis/Control Evaluation Technique Development

The purpose of this effort would be to develop control evaluation and risk assessment techniques specifically designed for logistics systems. The first step in the process would be a study to determine the exact nature and extent of NAVSUP's computer control and audit problem. By accumulating statistics on items such as the number of inventory adjustments, the number of reversal transactions, number of vendor complaints, number of user complaints, plus interviews with appropriate personnel, an opinion would be formulated as to the reliability of the records, the trend of the reliability, causes for any change, and impact of the reliability on overall performance.

This information would be used as the basis for determining causes of exposure and estimating exposure in risk analysis and control evaluation procedures. The various techniques of quantification and rating used by existing approaches, such as those described in Section 3, would be analyzed and the most appropriate chosen for logistics systems. In this manner, a new technique combining the features of the other approaches most suitable to logistic systems would be developed.

5.3.2 Real-Time Software Auditing - Language Processor

This effort would be divided into two parts: requirements analysis and conceptual design, and design and development of an audit language processor. The requirements analysis phase would involve determining the capabilities that such a language should possess. This would be based on an analysis of existing auditing language processing packages and a determination of their advantages and shortcomings. During this phase, a determination would be made as to whether an existing processor would be satisfactory, whether

modification would be required, or whether an entirely new version would be required. Equipment required to run the language processor would be considered.

The second phase, assuming it were required, would be the design and development of the approved conceptual design.

5.3.3 Real-Time Software Auditing - Integrated Test Facility (ITF)

The ITF has drawbacks, as discussed in Section 4 of this report, because live records may be modified with fictitious transactions. This research effort would be devoted to finding a generalized way to eliminate the effects of ITF processing automatically, without modifying the application programs, and without utilizing an undue amount of mainframe computer time.

5.3.4 Real-Time Software Auditing - On-Line Monitor

This effort would involve developing a concept of selectively auditing the application of input controls, particularly identification, authorization, and approval procedures, in a real-time on-line mode.

5.3.5 Controls - Generalized Techniques for Interactive Systems

Interactive systems require different approaches than batch systems to prevent input errors, lost transactions, duplicate transactions, etc. Techniques are suggested in Section 3. The effort would be to study this problem in depth and to develop techniques, including generalized software frameworks which could be incorporated in on-line logistics systems.

APPENDIX A

REFERENCES

Date Published	Document	Author/ Publisher	Comments
1979	Security: Checklist for Computer Center Self-Audits	Peter S. Browne AFIPS	Checklist which implies certain controls and "how to" covering 10 aspects of security, including Security Audit and Applications. Also, introductory paragraphs giving rationale for the controls. No specific examples of frauds or controls.
Sept. 1978	Security for Computer Applications	U.S. Dept. of Commerce, NBS	Accidental vs. deliberate p.7. Generalized description of major types of controls, including some dynamic. Conceptual discussion of selection of controls, planning for security during initiation, building in security during development, preserving security during operations.
1978	Internal Control for Computerized Systems	Jerry Fitzgerald E.M. Underwood, P.O. Box 4295, San Leandra, CA 94579	Correlates hundreds of specific controls, with assets being protected and possible exposures. Organized by 9 components of computer system.
Feb. 1980	Audit and Evaluation of Computer Security II: System Vulnerabilities and Controls (Proceedings of NBS Invitational Workshop Nov. 1978)	U.S. Dept. of Commerce, NBS	See a-h on following pages.

Date Published	Document	Author/ Publisher	Comments
	a) Managerial and Organizational Vulnerabilities and Control - Staff Level	Donald L. Scantlebury, Chairperson NBS	Conceptual discussion of organizational structure, policy and control standards, allocation of resources, and reporting.
	b) ditto a), Line Level in Data Procesing	Richard D. Webb PM&M	Conceptual discussion of the data processing entity and its more important components of operations, data administration, applications, internal control, and hardware support.
	c) ditto - Line Level - General	Richard J. Guiltinan	Conceptual discussion of an organizational from the viewpoint of a) operational divisions, b) information systems project management, c) data handling, d) application program development, e) data communications, and f) program validation.
	d) Terminals and Remote Peripherals	William Hugh Murray	Detailed discussion of terminal vulnerabilities and the controls that can be used as countermeasures.
	e) Communications Components	Jerry Fitzgerald	Detailed discussion of communications vulnerabilities and the controls that can be used as countermeasures.

Date Published	Document	Author/ Publisher	Comments
	f) Processors, Operating Systems, and Nearby Peripherals	Theodore Lee	Conceptual discussion advocating certain policies, in particular development of an evaluation/accreditation process. Cites lack of security policy as biggest problem.
	g) Applications	Sheila Brand	Discusses three approaches for providing definitive lists of controls for the deterrence of vulnerabilities. a) Matrix approach b) NBS system control objective approach c) Transaction flow approach
	h) Data Base Management Systems	Hart Snive	Conceptual discussion of multi-level security issues and control objectives with recommendations.
1975	Security Monitoring Concept Formulation	DCA	Presents overall concept of an on-line station to assist Security Officer to monitor computer activity for purpose of detecting security breaches or attempted breaches and providing Security Officer with an on-line means of taking remedial action.

Date Published	Document	Author/ Publisher	Comments
Sept. 1976	Prototype WASSO Station Functionality	DCA CCTC	Elaborates on Security Officer station concept and describes functions that should be capable of being performed through the station.
May 1978	Security and Reliability in Electronic Systems for Payments	Bank for International Settlements	Discusses design requirements for security in EFTS. Includes list of over 350 controls. Presents techniques for evaluating controls using the 350 questions and a rating matrix.
Jan. 1978	An Analysis of Computer Security Safeguards for Detecting and Preventing Intentional Computer Misuse	Brian Ruder and J. D. Madden NBS	Includes descriptions of approximately 100 controls involving various combinations of procedures, software and hardware. Includes 16 in the credit category of which 15 involve software to some degree. Four involve embedded software.
1979	Computer Fraud and Countermeasures	Krauss and MacGahan Prentice-Hall	Includes descriptions of actual cases, detailed discussion of administrative and internal controls, security controls, communication and database controls (includes real time surveillance) and AUDIT FUNCTIONS and TECHNIQUES - during development, application controls, financial records. Audit management tools and techniques, application audit T&T, service center T&T, system develop T&T. Correlates

Date Published	Document	Author/ Publisher	Comments
	Computer Fraud and Countermeasures (Cont'd)		common methods of fraud with appropriate controls. Control vs. cause matrix. Definitions of 65-80 application controls. Software aids, evaluation 15 audit packages.
1980	Demonstrating Security for Trusted Applications on a Security Kernel Base	Ames & Keeton-Williams Mitre Corp.	Technical discussion of problem of interest to intelligence community.
1977	Principles of Auditing	Walter B. Meigs, E. John Larsen, Robert F. Meigs, Richard D. Irwin, Inc.	Conventional audit text.
1978	Computer Control & Audit	William C. Mair, Donald R. Wood, Keagle W. Davis, Touche Ross & Co.	In depth discussion of computer control and audit in three major categories -- applications, development, and information processing facility (operations).

APPENDIX B

AUDIT SOFTWARE PACKAGES

	A	B[15]	C	D	E[16]	F	G
Vendor:	Arthur Anderson Company	Computer Audit Systems	Callinane Corp.	Ernst & Ernst	Citibank, N.A.	Informatics,Inc	Program Products Inc.
Package:	AUDEX 100	CARS 2	EDP-Auditor	AUDITRONIC 32	PROBE	MARK IV Auditor	AUDIT ANALYZER
Trial Period	Demonstration	90 days	3 months	N/A	N/A	N/A	60 days
Trial Cost	Free	N/A	$1,500	N/A	N/A	N/A	$500
Price - Purchase	Lease only	$12,500	$15,000	N/A	$12,000	$12 to $18 M	$15 - $16 M
Price - Lease/Year	$7,500 perpetually; per year: $2,500/1, $1,000/2+	Installment 50%	$15,000/1 $2,000/2+	$2,400	N/A	$1,395	$7,700/'
Price - Maintenance	Incl.	(2)	(2)	Incl.	N/A	Incl.	(2)
Price - Installation	Incl.	N/A	Incl.	None	Incl.	Incl.	Incl.
Price - Training	Incl.	N/A	Incl. but travel ex.	$800 and travel exp. (9-day course)	Incl.	Incl.	Incl.
Man-hours of Training (Min.-Minimum number of hours)	25	40 (Min.)	35 (Min.)	64	21	16	40
Manuals Supplied	Incl.	10 Incl.	2-installation 2-sys. 10-user Incl.	1/User Incl.	Incl.	Incl.	10 Incl.
Forms Supplied	Starter set incl.	20 sets	Initially yes	Starter set yes	Initially yes	Initially yes	10 sets yes
Consultation Service	Incl.	Yes	Incl.	Maintenance/free, spec. applications/per diem	Incl.	Incl.	Telephone/free, on site/per diem $300
User's Group Meetings	No	$60/Year	Yes	No	Yes	Yes	Yes
Number of Users	N/A	60 & 100 installations	400(7)	35 +	85	400(9)	220
Years in Use	6[3]	7	5[3]	2	6	10	2[3]
Age of Supplier	>10	7	8	>10	>10	>10	5
Accessibility of Supplier	International	Very	Very	Very	Very	Very	Moderate
Periodic Package Updates (Current-New Modification to be announced)	Current	2 free years	Semiannual incl.	Current + / free	Yes	Current	1 to 2 / year
Number of Coding Sheets (av.) per request	6-10	2-16	2-4	5-7	1	1-6	1
PACKAGE REQUIREMENTS:							
Hardware	360/370	360/370(12) + others + European	AUDAX/IBM 360/370	360/370	All	360/370 + others	360/370
Special Hardware Options	None	None	None	None	None	None	Floating point
Core	80-140K	64K	80K	100K	50-64K	64K	80-120K
Operating Systems	DOS/OS/VS	Various	DOS/VS	Various OS/DOS	Std.	DOS/OS/VS	DOS/OS/VS
Sort Utilities	No	Incl.	IBM SORT	Incl.	Incl.	IBM SORT	Incl.
Output Utilities	No	System	System	System	System	System	System
Dedicated System	No	No	No	No	No	No	No
Runs in Multiprogramming Environment	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Runs in Time-Sharing Environment	Yes	Yes	Yes	Yes , but not interactive	Yes	N/A	Yes
Self-Generated J.C.L.	No	No	No	Yes	No	No	No
Written in (language)	BAL	(4)	BAL	(4)	COBOL/BAL	MARK IV	BAL
Special Program Language (MACRO)	No	No	No	No	No	No	No

H	I	J	K	L	M	N	O
Informatics,Inc.	Touche Ross & Co	U.S. Department of Commerce	Computer Audit Systems	Coopers & Lybrand	Dylakor Software Systems, Inc.	Computer Audit Systems	Peat, Marwick, Mitchell & Co.
SCORE IV	STRATA	AUDIT	CARS 3	Audit PAK II	Dyl-280	SYSAUDIT	P M & M Z170
30 days	N/A	No	90 days	N/A	30 days	90 days	None
$1,000	N/A	N/A	N/A	N/A	Free	$430	N/A
$14,000 (1)	$3,800 (average) perpetual lease	$97	$12,900 + interfaces	Lease only	$8,000	$2,000-$4,700	None
$6,000/1	N/A	No	Installment	$1,000 1st yr. & $500 subt.yrs.	N/A	2 year-6% of total per month Long Term-installment 50%	None
(2)	Incl.	No	10% after 2 yrs.	(2)	W/purchase -- $175 per yr. W/lease -- no charge	10% after 2 years	None
Incl.	Incl.	Users	N/A	Travel exp. only	None	$100 plus cost of disk pack	None
Incl.	2 students incl.	No	N/A	Variable	$250 per day if needed	Optional $200/ day plus expenses	Depends on amt. of trng. req; is chgd. at stand. rates of instr.
24-32	40	No	40	15 hours	1	Optional	24 hrs. classroom instr. followed by hands-on proc. that varies with skills of participant.
Incl.	2 incl.	$4.25/2	10	Yes	1 set	5	1 per participant in training course
Initially yes	Initially yes	No	Pods	Yes	1 set	Pods	Coding forms
Incl.	Incl.	No	Yes	Yes	Incl.	Yes	Yes, technological and use to most audit object.
Yes	No	No	$50/year	None	None	Yes	No
25(6)	170	N/A	100 & 300 installations	N/A	$1,000 +	19	Over 200
7(3)	8	N/A	7	1	4 +	1	Six
7-10	>10	>10	7	>10	8 +	7	>10
Very	Very	N/A	Very	International	Phone/mail	Very	Very
$1,000/2nd year on	Yes	None	2 yrs. free	Yes	$15 per lease	2 years free	Cost of reproducing tape
1	7	N/A	2 - 16	7	1 sheet/4 sides	2	5-7
360/370 + others	IBM 360/370 Burroughs 2500 to 4700 and 676 to 7700; IBM Systems 3 (see note 11)	360/370	360/370 + others + European(13)	360/370	360/370	IBM SYS/3	IBM 360/370 Burroughs 2500 thru 4700
None	None	None	None	None	None	None	None
88K	65-100K	Equal compiler	118K	DOS-50K,OS-75K	50K	16K	64K
OS/VS + others	DOS/OS/VS	Various	OS/VS/DOS	OS/VS/DOS	All	N/A	OS/DOS/MCP
Incl.	IBM SORT	User SORT	Incl.	Yes	IBM & DYLSORT	Mfg.	Mfg.
System	System	System	System	No	No	None	None
No	No	N/A	No	No	No	No	No
Yes	Yes	N/A	Yes	Yes	Yes	Yes	Yes
Yes, with TSL opt	Yes	N/A	Yes	Yes	Yes	No	Yes
$15,000 option	Yes	No	No	For compilation only	Yes	No	No
(4)	COBOL/BAL	BASIC and COBOL	(4)	BAL generates COBOL	Assembly load and go	SYS/3 Assembler	COBOL
No	No	BASIC	No	Yes	Yes	No	No

	A	B(15)	C	D	E(16)	F	G
Vendor:	Arthur Anderson Company	Computer Audit Systems	Callmane Corp.	Ernst & Ernst	Citibank, N.A.	Informatics,Inc.	Program Products Inc.
Package:	AUDEX 100	CARS 2	EDP-Auditor	AUDITRONIC 32	PROBE	MARK IV Auditor	AUDIT ANALYZER
ABILITIES:							
Can Handle Data Base Structures	Yes (6)	Yes (6) $1.5 to $4M	Yes (6) $8,000 per	Yes (5)	Yes (5)	Yes	Yes (6), $4-5,000 per interface
Contains User Exits	Yes	Yes	Yes	Yes	Yes	Yes	Yes, 70
Min/Max Input Files	1-2 (match, merge)	1-2	1-256	1-2	User control	1-11	No limit, 1-6 drives
Min/Max Output Files	0-6	1-2 with confirmations	0-100	0-98	User control	1-13	No limit, 0-6 drives
Max Reports on One Pass of File	6	11 plus confirms	100	98 plus 5 Frequency distributions	50	255	80
Source Program Utility (tape, disk, card, CRT)	Not CRT	Not CRT	Yes, incl. CRT W. one-equal MACRO	Not CRT	Not CRT	Not CRT	March 1977
Output Utility (tape, disk, card, CRT, print)	Not CRT	Not CRT	Yes	Not CRT/Card	Not CRT	Yes, CRT w/TSO	Not CRT
Degree of Required Programming Knowledge	Min.	Min	None	None	Min.	Min.	Min.
Can Be Catalogued on-Line	Yes	Yes	Yes	Yes	Library only	Yes	Yes
Is Package Portable	Yes	Yes	Yes	Yes	Yes	Per contract	Yes
Only Selected Modules Read in * = Yes	Yes	Generates COBOL*	Yes	Generates COBOL*	Overlayed *	Yes	Yes
Compile and Diagnostic Routines	Yes	Yes, program + COBOL	Generates machine codes directly-Yes	Yes, 2	Not at user level	Yes	Yes
Option to Limit Record Selection for Tests	Yes	Yes	Yes	Yes	Yes	Yes	Yes, read/ select
Conditional Changes on Extracted Fields	20 Compound	Essentially no limit	No limit	No limit	50	Yes	No limit
Max. Number of Logic Levels for Selection	9	99	No limit	9	Data controlled	9	No limit
I/O CAPABILITY: FILE STRUCTURES:							
Tape/Disk-Sequential	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Tape/Disk-Index Sequential	Yes	Yes	Yes	In only	Yes	Yes	Yes
Tape/Disk-Random Organization	With user exits	Yes	Yes	In only	Yes	Yes	Yes
Tape/Disk-Fixed Record Length	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Tape/Disk-Variable Record Length	Yes	Yes	Yes	In only	Yes	Yes	Yes
Tape/Disk-Mixed	Yes	Yes	Yes	With exits	Yes	Yes	Yes
Tape/Disk-Variable Number Fixed Length Trailers	Yes	Yes	Yes	With exits	Yes	Yes	Yes
Tape/Disk-Blocked	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Tape/Disk-V/S Randomized Files	In only with ISAM interface	Yes	Yes	In only with ISAM interface	Yes	Yes	Yes
File/Record Labels-Standard	Yes	Yes	Yes	Yes	Yes	Yes	Yes
File/Record Labels-User	In only	Yes	Yes	In only	Yes	Yes	Yes
File/Record Labels-None	In only	Yes	Yes	In only	Yes	Yes	Yes
Min/Max - Field Lengths (bit - byte)	0-99	Mfg.	1-999	1-99 in 0-30 out	Std.	IBM conventions	1-256
Min/Max - Record Lengths (bit - byte)	16K	Mfg.	1-Inf.	1-16K in Inf. out	Std.	IBM conventions	No limit
Min/Max - Block Sizes (bit - byte)	16K	Mfg.	1 -Inf.	1-16K in Inf. out	Std.	IBM conventions	No limit
Min/Max - File Lengths	No limit	Mfg.	No limit	No limit	Std.	IBM conventions	No limit
Maximum - SORT Levels	IBM SORT limit	3	20-46	IBM SORT limit	50/run, 6/report	9	30

H	I	J	K	L	M	N	O
Informatics, Inc.	Touche Ross & Co.	U.S. Department of Commerce	Computer Audit Systems	Coopers & Lybrand	Dylakor Software Systems, Inc.	Computer Audit Systems	Peat, Marwick, Mitchell & Co.
SCORE IV	STRATA	AUDIT	CARS 3	Audit PAK II	Dyl-260	SYSAUDIT	P M & M 2170
Yes (5)	Yes	No	Yes, $1.5 to $6M	Via user exit	TOTAL	No	Yes
Yes, 90	Yes	N/A	Yes	Yes	Yes	Yes	Yes
1-8	1-6	N/A	1-7	1-2	1-4	1-2	1-2
0-8	>10	N/A	1-2 with confirmation	0-9	1-4	1-3	Unlimited
90	20	N/A	11 + confirmation	9	1	3	5
Not CRT	Not CRT	Not CRT	Not CRT	N/A	Yes	N/A	No
Not CRT	Not CRT	Not CRT	Not CRT	N/A	Yes	N/A	N/A
Min.	None	Min.	Min.	None	Min.	None	None
Yes	Yes	No	Yes	Yes	No	No	Yes
Per contract	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Generates COBOL*	Yes	N/A	Generates COBOL*	Generates COBOL*	Yes	N/A (load and go)	N/A (COBOL program executed)
Yes, 2	Yes	N/A	Yes, program + COBOL	Yes	Yes	Yes	Yes
Yes	Yes	N/A	Yes	Yes	Yes	Yes	Yes
90	No limit	N/A	Essentially no limit	N/A	Yes	No	Unlimited
Within level supported by ANS/COBOL	No limit	N/A	99	N/A	No limit	No limit	No limit
Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Yes	Yes	N/A	Yes	Yes	Yes	Yes	Yes
Yes	Yes, with exits	N/A	Yes	Yes	Yes	Yes	No
Yes	Yes	N/A	Yes	Yes	Yes	Yes	Yes
Yes	Yes	N/A	Yes	N/A	Yes	Yes	Yes
Yes	Yes	N/A	Yes	Yes	Yes	Yes	Yes
Yes	Yes	N/A	Yes	Yes	Yes	Yes	Yes
Yes	Yes	N/A	Yes	Yes	Yes	N/A	No
Yes	Yes	N/A	Yes	Yes	Yes	Yes	Yes
Yes	Yes	N/A	Yes	Yes	Yes	No	Yes
Yes	Yes	N/A	Yes	Yes	Yes	Yes	Yes
COBOL limit	1-256	N/A	Mfg.	1-999	IBM Conventions	Mfg.	Mfg.
COBOL limit	1-600	N/A	Mfg.	1-999	IBM Conventions	N/A	N/A
COBOL limit	Std.	N/A	Mfg.	1-999	IBM Conventions	Mfg.	Mfg.
No limit	No limit	N/A	Mfg.	No limit	IBM Conventions	No limit	No limit
9	5	N/A	Input at 3 levels, 3 internal	9	IBM Conventions	5	Use vendor's utilities

	A	B (15)	C	D	E (16)	F	G
Vendor:	Arthur Anderson Company	Computer Audit Systems	Callimane Corp.	Ernst & Ernst	Citibank, N.A.	Informatics, Inc.	Program Products Inc.
Package:	AUDEX 100	CARS 2	EDP-Auditor	AUDITRONIC 32	PROBE	MARK IV Auditor	AUDIT ANALYZER
Maximum - SORT Key Size	IBM SORT limit	15	No limit	IBM SORT limit	12 bytes	IBM SORT limit	254
Maximum - Control Break Levels	5	3	20-45	3 merge, 1 summary	50/run, 6/report	9	9
Maximum - Accumulator Buckets	10/input, 20/report	15 plus control	900 +	40/run, 20/report	300/run, 6/report	No limit	100/report
Contains a Table-Driven Interpreter	Yes	No	Yes	No	N/A	Yes	No
Size * = Not a Limiting Factor	*	N/A	*	N/A	N/A	*	N/A
Dynamically Allocates Core	DOS, yes	Yes	Yes	N/A	N/A	Modified yes	Modified yes
Compresses/Decompress File and Record Lengths	No	Through user code	N/A	With user exits	No	Option	No
Must Input File Be Presorted	No	No	No	No	No	No	No
Must Input File be Predefined in a Glossary	No	No	No, however, generally done	No	No	Yes	Yes
Must Input File Be Reformatted	Yes, internally	No	No	Internally for output	No	No	No
Must Input File Be Free of Field Errors	No	Auto-Edit	No, but data exceptions could occur	No	No, but may cause data exceptions	No	No
Has Automatic Line-Folding Capability	No	No	Yes	Yes	User coded	Yes	Yes
Has Automatic Control/ Grand Totals	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Has Automatic Report Formatting	No	Partial	Yes	Yes	Yes	Yes	Yes
Has Automatic Page Counts	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Has Automatic Carry-Forward Totals	No	Yes	Yes	No	Yes	Yes	Yes
Has Special Print-Suppress Options	Yes	Yes	No limit	Yes	Yes	Yes	Yes
Maximum Calculations Per Field	40	No limit	No limit	No limit	No limit	No limit	No limit
Can Flag Input Errors Without Halts	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Can Compare Total Field to Detail Fields on DASD Files	No	Yes	Yes	No	No	Programmable via MARK IV	Yes
Has Option to Check Parameters via Intermediary Totals	Yes	Yes	Yes	No	User routine	Yes	Yes
Has Option to Generate Test Data with Flags	No	Yes	Yes	N/A	No	No	Yes
Has Option to Print Confirmation Requests	Yes	Yes	Yes	N/A	Yes	Yes	Yes
Maximum Fields Extractable per Record	60	No limit	No limit	90 in 12 numeric out 15 alpha out	N/A	No limit	No limit
Maximum Number of Aging Levels	8	7	No limit	9	5	20	6
Can Simulate an Application Program for Timing Tests	No	Yes	Yes	No	No	Yes	Yes
STATISTICAL SAMPLING CAPABILITIES:	Limited	Yes	Elaborate	Yes	Limited	Extensive	Limited
Can Handle Known and Unknown Universe	Yes	Yes	Yes	N/A	N/A	Yes	Yes
Generates Minimum of 3 Random Starts	No(14)	1 + user code	Yes	Yes, 10	User specified	Yes, 9	Yes
Contains Random Number Generator	Yes	Yes	Yes	Yes, 10 seeds	Yes	Yes	Yes

H	I	J	K	L	M	N	O
Informatics, Inc.	Touche Ross & Co.	U.S. Department of Commerce	Computer Audit Systems	Coopers & Lybrand	Dylakor Software Systems, Inc.	Computer Audit Systems	Peat, Marwick, Mitchell & Co.
SCORE IV	STRATA	AUDIT	CARS 3	Audit PAK II	Dyl-260	SYSAUDIT	P M & M 2170
Operating system limit	IBM SORT limit	N/A	15	256	IBM Conventions	15 bytes each	Use vendor's utilities
6	6	N/A	3	9	7	5	4
20	15	N/A	20 + control	No limit	Unlimited	10	30
Yes	Yes	N/A	No, but possible	No	N/A	Yes	Yes
*	*	N/A	N/A	N/A	N/A	Depends on available core	Depends on available core
No	No	N/A	Yes	Yes	Yes	Yes	Yes
No	No	N/A	Through user code	No	Yes, optional	No	Yes
No	No	N/A	No	No	No	No	No
No	No	N/A	No	No	No	No	No
No	No	N/A	No	No	No	No	No
Yes	No	N/A	Auto-Edit	Yes	No	Automatic Edit	Automatic edit
No	No	N/A	No	No	No	No	No
Yes	Yes	N/A	Yes	Yes	Yes	Yes	Yes
Yes	No	N/A	Partial	Yes	Yes	No (partial)	No
Yes	Yes	N/A	Yes	Yes	Yes	Yes	Yes
Yes	No	N/A	Yes	Yes	Yes	No	Yes
Yes	No	N/A	Yes	No	N/A	Yes	Yes
No limit	No limit	N/A	No limit	No limit	No limit	No limit	No limit
Yes	Yes	N/A	Yes	No	Only totalled	Yes	Yes
With user exits	Yes	N/A	Yes	Yes	Yes	No	No
Yes	Yes	N/A	Yes	Yes	Yes	No (future)	Yes
No	No	N/A	Yes	No	Yes	No	Yes
Yes	Yes	N/A	Yes	N/A	N/A	Yes	Yes
No limit	99	N/A	No limit	No limit	No limit	No limit	99
15	Programmable	N/A	7	2-9	No limit	7	Unlimited
Yes	Yes	N/A	Yes	Sometimes	Yes	No	Yes
Limited	Yes (10)	No	Yes	Limited	Limited	Yes	Yes
N/A	Yes	N/A	Yes	Yes	N/A	Yes	Yes
No	No	N/A	1 + user code	1 per report	User specified	No	N/A-uses unrestricted random sampling(stratified for variables)
Option	Yes	N/A	Yes	No	Option	Yes	Yes

	A	B(15)	C	D	E(16)	F	G
Vendor:	Arthur Andersen Company	Computer Audit Systems	Cullinane Corp.	Ernst & Ernst	Citibank, N.A.	Informatics, Inc.	Program Products Inc.
Package:	AUDEX 100	CARS 2	ERP-Auditor	AUDITRONIC 32	PROBE	MARK IV Auditor	AUDIT ANALYZER
Contains Random Number Table	No	No	Yes	No	No	No	Optional
- Size	N/A	N/A	Up to 21K	N/A	Appeat after 500K	N/A	N/A
Can Select Every Nth Item	No	Yes	Yes	Yes	User coded	Yes	Yes
Sample Size Can Be Specified	Yes	Yes	Yes (or) calculated	Yes	Yes	Yes	Yes
Calculates and Option to Print - Mean	No	Yes	Yes	Yes	Yes	User coded	Yes
- Standard Deviation	No	Yes	Yes	Calculates, no print	Power 10 residual method	User coded	Yes
Accepts Desired Precision Factor	No	Yes	Yes	Yes	Table lookup	Yes	Yes
Accepts Confidence Level and Factor	No	Yes	Yes	Yes	Table lookup	Yes	Yes
Accepts Expected Error Rate	No	Yes	Yes	Yes	N/A	Yes	Yes
Generates Bargraphs	No	User exit	Yes	Yes	No	User coded in MARK IV	Yes
Generates Histograms	No	User exit	Yes	Yes	No	User coded in MARK IV	No
Solves and Displays Graphic Analysis	No	User exit	Yes	No	No	User exit	No
Solves Linear Programming	No	No	Yes, limited	No	No	User exit	No
Does Trend-Line Analysis	No	User exit	User exit	No	No	User exit	No
Does Correlation Analysis	No	User exit	User exit	No	No	User exit	Yes
Does Multiple-Regression Analysis	No	User exit	User exit	No	No	User exit	User coded
Does Matrix Analysis	No	User exit	User Exit	No	No	User Exit	Yes
Has Capability for Interval Sampling	No	Yes	Yes, incl. with library of audit routine supplied with package	Yes	Yes	Yes, 60 strata	Yes
Has Capability for Stratification Sampling	5 Strata	Yes	Yes, incl. with library of audit routine supplied with package	Yes	Yes	Yes, 60 strata	Yes
Has Capability for Cluster or Multistage Sampling	No	Yes, proportionally	Yes, incl. with library of audit routine supplied with package	No	Yes	Yes	User coded
Has Capability for Attributes Sampling	No	Yes	Yes, incl. with library of audit routine supplied with package	Yes	Yes	Yes	Yes
Has Capability for Variables Sampling	No	Yes	Yes, incl. with library of audit routine supplied with package	Yes	Yes	Yes	User coded
Has Capability for Stop-or-Go Sampling	No	No	Yes, incl. with library of audit routine supplied with package	Yes	Yes	Yes	User coded
Has Capability for Discovery Sampling	No	Yes	Yes, incl. with library of audit routine supplied with package	Yes	Yes	Yes	User coded
Has Capability for Judgment Sampling	No	No	Yes, incl. with library of audit routine supplied with package	Yes	Yes	Yes	User coded
Has Capability for Probability Sampling	No	Planned	Yes, incl. with library of audit routine supplied with package	Yes	No	Yes	User coded

H	I	J	K	L	M	N	O
Informatics, Inc.	Touche Ross & Co.	U.S. Department of Commerce	Computer Audit Systems	Coopers & Lybrand	Dylakor Software System, Inc.	Computer Audit Systems	Peat, Marwick, Mitchell & Co.
SCORE IV	STRATA	AUDIT	CARS 3	Audit PAK II	Dyl-260	SYSTAUDIT	P M & M 2170
No	No	N/A	No	N/A	4-byte binary	No	No
N/A	N/A	N/A	N/A	N/A	2(31)	N/A	No
Yes	User coded	N/A	Yes	Yes	Yes	Yes	Yes
Yes	Yes	N/A	Yes	No	Yes	Yes	Yes
Yes	No	N/A	Yes	Yes	No	Yes	No
User exit	No	N/A	Yes	No	No	No	Yes, by stratum-no option
User exit	**	N/A	Yes	No	No	Yes	Yes (stated in $)
User exit	**	N/A	Yes	No	No	Yes	Yes
User exit	**	N/A	Yes	No	No	Yes	No
User exit	No	N/A	User exit	No	No	No	No
User exit	**	N/A	User exit	No	No	No	Yes
User exit	No	N/A	User exit	No	No	No	No
User exit	No	N/A	No	No	No	No	No
User exit	No	N/A	User exit	No	No	No	No
User exit	No	N/A	User exit	No	No	No	No
User exit	No	N/A	User exit	No	No	No	No
User exit	No	N/A	User exit	No	No	No	No
User exit	**	N/A	Yes	Yes	No	Yes	Yes
User exit	**	N/A	Yes	Yes	No	Yes	Yes
User exit	No	N/A	Yes, proportionally	No	No	No	No
User exit	**	N/A	Yes	No	No	Yes	Yes
User exit	**	N/A	Yes	No	No	No	Yes
User exit	No	N/A	No	No	No	No	No
User exit	No	N/A	Yes	No	No	Yes	Yes
User exit	No	N/A	No	No	No	No	Yes
User exit	No	N/A	Planned	No	No	No	Yes

Unclassified

SECURITY CLASSIFICATION OF THIS PAGE (When Data Entered)

SDC- REPORT DOCUMENTATION PAGE		READ INSTRUCTIONS BEFORE COMPLETING FORM
1. REPORT NUMBER: TM-WD-7999/400/01	2. GOVT ACCESSION NO. AD-A089345	3. RECIPIENT'S CATALOG NUMBER
4. TITLE (and Subtitle): Auditing Study Report.		5. TYPE OF REPORT & PERIOD COVERED: Final rept.
		6. PERFORMING ORG. REPORT NUMBER
7. AUTHOR(s): B. King Broadus/King		8. CONTRACT OR GRANT NUMBER(s): N000173-78-C-0455
9. PERFORMING ORGANIZATION NAME AND ADDRESS: System Development Corporation, 7929 Westpark Drive, McLean, Virginia 22102		10. PROGRAM ELEMENT, PROJECT, TASK AREA & WORK UNIT NUMBERS: Task #9
11. CONTROLLING OFFICE NAME AND ADDRESS: Naval Research Laboratory, Washington, D. C. 20375		12. REPORT DATE: 29 August 1980 13. NUMBER OF PAGES: 91
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.

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

N/A

18. SUPPLEMENTARY NOTES

None

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

Navy Supply Audit, ADP Audit, Audit tools.

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

This document analyzes various audit techniques and procedures which may be suitable for use in the Navy Supply Environment. A number of conclusions about the state of the art are drawn, and recommendations are made for using specific techniques and procedures within the Navy.

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

Unclassified

SECURITY CLASSIFICATION OF THIS PAGE (When Data Entered)